Parameter estimation of atmospheric continuous-variable quantum key distribution

Geng Chai,[1] Zhengwen Cao,[1,*] Weiqi Liu,[1] Shiyu Wang,[2] Peng Huang,[2,†] and Guihua Zeng[2,‡]

[1] *School of Information Science and Technology, Northwest University, Xi'an 710127, China*

[2] *State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, China*

(Received 9 January 2019; published 18 March 2019)

Atmospheric effects are the chief threats to the quantum properties of propagating quantum signals and may degrade the performance of quantum key distribution seriously. As one of the most important parts of continuous-variable quantum key distribution (CVQKD), a parameter estimation method has not been specially proposed in an atmospheric channel, and usually the security analysis is based on the assumption that the relevant parameters, especially the excess noise, have been previously obtained. Here we propose a parameter estimation method for Gaussian modulated coherent state continuous-variable quantum key distribution over the atmospheric link, and we investigate the impact of the atmospheric channel on the estimated values of the parameters. Based on this method, we study theoretically the effect of link fluctuations on the achievable secret key rate of CVQKD under different practical transmitted conditions. The results show that this method is unified with the physical model and can effectively resist entanglement-distillation attack. The proposed method fills in the blank of parameter estimation for implementation of practical atmospheric CVQKD.

DOI: 10.1103/PhysRevA.99.032326

I. INTRODUCTION

Discrete-variable quantum key distribution (DVQKD) [1] and continuous-variable quantum key distribution (CVQKD) [2,3] are two important technologies to realize quantum key distribution (QKD), and optical fiber and free space are common channel implementations for QKD. Compared with optical fiber, free space provides more flexibility in infrastructure construction and easier links to moving objects. Currently, free-space QKD has become a hot research issue and has been developing rapidly with propagation distance ranging from short-distance intracity [4,5] to long-distance ground-based [6–8], and satellite-mediated [9–13]. Even though QKD between satellite and ground has been initially achieved, these experiments based on discrete quantum variables and single-photon threshold detectors involve spatial, spectral, and/or temporal filtering in order to reduce background noise [14].

As is known, CVQKD under optical fiber can be compatible with fully developed optical telecommunication technologies, which have been extensively studied recently [15–17]. Moreover, CVQKD has the ability to resist disturbance of background noise and has higher channel capacity, and some progress [18–22] has already been achieved in free space, but more needs to be done. What is strikingly noticeable is that the elliptical beam model established for transmitted quantum light through the atmospheric channel [20,21] and the study of the entanglement of Gaussian states and its applicability to quantum key distribution over fading channels [23] verify the feasibility of realizing CVQKD in free space. The atmospheric effects on continuous-variable quantum key distribution has been subsequently investigated [22], which lays the foundation for the further study and implementation of this topic. These experiments and theoretical investigations have shown that the free space is a reliable medium for continuous-variable quantum communication even if the quantum signal is affected by atmospheric effects.

However, the performance analysis of a free-space channel is based on the condition that the relevant parameters are known. It is obvious that these assumptions about the proof of the security analysis cannot be justified in practical implementations. Actually, parameter estimation is a vital step in CVQKD, which helps us to evaluate the practical security of the key distribution and obtain relevant parameters for further postprocessing the procedure [24,25]. The principles of quantum mechanics impose an upper bound on the information that has possibly leaked to a potential eavesdropper in the case that the quantum channel is estimated by legitimate communication parties [24–26]. The study of parameter estimation method for practical CVQKD over free-space channel is almost nonexistent at the moment. Compared with a fiber channel, the transmittance of a free-space channel fluctuates randomly in time [20,27], therefore, the parameter estimation method under fiber cannot be directly applied to free space.

The purpose of this paper is to study the parameter estimation for free-space Gaussian modulated coherent state continuous-variable quantum key distribution (GMCS CVQKD) and verify its feasibility and availability. In this paper, we first propose a parameter estimation method for GMCS CVQKD over an atmospheric link based on the theory of a maximum-likelihood estimate. Our deduction shows that the proposed method coincides well with a physical model. Then we observe that the estimated values of parameters which have an appreciable impact on the secret key rate are

[*] caozhw@nwu.edu.cn

[†] huang.peng@sjtu.edu.cn

[‡] ghzeng@sjtu.edu.cn

2469-9926/2019/99(3)/032326(12)

affected by various atmospheric effects, which mainly include atmospheric attenuation, turbulence, and other constraints, and simulation conclusions indicate that the proposed method from the data level tallies with the consequence of previous theoretical analysis of atmospheric effects on CVQKD from a physical level. This proves the feasibility and rationality of the proposed method. Moreover, we discover that phase variations caused by atmospheric turbulence is another important factor affecting the performance of CVQKD besides beam wandering and beam scintillation. Furthermore, the analysis demonstrates that the proposed method can effectively resist the previously proposed entanglement-distillation attack.

The paper is organized as follows. In Sec. II we deduce the parameter estimation method of GMCS CVQKD over the atmospheric channel. In Sec. III with the results of Sec. II, we analyze how atmospheric effects affect the channel parameter estimation of GMCS CVQKD. Then we perform achievable secret key rate analysis based on parameter estimation under different practical transmitted conditions and security analysis of an entanglement-distillation attack in Sec. IV. A summary and discussion are given in Sec. V.

II. PARAMETER ESTIMATION OF THE ATMOSPHERIC GMCS CVQKD

For common GMCS CVQKD, the transmitter Alice usually modulates quadrature components of the light with Gaussian modulation, and the receiver Bob measures a weak quantum signal with the help of strong local oscillator (LO) in a shot-noise-limited homodyne or heterodyne detector [2,3]. CVQKD generally consists of two segments, a quantum information transmission phase, where quantum signals are transmitted through a quantum channel and then measured by a homodyne-heterodyne detector, and a classical information postprocessing phase, where local data are applied for parameter estimation to evaluate system security, and the rest is used to obtain the final secret key through reverse reconciliation [28] and privacy amplification [29].

Following a brief review of the parameter estimation of fiber-based GMCS CVQKD in Sec. II A, we move on to describe in detail the proposed parameter estimation of an atmospheric channel in Sec. II B.

A. Optical fiber GMCS CVQKD

In a fiber channel, parameters required to compute a secret key rate are estimated through the sampling of $m = N - n$ pairs of correlated variables $\{(x_i, y_i)|i = 1, 2, \dots, m\}$, where N is the total number of transmitted quantum signals and variables of Alice and Bob are represented as $\{x_i\}_{i=1,2,\dots,N}$ and $\{y_i\}_{i=1,2,\dots,N}$, and n is the number of signals used for the key establishment. Usually, some parameters are acquired ahead of time, and others must be estimated in real time in the process of parameter estimation. Since detector efficiency η and electrical noise v_{el} are calibrated in advance, Bob can obtain $\{y_{0_i}\}_{i=1,2,\dots,N'}$ via forcing a quantum channel with zero transmission. So the set of Bob's variables $\{y_{0_i}\}_{i=1,2,\dots,N'}$ can be used to measure the noise,

$$y_0 = z_0, \tag{1}$$

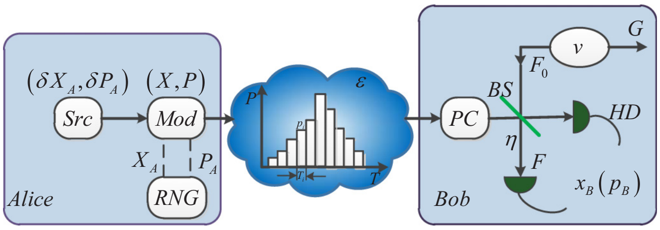

FIG. 1. The prepare-and-measure (P&M) description of CVQKD over the atmospheric channel. RNG, random number generator; PC, polarization controller; BS, beam splitter; HD, homodyne detection or heterodyne detection; T, atmospheric transmittance; ε, excess noise; the imperfection of the detector is described by the detection efficiency η and the electronic noise $v_{\rm el}$ contained in variance v.

where z_0 is a Gaussian noise with variance $\sigma_0^2 = N_0(1 + v_{\rm el})$ and mean zero. Thus, Alice's and Bob's correlated variables $\{(x_i, y_i) \mid i = 1, 2, \dots, m\}$ are linked through the following normal linear model [25]:

$$y = tx + z, \tag{2}$$

where $t = \sqrt{\eta T} \in \mathbb{R}$, and z is a Gaussian noise with variance $\sigma^2 = N_0(1 + \eta T\varepsilon + v_{\rm el})$ and mean zero, where N_0 is the shot noise variance. Furthermore, the random variable x is a normal random variable with variance V_A in the case of Gaussian modulation. Similarly to the analysis in Ref. [24], maximum-likelihood estimators $\hat{V}_X$, $\hat{t}$, $\hat{\sigma}^2$, and $\hat{\sigma}_0^2$ are known for the normal linear mode:

$$\hat{t} = \frac{\sum_{i=1}^m x_i y_i}{\sum_{i=1}^m x_i^2}, \quad \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^m (y_i - \hat{t}x_i)^2, \tag{3}$$

$$\hat{V}_X = \frac{1}{m}\sum_{i=1}^m x_i^2, \quad \hat{\sigma}_0^2 = \frac{1}{N'}\sum_{i=1}^{N'} y_{0_i}^2. \tag{4}$$

Consequently, through the above parameter estimation process, modulation variance V_A, channel transmittance T, excess noise ε, and total noise $\chi_{\rm tot}$ can be obtained as follows:

$$\hat{T} = \frac{\hat{t}^2}{\eta}, \quad \hat{\varepsilon} = \frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{t}^2 N_0}, \tag{5}$$

$$\hat{V}_A = \frac{\hat{V}_X}{N_0}, \quad \hat{\chi}_{\rm tot} = \frac{\hat{\sigma}^2}{\hat{t}^2} - 1. \tag{6}$$

B. Atmospheric GMCS CVQKD

We first consider the propagation of quantum signals in the atmosphere. The atmosphere channel model of GMCS CVQKD over free space is illustrated in Fig. 1, and the quantum transmission of the communication between Alice and Bob is described as follows:

> Alice prepares coherent state $|X_A + iP_A\rangle$ through modulating X_A and P_A with Gaussian random numbers of zero mean and variance $V_A N_0$, and transmits it to Bob through an atmosphere channel which is characterized by a distribution of transmittance $\{T_i\}$ with probabilities $\{p_{T_i}\}$ and corresponding excess noise $\{\varepsilon_i\}$ with probabilities $\{p_{\varepsilon_i}\}$, resulting in a noise variance $1 + \langle T\rangle\varepsilon$ at the input of Bob. The total channel-added noise that is expressed in shot noise units referred to as channel

input is defined as $\chi_{\text{line}} = \frac{1+\langle T\rangle\varepsilon}{\langle T\rangle} - 1 = \frac{1}{\langle T\rangle} - 1 + \varepsilon$, where $\langle T\rangle = \sum_i^M p_{T_i} T_i$ and $\varepsilon = \sum_i^M p_{\varepsilon_i}\varepsilon_i$.

Bob employs a homodyne detector to measure either one of the two quadratures randomly or adopts a heterodyne detector to measure both quadratures simultaneously to obtain the secret key. The detection-added noise referred to Bob's input can be defined as χ_h and is expressed by $\chi_{\text{hom}} = \frac{(1-\eta)+v_{\text{el}}}{\eta}$ and $\chi_{\text{het}} = \frac{(1-\eta)+2v_{\text{el}}}{\eta}$ for homodyne and heterodyne detection, respectively. Therefore, the total noise referred to the channel input can then be expressed as $\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_h}{\langle T\rangle}$, so that Bob's measured variance $V_B = \eta\langle T\rangle(V + \chi_{\text{tot}})$.

Then, with regard to parameter estimation in classical information postprocessing under an atmosphere channel, it is sufficient to estimate the covariance matrix of the state shared by Alice and Bob, including the variance for Alice and Bob, respectively, $\langle x^2\rangle$ and $\langle y^2\rangle$ and $\langle y_0^2\rangle$, and the covariance $\langle xy\rangle$ between Alice and Bob:

$$\begin{aligned}
\langle x^2\rangle &= V_A, \quad \langle y^2\rangle = V_B,\\
\langle xy\rangle &= \sqrt{\eta\langle T\rangle}V_A,\\
\langle y_0^2\rangle &= V_{B0} = N_0(1+v_{\text{el}}).
\end{aligned} \tag{7}$$

Unlike a fiber channel, the transmittance of free space varies randomly due to the random characteristics of an atmospheric channel. Thus, parameter $\hat{V}_A$ can be derived from Eq. (6), but, on the other hand, parameters $\hat{\chi}_{\text{tot}}$, $\hat{\varepsilon}$, and $\langle\hat{T}\rangle$ cannot be directly calculated by Eqs. (5) and (6). The parameters $\hat{\chi}_{\text{tot}}$, $\hat{\varepsilon}$ are all related to $\langle\hat{T}\rangle$, so next we focus on the estimation method of parameter $\langle\hat{T}\rangle$.

1. *Bayesian parameter estimation*

Influenced by atmospheric effects, channel transmittance varies randomly, that is to say, it can be regarded as a random variable satisfying a certain distribution. The purpose of parameter estimation is to obtain the variation of transmittance and other parameters in a quantum channel. The idea of Bayesian parameter estimation accords with this process, that is, the prior distribution of parameters is constructed by historical empirical data, and then the prior distribution is adjusted by sampling information to obtain the posterior distribution of parameters. In the posterior distribution, the estimated values of parameters are obtained according to some principle.

In Bayesian estimation, all uncertainty about parameter $\langle T\rangle$ is quantified by probability distributions. Prior parameter distribution $p(T)$ is updated by incoming variables $\{y_i\}_{i=1,2,\dots,m}$ to yield posterior distributions $p(T|y)$. The posterior distributions $p(T|y)$ quantify our uncertainty about the parameter $\langle T\rangle$ after having seen the variables $\{y_i\}_{i=1,2,\dots,N}$:

$$\begin{aligned}
p(T|y) &= \frac{p(y|T)p(T)}{p(y)}\\
&= \frac{p(y|T)p(T)}{\int p(y|T)p(T)\,dT}.
\end{aligned} \tag{8}$$

The same as for the quantum signal, LO is also inevitably affected by an atmospheric effect, resulting in fluctuation of variance of shot noise at the receiver Bob. Similarly, the posterior probability of shot noise under an atmospheric effect is

$$p(N_0|y) = \frac{p(y|N_0)p(N_0)}{p(y)} = \frac{p(y|N_0)p(N_0)}{\int p(y|N_0)p(N_0)\,dN_0}. \tag{9}$$

Therefore, the Bayesian estimated values of parameters $\langle\hat{T}\rangle$ and $\hat{N}$ are given by

$$\begin{aligned}
\langle\hat{T}\rangle &= \int_0^1 p(T|y)T\,dT,\\
\hat{N_0'} &= \int_0^{N_0} p(N_0|y)N_0\,dN_0.
\end{aligned} \tag{10}$$

Furthermore, we can obtain the estimated values of other parameters:

$$\begin{aligned}
\hat{\varepsilon} &= \frac{\hat{V}_B - \hat{V}_{B0}}{\eta\langle\hat{T}\rangle} - \hat{V}_A\\
&= \frac{\frac{N_0}{m}\sum_{i=1}^m y_i^2 - \frac{N_0'}{N'}\sum_{i=1}^{N'} y_{0_i}^2}{\eta\langle\hat{T}\rangle\hat{N}_0'N_0} - \hat{V}_A,\\
\hat{\chi}_{\text{tot}} &= \frac{\hat{V}_B}{\eta\langle\hat{T}\rangle} - \hat{V} = \frac{\frac{1}{m}\sum_{i=1}^m y_i^2}{\eta\langle\hat{T}\rangle} - (\hat{V}_A + 1).
\end{aligned} \tag{11}$$

It is noteworthy that when using the Bayesian method, we must know the prior probability distribution of channel transmittance $p(T)$ before the information is transmitted to an atmospheric channel and the conditional probability $p(y|T)$ after information is transmitted to Bob through atmospheric channel. Then, when Bob completes the measurement of quadratures, he can obtain the transmittance through Eqs. (8) and (10). Therefore, the acquisition of prior probability of the channel transmittance $p(T)$ and conditional probability $p(y|T)$ in an atmospheric channel is a major obstacle to the practical application of Bayesian parameter estimation method. Moreover, this method inevitably increases experimental complexity and affects the data postprocessing process thereafter.

Compared with the Bayesian method, the maximum-likelihood method does not need to know the prior probability of relevant parameters, and the latter has lower implementation complexity than the former. On the other hand, the typical rate of atmospheric channel fluctuations is of the order of kHz, while the modulation and detection rate is typically of the order of several MHz, i.e., at least thousands of signal or probe states can be transmitted during the stability time of the fading atmospheric channel [23]. In addition, the Fried parameter, which is employed for describing the quality of the optical wavefront through the atmosphere, and the isoplanatic angle, which is the maximum angle that light can enter the receiving aperture, imply that the quantum signal has passed through the same turbulence [30]. Therefore, we delineate a relatively stable transmittance as a subchannel of free space, and we next consider the maximum-likelihood parameter estimation under the standard CVQKD assumption [23] that the trusted parties are able to estimate the sub-channel transmittance T_i and check its stability during the transmission of quantum signals, which contributes to the secret key.

2. Maximum-likelihood parameter estimation

We estimate the transmission T_i and excess noise ε_i of the ith subchannel ($i \in \{1, 2, \dots, M\}$, and M is the number of subchannels) from the Gaussian variables that Alice modulates X and Bob measures Y. Here we take into account that

$$y_i = t_i x_i + z_i, \tag{12}$$

where $t_i = \sqrt{\eta T_i} \in \mathbb{R}$, and z_i is a Gaussian noise with variance $\sigma_i^2 = N_{0i}(1 + \eta\, T_i \varepsilon_i + v_{\mathrm{el}})$ and mean zero, and N_{0i} is the shot noise of the ith subchannel obtained by real-time shot noise measurement [31]:

$$\begin{aligned} X &= A\cos\varphi, \\ Y &= \sqrt{\eta} A_\alpha A \cos(\varphi + \phi) + A_N, \end{aligned} \tag{13}$$

where A and φ represent the amplitude and phase of the modulation coherent state without the effect of an atmospheric link, respectively, A_α and ϕ represent the amplitude fluctuations and phase variations introduced by an atmospheric link, respectively, and A_N is the amplitude caused by the noise. Without considering the finite-size effect of the parameter estimation block size m_i, we employ Eq. (13) to modify $\hat{t}_i$ and $\hat{\sigma}_i^2$ in Eq. (12):

$$\begin{aligned} \hat{t}_i &= \frac{\frac{1}{m_i}\sum_{j=1}^{m_i} x_j y_j}{\frac{1}{m_i}\sum_{j=1}^{m_i} x_j^2} = \frac{E[XY]}{E[X^2]} \\ &= \frac{E[\sqrt{\eta} A_\alpha A^2 \cos\varphi \cos(\varphi + \phi)] + E[A_N A \cos\varphi]}{E[A^2 \cos^2\varphi]}, \end{aligned} \tag{14}$$

$$\begin{aligned} \hat{\sigma}_i^2 &= \frac{1}{m_i}\sum_{j=1}^{m_i} (y_j - \hat{t}_i x_j)^2 = E[(Y - \hat{t}_i X)^2] \\ &= \eta E\big[A_\alpha^2 A^2 \cos^2(\varphi + \phi)\big] \\ &\quad + E\big[A_N^2\big] - 2\hat{t}_i E[XY] + \hat{t}_i^2 E[X^2]. \end{aligned} \tag{15}$$

In Eqs. (14) and (15), considering that the mean value of amplitude A_N caused by noise $E[A_N] = 0$, the mean value $E[A_N A \cos\varphi] = E[A_N]E[A\cos\varphi]$ can be ignored, and $E[A_N^2] = D[A_N] = N_{0i}(1 + v_{\mathrm{el}} + \hat{\varepsilon}_i \hat{t}_i^2)$. In addition, the mean value $E[X^2] = E[A^2\cos^2\varphi] = \hat{V}_X$. Substituting with these equations, we can simplify Eqs. (14) and (15) to

$$\begin{aligned} \hat{t}_i &= \frac{E[\sqrt{\eta} A_\alpha A^2 \cos\varphi \cos(\varphi + \phi)]}{\hat{V}_X} \\ &= \sqrt{\eta} E[A_\alpha \cos\phi] - \frac{\sqrt{\eta} A^2 \sin 2\varphi E[A_\alpha \sin\phi]}{2\hat{V}_X}. \end{aligned} \tag{16}$$

$$\begin{aligned} \hat{\sigma}_i^2 = {}& \eta\big\{\hat{V}_X E\big[A_\alpha^2 \cos^2\phi\big] + E[A^2 \sin^2\varphi] E\big[A_\alpha^2 \sin^2\phi\big] \\ & - E[A^2 \sin 2\varphi] E[(A_\alpha \cos\phi)(A_\alpha \sin\phi)]\big\} \\ & - \sqrt{\eta}\hat{t}_i \{2\hat{V}_X E[A_\alpha \cos\phi] - E[A^2 \sin 2\varphi] E[A_\alpha \sin\phi]\} \\ & + E\big[A_N^2\big] + \hat{t}_i^2 \hat{V}_X. \end{aligned} \tag{17}$$

Finally, we can get the estimated values of parameters:

$$\begin{aligned} \langle \hat{T} \rangle &= \sum_i^M p_{_{T_i}} \hat{T}_i = \frac{1}{\eta} \sum_i^M p_i \hat{t}_i^2, \\ \hat{\varepsilon} &= \sum_i^M p_{_{\varepsilon_i}} \frac{N_0 \hat{\sigma}_i^2 - N_{0i} V_{B0}}{\eta \hat{T}_i N_{0i} N_0}, \\ \hat{\chi}_{\mathrm{tot}} &= \frac{\sum_i^M p_{_{\varepsilon_i}} \hat{\sigma}_i^2}{\eta \langle \hat{T} \rangle} - 1. \end{aligned} \tag{18}$$

Generally, the covariance matrix of a coherent state based on the estimated modulation variance $\hat{V}_A$

$$\hat{\gamma}_{_{AB}} = \begin{pmatrix} \hat{V}\mathbb{I} & \sqrt{\hat{V}^2 - 1}\sigma_z \\ \sqrt{\hat{V}^2 - 1}\sigma_z & \hat{V}\mathbb{I} \end{pmatrix} \tag{19}$$

after a subchannel with the estimated transmittance $\hat{T}_i$ and excess noise ε_i based on maximum-likelihood parameter estimation is given by

$$\hat{\gamma}^i_{_{AB_1}} = \begin{pmatrix} \hat{V}\mathbb{I} & \sqrt{\hat{T}_i}\sqrt{\hat{V}^2 - 1}\sigma_z \\ \sqrt{\hat{T}_i}\sqrt{\hat{V}^2 - 1}\sigma_z & (\hat{V}\hat{T}_i + 1 - \hat{T}_i + \hat{\varepsilon}_i \hat{T}_i)\mathbb{I} \end{pmatrix}. \tag{20}$$

So the overall state after an atmospheric channel is the mixture of states after individual sub-channels, and the covariance matrix of the resulting mixed state after an atmospheric channel with the estimated transmittance $\{\hat{T}_i\}$ and excess noise $\{\hat{\varepsilon}_i\}$ based on maximum-likelihood parameter estimation is given by

$$\hat{\gamma}_{_{AB_1}} = \begin{pmatrix} \hat{V}\mathbb{I} & \langle\sqrt{\hat{T}}\rangle\sqrt{\hat{V}^2 - 1}\sigma_z \\ \langle\sqrt{\hat{T}}\rangle\sqrt{\hat{V}^2 - 1}\sigma_z & [\langle\hat{T}\rangle(\hat{V} + \hat{\varepsilon}) + 1]\mathbb{I} \end{pmatrix}, \tag{21}$$

where $\hat{V} = \hat{V}_A + 1$, $\mathbb{I} = \mathrm{diag}(1, 1)$ is the unity matrix and $\sigma_z = \mathrm{diag}(1, -1)$ is the Pauli matrix.

We can derive the practical covariance matrix by introducing the estimated values $\langle\sqrt{\hat{T}}\rangle$, $\langle\hat{T}\rangle$ and $\hat{\varepsilon}$ from Eq. (18) into Eq. (21). It is simpler than the previous method of calculating transmittance with the help of elliptic beam model [20]. In addition, when deducing covariance matrix, it is generally considered that excess noise is constant [23]. However, the proposed method can get the corresponding excess noise ε_i of each subchannel and then obtain the general excess noise dynamically over the whole channel, which is more systematic, extensive, and comprehensive than the elliptic beam model. Through the above analysis, the estimation results are very consistent with the physical model [23] of CVQKD in an atmospheric channel. Therefore, this method provides a feasible parameter estimation method for atmospheric CVQKD.

III. THE ATMOSPHERIC EFFECTS ON PARAMETER ESTIMATION

Considering the influence of the atmosphere on the transmission of an optical signal, the feasibility and availability of the proposed method in practical implementations for further experiments and applications of the free-space-based CVQKD system need further investigation and demonstration. From the analysis of Sec. II B 2, the parameters $\hat{t}_i$

and $\hat{\sigma}_i^2$ depend on the amplitude fluctuations A_α and phase variations ϕ introduced by an atmospheric link and other relevant parameters. in this case, we analyze the atmospheric effects on the estimated values of the parameters in detail.

A. Atmospheric attenuation channel

Absorption and scattering that are strongly wavelength dependent mainly cause attenuation of the intensity of an optical beam. The attenuation coefficient of atmosphere $\alpha(\lambda)$ is defined as the sum of the absorption coefficient $\alpha_{\text{abs}}(\lambda)$ and scattering coefficient $\alpha_{\text{sca}}(\lambda)$. The attenuation $A_\alpha(L)$ of the intensity for horizontal path obeys the Lambert-Beer law [32],

$$A_\alpha(L) = \sqrt{e^{-\alpha(\lambda)L}}, \tag{22}$$

where the attenuation coefficient $\alpha(\lambda)$ consists of aerosol absorption $\alpha_{\text{abs}}^{\text{aer}}$, molecular absorption $\alpha_{\text{abs}}^{\text{mol}}$, aerosol scattering $\alpha_{\text{sca}}^{\text{aer}}$, and molecular scattering $\alpha_{\text{sca}}^{\text{mol}}$: $\alpha(\lambda) = \alpha_{\text{abs}}^{\text{aer}} + \alpha_{\text{abs}}^{\text{mol}} + \alpha_{\text{sca}}^{\text{aer}} + \alpha_{\text{sca}}^{\text{mol}}$. Here λ is the wavelength of optical beam, and L is the horizontal propagation distance. For the slant path, the attenuation $A_\alpha(H, \theta_z)$ of the intensity is given by

$$A_\alpha(H, \theta_z) = \sqrt{e^{[-\int_0^H \sec\theta_z \alpha(\lambda,h)\,dh]}}, \tag{23}$$

where H is the height from the ground, and θ_z is the zenith angle. The parameter $\langle\hat{T}\rangle$ is determined by substituting Eqs. (22) and (23) into Eqs. (16) and (5) for a horizontal path $\langle\hat{T}\rangle_h$ and slant path $\langle\hat{T}\rangle_s$, respectively, and reads

$$\begin{aligned}\langle\hat{T}\rangle_h &= \sum_i^M p_i \hat{T}_i = \frac{1}{\eta}\sum_i^M p_{t_i}\hat{t}_i^2 = E^2[A_\alpha(L)] = e^{-\alpha(\lambda)L},\\ \langle\hat{T}\rangle_s &= \sum_i^M p_i \hat{T}_i = \frac{1}{\eta}\sum_i^M p_{t_i}\hat{t}_i^2 = E^2[A_\alpha(H, \theta_z)]\\ &= e^{[-\int_0^H \sec\theta_z \alpha(\lambda,h)\,dh]}.\end{aligned} \tag{24}$$

In addition, the expression of parameter $\hat{\sigma}_a^2$ under an atmospheric attenuation channel is given correspondingly by

$$\hat{\sigma}_a^2 = \sum_i^M p_{\varepsilon_i}\left(\varepsilon_i \hat{t}_i^2 N_{0i} + \frac{N_{0i}\hat{\sigma}_0^2}{N_0}\right). \tag{25}$$

Since we consider the case of horizontal link propagation, Eqs. (24) and (25) will be applied to conduct the analysis of the achievable secret key rate based on parameter estimation in Sec. IV.

B. Atmospheric turbulence channel

The most important factor limiting the performance of free-space optical communication is atmospheric turbulence; in general, large scales produce refractive effects and mostly distort the phase of the propagating beam, whereas small scales are mostly diffractive in nature and therefore distort the amplitude of the beam [33,34], and the main effects resulting from the atmospheric turbulent eddies are beam spreading, beam wandering, and beam scintillation:

The beam wandering is caused by large-scale turbulent eddies whose size is large compared with the beam width, which means that the random deviation of the beam from its original path causes time-varying power fades.

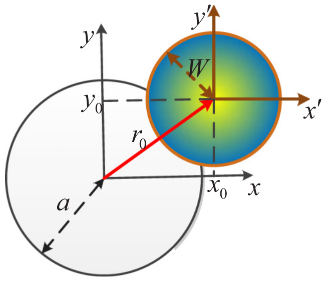

FIG. 2. Received beam profile through atmospheric channel where the beam radius is W relative to the aperture radius a. The beam centroid is displaced relative to the aperture center due to beam wandering, and its position is given by $\mathbf{r_0}$. The beam cross section of spatial distribution of the light intensity is introduced by the scintillation effect, and the intensity from weak to strong corresponds to the color from wathet blue to bright yellow.

The beam scintillation is mainly caused by small-scale turbulent eddies and is defined by fluctuations in the received irradiance (intensity) within the beam cross section.

The influence of beam spreading is actually negligible in the regime of weak turbulence and that in the region of strong turbulence does not have an analytical formula [35]. Therefore, the fluctuation caused by beam spreading will not be considered in the following analysis. Now we analyze the joint impact of beam wandering and beam scintillation on the parameter estimation of CVQKD.

1. The amplitude fluctuations

The propagation of a laser beam in atmospheric turbulence is followed by a decrease of coherence, wavefront distortion, and fluctuations of beam amplitude and phase. The intensity profile of a transmitted beam which randomly displaces from the receiver aperture due to beam wandering has an irregular form (see Fig. 2). The fluctuations of the received irradiance evidently depend on the instantaneous beam profile and position of its centroid relative to the aperture center, and the intensity fluctuations due to turbulent atmosphere can be assumed to be a log-normal distribution in the regime of weak fluctuations and gamma-gamma distribution in the regime of medium-to-strong losses.

Under weak turbulence, the log-normal probability distribution of irradiance of a Gaussian-beam wave takes the following form:

$$\begin{aligned}\rho(I(\mathbf{r}, L))_{LN} &= \frac{1}{\sqrt{2\pi} I(\mathbf{r}, L)\sigma_I(\mathbf{r}, L)}\\ &\quad\times \exp\left\{-\frac{\left[\ln(I(\mathbf{r}, L)) + \frac{\sigma_I^2(\mathbf{r}, L)}{2}\right]^2}{2\sigma_I^2(\mathbf{r}, L)}\right\},\end{aligned} \tag{26}$$

On the other hand, the gamma-gamma probability distribution of irradiance of a Gaussian-beam wave under medium-to-strong turbulence is described by

$$\rho(I(\mathbf{r},L))_{GG} = \frac{2(\alpha\beta)^{\frac{\alpha+\beta}{2}}}{\Gamma(\alpha)\Gamma(\beta)} I(\mathbf{r},L)^{\frac{\alpha+\beta}{2}-1} K_{\alpha-\beta}[2\sqrt{\alpha\beta I(\mathbf{r},L)}], \tag{27}$$

where $\mathbf{r}$ is a transverse vector, which describes the position of the deflected beam centroid relative to the aperture center, $\sigma_I^2(\mathbf{r},L)$ is the scintillation index, $\Gamma(\cdot)$ is the gamma function, $K_{\alpha-\beta}$ is the modified Bessel function of the second kind, α is the effective number of large-scale cells of the scattering process, and β is the effective number of small-scale cells. Both α and β are related to the scintillation index (see the Appendix for details).

2. The phase variations

With regard to phase variations, ϕ after modal compensation introduced by atmospheric turbulence is generally considered to obey the Gaussian phase variation with variance σ_ϕ^2:

$$\rho_\phi(\phi) = \frac{1}{\sqrt{2\pi}\sigma_\phi} \exp\left(-\frac{\phi^2}{2\sigma_\phi^2}\right). \tag{28}$$

In this case, the characteristic function $M_\phi(\omega)$ with the Fourier transform of its probability density function $\rho_\phi(\phi)$ of phase ϕ is

$$M_\phi(\omega) = \exp\left(-\frac{\omega^2\sigma_\phi^2}{2}\right). \tag{29}$$

The statistics of phase variations caused by atmospheric turbulence were characterized in Ref. [36], considering a Kolmogorov spectrum of turbulence. It is known that the residual phase variance after modal compensation of J Zernike terms is given by

$$\sigma_\phi^2 = C_J\left(\frac{2a}{d_0}\right)^{\frac{5}{3}}, \tag{30}$$

where a is the receiving aperture radius, d_0 represents the wavefront coherence diameter, which describes the spatial correlation of phase fluctuations in the receiver plane [37], and coefficient C_J is determined by the number (J) of Zernike terms, which are corrected by the active modal compensation of the receiver [38,39]. Ideally, it is desirable to choose J large enough so that the residual variance (30) becomes negligible.

Furthermore, in conjunction with Secs. III B 1 and III B 2, the mean value of $A_\alpha \cos\phi$, $A_\alpha \sin\phi$, $A_\alpha^2 \cos^2\phi$, and $A_\alpha^2 \sin^2\phi$ in both Eqs. (16) and (17) can be obtained:

$$\begin{aligned} E[A_\alpha \cos\phi] &= \frac{[M_\phi(1)+M_\phi(-1)]}{2} \\ &\quad\times \int_{\mathcal{A}} \sqrt{I(\mathbf{r},L)}\rho(I(\mathbf{r},L))\,d\mathbf{r} \\ &= \exp\left(-\frac{\sigma_\phi^2}{2}\right)\int_{\mathcal{A}} \sqrt{I(\mathbf{r},L)}\rho(I(\mathbf{r},L))\,d\mathbf{r}, \\ E[A_\alpha \sin\phi] &= \frac{-j[M_\phi(1)-M_\phi(-1)]}{2} \\ &\quad\times \int_{\mathcal{A}} \sqrt{I(\mathbf{r},L)}\rho(I(\mathbf{r},L))\,d\mathbf{r} = 0, \\ E[A_\alpha^2 \cos^2\phi] &= \frac{2+[M_\phi(2)+M_\phi(-2)]}{4} \\ &\quad\times \int_{\mathcal{A}} I(\mathbf{r},L)\rho(I(\mathbf{r},L))\,d\mathbf{r}, \\ &= \frac{1+\exp\left(-\sigma_\phi^2\right)}{2}\int_{\mathcal{A}} I(\mathbf{r},L)\rho(I(\mathbf{r},L))\,d\mathbf{r}, \\ E[A_\alpha^2 \sin^2\phi] &= \frac{2-[M_\phi(2)-M_\phi(-2)]}{4} \\ &\quad\times \int_{\mathcal{A}} I(\mathbf{r},L)\rho(I(\mathbf{r},L))\,d\mathbf{r}, \\ &= \frac{1-\exp(-\sigma_\phi^2)}{2}\int_{\mathcal{A}} I(\mathbf{r},L)\rho(I(\mathbf{r},L))\,d\mathbf{r}. \end{aligned}$$

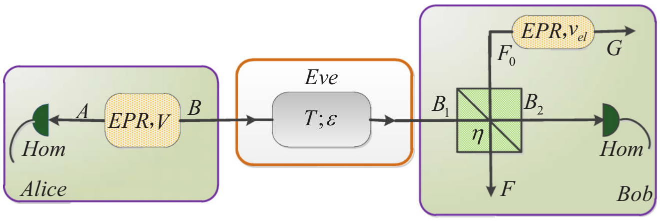

FIG. 3. The equivalent theoretical model of the atmospheric CVQKD with Gaussian-modulated states. T, atmospheric transmittance; ε, excess noise; Hom, homodyne detector; η and $\upsilon_{\rm el}$, the efficiency and electrical noise of the homodyne detector, respectively.

In addition, parameters $\langle\hat{T}\rangle$ and $\hat{\varepsilon}$ under atmospheric turbulence channel $\langle\hat{T}\rangle_t$ and $\hat{\varepsilon}_t$ will be obtained:

$$\begin{aligned} \langle\hat{T}\rangle_t &= \sum_i^M p_i\hat{t}_i^2 = \sum_i^M p_i E^2[A_{\alpha_i}\cos\phi_i] \\ &= \sum_i^M p_i\left[\exp\left(-\frac{\sigma_{\phi_i}^2}{2}\right)\int_{\mathcal{A}} \sqrt{I_i(\mathbf{r},L)}\rho(I(\mathbf{r},L))\,d\mathbf{r}\right]^2, \end{aligned} \tag{31}$$

$$\hat{\varepsilon}_t = \sum_i^M p_{\varepsilon_i}\frac{\sigma_i^2 - N_{0i}(1+\upsilon_{\rm el})}{\hat{t}_i^2 N_{0i}}, \tag{32}$$

where $I(\mathbf{r},L)$ represents the normalization irradiance at a distance of L away from transmitting plane, where the offset of a beam centroid relative to the aperture center is $r = |\mathbf{r}|$, and $\mathcal{A}$ is the plane of the receiver aperture.

IV. PERFORMANCE ANALYSIS BASED ON PARAMETER ESTIMATION

The analysis of the achievable secret key rate of atmospheric GMCS CVQKD will be introduced in this section based on the results of Secs. II and III. An equivalent theoretical model of the atmospheric CVQKD with modulated entangled states is presented in Fig. 3. Alice modulates the initial entanglement state with a variance of V_A and measures half of the state (mode A), and the other half (mode B) is transmitted through the atmosphere to Bob. Bob measures the amplitude or phase quadrature of the state (mode B_1) transmitted through an atmospheric channel using a homodyne or heterodyne detector. In the asymptotic regime, the achievable secret key rate K under reconciliation efficiency β_R is given as [22]

$$K = (1-P)(\beta_R I_{AB} - \chi_{BE}), \tag{33}$$

where I_{AB} is the Shannon mutual information of Alice and Bob, and χ_{BE} is the Holevo quantity of Bob and Eve. P stands for interruption probability due to the angle of arrival fluctuations. According to previous works [23,40], the covariance matrix of the mode AB_1 is expressed by

$$\gamma_{AB_1} = \begin{pmatrix} V\mathbb{I} & \langle\sqrt{T}\rangle\sqrt{V^2-1}\sigma_z \\ \langle\sqrt{T}\rangle\sqrt{V^2-1}\sigma_z & \langle T\rangle(V+\chi_{\text{line}})\mathbb{I} \end{pmatrix}. \tag{34}$$

Thus, considering detection efficiency η and electronic noise υ_{el}, the mutual information of Alice and Bob can be obtained:

$$I_{AB} = \frac{1}{2}\log_2\frac{\langle T\rangle(V+\chi_{\text{tot}})}{\langle T\rangle(V+\chi_{\text{tot}}) - \langle\sqrt{T}\rangle^2 V_A}. \tag{35}$$

The Holevo quantity χ_{BE} can also be obtained based on Eq. (34) and simplified to [41]

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{36}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ can be calculated for both homodyne and heterodyne detection by

$$\lambda_{1,2} = \sqrt{\frac{1}{2}[A \pm \sqrt{A^2 - 4B}]},$$

with

$$A = V^2(1 - 2\langle\sqrt{T}\rangle^2) + 2\langle\sqrt{T}\rangle^2 + [\langle T\rangle V_A + 1 + \varepsilon\langle T\rangle]^2,$$
$$B = [V^2(\langle T\rangle - \langle\sqrt{T}\rangle^2) + \langle\sqrt{T}\rangle^2 + \langle T\rangle V\chi_{\text{line}}]^2.$$

The symplectic eigenvalues $\lambda_{3,4}$ can take the same form as $\lambda_{1,2}$ for both the homodyne and heterodyne cases, while λ_5 is found to be 1; that is,

$$\lambda_{3,4} = \sqrt{\frac{1}{2}[C \pm \sqrt{C^2 - 4D}]}, \quad \lambda_5 = 1.$$

Specifically, C and D for the homodyne and heterodyne cases can be expressed as

$$C_{\text{hom}} = \frac{A\chi_{\text{hom}} + V\sqrt{B} + c_1}{c_1 + \chi_{\text{hom}}},$$
$$D_{\text{hom}} = \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{c_1 + \chi_{\text{hom}}},$$
$$C_{\text{hete}} = \frac{A\chi_{\text{het}}{}^2 + 2\chi_{\text{het}}(V\sqrt{B} + c_1) + B + 2c_2^2 + 1}{(c_1 + \chi_{\text{het}})^2},$$
$$D_{\text{hete}} = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{c_1 + \chi_{\text{het}}}\right)^2,$$

where $c_1 = \langle T\rangle(V + \chi_{\text{line}})$, $c_2 = \langle\sqrt{T}\rangle\sqrt{V^2-1}$, and noise χ_{line}, χ_{hom}, χ_{het}, and χ_{tot} involved in the above analysis have been explained in Sec. II B.

TABLE I. Parameter settings of parameter estimation, all variances and noises in SNUs.

Variable	Value	Description
W_0	30 mm	Transmitting aperture radius
a	1 mm	Receiving aperture radius
λ	1550 nm	Laser wavelength
L	0–100 km	Propagation distance
β_R	90%	Reconciliation efficiency
η	60%	Detection efficiency
V_A	8	Modulation variance
υ_{el}	0.01	Electronic noise
W	$W_0\sqrt{1+(\lambda L/\pi W_0^2)^2}$	Receiving beam radius
$\lvert\mathbf{r}\rvert$	$[0, a+W]$	Offset of beam wandering
$\alpha_{\text{sca}}^{\text{aer}}$	3.28×10^{-2} km^{-1}	Aerosol scattering coefficient
$\alpha_{\text{sca}}^{\text{mol}}$	1.72×10^{-4} km^{-1}	Molecule scattering coefficient
$\alpha_{\text{abs}}^{\text{aer}}$	6.25×10^{-3} km^{-1}	Aerosol absorption coefficient
$\alpha_{\text{abs}}^{\text{mol}}$	4.08×10^{-3} km^{-1}	Molecule absorption coefficient

A. The achievable secret key rate

Therefore, the achievable secret key rate $\bar{K}(\langle\hat{T}\rangle, \hat{\varepsilon})$ based on parameter estimation under the reconciliation efficiency β_R can be expressed as

$$\bar{K}(\langle\hat{T}\rangle, \hat{\varepsilon}) = (1-P)[\beta_R \bar{I}_{AB}(\langle\hat{T}\rangle, \hat{\varepsilon}) - \bar{\chi}_{BE}(\langle\hat{T}\rangle, \hat{\varepsilon})], \tag{37}$$

where $\langle\hat{T}\rangle$, $\hat{\varepsilon}$, $\hat{\chi}_{\text{tot}}$, and $\hat{V}_A$ are the estimated parameters, which can be calculated using Eq. (18). The mutual information $\bar{I}_{AB}(\langle\hat{T}\rangle, \hat{\varepsilon})$ and $\bar{\chi}_{BE}(\langle\hat{T}\rangle, \hat{\varepsilon})$ can be calculated using Eq. (35) and Eq. (36), respectively. In order to simulate the achievable secret key rate, we need to obtain the estimated value of $\langle\hat{T}\rangle$, $\hat{\varepsilon}$, $\hat{\chi}_{\text{tot}}$, and $\hat{V}_A$ by employing $\hat{t}$, $\hat{\sigma}^2$, $\hat{\sigma}_0^2$, and $\hat{V}_X$, which has been already analyzed in Secs. II and III.

Since it is quite difficult to directly calculate $I(\mathbf{r}, L)$, which is a random variable, here we assume that the received beam radius is much larger than the receiving aperture radius, that is, the receiver is approximately a point receiver. The interruption probability P due to the angle of arrival fluctuations is not considered. All variables needed in the secret key rate analysis are presented in Table I. The parameter estimation-based achievable secret key rate $\bar{K}_A$ under an atmospheric attenuation channel is depicted in Fig. 4. In addition, under an atmospheric turbulence channel, the parameter estimation-based achievable secret key rate $\bar{K}_T$ without considering beam wandering and that with considering beam wandering are depicted in Figs. 5 and 6, respectively.

Whether fiber or free space, homodyne detection is propitious to achieve distant propagation, while heterodyne detection performs better in short-range propagation. On the other hand, the parameter estimation-based achieve secret key rate of an atmospheric attenuation channel is superior to that of a fiber channel, and the former two are better than an atmospheric turbulence channel, as shown in Figs. 4 and 5. Therefore, an atmospheric channel has the potential to break the distance constraints of fiber channel due to attenuation

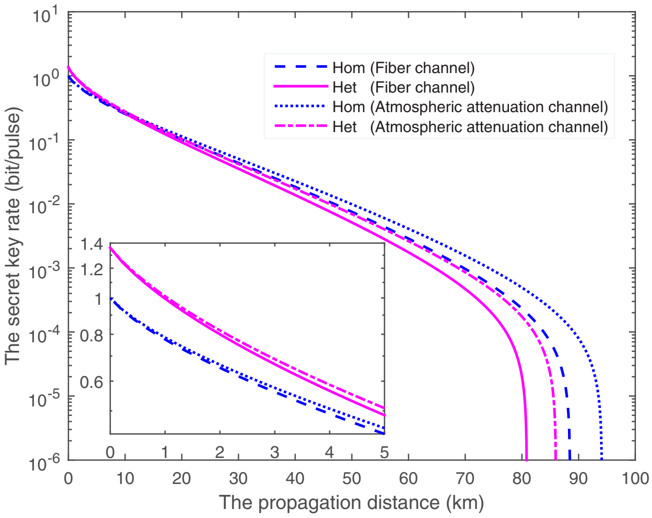

FIG. 4. The parameter estimation-based achievable secret key rate $\bar{K}_A$ under an atmospheric attenuation channel.

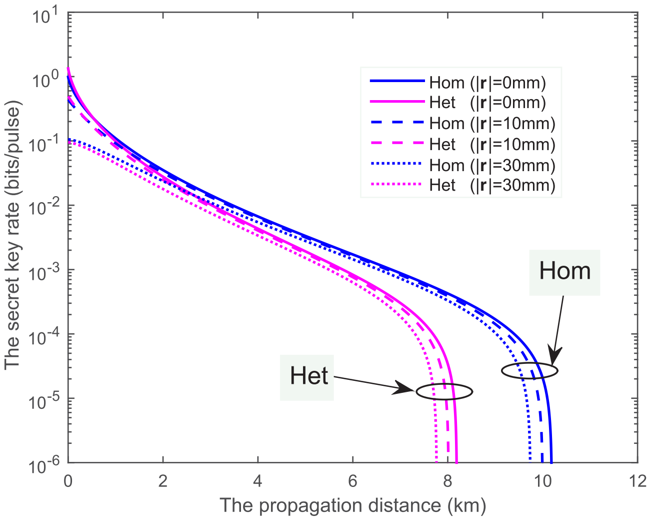

FIG. 6. The parameter estimation-based achievable secret key rate $\bar{K}_T$ considering beam wandering under an atmospheric weak turbulence channel.

and polarization preservation to establish global quantum communications; nevertheless, beam scintillation and beam wandering caused by atmospheric turbulence have a significant impact on CVQKD, as shown in Figs. 5 and 6; that is, Figs. 5 and 6 describe the impact of beam scintillation and beam wandering on $\bar{K}_T$, respectively.

In addition, simulation results based on parameter estimation show that the secret key rate and propagation distance of CVQKD in a medium-to-strong turbulent channel are less than those in a weak turbulent channel in the case of the same beam wandering and phase variations, and phase variations can further reduce the secret key rate and propagation distance of CVQKD, whether medium-to-strong turbulent or weak turbulence, so phase variations caused by atmospheric turbulence is another important factor affecting the performance of CVQKD besides beam wandering and beam scintillation, and this reflects the importance of phase compensation technology in CVQKD. Furthermore, taking the influence of beam wandering on CVQKD in a weak turbulent channel as an example, the influence of beam wandering on the secret key rate and propagation distance as shown in Fig. 6 is no less than that of phase variations as shown in Fig. 5. Accordingly, the main effort in practice should be devoted to inhibiting the effects of beam wandering and scintillation as well as phase variations. The development and application of related technology such as compensation technology under beam scintillation and acquisition tracking pointing (ATP) technology under beam wandering based on parameter estimation of atmospheric GMCS CVQKD can directly or indirectly fade down the atmospheric effect and improve the performance of CVQKD.

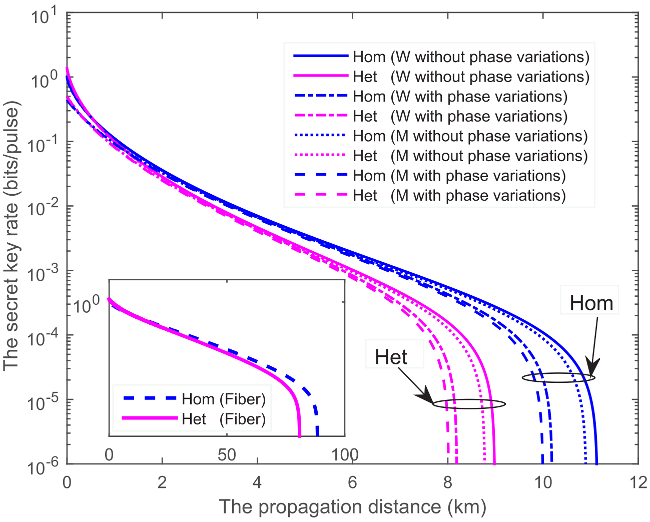

FIG. 5. The parameter estimation-based achievable secret key rate $\bar{K}_T$ without considering beam wandering under an atmospheric turbulence channel. W indicates the weak turbulence channel, and M indicates the medium-to-strong turbulence channel.

In summary, the simulation results based on this parameter estimation method coincide with previous theoretical analysis of atmospheric effects on CVQKD [22], which proves the availability and rationality of this method and provides a feasible method for parameter estimation of free-space CVQKD.

B. The security analysis

The entanglement-distillation attack against CVQKD systems whose channels are affected by non-Gaussian noise in a turbulent atmospheric environment is proposed in Ref. [42] on the assumption that quantum repeaters can be employed in long-distance links, such as satellite-to-ground channels and ground-to-ground networks, where Alice and Bob may not be able to discover Eve by simple monitoring of light. According to Ref. [42], in a such case that security bounds can be overestimated if the fluctuating transmittance is regarded as a constant, Alice and Bob may not be able to discover the eavesdropper's interference under general parameter estimation, which created a potential loophole.

We can employ the parameter estimation described in Sec. II B 2 to obtain transmission T_i and excess noise ε_i of

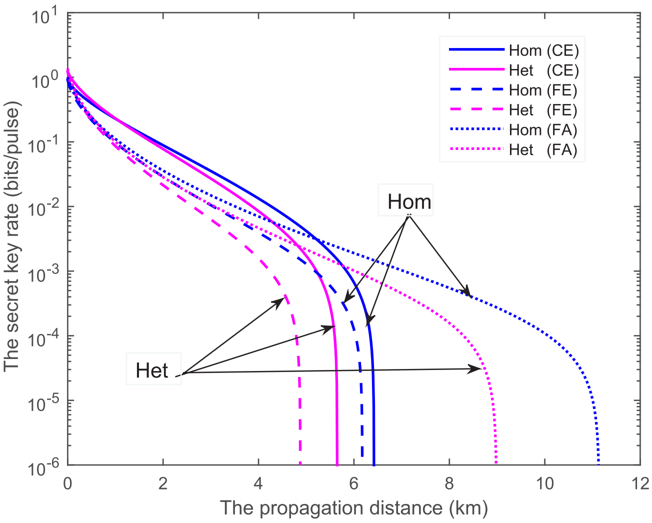

FIG. 7. Secret key rate with a distribution of transmittance $\{\hat{T}_i\}$. C indicates the constant transmittance T, F indicates the fluctuating transmittance $\{T_i\}$, E indicates the estimated value $\hat{\varepsilon}$, and A indicates the actual value ε.

each subchannel during the stability time of the atmospheric turbulence channel that is described in Fig. 1, that is, a distribution of transmittance $\{\hat{T}_i\}$ with probabilities approximated to frequency $\{\hat{p}_{T_i}\}$ and a corresponding distribution of excess noise $\{\hat{\varepsilon}_i\}$ with probabilities approximated to frequency $\{\hat{p}_{\varepsilon_i}\}$. The covariance matrix of the resulting mixed state after the ith subchannel is given by Eq. (20). Therefore, the secret key rate of ith subchannel $\bar{K}_{T}^{i}(T_i, \varepsilon_i)$ can be calculated through the analysis of Sec. IV A. So we can get a real-time transmission key rate dynamically in a relatively stable subchannel interval to effectively resist an entanglement-distillation attack.

Furthermore, we can see that there is a deviation between the estimated value $\hat{\varepsilon}$ and the actual value ε by Eqs. (32) and (17):

$$\hat{\varepsilon} - \varepsilon = \hat{V}_A \left\{ \frac{E\left[A_\alpha^2 \cos^2 \phi\right]}{E^2[A_\alpha \cos \phi]} - 1 \right\} + (E[A^2] - \hat{V}_X) \frac{E\left[A_\alpha^2 \sin^2 \phi\right]}{E^2[A_\alpha \cos \phi]}, \tag{38}$$

where $\mathrm{Var}[A_\alpha \cos \phi] = E[A_\alpha^2 \cos^2 \phi] - E^2[A_\alpha \cos \phi] \geqslant 0$, and $E[A^2 \cos^2 \phi] \leqslant E[A^2]$; hence, we can obtain the result $\hat{\varepsilon} - \varepsilon \geqslant 0$. The estimation method leads to a conservative lower bound of the secret key rate, which guarantees the security of the communication to effectively resist an entanglement-distillation attack.

As noted in Fig. 7, the achievable secret key rate estimated by fluctuating transmittance $\{T_i\}$ and excess noise $\hat{\varepsilon}$ is lower than the real secret key rate calculated by fluctuating transmittance $\{T_i\}$ and excess noise ε. Meanwhile, the achievable secret key rate estimated by fluctuating transmittance $\{T_i\}$ is lower than the achievable secret key rate estimated by the constant transmittance T. This indicates that parameter estimation underestimates the secure propagation distance in the case of effectively resisting an entanglement-distillation attack and guaranteeing security.

From the above analysis, it can be seen that the secure propagation distance of GMCS CVQKD under an atmospheric effect is very limited. Currently, it is known that discrete modulation can achieve a longer propagation distance in fiber channel [43], but the secret key rate is lower than that of Gaussian modulation. Naturally, different coding schemes under different modulations and other related research work to enhance secure propagation distance and the secret key rate of CVQKD under free space will be the next direction for research.

V. CONCLUSIONS AND DISCUSSIONS

In conclusion, we have employed free-space-based Gaussian modulated coherent state continuous-variable quantum key distribution (GMCS CVQKD) to study the parameter estimation method of an atmospheric channel and analyzed the achievable secret key rate. The proposed parameter estimation method coincides well with a physical model, which is more systematic, extensive, and comprehensive and has certain reference value and guidance significance to the classical information postprocessing part of CVQKD. With the help of the parameter estimation in CVQKD and the analysis of beam propagation in an atmospheric channel, we have studied the link fluctuations on free-space CVQKD and found that the atmospheric attenuation channel delivers a better advantage than the fiber channel in terms of the secret key rate and propagation distance, while beam scintillation and beam wandering caused by the atmospheric turbulence channel bring a serious impact to CVQKD. Moreover, phase variations caused by atmospheric turbulence are another important factor affecting the performance of CVQKD besides beam wandering and beam scintillation.

Consequently, the simulation results based on this parameter estimation method coincide with the atmospheric effects on CVQKD, which proves the availability and rationality of this method and provides a feasible method for parameter estimation of free-space CVQKD. Further, the results show that the parameter estimation method provides a practical and available parameter evaluation method for CVQKD in a practical free-space channel. Finally, based on the analysis mentioned above, we obtain that the proposed method can effectively resist the previously proposed entanglement-distillation attack.

As illustrated in this paper, we can obtain a distribution of transmittance with its probabilities and a corresponding distribution of excess noise with its probabilities through the proposed method as well as a conservative lower bound of the secret key rate which guarantees the security of the communication results from the estimated parameters. But there still exist some problems, such as it is difficult to extract a secret key under poor parameters and so on. Therefore, postselection of subchannels, which is achieved by filtering out the low contribution region of transmittance and excess noise, provides an effective way to improve the secret key rate. There is a distinct improvement in the entanglement and security properties of the state via postselection of subchannels with higher transmittance. However, the secret key rate eventually is up to the overall success probability of the postselection, that is, the optimal postselection region, and the choice of the optimal postselection region of free-space CVQKD is still an open-ended question.

ACKNOWLEDGMENTS

This work is supported by the National Key Research and Development Program (Grant No. 2016YFA0302600), the Nature Fund of Science in Shaanxi in 2018 (Grant No. 2018JM6123), and the National Natural Science Foundation of China (Grants No. 61801385, No. 61332019, No. 61671287, and No. 61631014).

APPENDIX: THE SCINTILLATION INDEX

The scintillation index can be expressed as [33]

$$\sigma_I^2(\mathbf{r}, L) = \sigma_{I,r}^2(\mathbf{r}, L) + \sigma_I^2(\mathbf{0}, L), \tag{A1}$$

where $\sigma_{I,r}^2(\mathbf{r}, L)$ and $\sigma_I^2(\mathbf{0}, L)$ are radial component and longitudinal components, respectively. The radial component can be expressed as Eq. (A2), when the outer scale is not very large,

$$\sigma_{I,r}^2(\mathbf{r}, L) = 4.42\sigma_I^2 \Lambda_e^{5/6} \frac{r^2}{W_e^2}, \quad r < W_e, \tag{A2}$$

where r is the distance from the beam center line in the transverse direction, $\Lambda_e = 2L/kW_e^2$ represents the effective beam parameter, and W_e is a measure of the effective beam spot size given by Eq. (A3) with $\Lambda = 2L/kW^2$, which describes Gaussian-beam amplitude change due to diffraction, and $W = W_0\sqrt{1 + (\lambda L/\pi W_0^2)^2}$ is the free-space beam radius at the receiver:

$$W_e = \begin{cases} W\sqrt{1 + 1.33\sigma_I^2 \Lambda^{\frac{5}{6}}} & \text{weak turbulence} \\ W\sqrt{1 + 1.63\sigma_I^{\frac{12}{5}} \Lambda} & \text{strong turbulence.} \end{cases} \tag{A3}$$

In addition, the Rytov variance is expressed as $\sigma_I^2 = 1.23C_n^2 k^{7/6} L^{11/6}$ with the optical wave number $k = 2\pi/\lambda$, where λ is the wavelength of beam, the horizontal propagation distance L, and the index of refraction structure parameter C_n^2. The Hufnagel-Valley (H-V) model [33] for C_n^2 is given by

$$\begin{aligned} C_n^2(h) = {} & 0.00594\left(\frac{v}{27}\right)^2 (10^{-5}h)^{10} \exp\left(-\frac{h}{1000}\right) \\ & + 2.7 \times 10^{-16} \exp\left(-\frac{h}{1500}\right) + A \exp\left(-\frac{h}{100}\right), \end{aligned} \tag{A4}$$

with the root-mean-square wind speed (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 the H-$V_{5/7}$ model. However, the radial component in Eq. (A2) is quite sensitive to outer-scale effects when the outer scale is large enough, and it is given as

$$\sigma_{I,r}^2(\mathbf{r}, L) = 4.42\sigma_I^2 \Lambda_e^{5/6} \left[1 - 1.55\left(\frac{\Lambda_e L}{kL_0^2}\right)^{\frac{1}{6}}\right] \frac{r^2}{W_e^2}, \tag{A5}$$

where L_0 is the outer scale. $L_0(h)$ models based on experimental data are expressed as below. However, the radial component approaches zero in strong fluctuations:

$$L_0(h) = \begin{cases} 0.4, \ h \leqslant 1 \text{ m}, \\ 0.4h, \ 1 < h \leqslant 25 \text{ m}, \\ 2\sqrt{h}, \ 25 < h \leqslant 1 \text{ km}, \\ 2\sqrt{1000}, \ 1 \text{ km} < h \leqslant 2 \text{ km}, \\ 5\left[1 + \left(\frac{h-7500}{2000}\right)^2\right]^{-1}, \ 2 \text{ km} < h \leqslant 17 \text{ km}. \end{cases}$$

The longitudinal component is given by

$$\sigma_I^2(\mathbf{0}, L) = \exp\left[\sigma_{\ln x}^2 + \sigma_{\ln y}^2\right] - 1, \tag{A6}$$

where $\sigma_{\ln x}^2$ and $\sigma_{\ln y}^2$ are large- and small-scale log-irradiance variances, respectively. Here we find the relations

$$\begin{aligned} \alpha &= \left[\exp\left(\sigma_{\ln x}^2\right) - 1\right]^{-1}, \\ \beta &= \left[\exp\left(\sigma_{\ln y}^2\right) - 1\right]^{-1}, \end{aligned} \tag{A7}$$

where α and β are the effective number of large- and small-scale cells in the gamma-gamma distribution (27), respectively. When effects of inner scale l_0 and outer scale L_0 are both involved, the longitudinal component can be expressed as

$$\begin{aligned} \sigma_I^2(\mathbf{0}, L) = \exp & \left[\sigma_{\ln x}^2(l_0) - \sigma_{\ln x}^2(L_0)\right. \\ & \left. + \sigma_{\ln y}^2(l_0)\right] - 1, \end{aligned} \tag{A8}$$

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

$$\begin{aligned} \sigma_{\ln x}^2(l_0) = {} & 0.49\sigma_I^2 \left(\frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\bar{\Theta}}{5}\right)\left(\frac{\eta_x Q_l}{\eta_x + Q_l}\right)^{\frac{7}{6}} \\ & \times \left[1 + 1.75\sqrt{\frac{\eta_x}{\eta_x + Q_l}} - 0.25\left(\frac{\eta_x}{\eta_x + Q_l}\right)^{\frac{7}{12}}\right], \end{aligned} \tag{A9}$$

where $Q_l = 10.89L/kl_0^2$, and $\bar{\Theta} = -L/F$ with the phase front radius of curvature $F = L[1 + (\pi W_0^2)/(\lambda L)]$ in free space at the receiver, and

$$\begin{aligned} \frac{1}{\eta_x} = {} & \frac{0.38}{1 - 3.21\bar{\Theta} + 5.29\bar{\Theta}^2} \\ & + 0.47\sigma_I^2 Q_l^{\frac{1}{6}} \left(\frac{\frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\bar{\Theta}}{5}}{1 + 2.2\bar{\Theta}}\right)^{\frac{6}{7}}. \end{aligned} \tag{A10}$$

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

$$\begin{aligned} \sigma_{\ln x}^2(L_0) = {} & 0.49\sigma_I^2 \left(\frac{1}{3} - \frac{\bar{\Theta}}{2} + \frac{\bar{\Theta}}{5}\right)\left(\frac{\eta_{x0} Q_l}{\eta_{x0} + Q_l}\right)^{\frac{7}{6}} \\ & \times \left[1 + 1.75\sqrt{\frac{\eta_{x0}}{\eta_{x0} + Q_l}} - 0.25\left(\frac{\eta_{x0}}{\eta_{x0} + Q_l}\right)^{\frac{7}{12}}\right], \end{aligned} \tag{A11}$$

where $\eta_{x0} = \eta_x Q_0/(\eta_x + Q_0)$, and $Q_0 = 64\pi^2 L/(kL_0^2)$ is a nondimensional outer-scale parameter. The small-scale log-irradiance variance $\sigma^2_{\ln y}(l_0)$ can be written as

$$\sigma^2_{\ln y}(l_0) = \frac{0.51\sigma_{_G}^2}{\left(1 + 0.69\sigma_G^{12/5}\right)^{5/6}}, \tag{A12}$$

where $\sigma_{_G}^2$ is the weak fluctuation scintillation index and can be written as

$$\begin{aligned}\sigma_{_G}^2 = 3.86\sigma_l^2\Bigg(0.4\frac{[(1+2\Theta)^2 + (2\Lambda + 3/Q_l)^2]^{11/12}}{\sqrt{(1+2\Theta)^2 + 2\Lambda^2}}\Bigg\{&\frac{2.61}{[(1+2\Theta)^2 Q_l^2 + (3+2\Lambda Q_l)^2]^{1/4}}\sin\left(\frac{4\varphi_2}{3} + \varphi_1\right)\\ &- \frac{0.52}{[(1+2\Theta)^2 Q_l^2 + (3+2\Lambda Q_l)^2]^{7/24}}\sin\left(\frac{5\varphi_2}{4} + \varphi_1\right) + \sin\left(\frac{11\varphi_2}{6} + \varphi_1\right)\Bigg\} - \frac{13.4\Lambda}{[(1+2\Theta)^2 + 4\Lambda^2]Q_l^{11/6}}\\ &- \frac{11}{6}\left[\left(\frac{1+0.31\Lambda Q_l}{Q_l}\right)^{5/6} + \frac{1.1(1+0.27\Lambda Q_l)^{1/3}}{Q_l^{5/6}} - \frac{0.19(1+0.24\Lambda Q_l)^{1/4}}{Q_l^{5/6}}\right]\Bigg)\end{aligned} \tag{A13}$$

and

$$\begin{aligned}\varphi_1 &= \tan^{-1}\left(\frac{2\Lambda}{1+2\Theta}\right),\\ \varphi_2 &= \tan^{-1}\left[\frac{(1+2\Theta)Q_l}{3+2\Lambda Q_l}\right],\end{aligned} \tag{A14}$$

with $\Theta = 1 - \bar{\Theta}$.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[4] M. J. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, Appl. Opt. **52**, 3311 (2013).

[5] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, and A. Zeilinger, Proc. Natl. Acad. Sci. U. S. A. **112**, 14197 (2015).

[6] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).

[7] I. Capraro, A. Tomaello, A. DallArche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **109**, 200502 (2012).

[8] M. Krenn, J. Handsteiner, M. Fink, R. Fickler, R. Ursin, M. Malik, and A. Zeilinger, Proc. Natl. Acad. Sci. U. S. A. **113**, 13648 (2016).

[9] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, and J.-W. Pan, Nat. Photonics **7**, 387 (2013).

[10] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Phys. Rev. Lett. **115**, 040502 (2015).

[11] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, and J.-W. Pan, Science **356**, 1140 (2017).

[12] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, and J.-W. Pan, Nat. Photonics **11**, 509 (2017).

[13] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J. G. Ren, W. Y. Liu, Y. Li, Q. Shen, Y. Cao, F. Z. Li, J. F. Wang, Y. M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N. L. Liu, F. Koidl, P. Wang, Y. A. Chen, X. B. Wang, M. Steindorfer, G. Kirchner, C. Y. Lu, R. Shu, R. Ursin, T. Scheidl, C. Z. Peng, J. Y. Wang, A. Zeilinger, and J.-W. Pan, Phys. Rev. Lett. **120**, 030501 (2018).

[14] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).

[15] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).

[16] D. Huang, P. Huang, D.-K. Lin, and G.-H. Zeng, Sci. Rep. **6**, 19201 (2016).

[17] P. Huang, J.-Z. Huang, Z. Zhang, and G.-H. Zeng, Phys. Rev. A **97**, 042311 (2018).

[18] B. Heim, D. Elser, T. Bartley, M. Sabuncu, C. Wittmann, D. Sych, C. Marquardt, and G. Leuchs, Appl. Phys. B **98**, 635 (2010).

[19] C. Peuntinger, B. Heim, C. R. Muller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).

[20] D. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **117**, 090501 (2016).

[21] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, Phys. Rev. A **96**, 043856 (2017).

[22] S. Wang, P. Huang, T. Wang, and G.-H. Zeng, New J. Phys. **20**, 083037 (2018).

[23] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, New J. Phys. **14**, 093048 (2012).

[24] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).

[25] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).

[26] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. Lett. **120**, 220505 (2018).

[27] D. Vasylyev, W. Vogel, and A. A. Semenov, Phys. Rev. A **97**, 063852 (2018).

[28] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. M. Merolla, in *2006 IEEE Information Theory Workshop-ITW'06 Punta del Este* (IEEE, New York, 2006), pp. 116–120.

[29] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[30] J. Gariano and I. B. Djordjevic, Appl. Opt. **57**, 8451 (2018).

[31] W.-Q. Liu, J.-Y. Peng, P. Huang, D. Huang, and G.-H. Zeng, Opt. Express **25**, 19429 (2017).

[32] J. C. Ricklin, S. M. Hammel, F. D. Eaton, and S. L. Lachinova, J. Opt. Fiber Commun. Rep. **3**, 111 (2006).

[33] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE Press, Bellingham, WA, 2001).

[34] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation through Random Media* (SPIE Press, Bellingham, WA, 2005).

[35] C. Chen, H. Yang, Y. Lou, S. Tong, and R. Liu, Opt. Express **20**, 7749 (2012).

[36] R. J. Noll, J. Opt. Soc. Am. **66**, 207 (1976).

[37] D. L. Fried, Proc. IEEE **55**, 57 (1967).

[38] A. Belmonte and J. M. Kahn, Opt. Express **16**, 14151 (2008).

[39] A. Belmonte and J. M. Kahn, Opt. Express **17**, 2763 (2009).

[40] R. Dong, M. Lassen, J. Heersink, C. Marquardt, R. Filip, G. Leuchs, and U. L. Andersen, Phys. Rev. A **82**, 012312 (2010).

[41] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).

[42] Y. Guo, C. Xie, Q. Liao, W. Zhao, G.-H. Zeng, and D. Huang, Phys. Rev. A **96**, 022320 (2017).

[43] Q. Liao, Y. Guo, D. Huang, P. Huang, and G.-H. Zeng, New J. Phys. **20**, 023015 (2018).