Practical security of continuous-variable quantum key distribution with an optical amplifier

Yi Zheng,[*] Yiliang Wang, Chenlei Fang, Haobin Shi, and Wei Pan

School of Computer Science, Northwestern Polytechnical University, Xi'an 710129, Shaanxi, China

(Received 16 October 2023; revised 26 December 2023; accepted 1 February 2024; published 20 February 2024)

In a practical continuous-variable quantum key distribution (CVQKD) system, the optical amplifier can be used to improve the performance of the system by compensating for the imperfections of the detectors. However, the eavesdropper Eve can actively utilize a reverse external magnetic field to deteriorate the performance of the optical amplifier, which may affect the practical security of the system. In this paper, we investigate the practical security of a CVQKD system with an optical amplifier under the effect of the reverse external magnetic field. Based on the investigation of the parameter estimation under the above influence, we find that the evaluation of the secret key rate may be overestimated, which will open a security loophole for Eve to successfully launch an intercept-resend attack in the practical CVQKD system with an optical amplifier. In order to close this security loophole, we can monitor the reverse external magnetic field or change the type of the optical isolator to make the secret key rate of the system evaluated exactly.

DOI: 10.1103/PhysRevA.109.022424

I. INTRODUCTION

In the field of quantum cryptography [1,2], quantum key distribution (QKD) allows Alice and Bob, two remote legitimate communication parties, to share the symmetric secret keys over an insecure quantum channel [3,4]. QKD technology is based on the fundamental laws of quantum physics, which ensures its unconditional security [5–8]. Currently, QKD can be categorized into discrete-variable quantum key distribution (DVQKD) and continuous-variable quantum key distribution (CVQKD). Different from DVQKD, CVQKD encodes the information in the quadrature variables of the light field, and has a higher secret key rate [9,10]. Therefore, it is significant to research CVQKD.

Among the implementations of CVQKD, the scheme based on Gaussian-modulated coherent states (GMCSs) is well known, and has made significant progress in both theory and experiment [11–18]. In theory, the unconditional security of the GMCS CVQKD scheme against collective and coherent attacks has been fully demonstrated [19–22]. However, in a practical CVQKD system, there are some deviations between the theoretical model and the realistic devices [23–25], which may open security loopholes for the eavesdropper Eve. Eve may exploit these security loopholes to launch some quantum hacking attacks, such as saturation attack [26], detector blinding attack [27], finite sampling bandwidth effects [28], jitter in clock synchronization [29], local oscillator (LO) fluctuation attack [30], LO calibration attack [31], and polarization attack [32]. In order to resist these attacks, the researchers have proposed some countermeasures, such as the continuous-variable measurement-device-independent quantum key distribution [33–35] protocol that removes all security loopholes in the detection, and the local LO CVQKD scheme [36,37] that resists the LO attacks. However, due to the complexity of the practical communication environment, these improved schemes may still have security problems. Therefore, researchers still focus on the practical security of the CVQKD system.

At the receiver side of the practical CVQKD system, the detectors have detection noise and limited detection efficiency. These imperfections reduce the secret key rate of the system. Fortunately, optical amplifiers can be used to compensate for the inherent imperfections by amplifying the optical signal [38,39]. Inside the optical amplifier, the optical isolator ensures unidirectional transmission of light. In recent years, rotators based on the Faraday effect play an important role in the practical operation of the optical isolator and are widely used in the manufacture of optical isolators. Meanwhile, the rotation angle of the Faraday rotator is closely related to the magnetic field intensity [40]. However, Eve can control the intensity of the external magnetic field and affect the normal operation of the Faraday rotator, which may threaten the practical security of a CVQKD system with an optical amplifier. Therefore, in this paper, we focus on the effect of external magnetic field on the practical security of a CVQKD system with an optical amplifier. We first introduce the working principle of the optical amplifier and further analyze amplification performance of the optical amplifier under a reverse external magnetic field. The result shows that in the CVQKD system with an optical amplifier, the practical intensity of the signal light after passing through the amplifier is less than its ideal value. Subsequently, we discuss the parameter estimation and analyze the total noise of the system under the above effects. Based on these analyses, we calculate the secret key rate under the effect of a reverse external magnetic field. The simulation results indicate that the practical evaluation of the secret key rate may be overestimated when the legitimate communicating parties are not aware of the existence of a reverse external magnetic field. Therefore, a reverse external magnetic field

[*] yizheng@nwpu.edu.cn

can open a security loophole for Eve to successfully execute an intercept-resend attack and obtain information about the secret key. Moreover, if the reverse external magnetic field intensity is the same, Eve can obtain more key information when the gain coefficient of the optical amplifier is smaller. To close the security loophole, we propose different resistance schemes. On the one hand, we can use a real-time monitoring module or Hall elements to determine the existence and intensity of a reverse external magnetic field. On the other hand, we can eliminate the effects of the external magnetic field by changing the type of optical isolator in the optical amplifier.

This paper is structured as follows. In Sec. II, we mainly introduce the effect of a reverse external magnetic field on the optical amplifier. Then, we discuss the parameter estimation and analyze the secret key rate under the above effect in Sec. III. And in Sec. IV, we propose different countermeasures to close this security loophole opened by the reverse external magnetic field. Finally, the conclusion is presented in Sec. V.

II. CVQKD SYSTEM WITH AN OPTICAL AMPLIFIER UNDER THE EFFECTS OF MAGNETIC FIELD

In this section, we mainly elaborate on a CVQKD system with an optical amplifier and analyze the effect of external magnetic fields on an optical amplifier.

A. CVQKD with an optical amplifier

In a practical CVQKD system, the detectors at the receiver side are imperfect due to the inherent noise and limited detection efficiency, which degrades the secret key rate of the system. In order to reduce the impact of the above imperfections, an optical amplifier is placed at the output of the quantum channel to boost the intensity of the signal light and increase the secret key rate of the system. Because the erbium-doped fiber amplifier (EDFA) has better amplification performance in amplifying C-band signal light (1530–1565 nm) [41,42], we can use the EDFA to amplify the signal light in a practical CVQKD system.

Figure 1 depicts the practical optical path of a CVQKD system with an EDFA. At the transmitter side of the system, Alice uses a 1550-nm continuous-wave laser to generate the initial coherent states. Subsequently, Alice uses a beam splitter to separate the initial coherent states into a signal optical path and a local oscillator optical path. In the signal optical path, Alice generates a series of Gaussian-modulated coherent states and modulates the polarization of the Gaussian-modulated coherent states by the polarization beam splitter, delay line, and Faraday mirror. Finally, both signal light and local oscillation light are attenuated to the quantum level by a variable optical attenuator and transmitted in the quantum channel by polarization multiplexing and time-division multiplexing. At the receiver side of the system, Bob uses a polarization beam splitter to separate the signal light and the local oscillation light. Then, the signal light is amplified by the EDFA in the signal optical path. Subsequently, Bob uses a heterodyne detector to measure the quadrature variables of the signal light. The above steps are followed by the classical data postprocessing phase, which includes parameter estimation, reverse reconciliation, and privacy amplification. After these steps, both communication parties will share the final bit string of secret key.

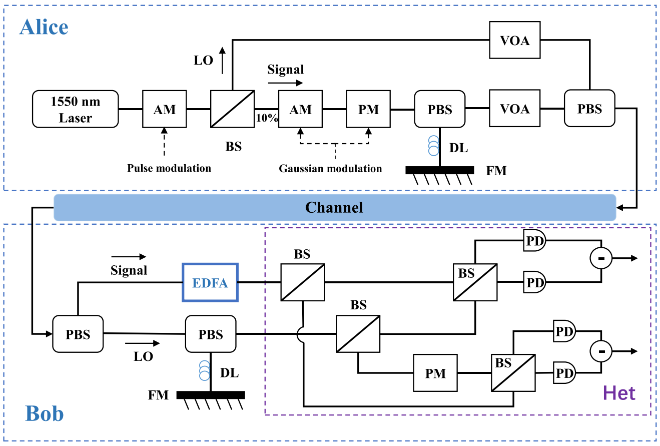

FIG. 1. Practical optical path of the CVQKD system with an optical amplifier. AM, amplitude modulator; PM, phase modulator; BS, beam splitter; PBS, polarization beam splitter; FM, Faraday mirror; DL, delay line; VOA, variable optical attenuator; LO, local oscillator; EDFA, erbium-doped fiber amplifier; Het, heterodyne detector; PD, photodetector.

B. The working principle of an erbium-doped fiber amplifier

EDFA is a fiber amplifier that utilizes rare-earth erbium ions (Er^{3+}) as the gain medium. Figure 2 illustrates that the EDFA consists mainly of an optical isolator, a pump source, a coupler, and an erbium-doped fiber. In particular, the optical isolator is used to ensure the unidirectional transmission of signal light and prevent reverse light from affecting the amplification process of signal light. When the signal light enters the EDFA, it first passes through the optical isolator. Secondly, the pump source emits pump light with a wavelength of 980 or 1480 nm, which is coupled with the signal light and enters the erbium-doped fiber. Subsequently, the Er^{3+} in the erbium-doped fiber realizes the transition from low-energy levels to high-energy levels under the effect of stimulated absorption of pump light. Finally, under the stimulation of signal light, Er^{3+} at high energy levels will jump to low-energy levels. As a result, the same photons as the signal light are emitted, which enhances the intensity of signal light. However, when the EDFA amplifies the signal light, it inevitably generates spontaneous emission noise, resulting in a decrease in the signal-to-noise ratio of the signal light. Therefore, it is

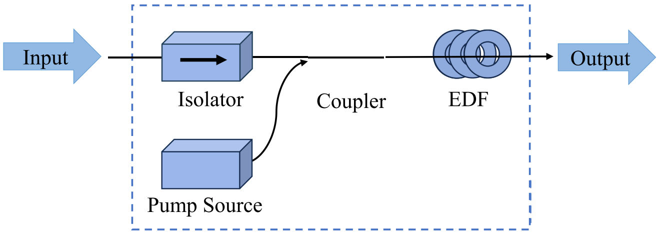

FIG. 2. Structural diagram of an erbium-doped fiber amplifier. EDF, erbium-doped fiber.

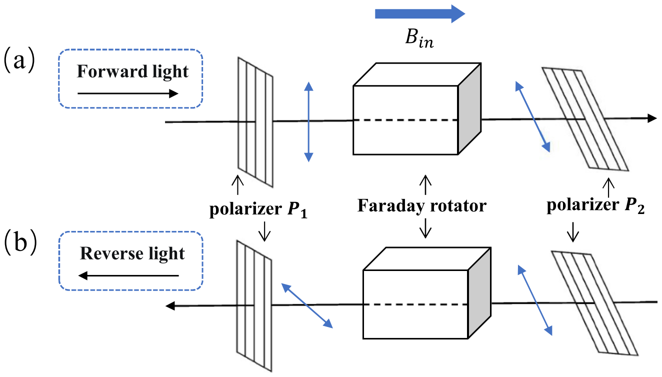

FIG. 3. Structure of the Faraday effect-based optical isolator. (a) Schematic of the forward light propagation. (b) Schematic of the reverse light propagation. B_{in}, the internal magnetic field.

necessary to consider the effect of this noise when modeling and analyzing the EDFA.

Before analyzing the effect of external magnetic fields on an optical amplifier, we need to know the components and the working principle of an optical isolator. Optical isolators are common nonreciprocal devices in optical communication systems, which are mainly used to achieve unidirectional transmission of light. Inside the optical amplifier, the optical isolator is one of the indispensable devices for achieving stable operation of the optical amplifier. Currently, optical isolators based on Faraday effect are widely used in scientific research and commerce due to their mature technology and low cost. Therefore, this paper focuses on the optical isolator based on Faraday effect.

Figure 3 shows that the Faraday effect-based optical isolator mainly consists of two polarizers and a Faraday rotator with a rotation angle of 45°. It is obvious that the Faraday rotator is the core device, which is composed of a magneto-optical crystal and a ring-shaped permanent magnet. And the working process of the Faraday rotator is that the permanent magnet provides the internal magnetic field. When signal light passes through the magneto-optical crystal, the polarization plane rotates due to the Faraday effect. More importantly, the rotation direction of the polarization plane is only related to the direction of the magnetic field.

Figure 3(a) shows that when the forward signal light enters the optical isolator, the signal light will completely pass through the polarizer P_1 because the polarization direction of the forward signal light is consistent with the polarization direction of the polarizer P_1. Subsequently, the signal light enters the Faraday rotator. Due to the Faraday effect, the polarization plane of the signal light will rotate 45°. Next, the signal light will completely pass through the polarizer P_2 because the angle between transmission axes of polarizer P_1 and polarizer P_2 is also 45°. It is worth noting that after passing through this polarization-correlated optical isolator, the polarization direction of the signal light will change, which may affect the subsequent detection process. Fortunately, in the practical optical path, we can first use a beam splitter to split a fraction of the signal light. Afterwards, we measure the polarization direction of this part of the signal light and calculate the polarization drift. Finally, we can use a dynamic polarization controller to correct the polarization drift.

Figure 3(b) shows that after the reverse light passes through the polarizer P_2 and the Faraday rotator, the reverse light cannot pass through the polarizer P_1 because the polarization direction of the reverse light is perpendicular to the polarization direction of the polarizer P_1. This achieves the isolation function of the optical isolator for the reverse light.

C. Optical amplifier under the influence of external magnetic fields

Inside the optical amplifier, the rotator based on the Faraday effect is one of the core components of the optical isolator. Faraday effect is a phenomenon in which the polarization plane of an optical field undergoes rotation. This rotation is the result of a change in the refractive index of the medium caused by the presence of a magnetic field. When light passes through a medium under the effect of a magnetic field, the rotation angle θ of the light polarization plane (magnetic rotation angle) is proportional to the length L of the light passing through the medium and the intensity B of the magnetic field in the direction of light propagation, which can be expressed as

$$\theta = VBL, \tag{1}$$

where V is the Verdet constant, which characterizes the magneto-optical properties of the medium. Based on Eq. (1), we know that the rotation angle of the light polarization plane is proportional to the intensity of the magnetic field when light passes through the Faraday rotator. As a result, the performance of the optical isolator will be affected by the external magnetic field, which has been shown experimentally [40]. Therefore, in a practical CVQKD system with an optical amplifier, the eavesdropper Eve may actively change the intensity of the external magnetic field to affect the performance of the optical amplifier by applying a reverse external magnetic field [see Fig. 4(a)]. According to Ref. [40], we can obtain the relationship diagram between the insertion loss of the signal light and the intensity of the reverse external magnetic field [see Fig. 4(b)]. Based on Fig. 4(b), it is obvious that as the intensity of the reverse external magnetic field increases, the insertion loss of the signal light also increases. This phenomenon further indicates that the reverse external magnetic field may have an effect on the performance of the optical amplifier. Therefore, when Eve applies a reverse external magnetic field with a sufficiently large magnetic field intensity, the insertion loss of the signal light will be large, which results in a reduction in the intensity of the signal light. As a consequence, under the effect of a reverse external magnetic field, the practical output optical signal intensity I'_{out} is less than its ideal value I_{out} when the signal light of input optical intensity I_{in} passes through the optical amplifier [see Fig. 4(c)].

In order to show more clearly the effect of the external magnetic field on the performance of the optical amplifier, we further analyze the intensity of the signal light from an optical perspective. In the ideal situation, according to Malus's law, the intensity of the signal light passing through the optical isolator is represented as

$$I_{\text{mid}} = I_{\text{in}}\cos^2(\rho - \theta), \tag{2}$$

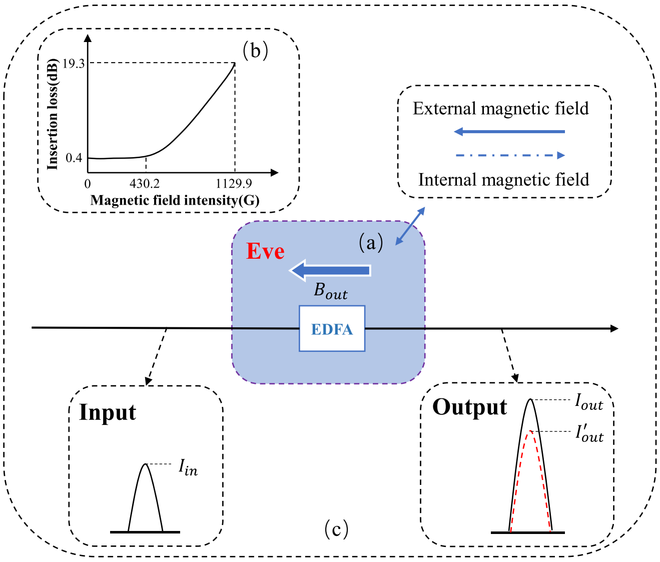

FIG. 4. Performance of optical amplifier when a reverse external magnetic field is applied. (a) Simplified diagram of applying a reverse external magnetic field. (b) Relationship diagram between the insertion loss of signal light and the reverse external magnetic field intensity. (c) Relationship diagram between the input signal intensity and the output signal intensity of the optical amplifier when a reverse external magnetic field is applied. B_{out}, the external magnetic field.

where I_{in} is the intensity of the signal light at the input of the optical isolator, I_{mid} is the intensity of the signal light at the output of the optical isolator, ρ is the angle between the transmittance axes of the polarizer P_1 and the polarizer P_2 in the optical isolator, and θ is the magnetic rotation angle of the signal light passing through the Faraday rotator in the optical isolator. Based on the working principle of the Faraday rotator, we know that $\rho = \pi/4$, $\theta = \pi/4$. Therefore,

$$I_{\text{mid}} = I_{\text{in}}\cos^2(\rho - \theta) = I_{\text{in}}\cos^2(\pi/4 - \pi/4) = I_{\text{in}}. \quad (3)$$

When a reverse external magnetic field exists, the practical intensity of the signal light at the output of the optical isolator is expressed as

$$\begin{aligned} I'_{\text{mid}} &= I_{\text{in}}\cos^2[\rho - (\theta + \Delta\theta)] \\ &= I_{\text{in}}\cos^2(-\Delta\theta) = I_{\text{in}}\cos^2(\Delta\theta), \end{aligned} \quad (4)$$

where $\Delta\theta$ is the changed angle of the magnetic rotation angle of the signal light under the effect of the reverse external magnetic field.

We usually express the amplification performance of an optical amplifier using the gain coefficient g, which is given by

$$g = \frac{I_{\text{out}}}{I_{\text{in}}}, \quad (5)$$

where I_{out} is the intensity of the signal light at the output of the optical amplifier. According to Eq. (5), we also obtain that, when there is a reverse external magnetic field,

$$g = \frac{I'_{\text{out}}}{I'_{\text{mid}}}, \quad (6)$$

$$g' = \frac{I'_{\text{out}}}{I_{\text{in}}}, \quad (7)$$

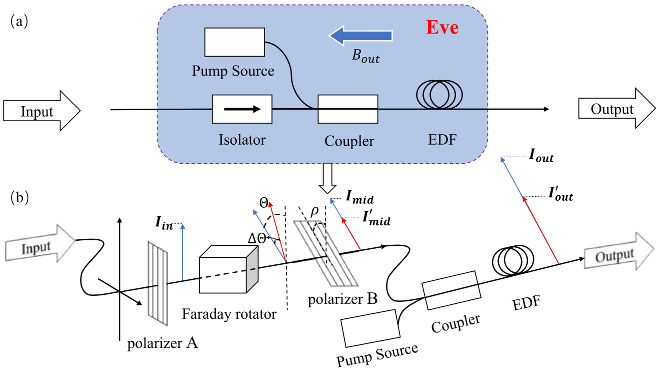

FIG. 5. (a) Practical optical path of the optical amplifier in a CVQKD system with an EDFA. (b) Amplification details of the signal light in the EDFA when a reverse external magnetic field is applied.

where I'_{out} is the practical intensity of the signal light at the output of the optical amplifier and g' is the gain coefficient of the optical amplifier under the effect of the reverse external magnetic field. Based on Eqs. (4), (6), and (7), and the derivations

$$g = \frac{I'_{\text{out}}}{I'_{\text{mid}}} = \frac{I'_{\text{out}}}{I_{\text{in}}\cos^2(\Delta\theta)} = \frac{g'}{\cos^2(\Delta\theta)}, \quad (8)$$

we can finally get

$$g' = g\cos^2(\Delta\theta). \quad (9)$$

Therefore, the reverse external magnetic field has an effect on the amplification performance of the optical amplifier. And it is evident that the practical intensity I'_{out} of the signal light amplified by the optical amplifier is less than its ideal value I_{out} [see Fig. 5(b)].

Based on the phase space, Gaussian-modulated coherent states $|\alpha_B\rangle$ received by Bob can be expressed as

$$\begin{aligned} |\alpha_B\rangle &= |\alpha_B|e^{i\varphi} = x_B + ip_B, \\ x_B &= |\alpha_B|\cos\varphi, \quad p_B = |\alpha_B|\sin\varphi, \end{aligned} \quad (10)$$

where $|\alpha_B|$ and φ are respectively the amplitude and phase of the received signal light, and x_B and p_B are the quadrature variables of the light field.

Furthermore, the intensity I_B and amplitude $|\alpha_B|$ of the signal light obey the following relationship:

$$I_B \propto |\alpha_B|^2. \quad (11)$$

According to Eqs. (5), (10), and (11), we can obtain that, when an optical amplifier is placed at the output of the quantum channel,

$$x_{B\text{amp}} = \sqrt{g}x_B, \quad p_{B\text{amp}} = \sqrt{g}p_B, \quad (12)$$

where $x_{B\text{amp}}$ and $p_{B\text{amp}}$ are the quadrature variables of the amplified signal light. Then we consider the existence of a reverse external magnetic field, and based on Eqs. (7) and (12) we can obtain that

$$x'_{B\text{amp}} = \sqrt{g'}x_B, \quad p'_{B\text{amp}} = \sqrt{g'}p_B, \quad (13)$$

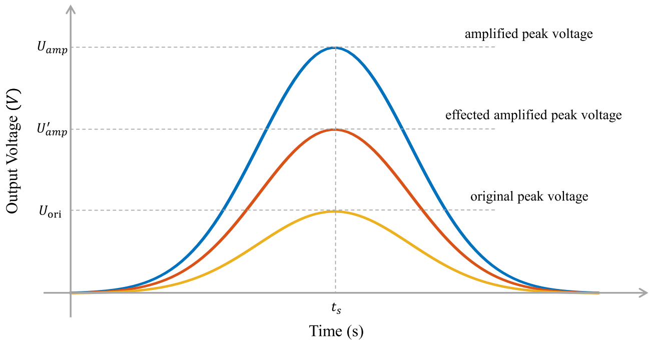

FIG. 6. Time-domain shape of an output pulse from the heterodyne detector. U_{ori}, the original peak voltage of the heterodyne detector; U_{amp}, the amplified peak voltage of the heterodyne detector; U'_{amp}, the amplified peak voltage of the heterodyne detector when a reverse external magnetic field exists; t_s, sampling time.

where $x'_{B\mathrm{amp}}$ and $p'_{B\mathrm{amp}}$ are the quadrature variables of the amplified signal light under the effect of a reverse external magnetic field.

It is noteworthy that the quadrature of the signal field is linearly proportional to the peak value of the heterodyne detector [28]. Therefore, in a practical CVQKD system with an optical amplifier, the peak value of the heterodyne detector will undergo corresponding changes under the effect of a reverse external magnetic field, which is revealed in Fig. 6.

In this section, we mainly analyze the effect of a reverse external magnetic field on the performance of the optical amplifier and the peak value of the heterodyne detector. In order to show more clearly the above effect, we will further discuss the parameter estimation and analyze the secret key rate of the system under a reverse external magnetic field in the next section.

III. SECURITY ANALYSIS

A. Modeling the system

EDFA is a member of phase-insensitive amplifiers, which can be used to simultaneously amplify the quadrature variable x and the quadrature variable p of the light field. The shaded portion of Fig. 7 shows the model of a phase-insensitive amplifier, which consists of an ideal amplifier and a two-mode squeezed vacuum [Einstein-Podolsky-Rosen (EPR)] state with variance V_0. The numerical model of the phase-insensitive amplifier is written as

$$\Upsilon^{\mathrm{PIA}} = \begin{bmatrix} \sqrt{g}I_2 & \sqrt{g-1}\sigma_z \\ \sqrt{g-1}\sigma_z & \sqrt{g}I_2 \end{bmatrix}, \tag{14}$$

where g denotes the gain coefficient of the optical amplifier and $I_2 = [\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}]$, $\sigma_z = [\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}]$. Meanwhile, the inherent noise of the optical amplifier modeled by the EPR state with variance V_0 is expressed as

$$\Upsilon^{\mathrm{noise}} = \begin{bmatrix} V_0 I_2 & \sqrt{{V_0}^2 - 1}\sigma_z \\ \sqrt{{V_0}^2 - 1}\sigma_z & V_0 I_2 \end{bmatrix}. \tag{15}$$

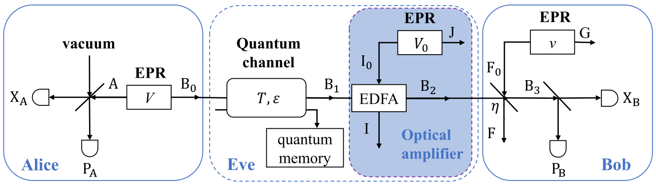

FIG. 7. EB model of a CVQKD system with an optical amplifier.

When analyzing and calculating the secret key rate of the system, we mainly use the entanglement-based (EB) model. In the EB model of a CVQKD system with an optical amplifier (see Fig. 7), Alice first prepares the EPR state with the variance $V = V_A + 1$, where V_A is Alice's modulation variance, and then measures the mode A by a heterodyne detector. Subsequently, the other mode B_0 of the EPR state is sent to the receiver Bob through the quantum channel with the transmissivity T and the excess noise ε. Due to the imperfections of the quantum channel, the noise at Bob's input is denoted as $\chi_{\mathrm{line}} = 1/T - 1 + \varepsilon$. At the receiver, the mode B_1 first enters the optical amplifier, and then after amplification by the EDFA, the mode B_2 is measured by a heterodyne detector with the detection efficiency η and the electronic noise υ_{el}. Here, we use a beam splitter with transmittance η to model the detection efficiency of the detector and an EPR state with variance υ to model the electrical noise of the detector. In addition, the detection-added noise referred to Bob's input is represented as $\chi_{\mathrm{het}}^{\mathrm{PIA}} = [1 + (1-\eta) + 2\upsilon_{\mathrm{el}} + V_0(g-1)\eta]/g\eta$, and the total noise of the CVQKD system with an optical amplifier is expressed as $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{het}}^{\mathrm{PIA}}/T$.

B. Parameter estimation under a reverse external magnetic field

After transmission and detection of the quantum state, Alice and Bob share two correlated vectors $X = \{(x_{A_i}, x_{B\mathrm{amp}_i})|i = 1, 2, \ldots, N\}$ and $P = \{(p_{A_i}, p_{B\mathrm{amp}_i})|i = 1, 2, \ldots, N\}$, where N is the total number of pulses received by Bob. The quantum channel involved in a CVQKD system conforms to a normal linear model, characterized by the following relation:

$$x_{B\mathrm{amp}} = \sqrt{g}tx_A + z, \tag{16}$$

where $t = \sqrt{\eta T}$, and vector z follows a centered normal distribution with variance $\sigma^2 = g\eta T\xi + N_0 + V_{\mathrm{el}}$. Here, N_0 is the variance of shot noise and $\xi = \varepsilon N_0$, $V_{\mathrm{el}} = \upsilon_{\mathrm{el}} N_0$. According to Eq. (16), we can obtain that x_A and $x_{B\mathrm{amp}}$ meet the following relations:

$$\langle x_A^2 \rangle = V_{x_A}, \quad \langle x_A x_{B\mathrm{amp}} \rangle = \sqrt{g\eta T}V_{x_A},$$
$$\langle x_{B\mathrm{amp}}^2 \rangle = g\eta T V_{x_A} + g\eta T\xi + N_0 + V_{\mathrm{el}}, \tag{17}$$

where $V_{x_A} = V_A N_0$ and there is no doubt that p_A and $p_{B\mathrm{amp}}$ also satisfy Eqs. (16) and (17).

In order to estimate the parameters T and ξ, Alice and Bob randomly select m ($m < N$) pairs of data from the vector X or P. The maximum-likelihood estimators $\hat{t}$ and $\hat{\sigma}^2$ are known with the normal linear model [43], i.e.,

$$\hat{t} = \frac{\sum_{i=1}^{m} x_{Ai}x_{Bi}}{\sum_{i=1}^{m} x_{Ai}^2}, \quad \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^{m}(x_{Bi} - \hat{t}x_{Ai})^2, \tag{18}$$

where $\hat{t}$ and $\hat{\sigma}^2$ are independent estimators with the following distributions:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_{Ai}^2}\right), \quad \frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \tag{19}$$

where t and σ^2 are the true values of the parameters. The χ^2 distributions will converge to a normal distribution when m is large enough (e.g., $m > 10^6$). Therefore, the confidence intervals for these estimators are $t \in [\hat{t} - \Delta t, \hat{t} + \Delta t]$ and $\sigma^2 \in [\hat{\sigma}^2 - \Delta\sigma^2, \hat{\sigma}^2 + \Delta\sigma^2]$. Here,

$$\Delta t = z_{\epsilon_{\rm PE}/2}\sqrt{\frac{\hat{\sigma}^2}{mV_{x_A}}}, \quad \Delta\sigma^2 = z_{\epsilon_{\rm PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}}, \tag{20}$$

where $\epsilon_{\rm PE}$ is the probability that the true value of the parameter is not in the confidence interval during the parameter estimation process. And erf(·) is the error function which can be expressed as

$$\mathrm{erf}(x) = 2\pi^{-\frac{1}{2}}\int_0^x e^{-t^2}dt. \tag{21}$$

By utilizing the above estimators, the quantum channel transmissivity T and excess noise ε can be estimated by

$$T = \frac{\hat{t}^2}{\eta}, \quad \varepsilon = \frac{\hat{\sigma}^2 - N_0 - v_{\rm el}N_0}{N_0\hat{t}^2}. \tag{22}$$

Based on the analysis in Sec. II C, the reverse external magnetic field affects the transmitted Gaussian-modulated coherent states, which causes the relations between vectors kept by Alice and Bob to become

$$\langle x_A^2\rangle = V_{x_A}, \quad \langle x_A x'_{B\rm amp}\rangle = \sqrt{g'\eta T}V_{x_A},$$
$$\langle (x'_{B\rm amp})^2\rangle = g'\eta T V_{x_A} + g'\eta T\xi + N_0 + V_{\rm el}. \tag{23}$$

If Alice and Bob are not aware of the existence of the reverse external magnetic field and still use Eq. (17) to estimate the parameters, they will obtain the following relations:

$$\sqrt{g\eta T'}V_{x_A} = \sqrt{g'\eta T}V_{x_A}, \quad g\eta T'V_{x_A} + g\eta T'\xi' + N_0 + V_{\rm el}$$
$$= g'\eta T V_{x_A} + g'\eta T\xi + N_0 + V_{\rm el}. \tag{24}$$

According to Eqs. (9) and (24), we can get that

$$T' = \cos^2(\Delta\theta)T, \quad \xi' = \xi. \tag{25}$$

Expressed in shot-noise units, the estimated excess noise becomes

$$\varepsilon' = \varepsilon. \tag{26}$$

Based on the analysis in Sec. III A and Eqs. (9), (25), and (26), when a reverse external magnetic field exists, the total noise of the CVQKD system with an optical amplifier can be expressed as

$$\begin{aligned}\chi_{\rm tot}^{\rm PIA} &= \frac{1}{T'} - 1 + \varepsilon' + \frac{1 + (1-\eta) + 2v_{\rm el} + V_0(g'-1)\eta}{g'\eta T'}\\ &= \frac{1}{\cos^2(\Delta\theta)T} - 1 + \varepsilon\\ &\quad + \frac{1 + (1-\eta) + 2v_{\rm el} + V_0[g\cos^2(\Delta\theta) - 1]\eta}{g\cos^2(\Delta\theta)\eta\cos^2(\Delta\theta)T}.\end{aligned} \tag{27}$$

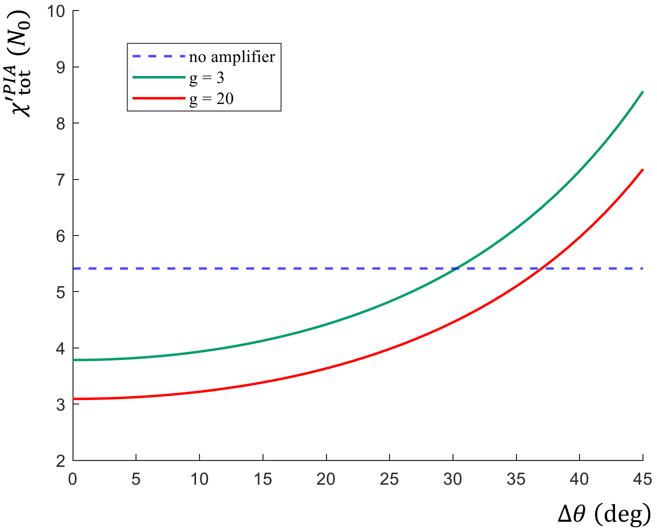

FIG. 8. Total noise vs changed angle of the magnetic rotation angle under different gain coefficients. The blue dotted line denotes the total noise of the CVQKD system without an optical amplifier.

However, when calculating the total noise of the system, if Alice and Bob are not aware of the existence of a reverse external magnetic field, they will calculate under the assumption that the optical amplifiers still perfectly amplify the received optical signal. Consequently, the total noise of the system calculated by Alice and Bob can be written as

$$\begin{aligned}\chi'^{\rm PIA}_{\rm tot} &= \frac{1}{\cos^2(\Delta\theta)T} - 1 + \varepsilon\\ &\quad + \frac{1 + (1-\eta) + 2v_{\rm el} + V_0(g-1)\eta}{g\eta\cos^2(\Delta\theta)T}.\end{aligned} \tag{28}$$

In order to show the total noise more clearly, we simulate the total noise ($\chi'^{\rm PIA}_{\rm tot}$) versus the changed angle of the magnetic rotation angle ($\Delta\theta$) under different gain coefficients of the optical amplifier (i.e., $g = 3, 20$). The fixed parameters for this simulation are set as $\eta = 0.5$, $v_{\rm el} = 0.01$, $V_0 = 1.5$, $T = 10^{-\alpha L/10}$, $\alpha = 0.2$ dB/km, $L = 10$ km, and $\varepsilon = 0.01$.

Figure 8 depicts the relationship between the total noise ($\chi'^{\rm PIA}_{\rm tot}$) and the changed angle of the magnetic rotation angle ($\Delta\theta$) under different gain coefficients (i.e., $g = 3, 20$). It is evident that in the absence of a reverse external magnetic field, i.e., $\Delta\theta = 0^\circ$, the total noise in the CVQKD system with an optical amplifier is lower than that in the CVQKD system without an optical amplifier. This explains why optical amplifiers can improve the performance of CVQKD systems. In addition, the simulation results also indicate that Eve can utilize a reverse external magnetic field to completely control the total noise calculated by Alice and Bob. These analysis results suggest that the application of a reverse external magnetic field could establish conditions for Eve to conceal her attacks in a practical CVQKD system. Subsequently, we employ the classical partial intercept-resend (PIR) attack as an illustrative example to analyze the security of a practical CVQKD system with an optical amplifier in the presence of a reverse external magnetic field.

In the PIR attack, the probability distribution of Bob's measurements is the weighted sum of two Gaussian distributions [31]. The first distribution corresponds to the intercepted resend data with a weight of μ, while the second distribution corresponds to the transmitted data with a weight of $1-\mu$. In theory, the excess noise estimated by Alice and Bob under the effects of the PIR attack should be expressed as

$$\xi_{\rm PIR} = \xi + 2\mu N_0, \tag{29}$$

where $\xi = \varepsilon N_0$ is the technical excess noise of the system and $2\mu N_0$ is the extra excess noise induced by the PIR attack. Expressed in shot-noise units, the estimated excess noise $\varepsilon_{\rm PIR}$ can be written as

$$\varepsilon_{\rm PIR} = \varepsilon + 2\mu. \tag{30}$$

Here, we use $\mu = 0.2$ as an example to analyze the PIR attack in a general situation. Correspondingly, the estimated excess noise $\varepsilon_{\rm PIR}$ becomes

$$\varepsilon_{\rm PIR} = \varepsilon + 0.4. \tag{31}$$

According to Eqs. (28) and (31), when Eve launches the PIR attack, the total noise of the system calculated by Alice and Bob can be expressed as

$$\chi'^{\rm PIA}_{{\rm tot}_{\rm PIR}} = \chi'^{\rm PIA}_{\rm tot} + 0.4. \tag{32}$$

Next, we introduce a possible attack scheme. First, we assume that the gain coefficient of the optical amplifier equals to 20 and the value of $\Delta\theta$ is set to 20°. Then, when executing the PIR attack, Eve can change the value of $\Delta\theta$ from 20° to 10° in order to reduce the increased total noise of the system. As a result, based on Eqs. (28) and (32), we can obtain that

$$\begin{aligned}\chi'^{\rm PIA}_{{\rm tot}_{\rm PIR}}(\Delta\theta = 10^\circ) &= \chi'^{\rm PIA}_{\rm tot}(\Delta\theta = 10^\circ) + 0.4\\ &< \chi'^{\rm PIA}_{\rm tot}(\Delta\theta = 20^\circ).\end{aligned} \tag{33}$$

According to Eq. (33), the noise value of 0.4 induced by the PIR attack will be concealed by Eve through manipulating the value of $\Delta\theta$. Subsequently, we will further illustrate this security loophole by calculating the secret key rate of the system in the following section.

C. Calculation of the secret key rate

Considering the reverse reconciliation and finite-size effect, the theoretical secret key rate of the GMCS CVQKD system against collective attacks can be expressed as

$$K = \frac{n}{N}\left[\beta I_{AB} - S_{BE}^{\epsilon_{\rm PE}} - \Delta(n)\right], \tag{34}$$

where $n = N - m$, β is the reverse reconciliation efficiency, I_{AB} represents the mutual information between Alice and Bob, $S_{BE}^{\epsilon_{\rm PE}}$ represents the maximal value of the Holevo information compatible with the statistics except with probability $\epsilon_{\rm PE}$, and $\Delta(n)$ is related to the security of the privacy amplification.

Subsequently, we calculate the mutual information between Alice and Bob I_{AB} in the case of heterodyne detection. And it is derived from Bob's measured variance V_B and conditional variance $V_{B|A}$ as

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

where $V = V_A + 1$ and $\chi_{\rm tot}$ is mentioned in Sec. III A.

Then, to get the mutual information between Eve and Bob $S_{BE}^{\epsilon_{\rm PE}}$, we need to calculate the covariance matrix between Alice and Bob:

$$\begin{aligned}\Upsilon_{AB} &= \begin{bmatrix}\Upsilon_A & \sigma_{AB}^T\\ \sigma_{AB} & \Upsilon_B\end{bmatrix}\\ &= \begin{bmatrix}(V_A+1)I_2 & \sqrt{T_{\min}\left(V_A^2+2V_A\right)}\sigma_z\\ \sqrt{T_{\min}\left(V_A^2+2V_A\right)}\sigma_z & [T_{\min}(V_A+\varepsilon_{\max})+1]I_2\end{bmatrix},\end{aligned} \tag{36}$$

where $I_2 = [\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}]$ and $\sigma_z = [\begin{matrix}1 & 0\\ 0 & -1\end{matrix}]$.$T_{\min}$ and $\varepsilon_{\max}$ are the lower limit of the channel transmissivity T and the upper limit of the excess noise ε, respectively. According to Ref. [43], when m is large enough (e.g., $m > 10^6$), $T_{\min}$ and $\varepsilon_{\max}$ can be calculated by

$$\begin{aligned}T_{\min} &= \frac{(\hat{t} - \Delta t)^2}{\eta},\\ \varepsilon_{\max} &= \frac{\hat{\sigma}^2 + \Delta\sigma^2 - N_0 - v_{\rm el}N_0}{\hat{t}^2 N_0},\end{aligned} \tag{37}$$

where Δt and $\Delta\sigma^2$ are defined in Eq. (20). Then, the mutual information $S_{BE}^{\epsilon_{\rm PE}}$ between Eve and Bob can be acquired by

$$S_{BE}^{\epsilon_{\rm PE}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{38}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and λ_i are the symplectic eigenvalues of the covariance matrix, which are given by

$$\begin{aligned}&\lambda_{1,2}^2 = \tfrac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right), \quad \lambda_{3,4}^2 = \tfrac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right),\\ &\lambda_5 = 1.\end{aligned} \tag{39}$$

Here,

$$\begin{aligned}A &= \det\Upsilon_A + \det\Upsilon_B + 2\det\sigma_{AB},\\ B &= \det\Upsilon_{AB},\\ C &= \frac{1}{\left[T_{\min}(V_A + \varepsilon_{\max}) + 1 + \chi_{\rm het}^{\rm PIA}\right]^2}\Big\{A\chi_{\rm het}^{\rm PIA^2} + B + 1\\ &\quad + 2\chi_{\rm het}^{\rm PIA^2}\left[(V_A + 1)\sqrt{B} + T_{\min}(V_A + \varepsilon_{\max}) + 1\right]\\ &\quad + 2T_{\min}\left({V_A}^2 + 2V_A\right)\Big\},\\ D &= \left[\frac{V_A + 1 + \sqrt{B}\chi_{\rm het}^{\rm PIA}}{T_{\min}(V_A + \varepsilon_{\max}) + 1 + \chi_{\rm het}^{\rm PIA}}\right]^2.\end{aligned} \tag{40}$$

Finally, the term $\Delta(n)$ related to the security of the privacy amplification is expressed as

$$\Delta(n) = 7\sqrt{\frac{\log_2(1/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2\frac{1}{\epsilon_{PA}}, \tag{41}$$

where $\bar{\epsilon}$ is the smoothing parameter and ϵ_{PA} is the failure probability of privacy amplification.

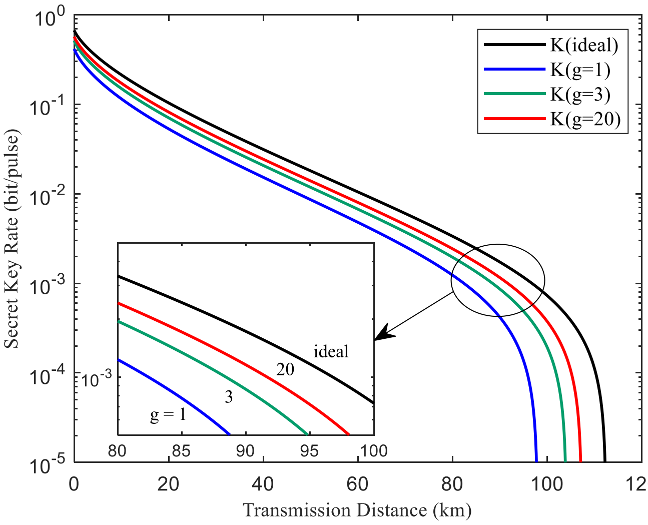

FIG. 9. Secret key rate vs transmission distance under no external reverse magnetic field. The K(ideal) curve corresponds to a perfect heterodyne detector ($\eta = 1$, $v_{\mathrm{el}} = 0$) and no amplifier.

D. Simulation and analysis

Based on the above Eqs. (34)–(41), Alice and Bob can calculate the secret key rate of the GMCS CVQKD system with an optical amplifier against collective attacks when considering reverse reconciliation and finite-size effect. In order to demonstrate clearly the effectiveness of the optical amplifier, we first simulate the relationship between the secret key rate and the transmission distance in the case of using optical amplifiers with different gain coefficients. And the fixed parameters for the simulation are set as $V_A = 4$, $\eta = 0.5$, $v_{\mathrm{el}} = 0.01$, $V_0 = 1.5$, $T = 10^{-\alpha L/10}$, $\alpha = 0.2$ dB/km, $\varepsilon = 0.01$, $\beta = 0.95$, $N = 10^9$, $n = 0.5N$, and $\bar{\epsilon} = \epsilon_{PA} = 10^{-10}$.

Figure 9 depicts the relationship between the secret key rate and the transmission distance for the practical CVQKD system with an optical amplifier under no reverse external magnetic field. The blue curve represents that the gain coefficient g of the optical amplifier is equal to 1, which is also the secret key rate curve when the optical amplifier is not placed. The green curve and the red curve are the secret key rate curves when placing an optical amplifier with the gain coefficient g equal to 3 and 20 in the optical path, respectively. Furthermore, the black curve represents the detection efficiency $\eta = 1$ and the electrical noise $v_{\mathrm{el}} = 0$ of the detector, which is also the secret key rate curve when the ideal detector is placed in the optical path. It is obvious that using optical amplifiers with different gain coefficients can compensate the imperfections of the detectors and improve the secret key rate of the system.

Subsequently, in order to demonstrate clearly the difference between the theoretical and practical evaluation of the secret key rate of the system, we also simulate the relationship between the secret key rate and the transmission distance under different intensities of the reverse external magnetic field. It is worth noting that when calculating the secret key rate under the effect of a reverse external magnetic field, the parameters g', T', and ε' defined in Eqs. (9), (25), and (26) should replace the parameters g, T, and ε involved in Eqs. (34)–(41), respectively. In particular, the larger value of $\Delta\theta$ indicates a stronger reverse external magnetic field.

Figures 10(a) and 10(b) show the relationship between the secret key rate and the transmission distance for a practical CVQKD system under different intensity of the reverse external magnetic field (i.e., $\Delta\theta = 0^\circ,\ 10^\circ,\ 20^\circ$) when the gain coefficient g of the optical amplifier is equal to 3. Figure 10(c) describes the relationship between the secret key rate and the transmission distance for a practical CVQKD system under different intensity of the reverse external magnetic field (i.e., $\Delta\theta = 0^\circ,\ 20^\circ$) when the gain coefficient g of the optical amplifier is equal to 20. For the secret key rate of the system under the effect of a reverse external magnetic field, these simulation results illustrate that the practical evaluation K_{pra} is overestimated compared with the theoretical evaluation K_{the}. It also indicates that in a practical CVQKD system with an optical amplifier, the reverse external magnetic field can open a security loophole for Eve to obtain the key information.

By comparing Figs. 10(a) and 10(b), it is observed that as the intensity of the reverse external magnetic field increases, the secret key rate of the system correspondingly decreases. In particular, the difference between K_{pra} and K_{the} reflects the information about the secret key that can be obtained by Eve. From the comparison of Figs. 10(b) and 10(c), it is evident that the smaller the gain coefficient of an optical amplifier is, the more secret key information Eve can acquire when the same intensity of the reverse external magnetic field is applied to a practical CVQKD system with an optical amplifier.

IV. COUNTERMEASURES

The above analysis shows that in a practical CVQKD system with an optical amplifier, Eve can use a reverse external magnetic field to acquire the information about the secret key. Therefore, it is necessary to monitor the external magnetic field around the system.

Figure 11 shows that we can place a real-time monitoring module in the practical optical path to monitor the polarization direction of the signal light. Specifically, when signal light enters or exits the optical amplifier, we first use a beam splitter to separate a small portion of the signal light. Then, a polarization analyzer is used to accurately measure the polarization direction of this portion and to calculate the changed value in polarization direction of the signal light after passing through the optical amplifier. Finally, we compare the changed value in the polarization direction of the signal light to the threshold. If the changed value in the polarization direction exceeds the threshold, we can determine that there may be a reverse external magnetic field affecting the normal communication.

Furthermore, in a practical CVQKD system with an optical amplifier, we can also use Hall elements to monitor the external magnetic field. And the Hall element is a magnetic sensor based on the Hall effect. When the current perpendicular to the magnetic field passes through the Hall element, a stable voltage difference (known as the Hall voltage) is generated in the direction perpendicular to both the magnetic field and the current. Because the Hall voltage is proportional to the

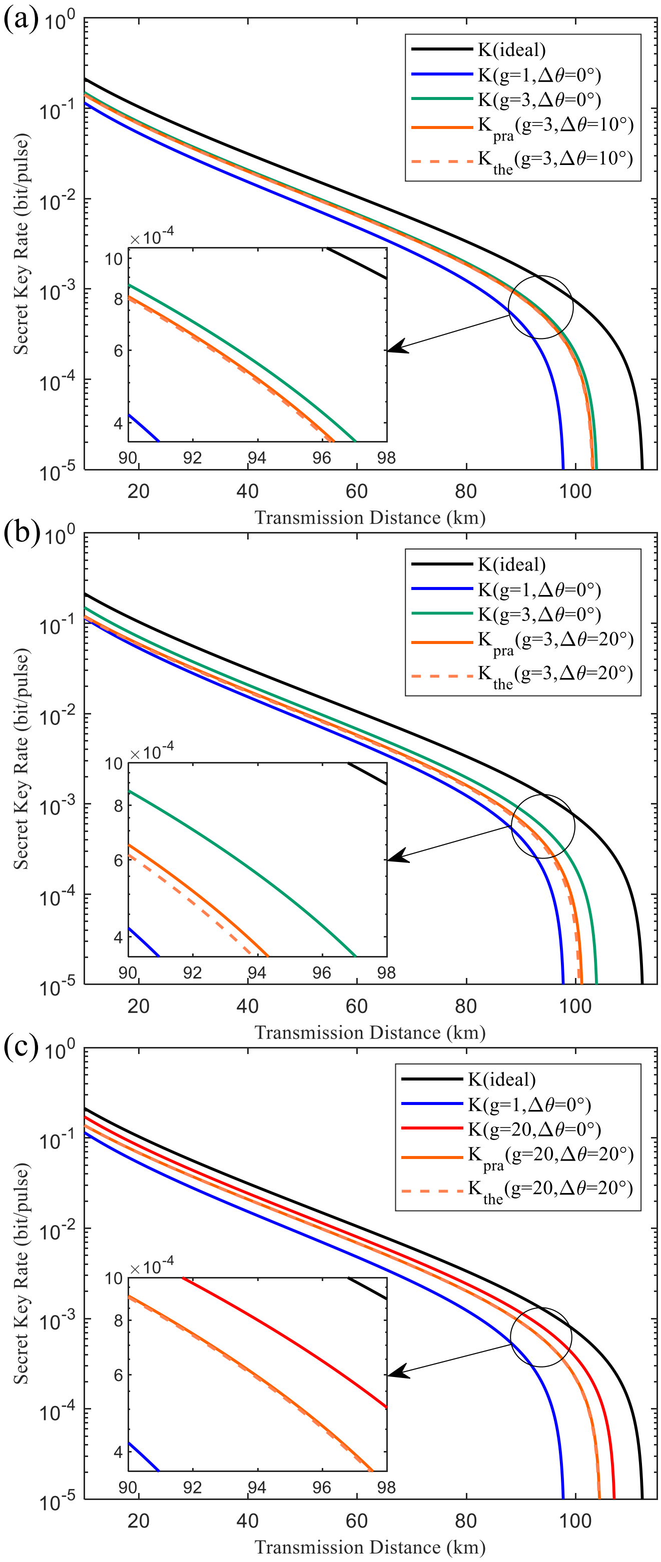

FIG. 10. Secret key rate vs transmission distance under a reverse external magnetic field when the gain coefficient g of an optical amplifier is equal to 3 and 20. K_{pra}, the practical evaluation of the secret key rate; K_{the}, the theoretical evaluation of the secret key rate.

intensity of the magnetic field, the Hall element can also be used to detect the existence and intensity of the external magnetic field.

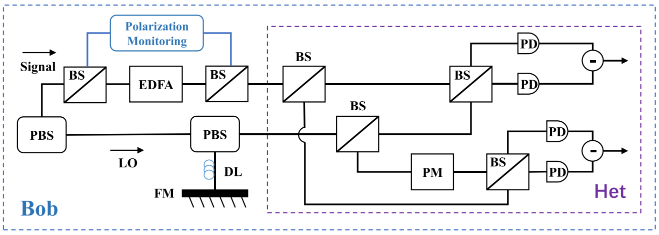

FIG. 11. Optical path of a real-time monitoring module for a practical CVQKD system with an optical amplifier.

Due to the fact that the magneto-optical isolator of a CVQKD system with an optical amplifier operates based on the Faraday effect, a reverse external magnetic field can have an impact on the amplification performance of the optical amplifier, which will threaten the practical security of the system. Therefore, we propose to compensate this imperfection by replacing the magneto-optical isolator with a nonmagnetic optical isolator.

V. CONCLUSION

We have investigated the effect of a reverse external magnetic field on a practical CVQKD system with an optical amplifier. We reveal that using an optical amplifier to compensate the imperfection of the detectors cannot achieve the preset effect when a reverse external magnetic field exists. In addition, we find that if the legitimate communicating parties are not aware of the existence of the reverse external magnetic field, the evaluation of the secret key rate of the system will be overestimated, which will open a security loophole for Eve in a practical CVQKD system with an optical amplifier. The simulation results indicate that, in a practical CVQKD system with an optical amplifier, the smaller the gain coefficient of the optical amplifier is, the more secret key information Eve can acquire when the same intensity of the reverse external magnetic field is applied. Moreover, as the intensity of the reverse external magnetic field further increases, the secret key rate of the system correspondingly decreases. In order to close the security loophole caused by the reverse external magnetic field, we propose three countermeasures. First, we can place a real-time monitoring module for the value of change in polarization direction of the signal light. And through the comparison and analysis of the value of change in the polarization direction, we can judge whether there is a reverse external magnetic field around the system. Secondly, we can also determine the existence and intensity of a reverse external magnetic field in a practical CVQKD system with an optical amplifier by using Hall elements. Lastly, we propose that a nonmagnetic optical isolator can be used to replace the magneto-optical isolator in the optical amplifier. These countermeasures can help us to monitor the reverse external magnetic fields and change the type of optical isolator, which will effectively close the security loophole caused by the reverse external magnetic field.

ACKNOWLEDGMENTS

This work was supported by the Joint Funds of the National Natural Science Foundation of China under Grant

No. U22B2025, Key Research and Development Program of Shaanxi under Grant No. 2024GX-YBXM-077, and the Fundamental Research Funds for the Central Universities under Grant No. D5000210764.

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptology **5**, 3 (1992).

[2] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opti. Photon. **12**, 1012 (2020).

[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[5] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[6] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

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

[8] R. Renner, Security of quantum key distribution, Int. J. Quantum Inform. **06**, 1 (2008).

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[10] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, Phys. Rev. A **76**, 052323 (2007).

[11] P. Huang, T. Wang, R. Chen, P. Wang, Y. Zhou, and G. Zeng, Experimental continuous-variable quantum key distribution using a thermal source, New J. Phys. **23**, 113028 (2021).

[12] M. Zhang, P. Huang, P. Wang, S. Wei, and G. Zeng, Experimental free-space continuous-variable quantum key distribution with thermal source, Opt. Lett. **48**, 1184 (2023).

[13] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Security of continuous-variable quantum key distribution against canonical attacks, in *Proceedings of the 2021 International Conference on Computer Communications and Networks* (IEEE, New York, 2021), pp. 1–6.

[14] N. Jain, H.-M. Chin, H. Mani, C. Lupo, Dino S. Nikolic, A. Kordts, S. Pirandola, Thomas B. Pedersen, M. Kolb, B. Ömer *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).

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

[16] Y. 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).

[17] T. Wang, P. Huang, L. Li, Y. Zhou, and G. Zeng, High key rate continuous-variable quantum key distribution using telecom optical components, New J. Phys. **26**, 023002 (2024).

[18] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, Phys. Rev. Res. **3**, 043014 (2021).

[19] F. Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 057902 (2002).

[20] F. Grosshans, Collective attacks and unconditional security in continuous variable quantum key distribution, Phys. Rev. Lett. **94**, 020504 (2005).

[21] M. Navascués and A. Acín, Security bounds for continuous variables quantum key distribution, Phys. Rev. Lett. **94**, 020505 (2005).

[22] S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[23] F. Xu, X. Ma, Q. Zhang, Hoi-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[24] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 16025 (2016).

[25] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: A review and perspective, arXiv:2310.04831.

[26] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, Phys. Rev. A **94**, 012325 (2016).

[27] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, Phys. Rev. A **98**, 012312 (2018).

[28] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects, Phys. Rev. A **93**, 022315 (2016).

[29] C. Xie, Y. Guo, Q. Liao, W. Zhao, D. Huang, L. Zhang, and G. Zeng, Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization, Phys. Lett. A **382**, 811 (2018).

[30] L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, Quantum hacking against discrete-modulated continuous-variable quantum key distribution using modified local oscillator intensity attack with random fluctuations, Phys. Rev. Appl. **20**, 024073 (2023).

[31] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, Phys. Rev. A **87**, 062313 (2013).

[32] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, Polarization attack on continuous-variable quantum key distribution, J. Phys. B **52**, 015501 (2018).

[33] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052301 (2014).

[34] Yi-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution using squeezed states, Phys. Rev. A **90**, 052325 (2014).

[35] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, Optica **9**, 492 (2022).

[36] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation, Opt. Express **28**, 32882 (2020).

[37] S. Ren, S. Yang, A. Wonfor, I. White, and R. Penty, Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator, Sci. Rep. **11**, 9454 (2021).

[38] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B **42**, 114014 (2009).

[39] Y. Guo, R. Li, Q. Liao, J. Zhou, and D. Huang, Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier, Phys. Lett. A **382**, 372 (2018).

[40] H. Tan, W.-Y. Zhang, L. Zhang, W. Li, Sheng-K. Liao, and F. Xu, External magnetic effect for the security of practical quantum key distribution, Quantum Sci. Technol. **7**, 045008 (2022).

[41] J. A. Bebawi, I. Kandas, M. A. El-Osairy, and M. H. Aly, A comprehensive study on EDFA characteristics: Temperature impact, Appl. Sci. **8**, 1640 (2018).

[42] A. Malakzadeh, R. Pashaie, and M. Mansoursamaei, Gain and noise figure performance of an EDFA pumped at 980 nm or 1480 nm for DOFSs, Opt. Quantum Elect. **52**, 1 (2020).

[43] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).