


Bayesian Parameter Estimation for Continuous-Variable Quantum Key Distribution

Kexin Liang,^{1,2,†} Geng Chai^{1,†}, Zhengwen Cao,^{1,2,*} Yang Yuan,¹ Xinlei Chen,¹ Yuan Lu,¹ and Jinye Peng¹

¹Laboratory of Quantum Information and Technology, School of Information Science and Technology, Northwest University, Xi'an 710127, China

²State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an 710071, China

 (Received 21 April 2022; revised 21 August 2022; accepted 11 October 2022; published 23 November 2022)

The effectiveness and accuracy of parameter estimation are guarantees for the high-performance and high-safety operation of practical continuous-variable quantum key distribution systems. A scheme based on Bayesian estimation is proposed to tackle the fluctuations of channels. In free-space channel, the Bayesian random-effects model is employed to construct complete prior information, and the channel state information extracted through pilot signals is applied to rectify the prior information. Compressed sensing technology is applied due to the sparsity of the free-space channel to reduce the cost of the system. Experimental results show that the proposed scheme has higher estimation accuracy under the free space, and the system performance is also enhanced. Moreover, the results under fiber show higher estimation accuracy and better stability than that of traditional methods. In conclusion, the scheme can create practical conditions for the construction of future global quantum networks.

DOI: [10.1103/PhysRevApplied.18.054077](https://doi.org/10.1103/PhysRevApplied.18.054077)

I. INTRODUCTION

Information security is a strategic field concerning the national economy and people's livelihood. Nowadays, legal parties can share encryption keys with unconditional security by quantum states, which is called quantum key distribution (QKD) [1–4]. According to different sources and detection methods, it can be divided into the discrete variable scheme (DVQKD) and the continuous-variable scheme (CVQKD) [5,6]. Different from the former, the latter has a higher key rate and a cheaper implementation cost [7,8]. The Gaussian modulation coherent state (GMCS) CVQKD system [9,10] has become the mainstream protocol since its technologies for the physical part and the postprocessing part are mature. The farthest transmission distance of CVQKD reported so far has reached 202.81 km [11] through high-precision phase compensation technology and lossless fiber channel. Compared with the fiber transmission, quantum signals are hardly affected by birefringence as they travel through the free space [12], which

leaves many nonclassical properties unaffected [13,14]. Therefore, free-space CVQKD is an indispensable part of realizing global communication and will help to complete the goal of long-distance, large-scale, high-capacity network construction. Nowadays, the schemes for post-processing of free-space CVQKD were put forward one after another. Parameter estimation [15–18], phase compensation [19], and polarization control [20] are gradually completed, respectively, which laid a solid foundation for the followup work.

Parameter estimation is worth paying attention to because it is a crucial aspect that connects the quantum information stage and the data processing stage. Numerous fiber channel parameter estimation solutions have been analyzed [21–24], which all need to sacrifice part of the raw keys to ensure a superior estimation accuracy. In order to solve this problem, the work [25] gives a method based on quantum tomography, in which all the raw keys can be used for both parameter estimation and key extraction, but it is rather impractical. Another work [26] proposes a double-modulation method to avoid wasting raw keys at the cost of increased system complexity. Therefore, in the current parameter estimation research under the fiber channel, the goals that need to be achieved are full use of quantum resources, low complexity, and high estimation accuracy even in the fiber jitter environment.

*Corresponding author. caozhw@nwu.edu.cn

†These authors contributed equally to this work and should be considered co-first authors.

Different from fiber, the turbulence effect [27–29] makes the atmospheric channel fluctuate, which causes random variations of the signal and ultimately exacerbates the communication quality. In view of this, different parameter estimation schemes for free-space CVQKD [15–18] have been proposed. The work [15] presents a parameter estimation method for GMCS CVQKD over an atmospheric link based on the maximum-likelihood estimate (MLE) and subchannel theory and shows that the estimated values of the parameters are influenced by the amplitude attenuation and phase fluctuation of the quantum signals. Another estimation scheme through clustering massive transmission data is studied in the work [16], which proves that in a highly fluctuating channel, as long as the measurement data set is large enough, one can get a secret key rate that is about the same as that passing through a stable channel. The research [17] investigates a blind parameter estimation (BPE) for free-space CVQKD and verifies its feasibility and availability. The work [18] studies the channel parameter estimation of OAM-based CVQKD, and the results show that the OAM multiplexing can significantly improve the secret key rate, and estimations for transmittance and excess noise are of great significance. Although the above methods have been effectively applied in the free-space CVQKD system, their basic principles are to divide a volatile free-space channel into a series of stable subchannels without systematically considering its overall characteristics. Bayesian estimation is to obtain a different probability by combining other evidence and prior probability with the Bayesian theorem. At present, Bayesian estimation has been well used in the field of quantum information, such as quantum metrology [30–32], and it also has an excellent combination with machine learning, making the algorithm more adaptive [33,34]. Thus, Bayesian estimation can well target the fluctuation characteristics of free-space channel, but there is no relevant application of Bayesian estimation in this field.

This paper proposes a general CVQKD parameter estimation scheme based on Bayesian estimation. To give full play to the superiority of this estimation method, robust prior information is required. In the free-space channel, the elliptical beam model [35,36] and the atmospheric scintillation [37] are combined through the Bayesian random-effects model [38,39] to obtain complete prior information about atmospheric transmittance. Pilot signals are used to acquire channel state information, and all quantum signals are applied to generate raw keys. Considering the sparsity of the atmospheric channel, compressed-sensing (CS) technology [40] is employed to reconstruct the pilot signals, and the position and length of the pilot signals are designed according to the reconstruction accuracy [41]. Referring to the experiment of the work [42], the experimental verification under the free-space channel is completed. The results show that the proposed scheme

has stronger robustness and higher accuracy compared to another method [16] and the system performance is enhanced. This paper also completes the validation under the fiber channel and compared with the MLE, the scheme has high robustness and accuracy without wasting quantum resources, and ensures the practical security of the system to a certain extent. Our work supports the experimental development of free-space CVQKD and creates conditions for the construction of a global CVQKD system in the future.

II. RESULTS

A. Bayesian parameter estimation

The traditional parameter estimation for fiber GMCS CVQKD is executed by MLE, using a part of sampled variables of Alice and Bob. Specifically, it is executed by randomly extracting $\{(x_i, y_i) | i = 1, 2, 3, \dots, m\}$, m is the number of samples from Alice's variable $\{x_i\}_{i=1,2,3,\dots,N}$ and Bob's variable $\{y_i\}_{i=1,2,3,\dots,N}$, N is the total number of transmitted quantum signals. The respective variances of Alice $\langle x^2 \rangle$ and Bob $\langle y^2 \rangle$ and the covariance of them $\langle xy \rangle$ are described as

$$\begin{aligned}\langle x^2 \rangle &= V_A, \\ \langle y^2 \rangle &= \eta TV_A + N_0 + \eta T\varepsilon + \nu_{\text{el}}, \\ \langle xy \rangle &= \sqrt{\eta TV_A},\end{aligned}\quad (1)$$

where V_A is variance of Alice's variable, N_0 is shot noise, ν_{el} is electrical noise, η is detection efficiency, T is channel transmittance, and ε is excess noise. Among them, ν_{el} , η , and N_0 need to be calibrated in advance. η can be calculated based on the responsiveness R of the diode. In the absence of any light input, the absolute value of ν_{el} can be obtained by measuring the variance of the output electrical signal $\{y_{0i}\}_{i=1,2,3,\dots,N}$. Only the local oscillator (LO) light is allowed to pass through the beam Q5 splitter (BS), and the homodyne detector is used for differential amplification to measure the variance of the output electrical signal, and the variance value after subtracting the variance of the ν_{el} is the required N_0 . The variables of Alice and Bob $\{(x_i, y_i) | i = 1, 2, 3, \dots, N\}$ satisfy the following normal linear model:

$$y = tx + z, \quad (2)$$

where $t = \sqrt{\eta T}$, and z is a Gaussian noise with variance $\sigma^2 = N_0(1 + \eta T\varepsilon + \nu_{\text{el}})$. According to MLE, the

estimated values of these parameters are described as

$$\begin{aligned}\hat{\sigma}_0^2 &= \frac{1}{N} \sum_{i=1}^N y_{0i}^2, \\ \hat{V}_A &= \frac{1}{N} \sum_{i=1}^N x_i^2, \\ \hat{t} &= \frac{\sum_{i=1}^m x_i y_i}{\sum_{i=1}^m x_i^2}, \\ \hat{\sigma}^2 &= \frac{1}{m} \sum_{i=1}^m (y_i - \hat{t}x_i)^2.\end{aligned}\quad (3)$$

Then the T , ε , V_A , and χ_{tot} can be obtained by

$$\begin{aligned}\hat{T} &= \frac{\hat{t}^2}{\eta}, \\ \hat{\varepsilon} &= \frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{t}^2}, \\ \hat{V}_A &= \frac{\hat{V}_A}{N_0}, \\ \hat{\chi}_{\text{tot}} &= \frac{\hat{\sigma}^2}{\hat{t}^2} - 1.\end{aligned}\quad (4)$$

Different from the fiber channel, because of the influence of atmospheric turbulence, the transmittance of the atmospheric channel is no longer a fixed constant, but a random variable that satisfies a certain probability distribution. Thus, Eq. (1) needs to be rewritten as

$$\begin{aligned}\langle x^2 \rangle &= V_A, \\ \langle y^2 \rangle &= V_B, \\ \langle xy \rangle &= \sqrt{\eta \langle T \rangle} V_A, \\ \langle y_0^2 \rangle &= V_{B0} = \langle N_0 \rangle (1 + \nu_{\text{el}}),\end{aligned}\quad (5)$$

where $\langle \bullet \rangle$ represents the ensemble mean.

N_0 is the basic unit of subsequent estimated values, and it is proportional to the intensity of LO [43]. In the traditional CVQKD scheme, LO and quantum light pass through the same channel, therefore, the intensity of LO will fluctuate, which will affect the value of N_0 further. Therefore, it is necessary to perform the estimation of N_0 to ensure the accuracy and effectiveness of subsequent parameter estimation will not be affected. In view of this, Bayesian estimation for traditional CVQKD can be described as

$$p(T, N_0 | y) = \frac{p(y | T, N_0) p(T)}{p(y)}, \quad (6)$$

where $p(T)$ is prior probability and its accuracy largely determines the final estimation result. Under the premise

of accurate prior probability, a small amount of pilot signal is used to acquire the conditional probability $p(y | T, N_0)$ by its statistical characteristics. Finally, a more accurate posterior probability $p(T, N_0 | y)$ is received. This method gathers all the information about the estimated parameter in the three kinds of information of population, sample, and prior, and excludes all information that has nothing to do with the estimated parameter.

It should be noted that the distribution of channel parameters result of Bayesian estimation can fully reflect the communication process. According to the estimation results, subsequent parameter estimation can indeed be carried out. However, in CVQKD, we need only to pay attention to the overall situation of a secret key distribution process, because the insecure secret keys can be corrected and compressed by subsequent reconciliation and privacy amplification, respectively. And finally, the communication parties can get a string of completely consistent security secret keys. Therefore, in the study of free-space CVQKD, the mean value of transmission T is used to characterize the communication status of this communication process and then substituted into the secret key rate formula to further judge the security of the communication process. The accurate probability $p(T, N_0 | y)$ obtained by Bayesian estimation is the basis for obtaining the accurate mean value.

The final Bayesian estimated values of parameters $\langle \hat{T} \rangle$ and $\langle \hat{N}_0 \rangle$ are given by

$$\begin{aligned}\langle \hat{T} \rangle &= \int T \int dN_0 P(T, N_0 | y) dT, \\ \langle \hat{N}_0 \rangle &= \int N_0 \int dT P(T, N_0 | y) dN_0.\end{aligned}\quad (7)$$

In this work, the LO is provided by Bob, that is to say, the strength of the LO is not interfered with by the channel fluctuation, only one calibration is required to be done once and for all. In this case, N_0 is constant and does not have to be estimated in real time. Bob needs only to pass the LO alone through a 50:50 BS and obtain N_0 by differential amplification with a homodyne detector. Thus, Eq. (6) is simplified as

$$p(T | y) = \frac{p(y | T) p(T)}{p(y)}, \quad (8)$$

and the Bayesian estimated values of parameter $\langle \hat{T} \rangle$ is

$$\langle \hat{T} \rangle = \int p(T | y) T dT. \quad (9)$$

Other estimated values can be calculated by

$$\begin{aligned}\hat{\varepsilon} &= \frac{\hat{V}_B - \hat{V}_{B0}}{\eta \langle \hat{T} \rangle} - \hat{V}_A, \\ \hat{\chi}_{\text{tot}} &= \frac{\hat{V}_B}{\eta \langle \hat{T} \rangle} - (\hat{V}_A + 1).\end{aligned}\quad (10)$$

Thus, in order to make the most of the advantages of the Bayesian method, it needs accurate prior information and conditional information.

B. Prior information

A free-space quantum channel is defined as a quantum channel with fluctuating transmission characteristics, and the relationship between its input quantum state $\rho_{\text{in}}(\alpha)$ and output quantum state $\rho_{\text{out}}(\alpha)$ is described as [14]

$$\rho_{\text{out}}(\alpha) = \int_0^1 dTP(T) \frac{1}{T} \rho_{\text{in}}\left(\frac{\alpha}{\sqrt{T}}\right), \quad (11)$$

where $P(T)$ is the probability distribution of the transmittance and is used to describe fluctuations. Random fluctuation of atmospheric refractive index caused by randomly changing pressure and temperature forms the atmospheric turbulence effect. Under its influence, the beam deviates from the predetermined propagation direction, resulting in beam wandering and broadening. The constructive interference and destructive interference of the refracted beam of different intensities in the receiving aperture also cause scintillation and deformation. C_n^2 is the index of refraction structure parameter describing the intensity of turbulence, which is related to geographical location, weather, and ambient temperature.

The elliptical beam model [35], as shown in Fig. 1, describes quantitatively beam wandering, broadening, and deformation in weak and strong turbulence, providing a method for the analysis of transmission estimation in the CVQKD system. It assumes that the turbulence effect deforms the beam profile into an ellipse, and the beam on the plane of the receiving aperture can be described as

$$I(\mathbf{r}, L) = \frac{2}{\pi \sqrt{\det \mathbf{S}}} \exp[-2(\mathbf{r} - \mathbf{r}_0)^T \mathbf{S}^{-1} (\mathbf{r} - \mathbf{r}_0)], \quad (12)$$

where I is the intensity of beam at a point on the received plane, $\mathbf{r} = (x, y)^T$, $\mathbf{r}_0 = (x_0, y_0)^T$ is the beam-centroid position, \mathbf{S} is the real, symmetric, positive-definite spot-shape matrix on receiving aperture plane, and L is the transmission distance.

There exists multiple turbulence when the diameter of the beam is much larger than the turbulence. This turbulence independently scatters and diffracts a part of the

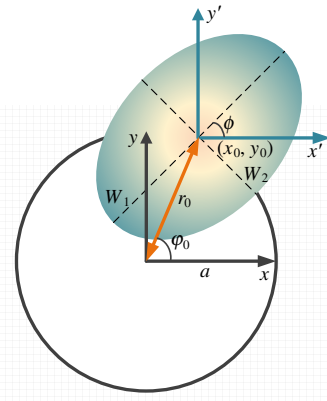


FIG. 1. Elliptical beam approximation model. a is the radius of receiving aperture. The eigenvalues of this matrix W_i^2 ($i = 1, 2$) are square of the major axis and the minor axis of the ellipse. ϕ and ϕ_0 are the angles between the W_1 and the center of the elliptical beam (x_0, y_0) and the x axis of the receiving aperture, respectively. Any point in the transmitted beam can be uniquely determined by the parameters $\{x_0, y_0, W_1^2, W_2^2, \phi\}$ in the ellipse model.

beam, resulting in random decay of intensity and random fluctuations of phase, bringing about an atmospheric scintillation effect. Under weak turbulence conditions, the scintillation effect can be described by the Rytov approximation [27]

$$\beta_I^2 = 1.23k^{7/6} C_n^2 L^{6/11}, \quad (13)$$

where k is wave numbers ($k = 2\pi/\lambda$, λ is wavelength). In the case of strong turbulence, the irradiance of the beam becomes saturated with the increase of C_n^2 , which is called scintillation saturation.

However, scintillation is not considered in the elliptical beam model. In order to show the effect of scintillation on the beam, numerical simulation is employed to generate a series of phase screens to simulate the turbulence on the beam propagation path. This is because the effect of atmospheric turbulence can be equivalent to the effect of a random phase screen (need to meet the turbulence statistical theory) and the effect of beam vacuum propagation after a certain distance of transmission. Specifically, the turbulent random medium can be divided into a series of parallel plates with a certain thickness. Each plate generates random phase modulation, and the beam between adjacent plates propagates as a vacuum. Figure 2 describes the random phase change of the received beam considering the scintillation, which cannot be ignored during the subsequent studies.

The Bayesian random-effects model is an extension of the classic linear model, which treats the regression coefficients of the original (fixed effects model) as random

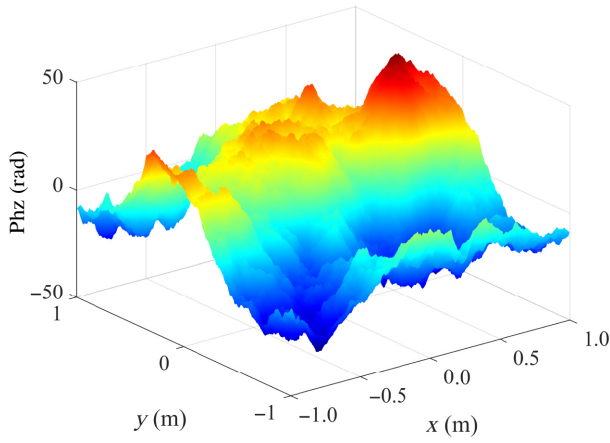


FIG. 2. Scintillation effect under weak turbulence. A square phase screen with a length and width of 2 m is simulated, the number of grid points is 512×512 , the atmospheric coherence length r_0 is 0.1 m, and the internal and external scales of turbulence are considered. The average value of the phase structure function obtained by statistics of 500 phase screens generated by the fast Fourier transform (FFT) method, $C_n^2 = 2 \times 10^{-17}$ belongs to the weak turbulence condition and Phz represents phase fluctuation.

variables. Consider the following linear model:

$$y_{ij} = \mu + v_i + \mathbf{e}_{ij} \quad (i = 1, 2, \dots, k; j = 1, 2, \dots, n), \quad (14)$$

where μ is a total mean fixed effect, a known quantity that represents the characteristic of the overall mean. v is a random effect vector that is used to express differences, and \mathbf{e} is the random error vector. Usually assume $v_i \sim N(0, \sigma_v^2)$, $\mathbf{e}_{ij} \sim n(0, \sigma_e^2)$ and the two are independent of each other. Such a model is the Bayesian mixed model. When μ is 0, the Bayesian mixed model is reduced to the Bayesian random-effects model.

Assuming the conditional posterior distribution of Y is $f(y|\sigma_v^2 + \sigma_e^2)$, the joint prior distribution of σ_v^2 and σ_e^2 is $G(\sigma_v^2, \sigma_e^2)$, then the joint posterior distribution $H(\sigma_v^2, \sigma_e^2|y)$ can be obtained by

$$dH(\sigma_v^2, \sigma_e^2|y) \propto f(y|\sigma_v^2 + \sigma_e^2) dG(\sigma_v^2, \sigma_e^2). \quad (15)$$

Since σ_v^2 and σ_e^2 may or may not be independent, the expression of the joint prior probability density function in the two cases is further given,

$$G(\sigma_v^2, \sigma_e^2) = \begin{cases} G(\sigma_v^2)G(\sigma_e^2) & \sigma_v^2 \text{ and } \sigma_e^2 \text{ are independent,} \\ G(\sigma_v^2)G(\sigma_e^2|\sigma_v^2) & \sigma_v^2 \text{ and } \sigma_e^2 \text{ are not independent.} \end{cases} \quad (16)$$

In this work, the Bayesian random-effects model is employed to comprehensively consider the various negative effects brought by atmospheric turbulence to construct

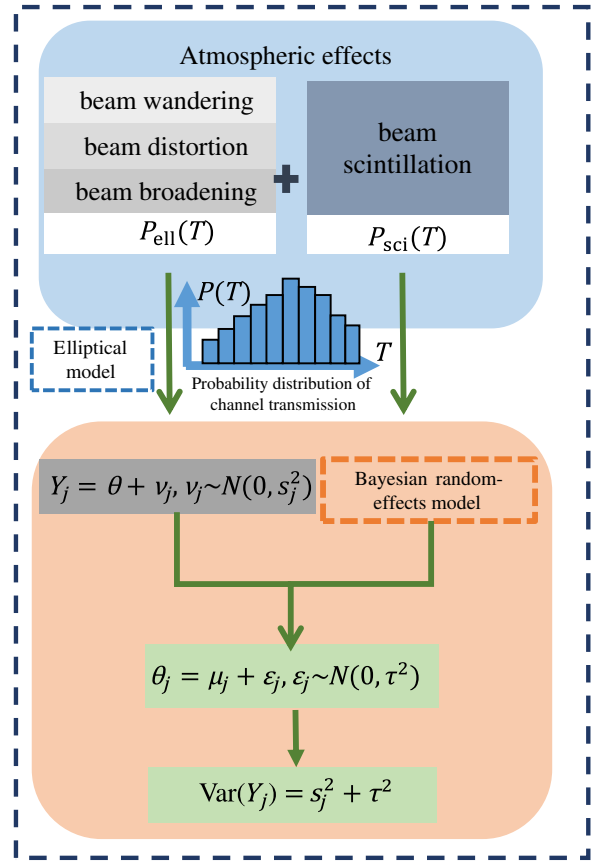


FIG. 3. Construction of robust prior information for atmospheric channel based on Bayesian random-effects model. Considering the influence of scintillation, the fixed θ becomes the random variable θ_j , Y represents the overall atmospheric effect, $P_{\text{ell}}(T)$ represents the probability distribution of transmittance under the ellipse model, and $P_{\text{sci}}(T)$ represents the probability distribution of transmittance under the scintillation model.

more robust and complete prior information in order to maximize the advantages of Bayesian estimation, as shown in Fig. 3.

In the case of weak turbulence, the distribution of channel transmittance reduces to the log-negative Weibull distribution [14]. Supposing that the beam-center position is normally distributed with variance σ^2 around a point at the distance d from the aperture center [44]. Under the ellipse model, the distribution of channel transmittance $P_{\text{ell}}(T)$ is expressed as

$$P_{\text{ell}}(T) = \frac{2R^2}{\sigma^2 Q T} \left(2 \ln \frac{T_0}{T} \right)^{(2/Q)-1} \times \exp \left[-\frac{1}{2\sigma^2} R^2 \left(2 \ln \frac{T_0}{T} \right)^{(2/Q)} \right], \quad (17)$$

for $T \in [0, T_0]$ and $P(T) = 0$ else, where Q and R are the shape parameter and the scale parameter,

$$Q = 8 \frac{a^2}{W^2} \frac{\exp\left[-4\frac{a^2}{W^2}\right] I_1\left(4\frac{a^2}{W^2}\right)}{1 - \exp\left[-4\frac{a^2}{W^2}\right] I_0\left(4\frac{a^2}{W^2}\right)} \times \left[\ln\left(\frac{2T_0^2}{1 - \exp\left[-4\frac{a^2}{W^2}\right] I_0\left(4\frac{a^2}{W^2}\right)}\right) \right]^{-1},$$

$$R = a \left[\ln\left(\frac{2T_0^2}{1 - \exp\left[-4\frac{a^2}{W^2}\right] I_0\left(4\frac{a^2}{W^2}\right)}\right) \right]^{-(1/\lambda)}, \quad (18)$$

and T_0^2 is the maximal transmission coefficient for the given beam-spot radius W ,

$$T_0^2 = 1 - \exp\left[-2\frac{a^2}{W^2}\right]. \quad (19)$$

In order to construct more complete prior information, all the negative factors caused by atmospheric turbulence should be contained. Given the influence of atmospheric scintillation on quantum signals, the distribution of the transmittance of the scintillation in the weak turbulence is

$$P_{\text{sci}}(T) = \frac{P_{\text{total}}}{S_D} P_{I_D}\left(\frac{P_{\text{total}}}{S_D} T\right) = \frac{\exp\left[-\frac{(\ln T/\bar{T})^2}{2\beta_D^2}\right]}{T\sqrt{2\pi\beta_D^2}}, \quad (20)$$

where P_{total} is the power emitted by the source, D is the telescope aperture, I_D and S_D denote the light intensity and the area in the receiving plane of the telescope. P_{I_D} is the probability density function of light intensity in receiving aperture, and \bar{T} is the average transmission that can be derived by

$$\bar{T} = \frac{\bar{P}_{\text{receive}}}{P_{\text{total}}} = \frac{\bar{I}_D S_D}{P_{\text{total}}} = 1 - \exp\left[-\frac{D^2}{2\omega^2(L)}\right] = 1 - \exp\left(-\frac{\pi^2\omega_0^2 D^2}{\pi^2\omega_0^4 + \lambda^2 L^2}\right), \quad (21)$$

where ω_0 is the waist radius. β_D^2 is the expression of the scintillation index considering aperture smoothing effect

that can be calculated by

$$\beta_D^2 = \beta_0^2 \times A = 1.23k^{7/6} C_n^2 L^{11/6} \times \left[1 + 1.812 \left(\frac{D^2}{\lambda L}\right)^{7/6}\right]^{-1}. \quad (22)$$

The Bayesian random-effects model is used to combine the elliptical beam model and scintillation model together to construct a complete probability distribution of atmospheric channel transmittance. Considering the independence of the two models, the complete and robust prior probability distribution of all atmospheric turbulence effects can be represented as

$$P_{\text{total}}(T) = P_{\text{ell}}(T) * P_{\text{sci}}(T). \quad (23)$$

C. Channel state information

Channel state information is used to further correct prior information by pilot signals. Taking into consideration the sparse nature of the free-space channel, CS [40] technology can reduce the amount of pilot signal used and reduce system overhead.

$$\mathbf{y} = \Phi \mathbf{x} + \mathbf{z} = \Phi \Psi \mathbf{s} + \mathbf{z} = \Theta \mathbf{s} + \mathbf{z}, \quad (24)$$

where \mathbf{y} is an N -dimensional measured value, Φ is the measurement matrix, \mathbf{x} is an N -dimensional original value, and \mathbf{s} , only has K ($K \leq N$) nonzero elements, is the sparse representation of the data \mathbf{x} in the domain Ψ . Θ is the sensing matrix, \mathbf{z} is an N -dimensional additive noise. When Φ satisfies the restricted isometry property (RIP) and the vector \mathbf{s} only has K ($K \leq N$) nonzero elements, the reconstruction methods, such as the OMP algorithm and the basis pursuit (BP) algorithm, can reconstruct the unknown vector \mathbf{s} exactly from the under determined equation with the acquired vector \mathbf{s} and matrix Θ . Under the conditions of RIP, if

$$S = \|\mathbf{s}\|_{l_0} < \frac{1}{2} \left[1 + \frac{1}{\mu(\Theta)}\right], \quad (25)$$

is satisfied, the reconstruction accuracy can reach

$$\|\hat{\mathbf{s}} - \mathbf{s}\|_{l_2} \leq \frac{\tau^2}{1 - \mu(\Theta)(2S - 1)}, \quad (26)$$

where τ is a constant greater than 0. $\mu(\Theta)$ represents the coherence of the matrix Θ ,

$$\mu(\Theta) = \max_{i \neq j} \frac{|\theta_i^T \theta_j|}{\|\theta_i\| \|\theta_j\|}, \quad (27)$$

where θ_i represents the column vector of the matrix Θ . It can be seen that the estimation performance can be

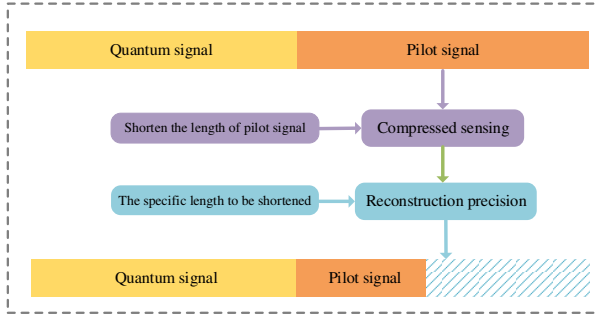


FIG. 4. The design of the pilot signal. Using compressed sensing technology can achieve parameter estimation with only a small amount of pilot signals, reducing the amount of calculation. The most suitable pilot length is determined by the reconstruction accuracy considering the accuracy and computational complexity.

improved by reducing the $\mu(\Theta)$. Research [41] reports the location and size of the pilot signals can affect the $\mu(\Theta)$. Considering these two factors at the same time is a complicated joint optimization problem. Therefore, all pilot signals are set at equal intervals, and the size of the pilots is adjusted to minimize $\mu(\Theta)$. The design process of the pilot signal is shown in Fig. 4.

III. EXPERIMENTS

A. Experimental verification under free-space channel

As shown in Fig. 5(a), the cw laser is employed to yield weak coherent light on Alice's side, then the light is processed into a pulse signal through an amplitude modulator (AM1). An unbalanced 1:99 BS divides it into signal pulses and pilot pulses. The signal pulses are modulated by AM2 and a phase modulator (PM1) to get zero-centered Gaussian distributions, then, it is attenuated by a fixed attenuator (ATT) and a variable attenuator (VOA) to adjust to the required modulation variance V_A . The delay line (DL) and Faraday mirror (FM) are employed to achieve the purpose of isolation from the signal pulse, and the strength is controlled by VOA to avoid the influence on the signal pulse during the simultaneous transmission. Some progress has been made in experimental research under free-space channel [42,45–47]. Here, this paper refers to the relevant information of free-space channel [42] to construct a set of y . The statistical relationship between Alice's variable and Bob's variable, the respective distributions, the covariance, and the correlation of the two variables are shown in Figs. 5(b)–5(e).

In this work, the free-space channel estimation is performed first. The estimated results and mean square errors of transmittance obtained by Bayesian estimation and MLE under the same channel are shown in Table I.

Therefore, Bayesian estimation can receive an appealing estimation result under the free-space channel. Compared with the result of MLE, the estimation accuracy is improved by an order of magnitude.

Then taking into account the fluctuation characteristics of free space, the secret key rate formula can be written as

$$\bar{K} \left(\langle \hat{T} \rangle, \hat{\epsilon} \right) = \frac{n}{N} (1 - P) (1 - ER_{\text{frame}}) \left[\beta_R \bar{I}_{AB} \left(\langle \hat{T} \rangle, \hat{\epsilon} \right) - \bar{\chi}_{BE} \left(\langle \hat{T} \rangle, \hat{\epsilon} \right) - \Delta(n) \right], \quad (28)$$

where n variables are employed for the establishment of the secret key of the N variables exchanged. P stands for interruption probability due to angle of arrival fluctuations under the atmospheric channel, FER is known as the frame error rate, I_{AB} is the Shannon mutual information of Alice and Bob, $S_{BE}^{\epsilon_{PE}}$ is defined as the maximum of the Holevo quantity of Bob and Eve compatible with the statistics except with failure probability ϵ_{PE} when the finite precision of the parameter estimation is taken into account. I_{AB} is information shared by Alice and Bob, it is expressed as

$$\bar{I}_{AB} = \frac{1}{2} \log_2 \frac{V_A}{V_{B|A}} = \frac{1}{2} \log_2 \frac{V + \chi_{\text{tot}}^{\text{FS}}}{1 + \chi_{\text{tot}}^{\text{FS}}},$$

$$\bar{\chi}_{BE} = \sum_{i=1}^2 G \left(\frac{\lambda_i^{\text{FS}} - 1}{2} \right) - \sum_{i=3}^5 G \left(\frac{\lambda_i^{\text{FS}} - 1}{2} \right). \quad (29)$$

In order to match the transmittance fluctuation, γ_{AB}^{FS} is

$$\gamma_{AB}^{\text{FS}} = \begin{pmatrix} V \mathbf{I}_2 & \langle T \rangle \sqrt{V^2 - 1} \sigma_z \\ \langle T \rangle \sqrt{V^2 - 1} \sigma_z & \langle T \rangle (V + \chi_{\text{line}}) \mathbf{I}_2 \end{pmatrix}. \quad (30)$$

The specific expression of λ_i^{FS} is

$$\lambda_{1,2}^{\text{FS}} = \sqrt{\frac{1}{2} \left[A_{\text{FS}} \pm \sqrt{A_{\text{FS}}^2 - 4B_{\text{FS}}} \right]},$$

$$\lambda_{3,4}^{\text{FS}} = \sqrt{\frac{1}{2} \left[C_{\text{FS}} \pm \sqrt{C_{\text{FS}}^2 - 4D_{\text{FS}}} \right]},$$

$$\lambda_5^{\text{FS}} = 1. \quad (31)$$

where

$$A_{\text{FS}} = V^2 - 2T_{\text{FS}}(V^2 - 1) + T_{\text{FS}}^2(V + \chi_{\text{line}}^{\text{FS}})^2,$$

$$B_{\text{FS}} = T_{\text{FS}}^2(1 + \chi_{\text{line}}^{\text{FS}})^2,$$

$$C_{\text{FS}}^{\text{hom}} = \frac{A_{\text{FS}}\chi_{\text{hom}} + V\sqrt{B_{\text{FS}}} + T_{\text{FS}}(1 + \chi_{\text{line}}^{\text{FS}})}{T_{\text{FS}}(V + \chi_{\text{tot}}^{\text{FS}})},$$

$$D_{\text{FS}}^{\text{hom}} = \frac{\sqrt{B_{\text{FS}}}V + B_{\text{FS}}\chi_{\text{hom}}}{T_{\text{FS}}(V + \chi_{\text{tot}}^{\text{FS}})}. \quad (32)$$

where $\chi_{\text{line}}^{\text{FS}} = 1/T_{\text{FS}} - 1 + \epsilon_{\text{FS}}$, $\chi_{\text{tot}}^{\text{FS}} = \chi_{\text{line}}^{\text{FS}} + \chi_h/T_{\text{FS}}$ and χ_h is detection noise in free space channel.

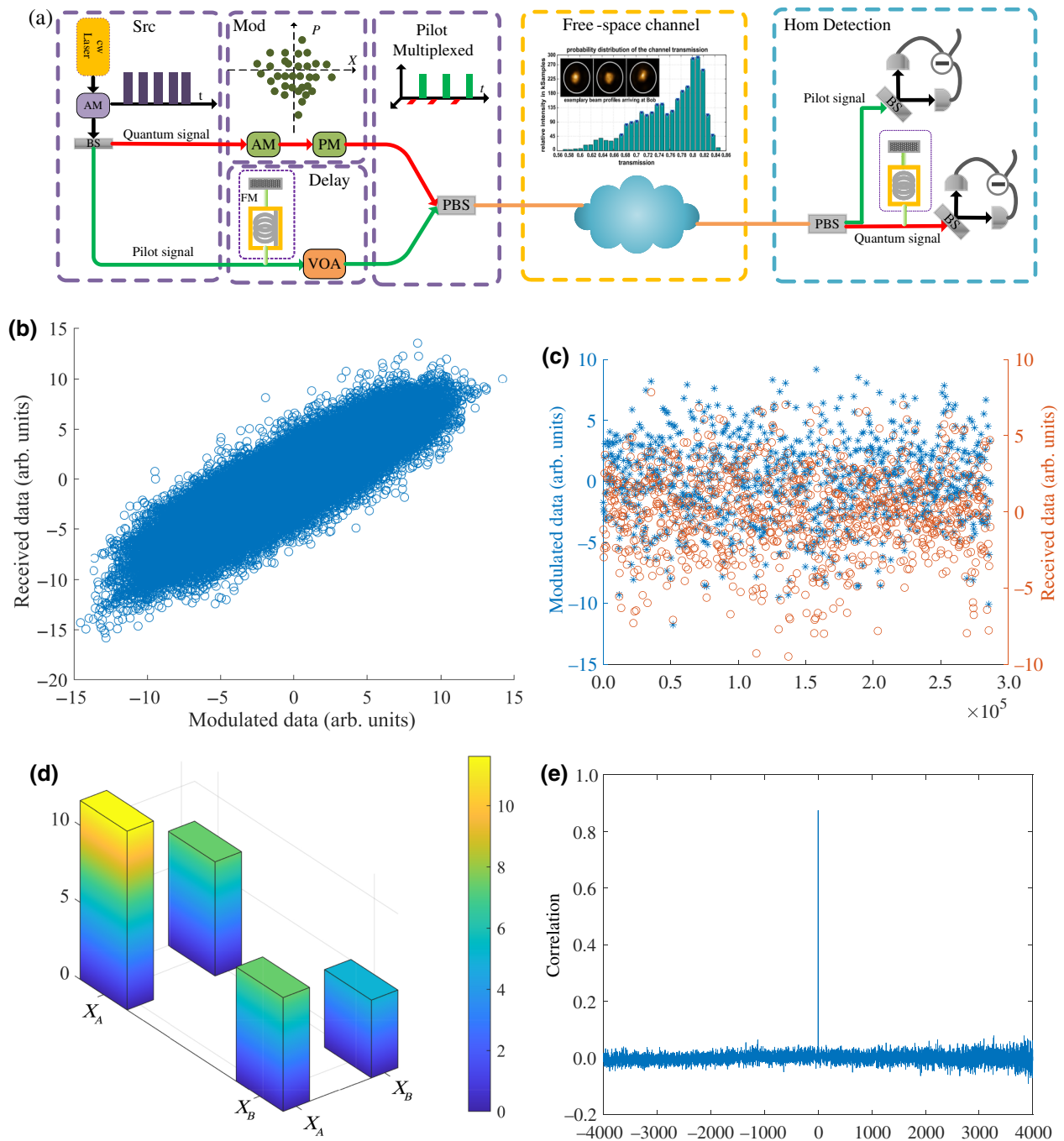


FIG. 5. Conceptual setup and data analysis under free-space link. (a) The conceptual design of the free-space CVQKD experiment. (cw, continuous wave; AM, amplitude modulator; PM, phase modulator; FM, Faraday mirror; BS, beam splitter; PBS, polarization beam splitter; VOA, variable optical attenuator. T is a random variable satisfying a certain probability distribution. The quantum signal is used to generate secret keys, and the pilot signal is used to obtain channel state information. The free-space channel is simulated according to Ref. [42].) (b) The statistical relationship between Alice’s data x and Bob’s data y , and they satisfy a linear relationship. This is done to evaluate the consistency of the modulated variable and the received variable to verify the effectiveness of Gaussian modulation. (c) Data distribution of Alice and Bob under the free-space channel. (d) The covariance matrix. (e) Analysis of the correlation.

The system performance is shown in Fig. 6. It can be seen that MLE consumes quantum resources during the estimation process, which leads to an overall decrease

in the key rate of the system, while Bayesian estimation makes use of pilot signals to avoid the loss of quantum signals. From this point of view, Bayesian estimation not only

TABLE I. Comparison of two different estimation methods.

Theoretical value	Bayesian estimation	MLE
0.761 [42]	0.7623	0.769 [16]
Mean square error (MSE)	10^{-6}	10^{-5}

can provide parameter estimation results with better stability and higher accuracy but also make full use of quantum signals and improve system performance.

B. Experimental verification under fiber channel

The experimental setup for signal pulses and pilot signals is shown in Fig. 7(a). Then, the signal pulses and pilot pulses are transmitted through a 10-km fiber channel. At Bob’s side, the signal pulses and pilot pulses interfere with the LO pulses on homodyne detectors, respectively. LO pulses are generated by Bob. The statistical relationship between Alice’s variable x and Bob’s variable y' , respective distributions, the covariance, and the correlation of the two are shown in Figs. 7(b)–7(e). Comparing the experimental results under the two channels, it can be seen that the relationship between Alice’s variable and Bob’s variable in free space is looser, the data fit is reduced, the difference between the variables becomes larger, and the correlation is weakened. This can be attributed to the fact that free space is more complicated than the channel

environment of the fiber channel, which brings more interference to the system, making the variable of Alice and Bob show greater differences.

Due to the influence of loss and dispersion, the optical quantum signal suffers signal distortion, such as amplitude attenuation and optical pulse broadening during its transmission process. Optical fiber loss mainly includes absorption loss and scattering loss, bending loss, connection loss, and coupling loss. In a quantum fiber channel with a loss factor of α_f (dB/km), the relationship between transmittance T and distance L is expressed as

$$T = 10^{-\alpha_f L/10}. \tag{33}$$

And the design of the pilot signal under the fiber channel is relatively simple, and the problem that needs to be paid attention to is that the pilot pulse cannot interfere with the quantum signal pulses.

According to the obtained variables, the T and ε are estimated through different estimation methods. A comparison between the estimation results of MLE and Bayesian estimation is shown in Fig. 8. It can also be seen that the estimation results of MLE have a great relationship with the quality and quantity of the selected data. Compared with MLE estimation, Bayesian estimation shows great superiority in terms of stability and accuracy. Specifically, the accuracy estimated by the MLE method fluctuates greatly, which is due to the different quality of the set of variables. Even under the same amount, the accuracy fluctuates. In order to get an accurate estimation result with MLE, a lot of calculations must be carried out. Different from MLE, Bayesian estimation can realize a high-accuracy parameter estimation through a few pilot signals. In the belief of adapting to different channel fluctuations, pilot signals of different lengths were designed. It can not only fulfill the requirements of estimation but also avoid the waste of quantum signals, thus improving the performance of the system. In Fig. 8(b), due to the estimation inaccuracy of the transmittance T , the system excess noise ε estimation fluctuates. However, Bayesian estimation still maintains a relatively high superiority.

The secret key rate of CVQKD with reconciliation efficiency β_R under the finite-size regime is given as [11]

$$K = \frac{n}{N} (1 - P) (1 - ER_{\text{frame}}) [\beta_R I_{AB} - S_{BE}^{\varepsilon_{PE}} - \Delta(n)], \tag{34}$$

where

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_A}{V_{B|A}} = \frac{1}{2} \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{35}$$

and

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

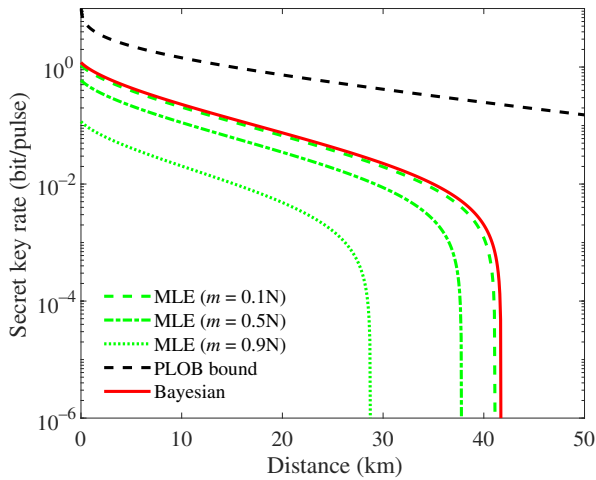


FIG. 6. System performance under different parameter estimation methods. From the top to bottom, the black dotted line represents the PLOB bound, the red solid line represents the system secret key rate under Bayesian estimation, the dashed line represents the secret key rate under MLE when the estimated amount is 0.1 times the total data amount, the dot-dash line represents the secret key rate under MLE when the estimated amount is 0.5 times the total data amount, the dotted line represents the secret key rate under MLE when the estimated amount is 0.9 times the total data amount. The PLOB bound is a fundamental limit on the quantum capacity of quantum communication [48].

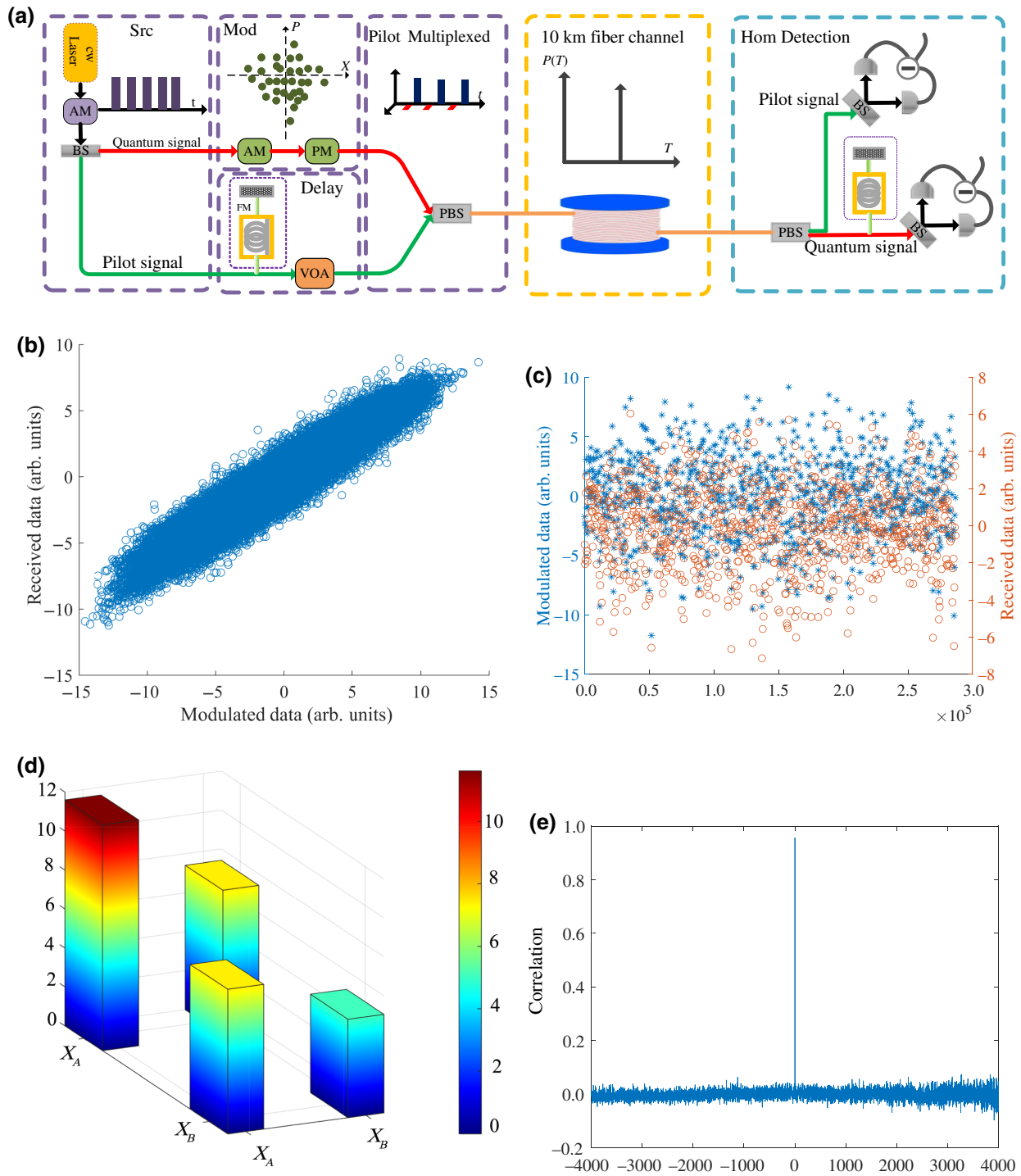


FIG. 7. Experimental setup and analysis of statistical characteristics under fiber link. (a) The experimental setup for the proposed scheme in the fiber link. [cw, continuous wave; FM, Faraday mirror; AM, amplitude modulator; PM, phase modulator; BS, beam splitter; PBS, polarization beam splitter; VOA, variable optical attenuator. T is a fixed value that is different from T in Fig. 5(a)]. (b) Statistical relationship between Alice’s variable x and Bob’s variable y' : they satisfy a linear relationship. Compared with Fig. 5(b), the linear regression of the fiber channel CVQKD system is better. (c) Variables of Alice and Bob under the fiber channel. Compared with Fig. 5(c), the distribution of the two variables is more compact, which means that the influence of the fiber channel on the system is less than that of the free-space channel. (d) Covariance matrix compared with Fig. 5(d), the value of the off-diagonal increases. (e) Analysis of the correlation and compared with Fig. 5(e), the value of correlation increases.

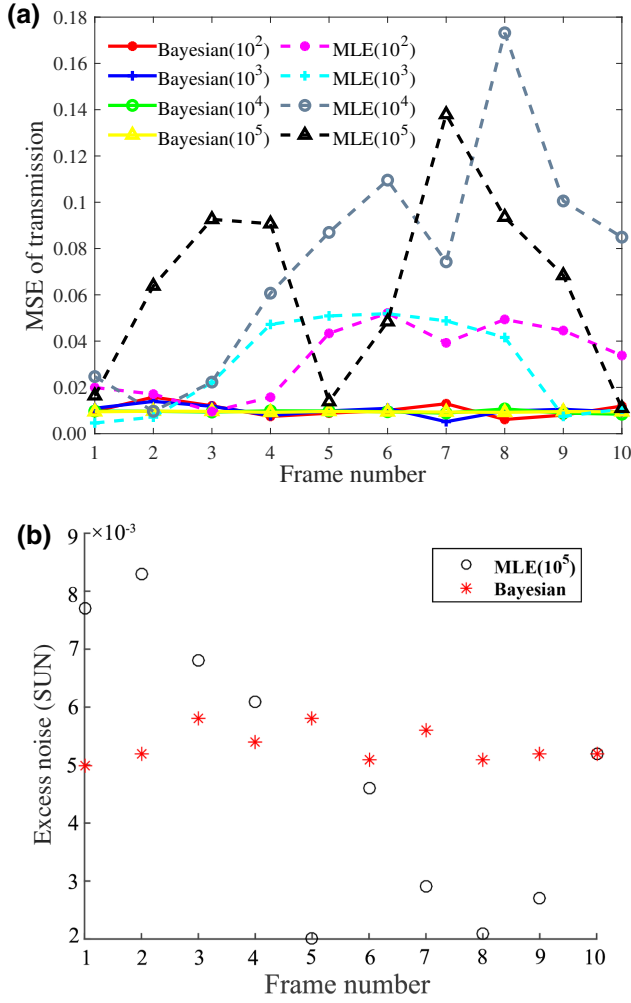


FIG. 8. Analysis of parameter estimation results under partial data. The accuracy of T is measured by MSE and the horizontal axis represents a total of ten sets of tests. (a) Estimation results of transmission T . The solid line and the dotted line represent the results using Bayesian estimation and using MLE, respectively. Different symbols represent the number of signals used for estimation, which refers to the number of pilot signals in the Bayesian scheme and the number of quantum signals in the MLE scheme. (b) Estimated results of excess noise ε . The black circle and the red star represent the estimation result of ε obtained by using MLE when the number of signals used for estimation reaches 10^5 , and the ε estimation result obtained by using Bayesian estimation, respectively. Since the pilot signal is used in the Bayesian scheme, the quantum resource for generating the secret key rate will not be wasted.

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$. The symplectic eigenvalues λ_i can be obtained from the covariance matrix of γ_{AB}

$$\gamma_{AB} = \begin{pmatrix} \mathbf{V}\mathbf{I}_2 & T\sqrt{V^2 - 1}\sigma_z \\ T\sqrt{V^2 - 1}\sigma_z & T(V + \chi_{\text{line}})\mathbf{I}_2 \end{pmatrix}. \quad (37)$$

The specific expression of λ_i is

$$\begin{aligned} \lambda_{1,2} &= \sqrt{\frac{1}{2} \left[A \pm \sqrt{A^2 - 4B} \right]}, \\ \lambda_{3,4} &= \sqrt{\frac{1}{2} \left[C \pm \sqrt{C^2 - 4D} \right]}, \\ \lambda_5 &= 1. \end{aligned} \quad (38)$$

where

$$\begin{aligned} A &= V^2 - 2T(V^2 - 1) + T^2(V + \chi_{\text{line}})^2, \\ B &= T^2(1 + \chi_{\text{line}})^2, \\ C &= \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(1 + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})}, \\ D &= \frac{\sqrt{B}V + B\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}. \end{aligned} \quad (39)$$

where $\chi_{\text{line}} = 1/T - 1 + \varepsilon$, $\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_h}{T}$ and χ_h is detection noise under fiber channel.

The system performance is shown in Fig. 9. It can be seen that system security is threatened by a higher parameter estimation result. The transmittance estimated by MLE leads to the overestimation of the secret key rate, which

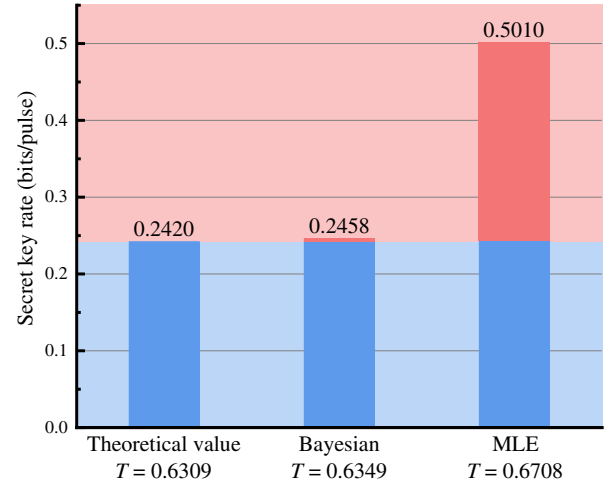


FIG. 9. The impact of parameter estimation results on system security. The blue area indicates that the system is secure, and the red area indicates that the system has security vulnerabilities that can be exploited by eavesdroppers. Taking the theoretical value $T = 0.6309$ as the standard, it can be seen that the difference between $T = 0.6349$ estimated by the Bayesian scheme and the theoretical value is small, the result of parameter estimation is relatively accurate, and the impact on the judgment of the system security is small. In contrast, the $T = 0.6708$ estimated by the MLE scheme deviates greatly from the theoretical value, and the accuracy of the parameter estimation results is reduced, which brings risks to the system security.

brings a security loophole to the system. In contrast, the transmittance estimated by the Bayesian method brings almost no risk to the system, which improves the practical security of the system.

IV. DISCUSSION

In this work, a free-space parameter estimation scheme based on Bayesian estimation is proposed, which considers the free-space channel as a whole, not a collection of different stable subchannels. Bayesian estimation is applied in this scheme, it is known that the accuracy of Bayesian estimation is determined by the accuracy of prior information on the estimated parameter. Thus, to give full play to the advantages of Bayesian estimation, the Bayesian random-effects model is employed to construct prior information on the transmittance. Since this model considered various negative effects brought by atmospheric turbulence, the prior information on the transmittance of the free-space channel is complete and robust. Secondly, compared with the traditional estimation method where half of the quantum signals are used to execute MLE, pilot signals are introduced in this proposed scheme to avoid wasting quantum resources. And because of the sparsity of the free-space channel, the length of the pilot signal is compressed using CS technology to reduce system overhead, and the specific length is determined by the reconstruction accuracy, which can be adaptive according to the weather conditions at that time. Thus, the alternative scheme has an advantage in terms of accuracy and robustness.

Due to some limitations of the free-space experiment, an existing atmospheric channel experiment is used to construct Bob's variable. The results prove that Bayesian estimation not only has good performance in parameter estimation but also improves the overall performance of the system. And the channel parameter estimation using the Bayesian method under the fiber channel is also completed and the comparison with the traditional MLE is implemented. The conclusion can be drawn that the Bayesian scheme has more advantages in terms of estimation accuracy and stability than MLE. It can also avoid threats to the practical security of the system.

Therefore, Bayesian estimation has good performance under the two different channels, which will provide help in realizing global CVQKD in the future.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 62071381), Shaanxi Provincial Key R&D Program General Project (Grant No. 2022GY-023), and ISN 23rd Open Project (Grant No. ISN23-06) of the State Key Laboratory of Integrated Services Networks (Xidian University).

- [1] C. H. Bennett and G. Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proc. of IEEE Int. Conf. on Comp. Syst. and Signal Proc. (1984).
- [2] K. E. Artur, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] H. B. Charles, Quantum Cryptography using any Two Nonorthogonal States, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [4] H. K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
- [5] T. C. Ralph, Continuous variable quantum cryptography, *Phys. Rev. A* **61**, 103031-103034 (1999).
- [6] T. C. Ralph, Security of continuous-variable quantum cryptography, *Phys. Rev. A* **62**, 062306 (2000).
- [7] P. Jouguet, K. J. Sébastien, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photonics* **7**, 378-381 (2013).
- [8] D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, *Sci. Rep.* **6**, 19201 (2016).
- [9] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [10] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature* **421**, 238 (2003).
- [11] Y. C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, *Phys. Rev. Lett.* **125**, 010502 (2020).
- [12] A. Krishnan, An overview of quantum wireless communication using quantum cryptography. In IEEE. INTERACT. (2010).
- [13] A. Fedrizz, R. Ursin, and T. Herbst, High-fidelity transmission of entanglement over a high-loss freespace channel, *Nat. Phys.* **5**, 389-392 (2009).
- [14] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality, *Phys. Rev. Lett.* **108**, 220501 (2012).
- [15] G. Chai, Z. Cao, W. Liu, S. Wang, P. Huang, and G. Zeng, Parameter estimation of atmospheric continuous-variable quantum key distribution, *Phys. Rev. A* **99**, 032326 (2019).
- [16] R. Laszlo, P. Christian, H., Bettina, K., Günthner, and M. Christoph, Fading channel estimation for free-space continuous-variable secure quantum communication, *New J. Phys.* **21**, 12 (2019).
- [17] G. Chai, D. Li, Z. Cao, M. Zhang, P. Huang, and G. Zeng, Blind channel estimation for continuous-variable quantum key distribution, *Quantum Eng.* **2**, e37 (2020).
- [18] D. Jin, Y. Guo, Y. J. Wang, and D. Huang, Parameter estimation of orbital angular momentum based continuous-variable quantum key distribution, *J. Appl. Phys.* **127**, 213102 (2020).
- [19] S. Y. Wang, P. Huang, T. Wang, and G. H. Zeng, Phase compensation for free-space continuous-variable quantum key distribution, *Opt. Express* **28**, 8 (2020).

- [20] S. Y. Wang, P. Huang, T. Wang, and G. H. Zeng, Dynamic polarization control for free-space continuous-variable quantum key distribution, *Opt. Lett.* **45**, 5921-5924 (2020).
- [21] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, *Phys. Rev. A* **81**, 062343 (2010).
- [22] P. Jouguet and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, *Phys. Rev. A* **86**, 032309 (2012).
- [23] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* **96**, 042332 (2017).
- [24] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables, *Phys. Rev. A* **96**, 042332 (2017).
- [25] A. Leverrier, Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [26] L. Ruppert, V. C. Usenko, and R. Filip, Long-distance continuous-variable quantum key distribution with efficient channel estimation, *Phys. Rev. A* **90**, 062310 (2014).
- [27] X. M. Zhu and J. M. Kahn, Free-space optical communication through atmospheric turbulence channels, *IEEE Trans. Commun.* **50**, 1293-1300 (2002).
- [28] J. C. Ricklin, S. M. Hammel, F. D. Eaton, and S. L. Lachinova, Atmospheric channel effects on free-space laser communication, *J. Opt. Fiber Commun. Rpt.* **3**, 111 (2006).
- [29] S. Wang, P., Huang, T., Wang, and G. H. Zeng, Atmospheric effects on continuous-variable quantum key distribution, *New J. Phys.* **20**, 083037 (2018).
- [30] S. Olivares and M. G. Paris, Bayesian estimation in homodyne interferometry, *J Phys. B-At. Mol. Opt.* **42**, 055506 (2009).
- [31] J. J. Meyer, J. Borregaard, and J. Eisert, A variational toolbox for quantum multi-parameter estimation, *NPJ Quantum Inf.* **7**, 1-5 (2021).
- [32] V. Gebhart, A. Smerzi, and L. Pezzè, Bayesian Quantum Multiphase Estimation Algorithm, *Phys. Rev. Appl.* **16**, 014035 (2021).
- [33] S. Nolan, A. Smerzi, and L. Pezzè, A machine learning approach to Bayesian parameter estimation, *NPJ Quantum Inf.* **7**, 1-8 (2021).
- [34] L. J. Fiderer, J. Schuff, and D. Braun, Neural-Network Heuristics for Adaptive Bayesian Quantum Estimation, *PRX Quantum* **2**, 020303 (2021).
- [35] D. Vasylyev, A. A. Semenov, and W. Vogel, Atmospheric Quantum Channels with Weak and Strong Turbulence, *Phys. Rev. Lett.* **117**, 090501 (2016).
- [36] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, Free-space quantum links under diverse weather conditions, *Phys. Rev. A* **96**, 043856 (2017).
- [37] L. C. Andrews, R. L. Phillips, and C. Y. Hopen, Laser beam scintillation with applications. **99**, SPIE press (2001).
- [38] S. G. Wang and S. J. Yin, A new estimate of the parameters in linear mixed models, *Sci. China. Math.* **45**, 1301-1311 (2002).
- [39] G. E. P. Box and G. C. Tiao, *Bayesian Inference in Statistical Analysis* (Wiley-Interscience, New Jersey, America, 2011).
- [40] B. Adcock, A. Hansen, C. Poon, and B. Roman, Breaking the coherence barrier: A new theory for compressed sensing, *Forum Math. Pi.* **5**, e4 (2017).
- [41] R. Xiang, W. Chen, and Z. J. Wang, Low coherence compressed channel estimation for high mobility MIMO OFDM systems. In IEEE GLOBECOM. (2013).
- [42] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, Atmospheric continuous-variable quantum communication, *New J. Phys.* **16**, 113018 (2014).
- [43] S. Kunz-Jacques and P. Jouguet, Robust shot-noise measurement for continuous-variable quantum key distribution, *Phys. Rev. A* **91**, 022307 (2015).
- [44] R. L. Fante, Electromagnetic beam propagation in turbulent media, *Proc. IEEE* **63**, 1669-1692 (1975).
- [45] V. C. Usenko, B. Heim, C. Peuntinger, C. Wittmann, C. Marquardt, G. Leuchs, and R. Filip, Entanglement of Gaussian states and the applicability to quantum key distribution over fading channels, *New J. Phys.* **14**, 093048 (2012).
- [46] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Impact of Turbulence in Long Range Quantum and Classical Communications, *Phys. Rev. Lett.* **109**, 200502 (2012).
- [47] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Distribution of Squeezed States through an Atmospheric Channel, *Phys. Rev. Lett.* **113**, 060502 (2014).
- [48] D. Miller, T. Holz, H. Kampermann *et al.*, Parameter regimes for surpassing the PLOB bound with error-corrected qudit repeaters, *Quantum* **3**, 216 (2019).