

Wavelength attack on atmospheric continuous-variable quantum key distributionXin Tan,^{1,2} Ying Guo,¹ Ling Zhang,^{1,*} Jingzheng Huang,³ Jinjing Shi,² and Duan Huang²¹*School of Automation, Central South University, Changsha 410083, China*²*School of Computer Science and Engineering, Central South University, Changsha 410083, China*³*State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-based Service, Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China*

(Received 13 September 2020; accepted 16 December 2020; published 22 January 2021)

Recently, several practical wavelength attacks on continuous-variable quantum key distribution (CVQKD) were proposed based on the wavelength-dependent property of a beam splitter in Bob's station. These attack schemes are limited to the fiber channel systems with a relatively stable transmittance. However, unlike the fiber channel, the transmittance of the atmospheric channel is complex and fluctuates dramatically in time, which may invalidate the attack equations that must be satisfied in the optical fiber channel. In this paper, we propose two wavelength attack schemes against complex atmospheric CVQKD systems and formulate the two schemes based on the parameter estimation method. To verify the feasibility and availability of this attack, we deduce the success criteria for the two attack schemes. By numerical analysis, our attack schemes are proved to be feasible in the permitted parameter regimes. The secret key rate and propagation distance of CVQKD can be further overestimated by selecting the condition parameters effectively. Moreover, we discuss the possible prevention countermeasures to resist these attack schemes. The proposed method will fill the gap of wavelength attack for the implementation of practical atmospheric CVQKD.

DOI: [10.1103/PhysRevA.103.012417](https://doi.org/10.1103/PhysRevA.103.012417)**I. INTRODUCTION**

Continuous-variable quantum key distribution (CVQKD) permits two authenticated parties Alice and Bob to share a group of secret keys through an insecure quantum channel, which is assumed to be manipulated by the potential eavesdropper Eve [1–5]. The unconditional security of the CVQKD protocol is guaranteed based on the quantum mechanics laws, especially the no-cloning theorem [6–10]. So far, the security of the Gaussian-modulated coherent-state (GMCS) CVQKD protocol has been fully proved against several attacks including individual attacks, collective attacks, and coherent attacks theoretically [11–13]. Therefore, the practical implementation of GMCS CVQKD schemes plays a crucial part in secure quantum communication [14–17].

However, there are still inevitably deviations between the implementation of practical GMCS CVQKD schemes and the underlying theoretical model, which are usually caused by the device imperfections, technical deficiencies, and operational imperfections of the key components [2,5,11,18,19]. It opens the security vulnerability which may be exploited by Eve to mount various types of powerful attacks. As a consequence, Eve can successfully steal information from legitimate parties and break the unconditional security of quantum communication. A great many related research works have been done on the typical attack strategies, such as Trojan horse attacks [20,21], saturation attacks [22,23], wavelength attacks [24–27], homodyne detector blinding attacks [28], local

oscillator (LO) calibration attacks [29], and LO intensity attacks [30].

In Refs. [25,26], the authors proposed a wavelength attack using the heterodyne detection CVQKD protocol. It is assumed that Eve can control the transmittance of Bob's wavelength-dependent beam splitter (BS) by switching the wavelength of the fake state. The excess noise measured by Bob can be controlled much lower than the tolerable threshold of theoretical security proofs; as a result, the legitimate parties can never discover the existence of Eve. In Ref. [27], another improved calibration-wavelength attack has been systematically studied in the practical homodyne detection CVQKD system, which can invalidate the countermeasure of real-time shot-noise measurement in the calibration attack. Eve can make the estimated excess noise arbitrarily close to zero by controlling the intensity and wavelength of the fake state. In principle, Eve can obtain all of the secret keys without being discovered, even if they have monitored the intensity of LO.

It should be noted that the wavelength attack schemes proposed above were limited to the case of all-fiber CVQKD systems, where the attenuation coefficient is usually assumed to be a constant. However, compared with the fiber-based channel, the environment in the atmospheric channel is unstable due to the turbulent effect [31], thus the transmittance fluctuating randomly in time. As a critical step in CVQKD, the parameter estimation method provides the legitimate communication parties an intuitive indicator to analyze the intervention of Eve [32–34]. It usually assumes the channel transmittance as a fixed value in the fiber-based CVQKD system. The aforementioned assumption for parameter estimation is improper in practical atmospheric CVQKD systems

*lingzhang2019@csu.edu.cn

which may invalidate the equation that must be satisfied in noiseless-fiber schemes. Therefore, the previous results of parameter estimation cannot be directly applied. That is, the instability of transmittance may have a significant impact on parameter estimation sequentially affecting the feasibility of wavelength attack in practical atmospheric CVQKD systems. Therefore, the effectiveness and functionality of these attack schemes for atmospheric CVQKD systems are ambiguous, which needs further investigation.

In this paper, we consider two wavelength attack schemes for the turbulent atmospheric CVQKD systems. Then we formulate the two schemes based on the parameter estimation method over the atmospheric channel. To demonstrate the feasibility of these attacks, we specifically discuss the criteria that must be satisfied in these attacks. Finally, we calculate the constraint condition accurately and conclude that Eve can always implement the attack schemes successfully by tuning the regime of condition parameters. Furthermore, we discuss the countermeasures against the atmospheric wavelength attack. Based on the parameter estimation method in atmospheric CVQKD, Eve can make the estimated shot-noise level seems normal and estimated excess noise lower than the true value. As a result, the slight manipulation of attack parameters can result in great overestimation of the achievable secure secret key rate and secure transmittance distance without being discovered, which will make the communication that was initially considered secure become insecure.

The paper is organized as follows: In Sec. II, we present the transmittance models in the atmospheric turbulent channel and explain how parameter estimation is performed in this CVQKD protocol. In Sec. III, we first briefly review the calibration attack and then introduce the wavelength attack in the fiber channel which can invalidate the countermeasure of calibration attacks. In Sec. IV, we propose two wavelength attack strategies in atmospheric-based CVQKD protocols. In Sec. V, we define the success criteria for the attack schemes in the atmospheric channel following the parameter estimation procedure. In Sec. VI, we perform security analysis to verify the influence of the wavelength attack on parameter estimation under different estimated transmittance, in particular on excess noise, and then discuss the impact on the secret key rate. Moreover, we discuss the possible countermeasures for the proposed attack schemes. Finally, conclusions are presented in Sec. VII.

II. PARAMETER ESTIMATION IN ATMOSPHERIC CHANNEL

In this section, we will concentrate on the transmittance characteristics of the atmospheric channel that is primarily affected by the turbulence effects. The Rytov variance σ_R^2 is used for characterizing the turbulent strength which can be expressed as [35]

$$\sigma_R^2 = 1.23 C_n^2 k^{\frac{7}{6}} L^{\frac{11}{6}}, \quad (1)$$

where k is the optical wave number and L is the horizontal propagation distance. C_n^2 represents the index of refraction structure parameter, which primarily determines the turbulence fluctuation along the propagation path. Based on the

TABLE I. The values (median) of C_n^2 within the boundary layer in four seasons.

	Spring	Summer	Autumn	Winter
C_n^2 ($\text{m}^{-2/3} \times 10^{-15}$)	2.03	2.12	5.56	7.46

long-term radiosonde measurement results in Hefei, Anhui, China, it is quite reasonable to assume C_n^2 to be a constant as shown in Table I [36].

The beam wandering in turbulent atmosphere can be described properly by an elliptical beam model [37], as shown in Fig. 1. We can describe any spot at the receiving aperture of the elliptical beam model with parameters $\mathbf{v} = (x_0, y_0, W_1, W_2)$ and Φ . Here, (x_0, y_0) is the position of the beam centroid and represents the degree of beam wandering, which is equal to $(r_0 \cos \phi_0, r_0 \sin \phi_0)^2$. (W_1, W_2) represents the half axis of the elliptical beam profile, and $\Phi \in [0, \pi/2]$ is the rotated angle between half axis W_1 and the x axis of the aperture. With this ellipse model, the analytical expression of atmosphere transmittance can be obtained by

$$T = T_0 \exp \left\{ - \left[\frac{r_0/a}{R(\frac{2}{W_{\text{eff}}(\Phi - \phi_0)})} \right]^{\lambda(\frac{2}{W_{\text{eff}}(\Phi - \phi_0)})} \right\}, \quad (2)$$

where a is the receiving aperture radius, $W_{\text{eff}}(\cdot)$ is the effective point radius, T_0 is the maximal transmittance coefficient for the centered beam, and $R(\cdot)$ and $\lambda(\cdot)$ are the scale and shape functions, respectively. The details of the above parameters are shown in Appendix A.

Based on the above analysis, the probability density distribution of transmittance in the atmospheric turbulence channel can be evaluated by the Monte Carlo method. It can be visualized by N simulated values of the transmittance via smooth

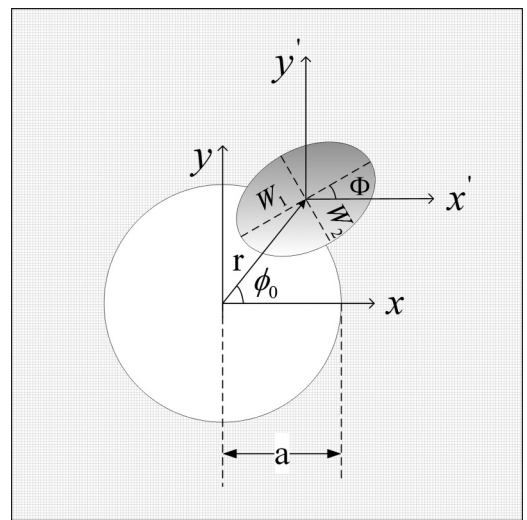


FIG. 1. The receiving aperture with radius a , and the elliptical beam profile with the half axis W_1 and W_2 , where W_1 rotates on the angle Φ relating to the x axis. Beam wandering is characterized by r , which represents the beam-centroid position with respect to the center of the aperture.

kernels techniques [38]:

$$\langle f(T) \rangle \approx \frac{1}{N} \sum_{i=1}^N f(\chi_{\text{ext}} T(\mathbf{v}_i, \varphi_i)), \quad (3)$$

where $T(\mathbf{v}_i, \varphi_i)$ is obtained from Eq. (2), and the extinction factor $\chi_{\text{ext}} \in [0, 1]$ is a random variable that indicates the absorption and scattering losses. Thus, the average value of the fading transmittance can be calculated via

$$\begin{aligned} \langle T \rangle &= \chi_{\text{ext}} \frac{1}{N} \sum_{i=1}^N T(\mathbf{v}_i, \varphi_i), \\ \langle \sqrt{T} \rangle &= \sqrt{\chi_{\text{ext}}} \frac{1}{N} \sum_{i=1}^N \sqrt{T(\mathbf{v}_i, \varphi_i)}. \end{aligned} \quad (4)$$

In the GMCS CVQKD protocol, Alice randomly encodes information on the coherent state with a laser source. The quadrature components X_A and P_A of coherent state $|X_A + iP_A\rangle$, with Gaussian random numbers of zero mean and variance $V_A N_0$ [6], are transmitted to Bob through an atmosphere channel, where N_0 is the variance of shot noise. Bob then randomly selects $\phi = 0$ or $\phi = \pi/2$ to measure either the X or P quadrature by a homodyne detector.

By repeating this process many times, Alice and Bob share a group of correlated vectors $\hat{X} = \{x_1, x_2, \dots, x_N\}$ and $\hat{Y} = \{y_1, y_2, \dots, y_N\}$, where N is the total number of signals. There are $m = N - n$ pairs of correlated variables $\{(x_i, y_i) | i = 1, 2, \dots, m\}$ applied for parameter estimation and security evaluation. The remaining n variables are used for the final secret key establishment through reverse error correction reconciliation and privacy amplification.

To estimate parameters from Alice's and Bob's correlated variables, we consider a normal linear model with the following relation:

$$y = tx + z, \quad (5)$$

where $t = \sqrt{\eta T}$ is a normal linear model, and vector z denotes the total noise term following a centered normal distribution with variance $\sigma^2 = \eta T \xi + N_0 + V_{\text{el}}$. Here, T is the transmittance of the atmospheric channel, ξ is the excess noise, and η and V_{el} are the detection efficiency and electronic noise of the homodyne detector, respectively. In particular, in order to evaluate the secret key rate, the excess noise ξ and electronic noise V_{el} must be expressed in shot-noise units (SNUs), i.e., $\xi = \varepsilon N_0$ and $V_{\text{el}} = v_{\text{el}} N_0$. Following the analysis in Refs. [32,33], the estimators $\hat{t}$ and $\hat{\sigma}^2$ can be obtained by

$$\hat{t} = \frac{\sum_{i=1}^m x_i y_i}{\sum_{i=1}^m x_i^2}, \quad \hat{\sigma}^2 = \frac{1}{m} \sum_{i=1}^m (y_i - \hat{t} x_i)^2. \quad (6)$$

According to the maximum likelihood estimation method, the estimated parameters $\hat{T}$ and $\hat{\varepsilon}$ have the following forms (see Appendix B for more details):

$$\hat{T} = \frac{\hat{t}^2}{\eta} = \frac{[\langle \sqrt{T} \rangle]^2}{\eta}, \quad \hat{\varepsilon} = \frac{V_A \langle T \rangle + \varepsilon \langle T \rangle - V_A [\langle \sqrt{T} \rangle]^2}{[\langle \sqrt{T} \rangle]^2}. \quad (7)$$

We can see from Eq. (7) that when the channel transmittance T is a constant, the estimated value $\hat{T}$ is equal to the ideal value T . However, there are obvious deviations between

our estimated parameters and the true values because the atmospheric channel transmittance fluctuates rapidly in time.

III. WAVELENGTH ATTACK IN FIBER CHANNEL

Before introducing the wavelength attack in optical fiber CVQKD system, we first take a brief review of the LO calibration attack. The principle of the LO calibration attack is modifying the shape of the LO pulse by introducing an attenuation or a delay trigger at the beginning of the LO pulse, thus resulting in a decrease of the detection response slope [29]. If Alice and Bob still use the previously calibrated relationship they will overestimate the shot noise. As a consequence, the excess noise will be underestimated, which is known as a calibration attack. To go against the LO calibration attack, the countermeasures based on real-time shot-noise measurement methods were proposed. See Appendix C for the detailed principle and corresponding countermeasures of calibration attacks.

However, there are some unsatisfactory characteristics in practical optical devices. These inevitable physical defects will be exploited by Eve to threaten the security of the CVQKD system. For example, a key component in practical CVQKD systems, the fused biconical taper (FBT) BS, has the characteristics of low insertion loss, excellent directivity, and low production cost. It works in confined bandwidths and has great performance at a specified central wavelength. The coupling ratio (also known as transmittance) of the FBT BS is closely related to the wavelength, which changes periodically with wavelength once deviating from the central wavelength [39,40]. The wavelength-dependent FBT BS can be utilized in wavelength attacks to invalidate the above countermeasures in LO calibration attack [26,27].

Specifically, we consider a dual-wavelength FBT BS at two different central wavelengths, $\lambda_0 = 1310$ nm and $\lambda_0 = 1550$ nm. The relationship between the wavelength λ and transmittance T of the FBT BS can be expressed as

$$T = F^2 \sin^2 \left(\frac{C \lambda^{2.5} \omega}{F} \right) \in T(\lambda), \quad (8)$$

where F^2 is the fraction of power coupled, $C \lambda^{2.5}$ is the coupling coefficient, and ω is the heat source width; here we set $F = 1$ for convenience. For central wavelength $\lambda_0 = 1310$ and $\lambda_0 = 1550$, we have $T(\lambda_0) = \sin^2 \left(\frac{C \omega}{F} \lambda_0^{2.5} \right) = 0.5$, hence $\frac{C \omega}{F} = \frac{\arcsin \sqrt{0.5}}{\lambda_0^{2.5}}$. It is simple to get the other wavelength around the central wavelength:

$$T(\lambda) = \sin^2 \left(\frac{\arcsin \sqrt{0.5}}{\lambda_0^{2.5}} \lambda^{2.5} \right). \quad (9)$$

We theoretically calculate the transmittance of this 50:50 dual-wavelength FBT BS, and the relationships between the transmittance and wavelength for central wavelengths $\lambda_0 = 1310$ and $\lambda_0 = 1550$ are shown in Table II and Table III, respectively.

Eve can exploit this vulnerability to implement wavelength attacks in the practical CVQKD systems. First, Eve intercepts the signal light pulse and LO light pulse sent by Alice, and makes a heterodyne detection on both the signal and LO

TABLE II. The transmittance T of 50:50 dual-wavelength FBT BS at different wavelength λ (central wavelength $\lambda_0 = 1310$ nm).

λ (nm)	1295	1295.9	1296.3	1297.5	1298.4	1299.6
T	0.47772	0.47904	0.47963	0.48140	0.48273	0.48451
λ (nm)	1300.3	1301.2	1302.5	1303.7	1304.1	1305
T	0.48554	0.48688	0.48881	0.49059	0.49119	0.49253
λ (nm)	1305.8	1306.5	1307	1308.1	1309.5	1310
T	0.49372	0.49476	0.49551	0.49716	0.49925	0.5
λ (nm)	1310.7	1311.6	1312.4	1313.4	1314.3	1315.5
T	0.50105	0.50240	0.50360	0.50511	0.50646	0.50827
λ (nm)	1316.3	1317.1	1318	1318.8	1319.2	1320
T	0.50948	0.51068	0.51204	0.51325	0.51386	0.51507
λ (nm)	1321.5	1322.3	1323.5	1324.7	1325.8	1326.4
T	0.51735	0.51856	0.52039	0.52221	0.52389	0.52480

for measuring the quadrature components X_E and P_E . Then Eve generates and resends two coherent state pulses by a wavelength-tunable laser, while the wavelength deviates from the central wavelength. Eve can control the measurement results deviating from the normal value by controlling the wavelength of forged signal states. In theory, it is considered that Eve can hijack all of the key information without being discovered by legitimate communication parties, as long as Eve chooses the appropriate wavelength and parameters to satisfy the attack equation.

However, the wavelength attack schemes proposed above were appropriate in the noiseless fiber CVQKD systems, where the fiber attenuation coefficient is usually assumed to be a constant, and the channel transmittance is usually assumed as a fixed value in the parameter estimation method, while in the practical atmospheric CVQKD system, the transmittance fluctuates randomly in time. This will bring about large deviations to our estimated parameters which may invalidate the equation that must be satisfied in the attack schemes. Therefore, the success criteria of wavelength attack in atmospheric CVQKD systems needs further investigation. In the following analysis, we will analyze the effectiveness and feasibility of atmospheric wavelength attacks under the framework of the parameter estimation method.

TABLE III. The transmittance T of 50:50 dual-wavelength FBT BS at different wavelength λ (central wavelength $\lambda_0 = 1550$ nm).

λ (nm)	1535	1535.9	1536.3	1537.5	1538.4	1539.6
T	0.48114	0.48226	0.48276	0.48426	0.48539	0.48689
λ (nm)	1540.3	1541.2	1542.5	1543.7	1544.1	1545
T	0.48777	0.48890	0.49053	0.49204	0.49255	0.49368
λ (nm)	1545.8	1546.5	1547	1548.1	1549.5	1550
T	0.49469	0.49557	0.49621	0.49759	0.49937	0.5
λ (nm)	1550.7	1551.6	1552.4	1553.4	1554.3	1555.5
T	0.50089	0.50203	0.50304	0.50431	0.50546	0.50699
λ (nm)	1556.3	1557.1	1558	1558.8	1559.2	1560
T	0.50800	0.50902	0.51017	0.51119	0.51209	0.51273
λ (nm)	1561.5	1562.3	1563.5	1564.7	1565.8	1566.4
T	0.51465	0.51567	0.51721	0.51875	0.52016	0.52093

IV. ATTACK STRATEGIES IN ATMOSPHERIC CHANNEL

The wavelength attack of GMCS CVQKD over the atmospheric channel is shown in Fig. 2. Alice first randomly chooses quadrature components X_A and P_A from Gaussian distribution with variance $V_A N_0$ and zero mean. The light pulses from the laser diode are divided into the weak signal pulse and strong LO pulse by a 1:99 BS. Then the weak signal is modulated as a coherent state by the PM and AM. To avoid interference, the signal is separated from LO in time and modulated into orthogonal polarizations by the PBS before arriving in the fluctuating atmospheric channel. Eve intercepts the signal light and LO light, then measures $\hat{X}$ and $\hat{P}$ quadratures of the signal state by heterodyne detection, which are denoted as X_E and P_E . According to the measurement results, Eve prepares and resends four extra light pulses $\{F^s, F^{lo}\}$ and $\{P^s, P^{lo}\}$ to Bob. When these pulses arrive at Bob's side, they must pass through a 10:90 BS in which 10% light intensities are sent to the detector D_{test} for the clock trigger. Subsequently, the PBS separates signal states $\{F^s, P^s\}$ and LO states $\{F^{lo}, P^{lo}\}$ into the signal path and LO path. In addition, Bob adds an AM in the signal path with a strong attenuation on some randomly selected pulse for real-time shot-noise measurements, which can be utilized to resist the LO calibration attack. Finally, Bob measures either $\hat{X}$ or $\hat{P}$ quadrature. After repeating this process many times, the final secret keys were obtained through reverse reconciliation.

It is worth noting that the transmittance of the 50:50 FBT BS diverges from 0.5 because the wavelengths of $\{P^s, P^{lo}\}$ depart from the central wavelength. Exploiting the wavelength-dependence feature of FBT BS, the wavelengths of $\{P^s, P^{lo}\}$ are randomly selected from the following two groups of parameters with equal probability (the details are given in Table II and Table III):

$$\begin{aligned}
 &\text{parameter 1 : } \lambda_1^s = 1298.4 \text{ nm, } T_1^s = 0.48273; \\
 &\quad \lambda_1^{lo} = 1536.3 \text{ nm, } T_1^{lo} = 0.48276; \\
 &\text{parameter 2 : } \lambda_2^s = 1321.5 \text{ nm, } T_2^s = 0.51735; \\
 &\quad \lambda_2^{lo} = 1563.5 \text{ nm, } T_2^{lo} = 0.51721;
 \end{aligned} \tag{10}$$

where λ_j^i ($i = s, lo; j = 1, 2$) is the wavelength and T_j^i is the transmittance of the 50:50 FBT BS in different wavelengths. The unbalanced distribution of light pulse between D_1 and D_2 will result in a differential current that is proportional to the light intensity. The light intensity of P^s and P^{lo} are defined as I^s and I^{lo} , respectively.

When Bob applies a strong attenuation to measure the shot noise ($r_1 \approx 0$), I^s has a tremendous attenuation and thus the differential current is mainly contributed by I^{lo} . The extra contribution of I^{lo} is recorded as D_j^{lo} with $D_j^{lo} \simeq \eta_j^{lo} [T_j^{lo} I_j^{lo} - (1 - T_j^{lo}) I_j^{lo}] \equiv \eta_j^{lo} (2T_j^{lo} - 1) I_j^{lo}$, where η_j^{lo} is the detector efficiency under different wavelengths. If there is only one set of wavelength parameters for $\{P^s, P^{lo}\}$ such as $\{\lambda_1^s, \lambda_1^{lo}\}$, the variance of the differential current can be written as $\langle (D_1^{lo})^2 \rangle - \langle D_1^{lo} \rangle^2 = 0$. In order to make the variance of the differential current remarkably larger than zero but maintain zero mean, the wavelengths of $\{P^s, P^{lo}\}$ should be chosen from the two sets of parameters randomly with equal probability. As shown in Eq. (10), the simplest approach to achieve zero mean is to

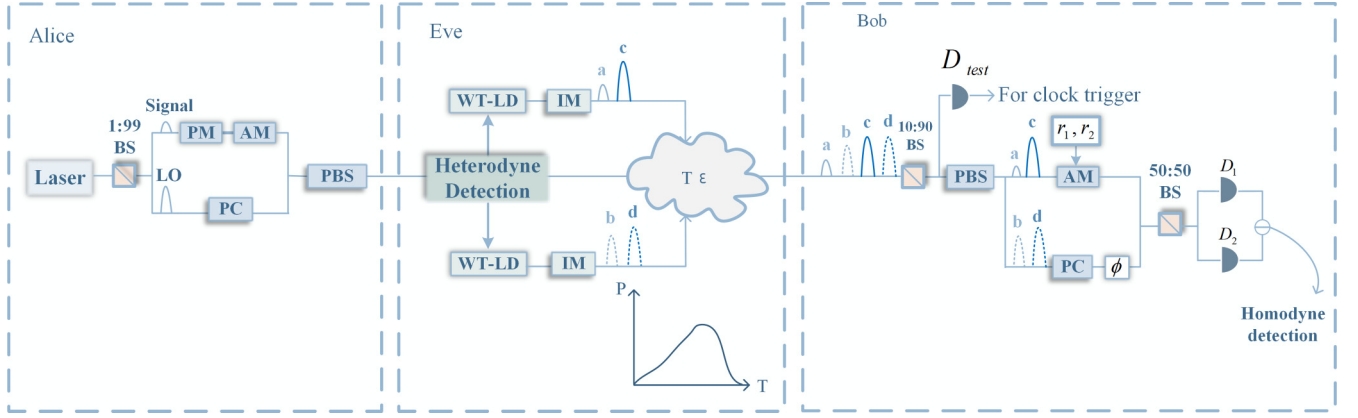


FIG. 2. Schematic diagram of the wavelength attack scheme on atmospheric CVQKD via homodyne detection. BS, beam splitter; PM, phase modulator; AM, amplitude modulator; PC, polarization controller; PBS, polarization beam splitter; WT-LD, wavelength tunable laser diode; IM, intensity modulator; ϕ , phase modulator with $\phi = 0$ or $\pi/2$; D, detector. Indices a, b, c, d denote F^s, F^{l0}, P^s, P^{l0} , respectively.

choose the appropriate wavelength λ_j^{l0} ($j = 1, 2$) with transmittance $T_2^{l0} \approx 1 - T_1^{l0}$, then choose the appropriate I_j^{l0} for ensuring $D_1^{l0} = -D_2^{l0}$.

By contrast, if Bob applies no attenuation to measure the signal state ($r_2 \approx 1$), the differential current is contributed by I^s and I^{l0} , which actually cancel each other out. The extra contribution of I^s is considered as $(1 - 2T_j^s)\eta_j^s I_j^s \equiv D_j^s$. Eve ensures $D_1^s = -D_2^s$ by choosing appropriate λ_j^s and I_j^s with the same probability. For the convenience of analyzing, we sum up the extra contribution defined above as

$$\begin{aligned} D_1^s &\equiv (1 - 2T_1^s)\eta_1^s I_1^s, \\ D_1^{l0} &\equiv (2T_1^{l0} - 1)\eta_1^{l0} I_1^{l0}, \\ D_2^s &\equiv (1 - 2T_2^s)\eta_2^s I_2^s, \\ D_2^{l0} &\equiv (2T_2^{l0} - 1)\eta_2^{l0} I_2^{l0}. \end{aligned} \quad (11)$$

We define $D_1^s = -D_1^{l0} = D_2^s = -D_2^{l0} \equiv D$. To make our attacks work, we should select the appropriate light intensity of $\{I^s, I^{l0}\}$ for the compensation of shot-noise and the measurement of excess noise.

Simply put, by introducing $\{P^s, P^{l0}\}$ with different wavelengths, the differential current response value close to zero when $r_2 \approx 1$ is selected to measure the signal state. Yet when Bob selects $r_1 \approx 0$ to measure the shot noise, the nonzero differential current response value is superposed with the measurement results of $\{F^s, F^{l0}\}$. As a result, the total response value will increase to the normal shot-noise variance value N_0 .

If Bob does not monitor the intensity of LO, Eve implements a full intercept-resend wavelength attack as *attack scheme A*. Furthermore, if Bob monitors the intensity of LO, Eve implements a calibration-wavelength attack as *attack scheme B*. However, in the practical atmospheric CVQKD systems, there are some apparent deviations between our estimated parameters and the ideal value. Therefore, the wavelength attack schemes and success criteria for atmospheric CVQKD systems need to be further investigated. In the following section, in order to distinguish from the previous

symbols, the estimated channel transmittance is denoted as $\hat{\eta}_{ch}$, and the BS transmittance is denoted as T .

A. Attack scheme A

In this situation, Eve implements a full intercept-resend wavelength attack, and the implementation steps are as follows:

Part 1: Based on the heterodyne measurement results and parameter estimation results, Eve prepares a fake signal state F^s with amplitude $\sqrt{N}\alpha_E = \sqrt{N\hat{\eta}_{ch}}(X_E + iP_E)/2$ and a fake LO state F^{l0} with amplitude $\alpha_{LO}/\sqrt{N}$, where N is a real number greater than 1. The F^s and F^{l0} are modulated to the same polarization as the original signal state and the original LO state, respectively.

Part 2: Eve prepares two extra light pulses P^s and P^{l0} . The wavelengths of $\{P^s, P^{l0}\}$ are randomly selected from the two groups of parameters in Eq. (10) with equal probability, then modulated to the same polarization as the original signal state and the original LO state, respectively. As shown in Fig. 2, P^s is sent to the upper path along with F^s , and P^{l0} is sent to the lower path along with F^{l0} .

For $\{P^s, P^{l0}\}$, the final measurement variance of Bob is $\eta\hat{\eta}_{ch}(V_A + 2)N_0 + N_0/N + \eta\hat{\eta}_{ch}\varepsilon N_0 + v_{el}N_0$, and the realistic shot noise is N_0/N since the F^{l0} declined N times. Here, ε is the excess noise in units of N_0 , and $N_0 \equiv \eta\alpha_{LO}^2$ is the shot-noise variance based on the calibrated relationship. The estimated excess noise is equal to $[2 + (1/N - 1)/\eta\hat{\eta}_{ch} + \varepsilon]N_0$. By selecting an appropriate N for the estimated channel transmittance, the excess noise estimated by Bob will be close to zero when N_0 is still set as SNU. For example, we select the specific values such as $\varepsilon = 0.1$, $\eta = 0.5$, and $N = 2.105$. It is obvious that the excess noise estimated by Bob is $(2.1 - 1.0499/\hat{\eta}_{ch})N_0$, which is close to zero when $\hat{\eta}_{ch}$ is equal to 0.5.

However, Bob can immediately regulate the parameters against such attacks as long as he measures the shot noise in real time [29]. Eve should improve her attack strategy to avoid the detection by legitimate parties; thus *attack scheme B* is proposed.

B. Attack scheme B

In this situation, Bob monitors the intensity of LO, Eve adopts a combination of LO calibration attack and wavelength attack. The implementation steps are as follows:

Part 1: Based on the measurement results of heterodyne detection and parameter estimation, Eve prepares F^s and F^{lo} with the same amplitude of the original signal state and the original LO state, respectively. Combining the LO calibration attack, Eve modifies the shape of the LO pulse by introducing an attenuation or a delay trigger; thus the measurement variance reduces to γ times than the true value ($\gamma < 1$).

Part 2: Eve prepares two extra light pulses $\{P^s, P^{lo}\}$, and sends them to Bob along with F^s and F^{lo} just like *attack scheme A*.

As we have seen, $\{F^s, F^{lo}\}$ implement the LO calibration attack, while $\{P^s, P^{lo}\}$ revise the measurement results of shot noise to the normal range. In the next section of this article, we analyze the effect of arbitrary changes in atmospheric transmittance on the feasibility of wavelength attack, under the framework of the parameter estimation method.

V. ATTACKING SUCCESS CRITERIA IN ATMOSPHERIC CHANNEL

In this section, we discuss the estimated parameters under the above attack scheme in the atmospheric GMCS CVQKD protocol. Following the parameter estimation procedure in Sec. II, we can obtain the variance $\langle \hat{x} \rangle$ and $\langle \hat{y} \rangle$ on Alice's and Bob's side, and the covariance $\langle \hat{x}\hat{y} \rangle$ between Alice and Bob (assuming that x and y are centered variables as $\langle \hat{x} \rangle = \langle \hat{y} \rangle = 0$):

$$\begin{aligned}\langle \hat{x}^2 \rangle &= V_A N_0, \\ \langle \hat{y}^2 \rangle &= \eta \hat{\eta}_{ch} (V_A + \varepsilon) N_0 + N_0 + v_{el} N_0, \\ \langle \hat{x}\hat{y} \rangle &= \sqrt{\eta \hat{\eta}_{ch}} V_A N_0,\end{aligned}\quad (12)$$

where $\hat{\eta}_{ch}$ is the estimated transmittance of atmospheric channel, $V_A N_0$ is the modulation variance, εN_0 is the excess noise, $v_{el} N_0$ is the electronic noise (all expressed in SNUs), and η is the homodyne detector efficiency. Note that η and v_{el} are calibrated before the parameter estimation.

In order to analyze conveniently, we set $\eta_j^i = \eta = 0.5$ ($i = s, lo; j = 1, 2$), and the light intensity of LO $I_{LO} = 1 \times 10^8$ (expressed in units of photoelectron number). $N_0 \equiv \eta I_{LO}$ is the calibrated shot noise based on the linear relationship established in a secure laboratory. Bob sets $r_1 = 0.001$ for the estimation of shot noise and $r_2 = 1$ for the measurement of signal state, which corresponds to the variance of $\langle \hat{y} \rangle_1$ and $\langle \hat{y} \rangle_2$:

$$\begin{aligned}\langle \hat{y} \rangle_1 &\equiv V_{s1} = r_1 \eta \hat{\eta}_{ch} (V_A + \varepsilon) N_0 + N_0 + v_{el} N_0, \\ \langle \hat{y} \rangle_2 &\equiv V_{s2} = r_2 \eta \hat{\eta}_{ch} (V_A + \varepsilon) N_0 + N_0 + v_{el} N_0.\end{aligned}\quad (13)$$

Based on Eq. (13), we can deduce the estimated shot noise $\hat{N}_0$ and the estimated excess noise $\hat{\varepsilon}$:

$$\begin{aligned}\hat{N}_0 &= \left[\frac{r_2 V_{s1} - r_1 V_{s2}}{r_2 - r_1} \right] / (1 + v_{el}), \\ \hat{\varepsilon} &= \left[\frac{V_{s2} - V_{s1}}{(r_2 - r_1) \eta \hat{\eta}_{ch}} - V_A \hat{N}_0 \right] / \hat{N}_0.\end{aligned}\quad (14)$$

Based on the estimated shot noise, estimated excess noise, and estimated channel transmittance, Alice and Bob can generate the final key rate. To achieve a full security break, Alice and Bob should accept the compromised key information while the secure key has been fully obtained by Eve. For these reasons, the successful attack under these schemes should satisfy a set of requirements for parameter estimation:

(a) For any estimated atmospheric transmittance, the estimated shot noise should always meet $\hat{N}_0 = N_0$.

(b) In particular, the estimated excess noise should satisfy $\hat{\varepsilon} \leq \varepsilon$ and can be made arbitrarily close to zero but remains positive.

In other words, the CVQKD protocol is considered to be secure by Alice and Bob if the estimated excess noise is below the original excess noise. When $\hat{\varepsilon}$ is as close to zero as possible, Eve can achieve all of the final key information without being discovered by the legitimate communication parties. What we are going to do, however, is take account of the numerical range of $\hat{N}_0$ and $\hat{\varepsilon}$ for the two attack schemes in the atmospheric GMCS CVQKD protocol.

A. Attack scheme A

The total differential current δi_{tot} in Bob's side can be expressed as the summation of δi_{part1} and δi_{part2} , which are generated from part 1 and part 2 of the attack scheme, respectively. We denote $\delta i_{tot,m} = \delta i_{part1,m} + \delta i_{part2,m}$, where $m = \{1, 2\}$ represents the attenuation ratio r_m . $\delta i_{part1,m}$ can be calculated by substituting $\hat{X}_\phi = \sqrt{r_m \hat{\eta}_{ch} N} (X_A + \delta \hat{X}_A + \delta \hat{X}_E)$ into Eq. (C1); the variance can be written as

$$\begin{aligned}V_{part1,m}^A &= \langle (\delta i_{part1,m})^2 \rangle - \langle \delta i_{part1,m} \rangle^2 \\ &= \eta \frac{\alpha_{LO}^2}{N} [r_m \eta \hat{\eta}_{ch} N (V_A + 2) + 1] + r_m \eta \hat{\eta}_{ch} \varepsilon N_0 + v_{el} N_0 \\ &= r_m \eta \hat{\eta}_{ch} (V_A + 2 + \varepsilon) N_0 + \frac{N_0}{N} + v_{el} N_0.\end{aligned}\quad (15)$$

The variance of $\delta i_{part2,m}$ can be computed by

$$V_{part2,m}^A = (1 - r_m)^2 D^2 + \eta \langle I_j^{lo} \rangle + \eta r_m^2 \langle I_j^s \rangle. \quad (16)$$

Here,

$$\begin{aligned}\eta \langle I_j^{lo} \rangle &= \frac{\eta}{2} I_1^{lo} + \frac{\eta}{2} I_2^{lo} \\ &= \frac{\eta}{2} \frac{D_1^{lo}}{\eta (2T_1^{lo} - 1)} + \frac{\eta}{2} \frac{D_2^{lo}}{\eta (2T_2^{lo} - 1)} \\ &= 29.028D, \\ \eta r_m^2 \langle I_j^{lo} \rangle &= r_m^2 \frac{\eta}{2} I_1^s + \frac{\eta}{2} I_2^s \\ &= r_m^2 \left[\frac{\eta}{2} \frac{D_1^s}{\eta (1 - 2T_1^s)} + \frac{\eta}{2} \frac{D_2^s}{\eta (1 - 2T_2^s)} \right] \\ &= 28.885 r_m^2 D.\end{aligned}\quad (17)$$

Based on Eq. (10) and Eq. (11), I_j^{lo} and I_j^s can be calculated according to the real numbers of D_j^i and T_j^i ($i = s, lo; j = 1, 2$). Therefore, Eq. (16) can be rewritten as

$$V_{part2,m}^A = (1 - r_m)^2 D^2 + (29.028 + 28.885 r_m^2) D. \quad (18)$$

Thus, the total variance can be expressed as

$$\begin{aligned} V_{s,m}^A &= V_{\text{part1},m}^A + V_{\text{part2},m}^A \\ &= r_m \eta \hat{\eta}_{\text{ch}} (V_A + 2 + \varepsilon) N_0 + \frac{N_0}{N} \\ &\quad + v_{\text{el}} N_0 + (1 - r_m)^2 D^2 + (29.028 + 28.885 r_m^2) D. \end{aligned} \quad (19)$$

Substituting Eq. (19) into Eq. (14), the estimated shot noise and the estimated excess noise under attack scheme A can be represented as

$$\begin{aligned} \hat{N}_0 &= \frac{(\frac{1}{N} + v_{\text{el}}) N_0 + (1 - r_1 r_2) D^2 + (29.028 - 28.885 r_1 r_2) D}{1 + v_{\text{el}}}, \\ \hat{\varepsilon} &= \left[(2 + \varepsilon) N_0 + V_A (N_0 - \hat{N}_0) + \frac{(r_1 + r_2 - 2) D^2}{\eta \hat{\eta}_{\text{ch}}} \right. \\ &\quad \left. + \frac{28.885 (r_1 + r_2) D}{\eta \hat{\eta}_{\text{ch}}} \right] / \hat{N}_0. \end{aligned} \quad (20)$$

We assume $N_0 = 5 \times 10^7$, $\varepsilon = 0.1$, and $v_{\text{el}} = 0.01$ in order to be consistent with the typical parameters in practical CVQKD systems. Based on Eq. (20), we can formalize and numerically study these constraint conditions in Sec. V, which can be written as

$$\begin{aligned} 5 \times 10^7 \left(1 - \frac{1}{N}\right) &= 0.999 D^2 + 28.999 D, -1.05 \times 10^8 \\ &\times \hat{\eta}_{\text{ch}} < -1.998 D^2 + 57.828 D \leq \\ &-1 \times 10^8 \times \hat{\eta}_{\text{ch}}. \end{aligned} \quad (21)$$

For the convenience of analyzing, we can further derive the feasible set of D and N :

$$\begin{aligned} N &= 5 \times 10^7 / (5 \times 10^7 - 0.999 D^2 - 28.999 D), 14.47 \\ &+ 7.07 \times 10^3 \times \sqrt{\hat{\eta}_{\text{ch}}} < D \leq 14.47 \\ &+ 7.25 \times 10^3 \times \sqrt{\hat{\eta}_{\text{ch}}}. \end{aligned} \quad (22)$$

In theory, the differential current coming from I^s and I^{l^0} can be completely compensated. However, the photoelectrons of coherent states obey a Poisson distribution in practice, which leads to the statistical fluctuations in the measurement of light intensity. The variance of light intensity fluctuations $\langle \Delta I^2 \rangle$ is equal to the square root of light intensity value $\sqrt{I}$ and the differential current from I^s and I^{l^0} will not be restricted to zero. In Ref. [26], the authors proved that the excess noise value will below the tolerance threshold even below the normal value, as long as the light intensity of the fake state is two orders of magnitude lower than the real LO. In other words, we constrain the maximum value of I^s and I^{l^0} as $10^6 \leq 10^{-2} \eta \alpha_{\text{LO}}^2$ to make the influence of the interference at a reasonable range.

For this reason, it should meet the requirements that $D_1^s = -D_1^{l^0} = D_2^s = -D_2^{l^0} \equiv D \leq 17210$. From the analysis above, we can conclude that even if there is some obvious transmittance fluctuating in the atmospheric communication channel, Eve can still manipulate the I^s and I^{l^0} to obtain an appropriate $D \leq 17210$ with the corresponding $N > 1$ in the feasible set. The estimated excess noise $\hat{\varepsilon}$ can be seriously underestimated

and even be made arbitrarily close zero by changing the value of I^s and I^{l^0} , which will introduce a critical security loophole.

B. Attack scheme B

In this attack scheme, Eve introduces a decrease in the detection response slope by attenuating or delaying the trigger. The realistic shot noise is set as γN_0 ($\gamma < 1$). The variance of $\delta i_{\text{part1},m}$ can be deduced from the same method described in attack scheme A:

$$V_{\text{part1},m}^B = \gamma [r_m \eta \hat{\eta}'_{\text{ch}} (V_A + 2 + \varepsilon) + 1] N_0 + v_{\text{el}} N_0, \quad (23)$$

where γ and $\hat{\eta}'_{\text{ch}}$ are controlled by Eve, which should satisfy $\gamma \hat{\eta}'_{\text{ch}} = \hat{\eta}_{\text{ch}}$ to meet the success criteria of the attack scheme. The variance $V_{\text{part2},m}^B$ is the same as the variance $V_{\text{part2},m}^A$ in Eq. (18). Therefore, the total variance can be expressed as

$$\begin{aligned} V_{s,m}^B &= V_{\text{part1},m}^B + V_{\text{part2},m}^B \\ &= \gamma [r_m \eta \hat{\eta}'_{\text{ch}} (V_A + 2 + \varepsilon) + 1] N_0 + v_{\text{el}} N_0 \\ &\quad + (1 - r_m)^2 D^2 + (29.028 + 28.885 r_m^2) D. \end{aligned} \quad (24)$$

Thus, substituting Eq. (24) into Eq. (14), the estimated shot noise in attack scheme B can be expressed as

$$\hat{N}_0 = \frac{(\gamma + v_{\text{el}}) N_0 + (1 - r_1 r_2) D^2 + (29.028 - 28.885 r_1 r_2) D}{1 + v_{\text{el}}}, \quad (25)$$

and the estimated excess noise $\hat{\varepsilon}$ is the same as in Eq. (20).

Furthermore, as discussed in Sec. V, we deduce the success criteria for this attack scheme:

$$\begin{aligned} \gamma &= (5 \times 10^7 - 0.999 D^2 - 28.999 D) / (5 \times 10^7), 14.47 \\ &+ 7.07 \times 10^3 \times \sqrt{\hat{\eta}_{\text{ch}}} < D \leq 14.47 \\ &+ 7.25 \times 10^3 \times \sqrt{\hat{\eta}_{\text{ch}}}. \end{aligned} \quad (26)$$

By selecting an appropriate D and γ in the feasible set under different estimated transmittance $\hat{\eta}_{\text{ch}}$, Eve can successfully implement the attack. Meanwhile, Eve can make the estimated excess noise within the normal range even arbitrarily close zero with the corresponding I^s and I^{l^0} . In addition, the estimated value of the shot noise is calibrated to the true value as $\hat{N}_0 = N_0$; thus the countermeasures of shot-noise real-time monitoring will be nullified. Eve can obtain all of the key information and the communication is not secure anymore.

VI. SIMULATION RESULTS

In order to meet the success criteria in the attack schemes that the estimated shot noise $\hat{N}_0 = N_0$ and the excess noise $\hat{\varepsilon}$ is arbitrarily lower than the true value, Eve should control the wavelength and intensity of I^s and I^{l^0} for the given estimated transmittance $\hat{\eta}_{\text{ch}}$. Before the performance analysis, three estimated transmittances $\hat{\eta}_{\text{ch}}$ of the atmospheric turbulence channel are randomly selected, and the corresponding parameters are calculated and recorded in Table IV.

As we have seen, with the randomly estimated transmittance $\hat{\eta}_{\text{ch}}$ of the atmospheric turbulence channel and arbitrarily small estimated excess noise $\hat{\varepsilon}$, Eve can always select a suitable N of $N > 1$ for attack scheme A and a suitable γ of $\gamma < 1$ for attack scheme B. Then Eve chooses the reasonable light intensity $I_1^s, I_1^{l^0}, I_2^s, I_2^{l^0}$ to meet the criteria for a successful

TABLE IV. Parameter values that satisfy the attack criteria in different $\hat{\eta}_{\text{ch}}$ and $\hat{\varepsilon}$. The estimated transmittance $\hat{\varepsilon}$ are in SNUs, the extra contribution D in units of 10^3 photoelectron number, and the light intensity $I_1^s, I_1^{\text{lo}}, I_2^s, I_2^{\text{lo}}$ in units of 10^5 photoelectron number.

$\hat{\eta}_{\text{ch}}$	$\hat{\varepsilon}$	D	I_1^s	I_1^{lo}	I_2^s	I_2^{lo}	Scheme A	Scheme B
							N	γ
0.88	0.1	6.643	3.846	3.853	3.829	3.859	8.732	0.115
	0.06	6.709	3.885	3.891	3.867	3.898	10.320	0.097
	0.03	6.758	3.913	3.920	3.895	3.927	11.951	0.084
	0.01	6.790	3.932	3.939	3.914	3.946	13.359	0.075
0.69	0.1	5.879	3.404	3.409	3.388	3.416	3.267	0.306
	0.06	5.937	3.438	3.444	3.422	3.450	3.421	0.292
	0.03	5.980	3.463	3.469	3.447	3.475	3.547	0.282
	0.01	6.009	3.480	3.486	3.464	3.492	3.636	0.275
0.47	0.1	4.883	2.827	2.832	2.814	2.837	1.920	0.521
	0.06	4.931	2.855	2.860	2.842	2.865	1.956	0.511
	0.03	4.967	2.876	2.881	2.863	2.886	1.984	0.504
	0.01	4.991	2.890	2.895	2.877	2.900	2.002	0.499

attack, which are three orders of magnitude smaller than I_{LO} . As a consequence, Alice and Bob will always overestimate the secret key rate that they believe to be a secure result, even though Eve has completely broken the security without being detected by Alice and Bob.

Now we analyze the security of the horizontal link GMCS CVQKD systems against the wavelength attack in the atmospheric environment. In the asymptotic situation, the reachable secret key rate $K(\langle\hat{\eta}_{\text{ch}}\rangle, \hat{\varepsilon})$ with reconciliation efficiency β is given as

$$K(\langle\hat{\eta}_{\text{ch}}\rangle, \hat{\varepsilon}) = \beta I_{AB}(\langle\hat{\eta}_{\text{ch}}\rangle, \hat{\varepsilon}) - \chi_{\text{BE}}(\langle\hat{\eta}_{\text{ch}}\rangle, \hat{\varepsilon}), \quad (27)$$

where I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo quantity of Bob and Eve (see Appendix D for more details). Considering that the atmospheric channel is primarily influenced by the estimated value of $\langle\hat{\eta}_{\text{ch}}\rangle$ and $\langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle$, the covariance matrix can be expressed by

$$\gamma_{AB_1} = \begin{pmatrix} V \Pi & \langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle\sqrt{V^2 - 1}\sigma_z \\ \langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle\sqrt{V^2 - 1}\sigma_z & \langle\hat{\eta}_{\text{ch}}\rangle(V + \chi_{\text{line}})\Pi \end{pmatrix}, \quad (28)$$

where $\Pi = \text{diag}(1, 1)$ is the unity matrix and $\sigma_z = \text{diag}(1, -1)$ is the Pauli matrix. To estimate the secret key rate, we first simulate the horizontal link transmittance distribution $\langle\eta_{\text{ch}}\rangle$ and $\langle\sqrt{\eta_{\text{ch}}}\rangle$ of the atmospheric turbulent channel by the Monte Carlo method, and then obtain the $\langle\hat{\eta}_{\text{ch}}\rangle$ and $\langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle$ based on the parameter estimation method. All parameters needed for the secret key rate analysis are presented in Table V.

Figure 3 shows the secret key rate versus the transmission distance for various estimated excess noise $\hat{\varepsilon}$. We simulate the transmittance of the atmospheric turbulent channel in summer ($C_n^2 = 2.12 \times 10^{-15} \text{ m}^{-2/3}$). The simulated results indicate that the security bound of the system can be overestimated if Eve initiates a wavelength attack. We have omitted the real secret key rates in Fig. 3, since they are identical to the purple dashed-dotted line as $\hat{\varepsilon} = \varepsilon$. As we have seen, $\hat{\varepsilon}$ can be reduced by selecting the condition parameter value effectively;

TABLE V. The parameters for final secret key rate analysis (all the variances and noises are in SNUs).

Parameters	Values	Description	References
λ	1550 nm	Laser wavelength	[27]
W_0	80 mm	Initial beam-spot radius	[31]
a	110 mm	Receiving lens radius	[31]
f	220 mm	Focal length of receiving lens	[31]
d_{cor}	4.5 μm	Fiber core diameter	[31]
C_n^2	$2.12 \times 10^{-15} \text{ m}^{-2/3}$	Index of refraction structure	[36]
v_{el}	0.01	Electronic noise	[27]
η	0.5	Detection efficiency	[27]
V_A	16	Modulation variance	[41]
β	90%	Reconciliation efficiency	[42]

thus the secret key rate and propagation distance of CVQKD can be further overestimated. This means that Alice and Bob may not be able to discover Eve's attack. Therefore, it may seriously threaten the security of atmospheric GMCS CVQKD protocols if there are a lack of specific countermeasures.

The kernel of this atmospheric wavelength attack is that Eve adjusts $I_1^s, I_1^{\text{lo}}, I_2^s, I_2^{\text{lo}}$ to underestimate the excess noise. In our previous numerical analysis, it assumes that $\hat{\varepsilon}$ can be made arbitrarily lower than the true value even close to zero. To confirm this hypothesis, we simulate the atmospheric transmittance in different seasons according to the corresponding C_n^2 in Table I, and then depict the relationship between $\hat{\varepsilon}$ and χ_{BE} in Fig. 4. The simulation results show that χ_{BE} always increases with $\hat{\varepsilon}$ despite the seasonal variation of the atmospheric environment. In particular, the values of χ_{BE} exceed zero when the values of $\hat{\varepsilon}$ infinitely approach to zero in different seasons, which indicates that Eve can successfully perform an attack and obtain the information of

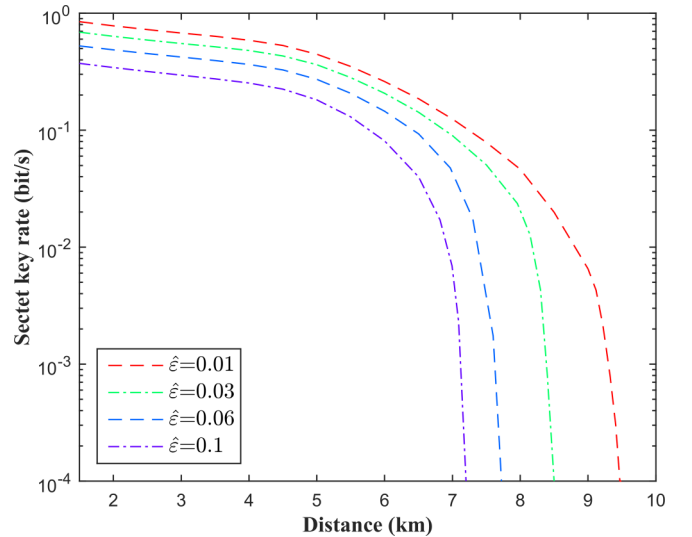


FIG. 3. The achievable secret key in atmospheric attenuation channel for various estimated excess noise $\hat{\varepsilon}$. The transmittance of atmospheric turbulent channel is simulated at summer ($C_n^2 = 2.12 \times 10^{-15}$). The abscissa axis represents the communication distance, and the corresponding estimated transmittance $\hat{\eta}_{\text{ch}}$ can be derived from Eq. (7).

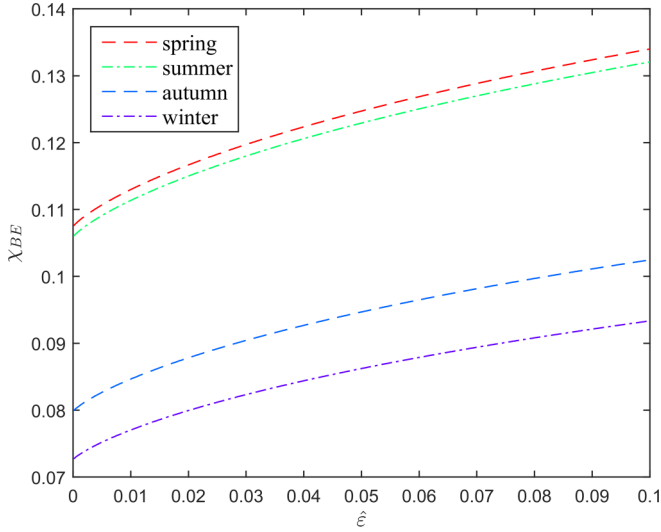


FIG. 4. The relationship between $\hat{\epsilon}$ and χ_{BE} when the channel transmittance is simulated in different seasons.

the final key. Moreover, we find that spring provides the best communication conditions, which is consistent with the trend of long-term radiosonde measurement results in Hefei, Anhui, China. In conclusion, Eve can always obtain the secret information without being discovered if these condition parameters are adjusted to the corresponding value according to the attack criteria.

The countermeasures against the atmospheric wavelength attack will consist of some high-quality wavelength filters before Bob's detection. However, the practical wavelength filters have an upper limit of attenuation for any specific wavelength; thus Eve can counteract the effect by increasing the light intensity. To resist these attacks completely, the wavelength filters and the real-time monitoring of LO intensity should be added together to the practical systems. Moreover, countermeasures based on peak-valley seeking and Gaussian postselection are proposed against the known practical attacks without increasing the complexity of CVQKD systems [43].

VII. CONCLUSION

In this article, we propose two wavelength attack schemes in atmospheric CVQKD systems. Differently from the noiseless fiber with fixed transmittance, the transmittance of turbulent atmospheric channels fluctuates randomly in time which may bias the parameter estimation results between the legitimate parties. We discuss the criteria specifically and calculate the constraint condition accurately for the attack schemes. We demonstrate the feasibility of this attack by selecting the appropriate wavelength and intensity to make the shot noise within the normal regime, no matter whether Bob monitors the shot noise in real time. Besides, we demonstrate the impact on both of the attacks in detail; i.e., Eve's slight manipulation of the condition parameters will lead to a large underestimation of the excess noise and corresponds to overestimation of the secure communication distance. The numerical results show that the security bound can be further overestimated if the estimated excess noise be made arbitrarily

close to zero, which is unified with the physical model of the refractive index structure parameter. To avoid the security loophole, wavelength filters and the real-time monitoring of LO intensity is effective, and the countermeasures based on peak-valley seeking and Gaussian postselection are also recommended.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 11904410), National Natural Science Foundation of China (Grant No. 61801522), and Natural Science Foundation of Hunan Province, China (Grant No. 2019JJ40352).

APPENDIX A: THE ATMOSPHERIC TRANSMITTANCE ANALYSIS

The maximal transmittance T_0 for the centered beam $r_0 = 0$ can be estimated by [37]

$$T_0 = 1 - I_0 \left(a^2 \frac{W_1^2 - W_2^2}{W_1^2 W_2^2} \right) \exp \left(-a^2 \frac{W_1^2 - W_2^2}{W_1^2 W_2^2} \right) - 2 \left\{ 1 - \exp \left[-\frac{a^2}{2} \left(\frac{1}{W_1} - \frac{1}{W_2} \right) \right] \right\} \times \exp \left[-\left\{ \frac{(W_1 + W_2)^2}{|W_1^2 - W_2^2|} \right\}^{\lambda(\frac{1}{W_1} - \frac{1}{W_2})} \right], \quad (A1)$$

which is a function of W_i^2 , $i = 1, 2$. $R(\cdot)$ and $\lambda(\cdot)$ are the scale and shape function, which can be expressed as

$$R(\xi) = \left\{ \ln \left[2 \frac{1 - \exp(-\frac{a^2 \xi^2}{2})}{1 - \exp(-a^2 \xi^2) I_0(a^2 \xi^2)} \right] \right\}^{\frac{1}{\lambda(\xi)}}, \quad (A2)$$

$$\lambda(\xi) = 2a^2 \xi^2 \frac{\exp(-a^2 \xi^2) I_1(a^2 \xi^2)}{1 - \exp(-a^2 \xi^2) I_0(a^2 \xi^2)} \times \left[\ln \left(2 \frac{1 - \exp(-0.5a^2 \xi^2)}{1 - \exp(-a^2 \xi^2) I_0(a^2 \xi^2)} \right) \right]^{-1}. \quad (A3)$$

Here, $I_i(\cdot)$ is the modified Bessel function of i th order. For the given angle $\varphi = \Phi - \phi_0$, the effective spot radius $W_{\text{eff}}(\varphi)$ can be estimated with Lambert function $\mathcal{W}(x)$:

$$W_{\text{eff}}(\varphi)^2 = 4a^2 \left[\mathcal{W} \left(\frac{4a^2}{W_1 W_2} \exp \left\{ \frac{a^2}{W_1^2} [1 + 2 \cos^2(\varphi)] \right\} \right) \times \exp \left\{ \frac{a^2}{W_2^2} [1 + 2 \sin^2(\varphi)] \right\} \right]. \quad (A4)$$

As for the isotropic turbulence, the randomly changed parameters $(x_0, y_0, W_1, W_2, \Phi)$ can be derived from the Gaussian distribution. As shown in Fig. 1, parameter Φ obeys uniform distribution and is independent of (x_0, y_0, W_1, W_2) . The beam-centroid position (x_0, y_0) follows a Gaussian distribution, which is influenced by the additive white Gaussian noise. Besides, the shape parameters (W_1, W_2) obey a log-normal distribution which can be obtained by $W_i^2 = W_0^2 \exp \Theta_i$, where W_0 is the initial beam-spot radius. Therefore, for a given

Θ_i , the correlation of $(x_0, y_0, \Phi_1, \Phi_2)$ can be defined by its covariance matrix,

$$\Xi = \begin{pmatrix} \langle x_0^2 \rangle & 0 & 0 & 0 \\ 0 & \langle y_0^2 \rangle & 0 & 0 \\ 0 & 0 & \langle \Theta_1^2 \rangle & \langle \Theta_2^2 \rangle \\ 0 & 0 & \langle \Theta_1 \Theta_2 \rangle & \langle \Theta_1 \Theta_2 \rangle \end{pmatrix}, \quad (\text{A5})$$

the elements of Ξ can be expressed by

$$\begin{aligned} \langle x_0^2 \rangle &= \langle y_0^2 \rangle = 0.33W_0^2\sigma_R^2\Omega^{-\frac{7}{6}}, \\ \langle \Theta_1^2 \rangle &= \langle \Theta_2^2 \rangle = \ln \left[1 + \frac{1.2\sigma_R^2\Omega^{\frac{5}{6}}}{(1 + 2.96\sigma_R^2\Omega^{\frac{5}{6}})^2} \right], \\ \langle \Theta_1 \Theta_2 \rangle &= \ln \left[1 - \frac{0.8\sigma_R^2\Omega^{\frac{5}{6}}}{(1 + 2.96\sigma_R^2\Omega^{\frac{5}{6}})^2} \right], \end{aligned} \quad (\text{A6})$$

and their expectations can be expressed by

$$\begin{aligned} \langle x_0 \rangle &= \langle y_0 \rangle = 0, \\ \langle \Theta_1 \rangle &= \langle \Theta_2 \rangle = \ln \left[\frac{(1 + 2.96\sigma_R^2\Omega^{\frac{5}{6}})^2}{\Omega^2 \sqrt{(1 + 2.96\sigma_R^2\Omega^{\frac{5}{6}})^2 + 1.2\sigma_R^2\Omega^{\frac{5}{6}}}} \right], \end{aligned} \quad (\text{A7})$$

where σ_R^2 is the Rytov variance, and Ω is the Fresnel parameter of the beam:

$$\Omega = \frac{kW_0^2}{2L}. \quad (\text{A8})$$

APPENDIX B: PARAMETER ESTIMATION METHOD

$\hat{t}$ and $\hat{\sigma}^2$ are two independent estimators following the normal distribution and χ^2 distribution, respectively:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^m x_i^2}\right), \quad \frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \quad (\text{B1})$$

where t and σ^2 are the true values of the parameters. Considering the finite-size effect on parameter estimation, the χ^2 distribution converges to a normal distribution in the limit of large block size m (e.g., $m > 10^6$); thus the confidence intervals of the estimators $\hat{t}$ and $\hat{\sigma}^2$ can be expressed as follows:

$$\begin{aligned} t &\in \left[\hat{t} - z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}^2}{mV_A N_0}}, \hat{t} + z_{\epsilon_{PE/2}} \sqrt{\frac{\hat{\sigma}^2}{mV_A N_0}} \right], \\ \sigma^2 &\in \left[\hat{\sigma}^2 - z_{\epsilon_{PE/2}} \frac{\hat{\sigma}^2 \sqrt{2}}{\sqrt{m}}, \hat{\sigma}^2 + z_{\epsilon_{PE/2}} \frac{\hat{\sigma}^2 \sqrt{2}}{\sqrt{m}} \right], \end{aligned} \quad (\text{B2})$$

where $\epsilon_{PE/2}$ is the probability that the estimated parameters do not belong to the confidence region (the typical value is 10^{-10}), $z_{\epsilon_{PE/2}}$ follows $1 - \frac{1}{2}\text{erf}(z_{\epsilon_{PE/2}}/\sqrt{2}) = \frac{1}{2}\epsilon_{PE/2}$, and $\text{erf}(\cdot)$ is the error function defined as

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt. \quad (\text{B3})$$

One can then estimate these parameters via the estimators and their confidence intervals:

$$T = \frac{\hat{t}^2}{\eta}, \quad \varepsilon = \frac{\hat{\sigma}^2 - N_0 - v_{\text{el}}N_0}{N_0\hat{t}^2}. \quad (\text{B4})$$

Alice and Bob can use the quadrature $\hat{X}$ modulated by Alice ($\hat{X}_A$ or $\hat{P}_A$) and the quadrature $\hat{Y}$ measured by Bob ($\hat{Y}_B$ or $\hat{P}_B$) to evaluate the channel parameters. Here we assume that

$$\hat{X} = |\alpha_A| \cos(\theta), \quad \hat{Y} = \sqrt{\eta T} |\alpha_A| \cos(\theta + \Delta\vartheta) + A_N, \quad (\text{B5})$$

where $|\alpha_A|$ and θ represents the amplitude and the phase of the modulation coherent state without the effect of the atmospheric link, respectively. ϑ is the phase shift generated by the atmospheric link, and A_N is the amplitude caused by the noise. From the above analyses, we can rewrite the parameters $\hat{t}$ and $\hat{\sigma}^2$ in Eq. (6) as

$$\hat{t} = \frac{E(\hat{X}\hat{Y})}{E(\hat{X}^2)}, \quad \hat{\sigma}^2 = E[(\hat{Y} - \hat{t}\hat{X})^2]. \quad (\text{B6})$$

Here,

$$\begin{aligned} E(\hat{X}^2) &= E[|\alpha_A|^2 \cos^2(\theta)] = V_X, \\ E(\hat{X}\hat{Y}) &= E[\sqrt{\eta T} |\alpha_A|^2 \cos(\theta) \cos(\theta + \Delta\vartheta)] \\ &\quad + E[A_N |\alpha_A| \cos(\theta)] \\ &= E[\sqrt{\eta T} |\alpha_A|^2 \cos^2(\theta)] = E(\sqrt{\eta T}) V_X, \\ E(\hat{Y}^2) &= \eta E[T |\alpha_A|^2 \cos^2(\theta + \Delta\vartheta)] + E[A_N^2] \\ &\quad + 2E[\sqrt{\eta T} A_N |\alpha_A| \cos(\theta + \Delta\vartheta)] \\ &= \eta V_X E(T) + \eta \varepsilon N_0 E(T) + N_0 + V_{\text{el}}, \end{aligned} \quad (\text{B7})$$

where $V_X = V_A N_0$, and V_A is the modulation variance. Considering $\Delta\vartheta \approx 0$, the mean value of amplitude A_N can be regarded as 0 [$E(A_N) = 0$], $E(A_N |\alpha_A| \cos(\theta)) = E(A_N)E(|\alpha_A| \cos(\theta))$ can be ignored, and $E[A_N^2] = D[A_N] = N_0(\eta E(T)\varepsilon + 1 + v_{\text{el}})$. It is worth noting that all the parameters in the above equations are expressed in SNU.

According to the maximum likelihood estimation method, the estimated atmosphere channel parameters $\hat{T}$ and $\hat{\varepsilon}$ have the following forms:

$$\begin{aligned} \hat{T} &= \frac{\hat{t}^2}{\eta} = \frac{[E(\hat{X}\hat{Y})]^2}{\eta[E(\hat{X}^2)]^2} = [E(\sqrt{T})]^2, \\ \hat{\varepsilon} &= \frac{V_A E(T) + \varepsilon E(T) - V_A [E(\sqrt{T})]^2}{[E(\sqrt{T})]^2}, \end{aligned} \quad (\text{B8})$$

where $\langle T \rangle = E(T)$ and $\langle \sqrt{T} \rangle = E(\sqrt{T})$ reflects the influences of atmospheric environments mainly. These estimated parameters are the foundation for calculating the maximal value of the Holevo information and the final secret key rate.

APPENDIX C: LO CALIBRATION ATTACK AND COUNTERMEASURES

In principle, the shot noise can be evaluated from the interference results between the LO and the vacuum mode. However, in practical CVQKD, the LO is transmitted publicly on the channel between Alice and Bob. Eve can easily access and manipulate the intensity, wavelength, or pulse shape of LO. In Ref. [29], the authors propose the LO calibration attack by introducing a delay trigger.

Before illustrating the LO calibration attack scheme, we first briefly review the basic principle of homodyne detection, which is shown in Fig. 5. The LO light is modulated to the

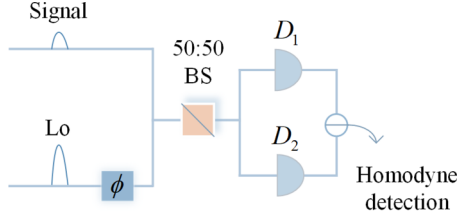


FIG. 5. Schematic diagram of the homodyne principle.

same frequency, polarization, and initial phase as the signal state, then interfere in a 50:50 BS. The differential photocurrent between the two photodetectors can be calculated as

$$\delta i = \sqrt{\eta} \alpha_{LO} \hat{X}_{Bob}^{\phi}, \quad (C1)$$

where α_{LO} is the LO state, and $\phi \in \{0, \pi/2\}$ is randomly selected by Bob. The variance of $\hat{X}_{Bob}^{\phi}$ can be calculated from δi as $V_B^{\phi} = \langle \delta i^2 \rangle = \eta V_{\phi} N_0 + N_0$, where N_0 is the SNUs estimated by $N_0 \equiv \eta \alpha_{LO}^2$.

When an optical pulse arrives at the photodetector, the photons interact with the medium. The accumulated charge reaches a maximum value until all of the photons are absorbed and converted to photoelectrons. This process will last for approximately 100 nanoseconds (depending on the pulse width). After that, the capacitor discharge and the voltage drop exponentially, which lasts for about a few hundred nanoseconds. Specifically, as the solid green curves in Fig. 6 show, the clock circuit is usually designed as a rising trigger signal once the intensity entering the photodiode exceeds a certain threshold I_0 . By delaying the trigger, the signal output of the homodyne detection is maximized. This means that the maximum shot-noise measurement variance is obtained when the trigger coincides with the end of the whole period.

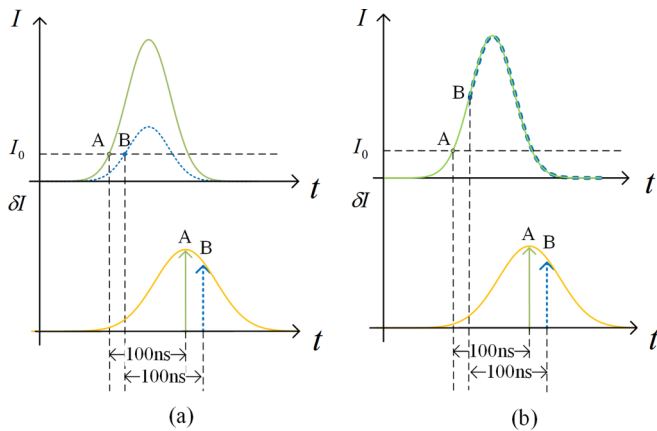


FIG. 6. The principle of calibration attack. The upper plots show the shape of the trigger signals generated at Bob's side. The solid green curves and dotted blue curves denote the original signal and the reshaped signal, respectively. The lower plots show the differential signal of homodyne detection after a delayed trigger about 100 nanoseconds; different measurement time corresponds to different measurement variance. (a) Introducing a delayed trigger by attenuating the LO pulse. (b) Introducing a delayed trigger by modifying the shape of LO pulse.

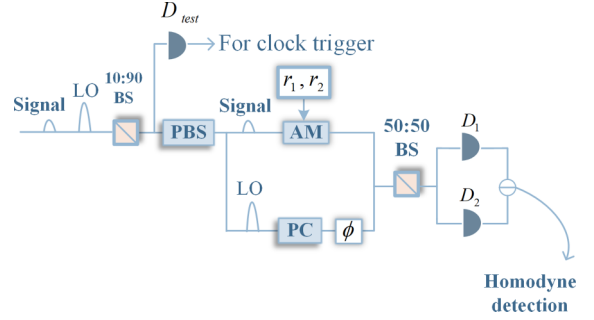


FIG. 7. Real-time shot-noise measurement resisting the LO calibration attack.

However, as shown by the dotted blue lines in Fig. 6, a potential loophole for Eve involves an attenuation at the beginning of the LO pulse or the shape modification of the LO pulse. As a result, Alice and Bob cannot obtain the true peak value of δI . If they still use the previously calibrated relationship to deduce the shot noise, the measurement results will be overestimated and the excess noise will be underestimated; thus the communication is not secure anymore.

To go against the LO calibration attack, a countermeasure based on the real-time shot-noise measurement method is depicted in Fig. 7. A non-attenuation ($r_1 \approx 0$) and a strong attenuation ($r_2 \approx 1$) are randomly applied on the selected pulse in Bob's signal path. This is actually measuring the vacuum state in real time when applying the strong attenuation with a probability of 10%. By analyzing the measurement results of the vacuum state statistically, the true shot noise can be calibrated to resist the calibration attack.

APPENDIX D: SECRET KEY RATE

The parameters I_{AB} and χ_{BE} can be calculated from the covariance matrix γ_{AB_1} . Considering the detection efficiency η and electronic noise v_{el} , the mutual information between Alice and Bob for homodyne detection can be expressed as

$$I_{AB} = \frac{1}{2} \log_2 \frac{1}{1 - \frac{(\sqrt{\eta_{ch}})^2 (V-1)}{(\eta_{ch})(V+\chi_{tot})}}, \quad (D1)$$

where $\chi_{tot} = \frac{1+v_{el}}{\eta(\eta_{ch})} - 1 + \hat{\epsilon}$. We can also obtain the Holevo quantity χ_{BE} based on γ_{AB_1} , which can be further simplified to

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \quad (D2)$$

where $G(x) = (x+1) \log_2(x+1) - x \log_2 x$. The symplectic eigenvalues λ_i of γ_{AB_1} can be represented as

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2} (A \pm \sqrt{A^2 - 4B}), \\ \lambda_{3,4}^2 &= \frac{1}{2} (C \pm \sqrt{C^2 - 4D}), \\ \lambda_5 &= 1, \end{aligned} \quad (D3)$$

with

$$\begin{aligned}
 A &= V^2(1 - 2\langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle^2) + 2\langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle^2 + [\langle\hat{\eta}_{\text{ch}}\rangle V_A + 1 + \hat{\varepsilon}\langle\hat{\eta}_{\text{ch}}\rangle]^2, \\
 B &= [V^2(\langle\hat{\eta}_{\text{ch}}\rangle - \langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle^2) + \langle\sqrt{\hat{\eta}_{\text{ch}}}\rangle^2 + \langle\hat{\eta}_{\text{ch}}\rangle V\chi_{\text{line}}]^2, \\
 C &= \frac{A\chi_{\text{hom}} + V\sqrt{B} + \langle\hat{\eta}_{\text{ch}}\rangle(V + \chi_{\text{line}})}{\langle\hat{\eta}_{\text{ch}}\rangle(V + \chi_{\text{tot}})}, \\
 D &= \frac{\sqrt{B}V + B\chi_{\text{hom}}}{\langle\hat{\eta}_{\text{ch}}\rangle(V + \chi_{\text{tot}})}
 \end{aligned} \tag{D4}$$

where $\chi_{\text{line}} = 1/\langle\hat{\eta}_{\text{ch}}\rangle - 1 + \hat{\varepsilon}$, $\chi_{\text{hom}} = \frac{1-\eta+v_{\text{el}}}{\eta}$.

-
- [1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [4] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nat. Phys.* **4**, 726 (2008).
- [5] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, Z. Ma, and V. Makarov, *Nat. Commun.* **2**, 349 (2011).
- [6] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [7] S. Takeda, M. Fuwa, P. van Loock, and A. Furusawa, *Phys. Rev. Lett.* **114**, 100501 (2015).
- [8] H. K. Lo, M. Curty, and K. Tamaki, *Nat. Photonics* **8**, 595 (2014).
- [9] B. Qi, C.-H. Fung, H.-K. Lo, and X. Ma, *Quantum Inf. Comput.* **7**, 73 (2007).
- [10] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [11] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, *Phys. Rev. A* **76**, 052323 (2007).
- [12] D. Huang, P. Huang, D. Lin, and G. Zeng, *Sci. Rep.* **6**, 19201 (2016).
- [13] F. Furrer, *Phys. Rev. A* **90**, 042325 (2014).
- [14] P. Huang, G. He, J. Fang, and G. Zeng, *Phys. Rev. A* **87**, 012317 (2013).
- [15] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouiri, and P. Grangier, *New J. Phys.* **11**, 045023 (2008).
- [16] D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, *Phys. Rev. A* **94**, 032305 (2016).
- [17] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, *Sci. Rep.* **5**, 14607 (2015).
- [18] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, *New J. Phys.* **13**, 013043 (2011).
- [19] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, *Phys. Rev. Lett.* **107**, 110501 (2011).
- [20] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, *IEEE J. Sel. Top. Quantum* **21**, 168 (2014).
- [21] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, *New J. Phys.* **16**, 123030 (2014).
- [22] S. Kunz-Jacques and P. Jouguet, *Phys. Rev. A* **91**, 022307 (2015).
- [23] H. Qin, R. Kumar, and R. Alléaume, *Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X*, Vol. 8899 (SPIE, 2013), pp. 122–128.
- [24] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, *Phys. Rev. A* **84**, 062308 (2011).
- [25] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, *Phys. Rev. A* **87**, 052309 (2013).
- [26] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **87**, 062329 (2013).
- [27] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **89**, 032304 (2014).
- [28] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, *Phys. Rev. A* **98**, 012312 (2018).
- [29] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, *Phys. Rev. A* **87**, 062313 (2013).
- [30] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, *Phys. Rev. A* **88**, 022339 (2013).
- [31] S. Wang, P. Huang, T. Wang, and G. Zeng, *New J. Phys.* **20**, 083037 (2018).
- [32] A. Leverrier, F. Grosshans, and P. Grangier, *Phys. Rev. A* **81**, 062343 (2010).
- [33] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, *Phys. Rev. A* **86**, 032309 (2012).
- [34] Y. Zheng, W. Liu, Z. Cao, and J. Peng, *Phys. Rev. A* **101**, 022319 (2020).
- [35] R. L. Fante, *Proc. IEEE* **63**, 1669 (1975).
- [36] C. W. H. Wang and Y. Fan, *Laser Beam Propagation and Applications through the Atmosphere and Sea Water* (National Defense Industry Press, Beijing, 2015).
- [37] D. Vasylyev, A. A. Semenov, and W. Vogel, *Phys. Rev. Lett.* **117**, 090501 (2016).
- [38] D. Vasylyev, A. A. Semenov, W. Vogel, K. Günthner, A. Thurn, O. Bayraktar, and C. Marquardt, *Phys. Rev. A* **96**, 043856 (2017).
- [39] A. Ankiewicz, A. Snyder, and X. H. Zheng, *J. Light. Technol.* **4**, 1317 (1986).
- [40] V. J. Tekippe, *Fiber Integr. Opt.* **9**, 97 (1990).
- [41] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Phys. Rev. A* **84**, 062317 (2011).
- [42] Z. Zuo, Y. Wang, Y. Mao, W. Ye, L. Hu, D. Huang, and Y. Guo, *J. Phys. B: At., Mol. Opt. Phys.* **53**, 185501 (2020).
- [43] P. Huang, J. Huang, T. Wang, H. Li, D. Huang, and G. Zeng, *Phys. Rev. A* **95**, 052302 (2017).