Source monitoring for plug-and-play continuous-variable quantum key distribution

Yun Shao,[1] Yan Pan,[1] Heng Wang,[1] Ao Sun,[1] Zhiwang Gan,[2] Yaodi Pi,[1] Ting Ye,[1] Jinlu Liu,[1] Yang Li,[1] Yichen Zhang,[3] Wei Huang,[1,*] and Bingjie Xu[1,†]

[1] *National Key Laboratory of Security Communication, Institute of Southwestern Communication, Chengdu 610041, China*

[2] *China Electronics Technology Group Corporation, Beijing 100876, China*

[3] *State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*

(Received 15 December 2023; revised 22 April 2024; accepted 25 July 2024; published 12 August 2024)

Continuous-variable quantum key distribution (CV-QKD) with plug-and-play design offers a promising route in simplifying the system implementation and shows intriguing prospects for quantum access network applications. However, such a scheme makes it possible for the eavesdropper (Eve) to completely control the source, helping her to gain more information since the laser travels through the unsecured channel before being modulated, which will severely compromise the performance of the system and limit its potential application. To fight against the security loophole, we propose a passive source monitoring scheme based on a combination of beam splitter and homodyne detector, as well as source noise suppression. The corresponding entanglement-based model is established to estimate the secret key rate for the proposed scheme. We show that the performance of the plug-and-play CV-QKD system can be significantly improved by using the source monitoring scheme compared with the untrusted source model. With typical parameters, the maximum transmission distance can be promoted by more than 50%, and the secret key rate can be increased by more than 25% when the transmission distance is longer than 50 km. This study provides a feasible approach for improving the security and performance of the plug-and-play CV-QKD and holds positive potential for practical applications.

DOI: 10.1103/PhysRevApplied.22.024033

I. INTRODUCTION

In the past decades, considerable attention has been paid to quantum key distribution (QKD) [1,2], which provides unconditional communication security based on the fundamental laws of physics, such as quantum no-cloning theorem and Heisenberg's uncertainty principle. In general, QKD protocols can be essentially divided into two categories: the discrete variable (DV) protocol and the continuous-variable (CV) protocol. In the DV-QKD protocol, the information is encoded into the polarization or phase of weak coherent states and decoded by single-photon detection. The CV-QKD protocol has been spotlighted as another promising protocol due to its potential low cost and compatibility with modern optical communication networks, in which the key information is encoded in quadratures of the quantized electromagnetic field and decoded by coherent detection. In recent years, CV-QKD has attracted extensive interest and encouraging progress has been made in the laboratory [3–18], field tests [19], and integrated implementations [20], as well as quantum access network [21–25]. Additionally, a considerable amount of literature has been carried out in the research of both theoretical security [11,26–29] and practical security [30–38] for CV-QKD.

Despite enormous progress in the field of CV-QKD, developing sufficiently compact schemes in practical applications of integrated photonics and quantum access networks still requires further research. CV-QKD with plug-and-play design [39] has emerged as an interesting candidate because it can automatically compensate for polarization drift and phase jitter, avoiding the stabilizing of the relative frequencies of two free-running lasers, which are necessary in the case of a local local oscillator (LO) CV-QKD scheme [7–9], and have intriguing prospects in quantum secret sharing [40] and quantum access networks [23]. For example, in the case of an $1 \rightarrow N$ quantum access network [23], the laser generated from Bob is sent to several quantum network user units (Alices) through a single optical fiber and a multiplex beam splitter. After receiving the laser signal, each Alice

*Contact author: huangwei096505@aliyun.com
†Contact author: xbjpku@pku.edu.cn

modulates the quantum signal independently and transmits the coherent states back to Bob via wavelength-division multiplexing or frequency-division multiplexing technologies. One can find that a simple optical structure and low excess noise implementation are provided for the quantum access network.

Initially, a plug-and-play CV-QKD scheme based on dual-phase modulated coherent states was proposed and demonstrated [39], which nevertheless exhibits a high Rayleigh back-scattering noise resulting from the fiber refractive index inhomogeneities. Recently, in order to reduce the Rayleigh back-scattering, such a scheme was further extended to a new case with two-way communication [41]. In this case, the distribution of the laser signal from Bob to Alice (referred to as the first delivery) and the transmission of the quantum signal after modulation from Alice to Bob (referred to as the second delivery) are realized through two independent optical fibers, respectively. The source noise in the above schemes is considered to be untrusted, which inevitably limits the secret key rate (SKR) and transmission distance of the plug-and-play CV-QKD system. More recently, a trusted equipment noise model for plug-and-play CV-QKD scheme was considered [42], where it is assumed that the noise of the first delivery and the noise of the receiver cannot be manipulated by Eve but only affect the Holevo bound. Nevertheless, this approach may lead to an overestimation of the SKR.

A challenging security problem originating from the configuration of the plug-and-play CV-QKD scheme is the first delivery of the laser that travels through the unsecured channel, which makes the CV-QKD system potentially vulnerable to the Trojan-horse attack [43,44] and makes it possible for the eavesdropper to obtain more side information. Although some prior works paid attention to the untrusted source and source monitoring issues in the QKD system [45–48], there are few studies on the plug-and-play CV-QKD system. Therefore, it is worthwhile devoting much effort to improving the performance and practical security of the plug-and-play CV-QKD system.

Here, we propose a real-time source monitoring scheme for the plug-and-play CV-QKD system, where the characteristic of the untrusted source noise is monitored by homodyne (or heterodyne) detection of a fraction of the quantum signal separated from a passive beam splitter. Based on the monitoring result, a variable-optical attenuator (VOA) is used to strongly suppress the excess noise caused by Eve's intervention on the laser source before the quantum signal enters the insecure quantum channel. Then, we establish the corresponding entanglement-based model to estimate the SKR for the proposed scheme. For the first time, it is quantitatively shown that monitoring the source noise of the plug-and-play CV-QKD system is of paramount importance, as our scheme can markedly improve the system's performance and practical security. The proposed scheme is helpful for the implication of CV-QKD in quantum secret sharing and quantum access networks.

This article is organized as follows. In Sec. II, we present a brief description of the schematic of the plug-and-play CV-QKD scheme with source monitoring. In Sec. III, we establish the entanglement-based model for the source noise monitoring scheme and compare the performance with that of the untrusted source noise model and the trusted source model. The results and discussions are presented in Sec. IV. Finally, we summarize the main results of our work.

II. THE PLUG-AND-PLAY CV-QKD SCHEME

The specific CV-QKD protocol adopted in this paper is the Gaussian-modulated coherent states (GMCS) protocol based on homodyne detection [5,6]. In Fig. 1, we present the experimental schematic of the designed plug-and-play GMCS CV-QKD system, including source monitoring on Alice's side. The laser is derived from a narrow line-width laser on Bob's side. Then, the strong optical carrier is split into two beams using a beam splitter (BS), of which one part is distributed from Bob to Alice through the optical fiber channel, and the other part behaves as an LO for homodyne (or heterodyne) detection of the quantum signal. This implementation has two advantages. Firstly, it avoids stabilizing the relative frequencies of two free-running lasers between the sender and the receiver, which is needed in the local LO CV-QKD system. Secondly, the locally generated LO eliminates the LO attacks.

To facilitate modulation and coherent detection of the signal, an optical circulator (OC) is arranged at Bob's output and Alice's input. On Alice's input, a beam splitter with a high-intensity ratio is used to split the laser carrier into a strong phase reference and a weak signal. Afterward, the weak signal propagates through a BS and is rotated by 90° after being reflected by a Faraday mirror (FM), which is composed of a 45° Faraday rotator and a reflection mirror. Notice that, in the plug-and-play scheme, the adoption of the FM can automatically compensate for any birefringence effect in the fiber channel after the forward and backward propagation, where the polarization of the outgoing state is orthogonal to that of the incoming state. Subsequently, the Gaussian-modulated coherent states $|x_A + ip_A\rangle$ are produced by modulating the amplitude and phase of the signal, in which x_A and p_A are two independent Gaussian random variables with zero mean and a variance of $V_A N_0$. Here, V_A and N_0 denote the modulation variance and the shot noise variance, respectively. All noise variances in this paper are expressed in shot noise units in the following.

To prevent potential Trojan-horse attacks, filters should be inserted at the input of Alice to ensure a single mode condition; a passive BS combined with a homodyne (or heterodyne) detector is used to monitor the variance of

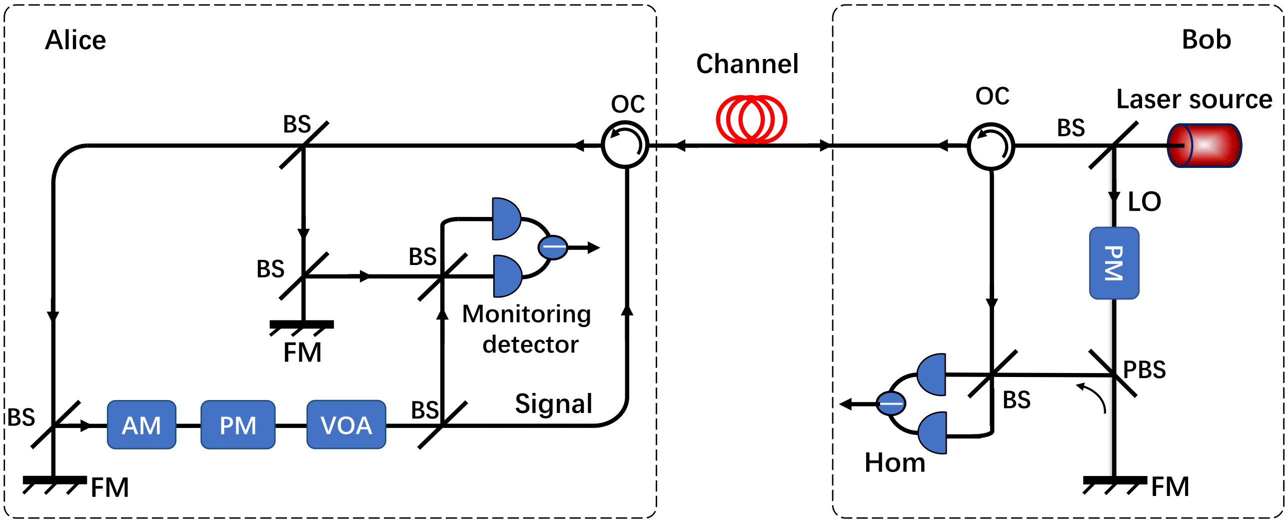

FIG. 1. Schematic illustration of the GMCS plug-and-play CV-QKD scheme with source monitoring. Here, AM is the amplitude modulator, PM is the phase modulator, VOA is the variable-optical attenuator, BS is the beam splitter, PBC is the polarization beam splitter, LO is the local oscillator, OC is the optical circulator, and FM is the faraday mirror.

the source noise on Alice's side. In this case, a fraction of the quantum signal interferes with the strong phase reference reflected by an FM on a balanced homodyne detector. Moreover, Alice uses a VOA before the BS to control the modulation variance of the quantum signal. Then, the quantum signal is transmitted back to Bob's side.

After the quantum signal propagates through the quantum channel, it interferes with the LO reflected by an FM on Bob's homodyne detector. Finally, Alice and Bob share a partially correlated Gaussian random variable after the phase compensation, based on which they can obtain the final secret key after parameter estimation, error correction, and privacy amplification.

III. THEORETICAL MODEL

Based on the framework of the plug-and-play CV-QKD scheme, the first delivery of the laser source from Bob to Alice makes it exposed to the risks of Eve's attack, that is, Eve can obtain more information by controlling or even preparing the source input for Alice. In this scheme, the source noise ε_S can be mainly decomposed into two parts based on its origin: one part is $\varepsilon_S^{\text{Eve}}$ resulting from the laser generation or from Eve's intervention, and the other part is ε_M introduced by Alice's imperfect modulation, so that $\varepsilon_S = \varepsilon_S^{\text{Eve}} + \varepsilon_M$.

In this section, we propose a source monitoring scheme for the plug-and-play CV-QKD scheme as a countermeasure of the untrusted source. The security analysis in the following is presented in the case of reverse reconciliation under general collective attack.

A. Untrusted source with source monitoring

The plug-and-play CV-QKD scheme under the untrusted source with source monitoring is shown in Fig. 2(a), where the source is completely controlled by Eve. It means that the source noise is unknown and untrusted. The legitimate communication parties can determine the source noise directly from the monitoring results and make the corresponding countermeasures. To simplify the security analysis, the corresponding entanglement-based model is shown in Fig. 2(b). In this case, Alice's quantum state preparation is modeled by an interference of two Einstein-Podolsky-Rosen (EPR) states. One EPR state with variance V_S is controlled by Eve (which models the untrusted source), and the other EPR state with variance $V = V_A + 1$ is controlled by Alice (which models the modulation process). One mode of Alice's EPR state is heterodyne detected, while the other one is directed into the BS. The interference state B_1 corresponds to the state sent to Bob through an insecure quantum channel. The additive phase-insensitive noise ε_S is used to characterize the untrusted source noise, which can be modeled by coupling one mode of an EPR state with variance V_S to the modulation signal via a beam splitter with transmittance $T_S \to 1$ [48–52]. The variance satisfies $V_S = 1 + T_S\varepsilon_S/(1 - T_S)$, and the total source-added noise referring to the channel input can be defined as $\chi_S = 1/T_S - 1 + \varepsilon_S$.

In the source monitoring scheme, a passive beam splitter combined with a homodyne (or heterodyne) detector is used to monitor the source noise on Alice's side. In practical implementation, Alice can obtain the sampled voltage value after the interference between the phase reference and the separated quantum signal, based on which Alice can receive the measured variance of the quadrature

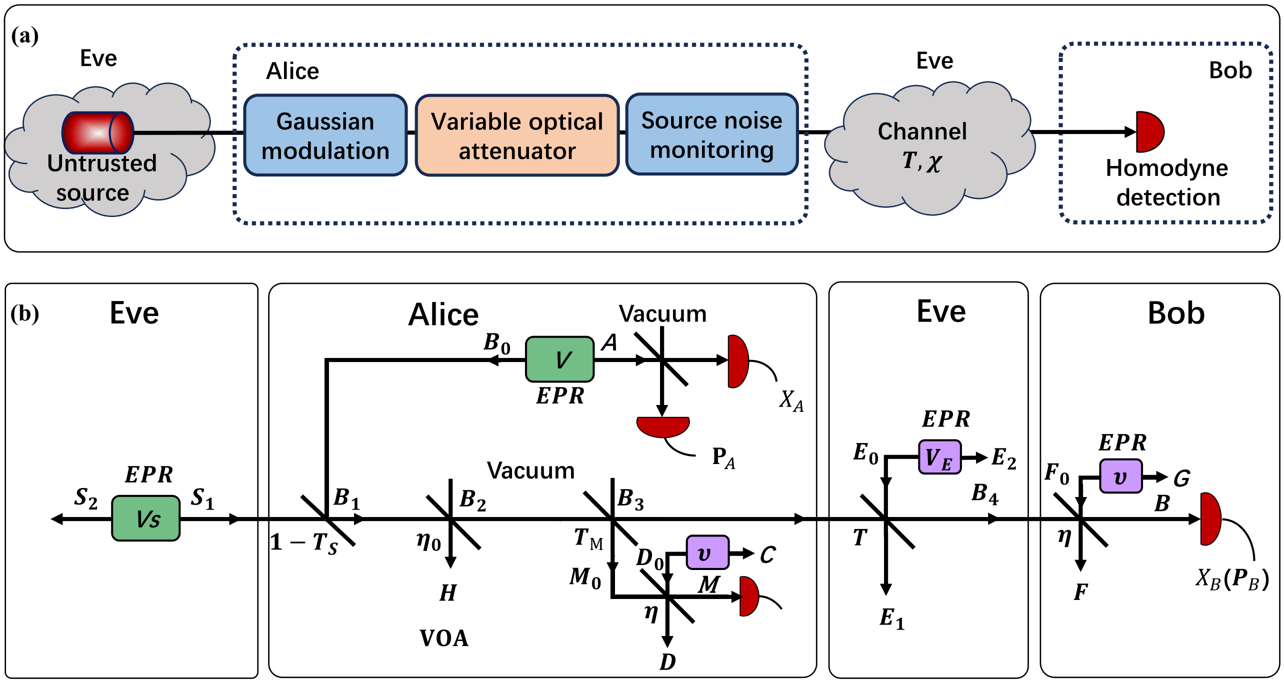

FIG. 2. (a) Simplified schematic of the prepare-and-measure model and (b) the corresponding entanglement-based model for the plug-and-play CV-QKD system with source monitoring. A passive beam splitter combined with a homodyne or heterodyne detection is used to monitor the statistical characteristics of the untrusted source, while a VOA is used to strongly attenuate the modulation variance according to the monitoring results, so as to suppress the untrusted excess noise caused by Eve's intercept on the distribution of the laser from Bob to Alice. The untrusted source noise can be simulated by coupling one-half of the EPR state with variance V_S to the signal state via a beam splitter with transmission $T_S \to 1$. The channel excess noise can be modeled by coupling one-half of the EPR state with variance V_E to the quantum channel via a beam splitter with channel transmittance T. The detector noise can be modeled by coupling one-half of the EPR state with variance υ to the input port of the beam splitter with transmission η on Bob's side.

variable of the quantum signal [53,54]. The source noise, except for the modulation noise, is completely controlled by Eve; the system performance of the plug-and-play CV-QKD is, thus, dramatically limited. One can suppress the noise caused by Eve's intervention on the laser source by first introducing a large modulation variance for the input signal, much larger than the noise introduced by Eve, and then performing a strong attenuation on the signal by a VOA, so that Eve's accessible information on the untrusted source is severely restricted. Apparently, after attenuating, the modulation variance and modulation noise are reduced to normal values, while the untrusted source noise controlled by Eve is attenuated to a very small value.

In the process of quantum signal transmission, the excess noise introduced by Eve can be simulated by coupling one-half of the EPR state with variance V_E to the signal state via a beam splitter with transmittance T, which satisfies $V_E = 1 + T\varepsilon/(1-T)$, with ε being the channel excess noise referred to as the channel input. Moreover, an EPR state is used to model the detector's electronic noise with variance $\upsilon = 1 + \upsilon_{el}/(1-\eta)$, with υ_{el} and η being the electronic noise and detection efficiency of the detector, respectively.

In the source monitoring model, the system $E_1E_2S_1S_2$ is controlled by Eve, as shown in Fig. 2(b). Hence, the corresponding asymptotic SKR for the plug-and-play CV-QKD system with the untrusted source is given by

$$K = \beta I(A:B) - \chi(B:E_1E_2S_1S_2), \tag{1}$$

where β is the reconciliation efficiency and $I(A:B)$ is the mutual information between Alice and Bob given by $I(A:B) = H(B) - H(B|A)$, with $H(B) = 1/2\log_2 V_B$ as the Shannon entropy (classical entropy) and $H(B|A) = 1/2\log_2 V_{B|A}$ as the conditional Shannon entropy, namely,

$$I(A:B) = \frac{1}{2}\log_2\frac{V_B}{V_{B|A}}, \tag{2}$$

which can be derived from Bob's variance V_B and the conditional variance $V_{B|A}$.

The maximum information available to Eve on Bob's raw key is upper bounded by the Holevo quantity [6], i.e.,

$$\chi(B:E_1E_2S_1S_2 = S(\rho_{E_1E_2S_1S_2}) - \int dm_B p(m_B) S(\rho^{m_B}_{E_1E_2S_1S_2}), \tag{3}$$

where $m_B = x_B$ or p_B denotes the homodyne measurement result of Bob, $S(\rho)$ is the Von Neumann entropy (quantum entropy) of the quantum sate ρ, $p(m_B)$ is the probability distribution of Bob's measurement outcome m_B, and $\rho^{m_B}_{E_1E_2S_1S_2}$ is the quantum state held by Eve conditional on Bob's measurement outcome m_B.

As depicted in Fig. 2(b), in the source monitoring scheme, Eve's system $E_1E_2S_1S_2$ purifies the system $HMDCAB_4$, and Eve can purify the system $HMDCAFG$ after Bob's measurement. The Holevo quantity in Eq. (3) becomes

$$\chi(B:E_1E_2S_1S_2) = S(\rho_{HDMCAB_4}) - S(\rho^{m_B}_{HDMCAFG}), \quad (4)$$

where $S(\rho_{HMDCAB_4})$ and $S(\rho^{m_B}_{HMDCAFG})$ can be calculated from the symplectic eigenvalues of the covariance matrices γ_{HMDCAB_4} and $\gamma^{m_B}_{HMDCAFG}$, respectively.

The process of deriving the above two covariance matrices is as follows. First, a VOA with variable transmittance η_0 is used to attenuate the signal to an appropriate value based on the measurement result of the source monitoring setup, and the covariance matrix becomes

$$\gamma_{AB_2H} = (Y^{BS_1})^{\mathrm{T}}(\gamma_{AB_1} \oplus \mathbb{I}_\upsilon)Y^{BS_1}, \quad (5)$$

with $Y^{BS_1} = I_A \oplus S^{BS}_{\eta_0}$, and $S^{BS}_{\eta_0}$ as the matrix that couples a fraction of the signal with a vacuum state, which can be written as

$$S^{BS}_{\eta_0} = \begin{bmatrix} \sqrt{\eta_0}\,\mathbb{I} & \sqrt{1-\eta_0}\,\mathbb{I} \\ -\sqrt{1-\eta_0}\,\mathbb{I} & \sqrt{\eta_0}\,\mathbb{I} \end{bmatrix}. \quad (6)$$

Therefore, the covariance matrix γ_{AB_2H} can be written as

$$\gamma_{AB_2H} = \begin{bmatrix} V\,\mathbb{I} & \sqrt{\eta_0 T_S(V^2-1)}\,\sigma_Z & \sqrt{(1-\eta_0)T_S(V^2-1)}\,\sigma_Z \\ \sqrt{\eta_0 T_S(V^2-1)}\,\sigma_Z & [\eta_0 T_S V + \eta_0(1-T_S)V_S + (1-\eta_0)]\,\mathbb{I} & \sqrt{\eta_0(1-\eta_0)}[T_S V + (1-T_S)V_S - 1]\,\mathbb{I} \\ \sqrt{(1-\eta_0)T_S(V^2-1)}\,\sigma_Z & \sqrt{\eta_0(1-\eta_0)}[T_S V + (1-T_S)V_S - 1]\,\mathbb{I} & [(1-\eta_0)T_S V + (1-\eta_0)(1-T_S)V_S + \eta_0]\,\mathbb{I} \end{bmatrix}. \quad (7)$$

For the source monitoring, a beam splitter with transmission T_M is used to split the mode B_2 into two modes. The mode M_0 is monitored, while the mode B_3 is sent to Bob. The covariance matrix after the beam splitter is given by

$$\gamma_{HAB_3M_0} = (Y^{BS_2})^{\mathrm{T}}(\gamma_{HAB_2} \oplus \mathbb{I}_\upsilon)Y^{BS_1}, \quad (8)$$

with $Y^{BS_2} = I_H \oplus I_A \oplus S^{BS}_{T_M}$. The covariance matrix γ_{HAB_2} can be derived from Eq. (7) and S^{BS}_{TM} is the matrix that couples a fraction of the signal with a vacuum state, which can be written as

$$S^{BS}_{TM} = \begin{bmatrix} \sqrt{T_M}\,\mathbb{I} & \sqrt{1-T_M}\,\mathbb{I} \\ -\sqrt{1-T_M}\,\mathbb{I} & \sqrt{T_M}\,\mathbb{I} \end{bmatrix}. \quad (9)$$

The covariance matrix characterizing the state after Alice's monitoring measurement is given by

$$\gamma_{HAB_3MDC} = (Y^{BS_3})^{\mathrm{T}}(\gamma_{HAB_3M_0} \oplus \gamma_{D_0C})Y^{BS_3}, \quad (10)$$

with $Y^{BS_3} = I_H \oplus I_A \oplus I_{B_3} \oplus S^{BS}_{M_0D_0} \oplus I_C$, $\gamma_{D_0C} = \gamma_{F_0G}$, and $S^{BS}_{M_0D_0} = S^{BS}_{B_4F_0}$.

The covariance matrix corresponding to the state after transmitting through the quantum channel can be expressed as

$$\gamma_{HMDCAB_4E_1E_2} = (Y^{BS_4})^{\mathrm{T}}(\gamma_{HMDCAB_3} \oplus \gamma_{E_0E_2})Y^{BS_4}, \quad (11)$$

where γ_{HMDCAB_3} can be derived from rearranging the lines and columns of the matrix γ_{HAB_3MDC}, and $Y^{BS_4} = I_H \oplus I_M \oplus I_D \oplus I_C \oplus I_A \oplus S^{BS}_{B_3E_0} \oplus I_{E_2}$. To this end, the covariance matrix γ_{HMDCAB_4} can be obtained.

Second, after Bob's projective measurement, the covariance matrix of the state can be given by

$$\gamma_{HMDCABFG} = (Y^{BS_5})^{\mathrm{T}}(\gamma_{HMDCAB_4} \oplus \gamma_{F_0G})Y^{BS_5}, \quad (12)$$

where $Y^{BS_5} = I_H \oplus I_D \oplus I_M \oplus I_C \oplus I_A \oplus S^{BS}_{B_4F_0} \oplus I_G$. To calculate the second term of Eq. (4), we need to calculate the symplectic eigenvalues of the covariance matrix $\gamma^{m_B}_{HMDCAFG}$, which can be written as

$$\gamma^{m_B}_{HMDCAFG} = \gamma_{HMDCAFG} - \sigma^{\mathrm{T}}_{HMDCAFGB} H \sigma_{HMDCAFGB}, \quad (13)$$

where $H = (X\gamma_B X)^{\mathrm{MP}}$ is the symplectic matrix that represents the homodyne measurement on mode B, with $X = \mathrm{Diag}(1,0)$, and MP stands for the Moore-Penrose inverse of a matrix. The matrices $\gamma_{HMDCAFG}$, $\sigma^{\mathrm{T}}_{HMDCAFGB}$, and γ_B are the submatrices of the covariance matrix $\gamma_{HMDCAFGB}$, with

$$\gamma_{HMDCAFGB} = \begin{bmatrix} \gamma_{HMDCAFG} & \sigma^{\mathrm{T}}_{HMDCAFGB} \\ \sigma_{HMDCAFGB} & \gamma_B \end{bmatrix}, \qquad (14)$$

which can be derived from the transformation of the matrix $\gamma_{HMDCABFG}$ in Eq. (12).

Thus, Eq. (4) can be expressed as

$$\chi(B:E) = \sum_{i=1}^{6} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=7}^{13} G\left(\frac{\lambda_i - 1}{2}\right). \qquad (15)$$

Here, $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ is the bosonic entropic function. The symplectic eigenvalues can be found using Williamson's form of a covariance matrix. In fact, for any N-mode covariance matrix γ, there exists a symplectic transmission S that can perform a symplectic diagonalization so that

$$S\gamma S^{\mathrm{T}} = \bigoplus_{i=1}^{N} \begin{bmatrix} \lambda_i & 0 \\ 0 & \lambda_i \end{bmatrix}, \qquad (16)$$

where λ_i is the symplectic eigenvalues of the matrix $|i\Omega\gamma|$, with Ω being the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \qquad (17)$$

At this point, the Holevo bound can be calculated. Therefore, one can obtain the asymptotic SKR under the source monitoring from Eqs. (1), (2), and (15). We provide a detailed security analysis of the plug-and-play CV-QKD scheme under the untrusted source model in Appendix A and the trusted model in Appendix B.

IV. RESULTS AND DISCUSSION

Based on the theoretical models described above, we present the numerical simulations in the asymptotical limit. Typical parameters used for practical scenarios are chosen: the channel attenuation coefficient $\alpha = 0.2$ dB/km, the channel transmittance $T = 10^{-\alpha L/10}$, the detection efficiency $\eta = 0.5$, the detector's electronic noise $\upsilon_{el} = 0.1$, the reconciliation efficiency $\beta = 0.95$, the modulation variance $V_A = 4$, and the channel excess noise $\varepsilon = 0.04$. Moreover, the transmittance of the beam splitter used to couple the noise with the signal is set at $T_S = 0.99$, and the transmittance of the beam splitter for monitoring the source noise is set at $T_M = 0.5$.

Figure 3 shows the simulation results of SKR with respect to transmission distance under the untrusted source model (black dash-dotted line) and source monitoring model (green dashed line). Here, the parameters characterizing the source noise are set at $\varepsilon_M = 0.01$ and $\varepsilon_S^{\mathrm{Eve}} = 0.02$. One can find that the system performance under the source monitoring model is significantly improved in comparison with that under the untrusted source model. With the above system parameters, the maximum transmission distance is anticipated to be promoted by over 50%, and the SKR is increased by more than 25% and 100% when the transmission distance is longer than 50 and 65 km, respectively. Note that no SKR can be generated when the transmission distance exceeds 92 km with an untrusted source. The above results are due to the fact that, with the untrusted source model, the source noise is all ascribed to Eve, which may pose an overestimation of Eve's information, thereby limiting the system performance. In the source monitoring model with a strong modulation regime, the source noise $\varepsilon_S^{\mathrm{Eve}}$ introduced by Eve can be heavily suppressed by attenuation of the signal. As a comparison, we further calculate the SKR under the assumption that the source noise is trusted, as depicted by the red dotted line in Fig. 3. Here, the source noise is considered to be out of Eve's control and can be calibrated by the trusted parties, which renders an optimistic overestimation of the system performance.

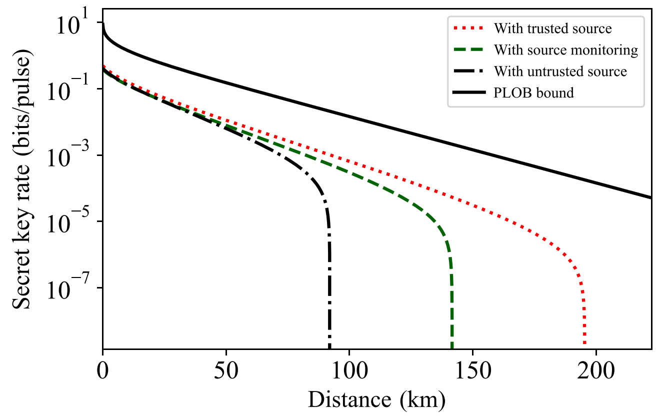

FIG. 3. Simulation secret key rate results for the plug-and-play CV-QKD scheme under the untrusted source model (black dash-dotted line), the source monitoring model (green dashed line), and the trusted source model (red dotted line). The black solid line corresponds to the standard PLOB bound [55]. The source noises are set at $\varepsilon_M = 0.01$ and $\varepsilon_S^{\mathrm{Eve}} = 0.02$.

It is worth noting that, in a practical plug-and-play CV-QKD system, the source noise plays a crucial role in determining the performance of the system, which may have a large noise value caused by Eve's disturbance. To further show the effect, we perform simulations with different source noise values. Here, considering the configuration of the plug-and-play CV-QKD scheme, we set $\varepsilon_S^{\mathrm{Eve}}$ as a variable while keeping ε_M unchanged. The value of the source noise $\varepsilon_S^{\mathrm{Eve}}$ is set at 0.02, 0.06, or 0.10. In Fig. 4(a), we plot the comparison of the SKR for the untrusted source model and source monitoring model. It is shown that the plug-and-play CV-QKD system under source monitoring

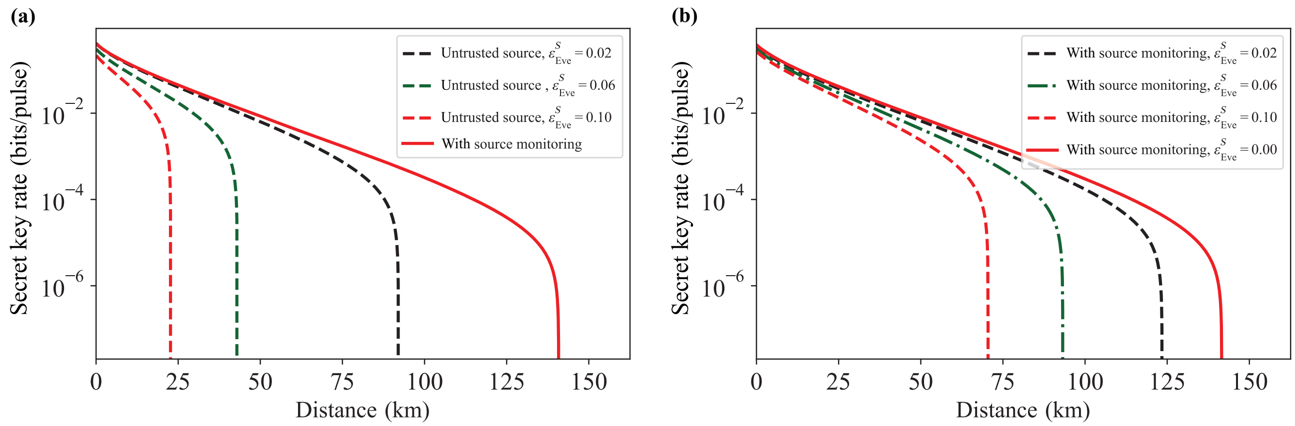

FIG. 4. Simulation secret key rate results for different source noise under the untrusted source model and the source monitoring model. (a) The source noise with source monitoring is heavily suppressed. The red dashed line, green dashed line, and black dashed line (from left to right) show the results for the untrusted model with the source noise $\varepsilon_S^{\text{Eve}}$ taking the values 0.02, 0.06, and 0.10, respectively, and the solid line shows the result for the source monitoring model. (b) Assuming that 20% of the source noise is unsuppressed with different source noise $\varepsilon_S^{\text{Eve}}$. The modulation noise ε_M is set at 0.01.

exhibits strong resistance to source noise due to heavy suppression of the source noise $\varepsilon_S^{\text{Eve}}$. In contrast, the system performance with the untrusted source model is particularly sensitive to the value of source noise $\varepsilon_S^{\text{Eve}}$, where the SKR and transmission distance decrease dramatically with the increase of $\varepsilon_S^{\text{Eve}}$. As an example, with $\varepsilon_S^{\text{Eve}}$ being 0.06, no SKR can be generated at any distance beyond 43 km under the untrusted source model, and the key rate at 25 km is less than 40% of that under the source monitoring model. In a practical system, the source noise cannot be completely eliminated in the regime of strong modulation under the source monitoring. For a conservative estimate, we assume that 20% of the source noise $\varepsilon_S^{\text{Eve}}$ is not eliminated with source monitoring, as shown in Fig. 4(b). One can find that, even in the case where the source noise is not totally suppressed, the system performance under the source monitoring is better than that without monitoring. From another perspective, the source noise of the plug-and-play CV-QKD system can also be ascribed to the side-channel effects [48,56–58], the negative influence of which can be reduced or removed by applying modulated coherent light on the side channel that is optimally correlated to the modulation on the main signal. Figure 5 clearly shows that the tolerance to excess noise (corresponding to the null key rate threshold) for the plug-and-play CV-QKD

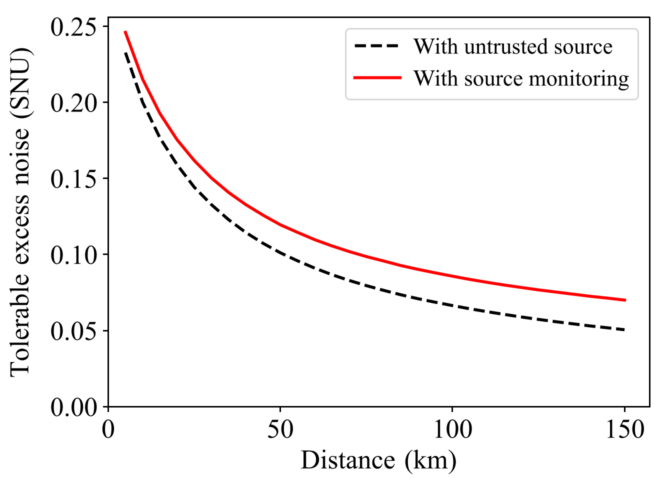

FIG. 5. Simulation results of the tolerable excess noise as a function of transmission distance under the untrusted source model (black dashed line) and the source monitoring model (red solid line).

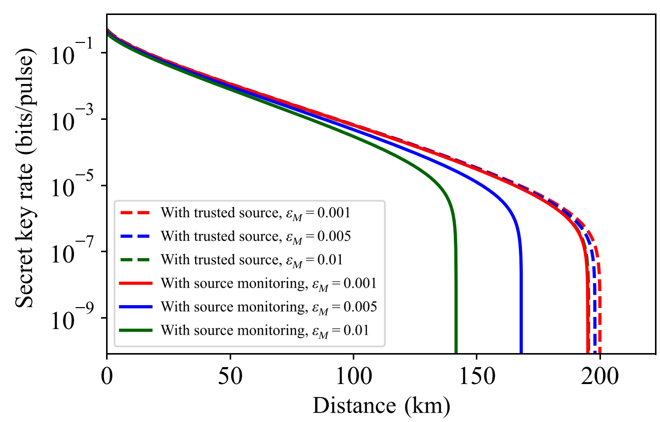

FIG. 6. Simulation secret key rate results for different modulation noise under the trusted source model and the source monitoring model. The green solid line, blue solid line, and red solid line (from left to right) show the results for the source monitoring model with the modulation noise ε_M taking the values 0.01, 0.005, and 0.001, respectively. The green dashed line, blue dashed line, and red dashed line (from left to right) show the results for the trusted source model with the modulation noise ε_M taking the values 0.01, 0.005, and 0.001, respectively.

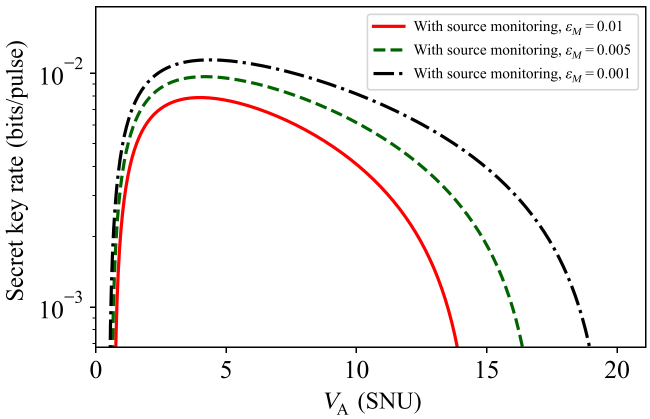

FIG. 7. Simulation results of the secret key rate as a function of modulation variance under the source monitoring model. The transmission distance is fixed at $L = 50$ km. The red solid line, green dashed line, and black dash-dotted line show the results for the source monitoring model with the modulation noise ε_M taking the values 0.01, 0.005, and 0.001, respectively. The corresponding optimal modulation variances are approximately 4, 4.18, and 4.35, respectively.

system under the source monitoring model is superior to that of the untrusted source model.

The results depicted by the curve of Fig. 3 show a certain gap in SKR and a transmission distance between the source monitoring scheme and the trusted source model. Due to the fact that the modulation noise ε_M is still considered as untrusted noise in the source monitoring scheme, it can be predicted that the lower the modulation noise ε_M, the closer the performance using the source monitoring model will be to that of the trusted source model. In Fig. 6, we depict the simulation SKR results for different modulation noise with $\varepsilon_M = 0.001,\ 0.005,$ and 0.01 under the trusted source model and source monitoring model. The results depicted in Fig. 6 effectively agree with the trends of the prediction.

Furthermore, in Fig. 7, we display the SKR as a function of the modulation variance for the source monitoring scheme. Taking the simulation results of a 50-km transmission distance with different modulation noise as an example, it can be found that the larger the excess noise, the smaller the span of the curve. Moreover, the optimal modulation variance tends to increase with a growth in the excess noise. Therefore, in practical QKD processing, setting the appropriate modulation variance enables higher system performance.

V. CONCLUSION

In conclusion, we have proposed an appealing real-time source noise monitoring scheme for the plug-and-play CV-QKD system. Here, a passive beam splitter combined with a homodyne detector is used to monitor the untrusted source on Alice's side, and a VOA is used to strongly suppress the excess noise caused by Eve's intervention on the source. We have established the corresponding entanglement-based model and analyzed the security of the CV-QKD protocol under the source monitoring scheme. The simulation results show that, for the plug-and-play CV-QKD setup, the performance of the system under the source monitoring model is significantly improved, and tolerance to excess noise is enhanced compared with that of the untrusted source model. The proposed source monitoring scheme improves the security and performance of the plug-and-play CV-QKD system. The plug-and-play scheme has clear advantages over the one-way scheme due to the feature of automatically compensating for polarization drift and phase fluctuation during long-distance transmission. The present study provides a long-distance and high-key-rate solution for the plug-and-play CV-QKD scheme, which will be helpful when building high-performance quantum access networks in the future.

It is worth noting that the phase reference used in coherent measurement for source monitoring is sent from Bob to Alice through the unsecured quantum channel. The noise added by Eve before and after modulation may be correlated to provide her with additional information advantage. It is of great importance to conduct the practical security analysis for the phase-reference attack in a more detailed and quantitative way. We leave this task as a future research topic.

ACKNOWLEDGMENTS

We acknowledge financial support from the National Key Research and Development Program of China (Grant No. 2020YFA0309704), the National Natural Science Foundation of China (Grants No. 62201530, No. 62101516, No. 62171418, No. 62301517 and No. 62001044), the Sichuan Science and Technology Program (Grants No. 2023ZYD0131, No. 2023JDRC0017, No. 2023YFG0143, No. 2022ZDZX0009 and No. 2021YJ 0313), the Natural Science Foundation of Sichuan Province (Grants No. 2023NSFSC1387, No. 2023NSFS C0449, No. 2024NSFSC0470, and No. 2024NSFSC0454), the Basic Research Program of China (Grant No. JCKY2021210B059), the Equipment Advance Research Field Foundation (Grant No. 315067206), the National Key Laboratory of Security Communication Foundation (Grant No. 6142103042201, No. 6142103042301), Stability Program of National Key Laboratory of Security Communication (2023).

APPENDIX A: THE UNTRUSTED SOURCE

The plug-and-play CV-QKD scheme with the untrusted source is shown in Fig. 8(a), and the corresponding entanglement-based model is shown in Fig. 8(b). In this case, the mutual information can be derived from Bob's variance V_B and the conditional variance $V_{B|A}$. Since $\rho_{AB_2E_1E_2S_1S_2}$ is a pure state and the source noise is controlled by Eve, one obtains $S(\rho_{E_1E_2S_1S_2}) = S(\rho_{AB_2})$. Moreover, after Bob's projective measurement, the state $\rho_{AE_1E_2S_1S_2FG}$ is also a pure state, thus $S(\rho^{m_B}_{E_1E_2S_1S_2}) = S(\rho^{m_B}_{AFG})$. As $S(\rho^{m_B}_{AFG})$ is independent of m_B for the Gaussian modulation CV-QKD protocol, Eq. (3) becomes

$$\chi(B : E_1E_2S_1S_2) = S(\rho_{AB_2}) - S(\rho^{m_B}_{AFG}), \tag{A1}$$

where $S(\rho_{AB_2})$ and $S(\rho^{m_B}_{AFG})$ can be calculated from the symplectic eigenvalues of the covariance matrices γ_{AB_2} and $\gamma^{m_B}_{AFG}$, respectively.

The derivation process of the above two covariance matrices is as follows. The covariance matrix γ_{AB_0} of the state ρ_{AB_0} can be expressed as

$$\gamma_{AB_0} = \begin{bmatrix} V\mathbb{I} & \sqrt{V^2-1}\,\sigma_Z \\ \sqrt{V^2-1}\,\sigma_Z & V\mathbb{I} \end{bmatrix}, \tag{A2}$$

where $\mathbb{I}$ is the 2×2 identify matrix and σ_Z is the Pauli-Z matrix. The covariance matrix $\gamma_{AB_1S_1S_2}$ can be calculated from

$$\gamma_{AB_1S_1S_2} = (Y^{BS_1})^{\mathrm{T}}[\gamma_{AB_0} \oplus \gamma_{S_0S_2}]Y^{BS_1}, \tag{A3}$$

with $Y^{BS_1} = I_A \oplus S^{BS}_{T_S} \oplus I_{S_2}$, where $S^{BS}_{T_S}$ is

$$S^{BS}_{T_S} = \begin{bmatrix} \sqrt{T_S}\,\mathbb{I} & \sqrt{1-T_S}\,\mathbb{I} \\ -\sqrt{1-T_S}\,\mathbb{I} & \sqrt{T_S}\,\mathbb{I} \end{bmatrix}. \tag{A4}$$

Therefore, the covariance matrix $\gamma_{AB_1S_1S_2}$ can be expressed as

$$\gamma_{AB_1S_1S_2} = \begin{bmatrix} V\mathbb{I} & \sqrt{T_S(V^2-1)}\,\sigma_Z & \sqrt{(1-T_S)(V^2-1)}\,\sigma_Z & 0 \\ \sqrt{T_S(V^2-1)}\,\sigma_Z & [T_SV+(1-T_S)V_S]\,\mathbb{I} & \sqrt{T_S(1-T_S)}(V-V_S)\,\mathbb{I} & -\sqrt{(1-T_S)(V_S^2-1)}\,\sigma_Z \\ \sqrt{(1-T_S)(V^2-1)}\,\sigma_Z & \sqrt{T_S(1-T_S)}(V-V_S)\,\mathbb{I} & [T_SV_S+(1-T_S)V]\,\mathbb{I} & \sqrt{T_S(V_S^2-1)}\,\sigma_Z \\ 0 & -\sqrt{(1-T_S)(V_S^2-1)}\,\sigma_Z & \sqrt{T_S(V_S^2-1)}\,\sigma_Z & V_S\,\mathbb{I} \end{bmatrix}, \tag{A5}$$

when the quantum signal travels through the quantum channel, assuming that an entangling-cloner attack is launched by Eve, which could reach the Holevo bound with optimal Gaussian collective attacks. Therefore, the covariance matrix corresponding to the state after transmitting through the channel can be given by

$$\gamma_{AB_2E_1E_2} = (Y^{BS_2})^{\mathrm{T}}[\gamma_{AB_1} \oplus \gamma_{E_0E_2}]Y^{BS_2}, \tag{A6}$$

with $Y^{BS_2} = I_A \oplus S^{BS}_{B_1E_0} \oplus I_{E_2}$, where $\gamma_{E_0E_2}$ is

$$\gamma_{E_0E_2} = \begin{bmatrix} V_E\,\mathbb{I} & \sqrt{V_E^2-1}\,\sigma_Z \\ \sqrt{V_E^2-1}\,\sigma_Z & V_E\,\mathbb{I} \end{bmatrix}, \tag{A7}$$

and $S^{BS}_{B_1E_0}$ is

$$S^{BS}_{B_1E_0} = \begin{bmatrix} \sqrt{T}\,\mathbb{I} & \sqrt{1-T}\,\mathbb{I} \\ -\sqrt{1-T}\,\mathbb{I} & \sqrt{T}\,\mathbb{I} \end{bmatrix}. \tag{A8}$$

Therefore, the covariance matrix γ_{AB_2} is obtained as

$$\gamma_{AB_2} = \begin{bmatrix} V\mathbb{I} & \sqrt{TT_s(V^2-1)}\,\sigma_Z \\ \sqrt{TT_s(V^2-1)}\,\sigma_Z & [TT_sV + T(1-T_s)V_S + (1-T)V_E]\,\mathbb{I} \end{bmatrix}. \tag{A9}$$

After Bob's projective measurement, the covariance matrix of the state can be written as

$$\gamma_{ABFG} = (Y^{BS_3})^{\mathrm{T}}(\gamma_{AB_2} \oplus \gamma^{EPR}_{F_0G})Y^{BS_3}, \tag{A10}$$

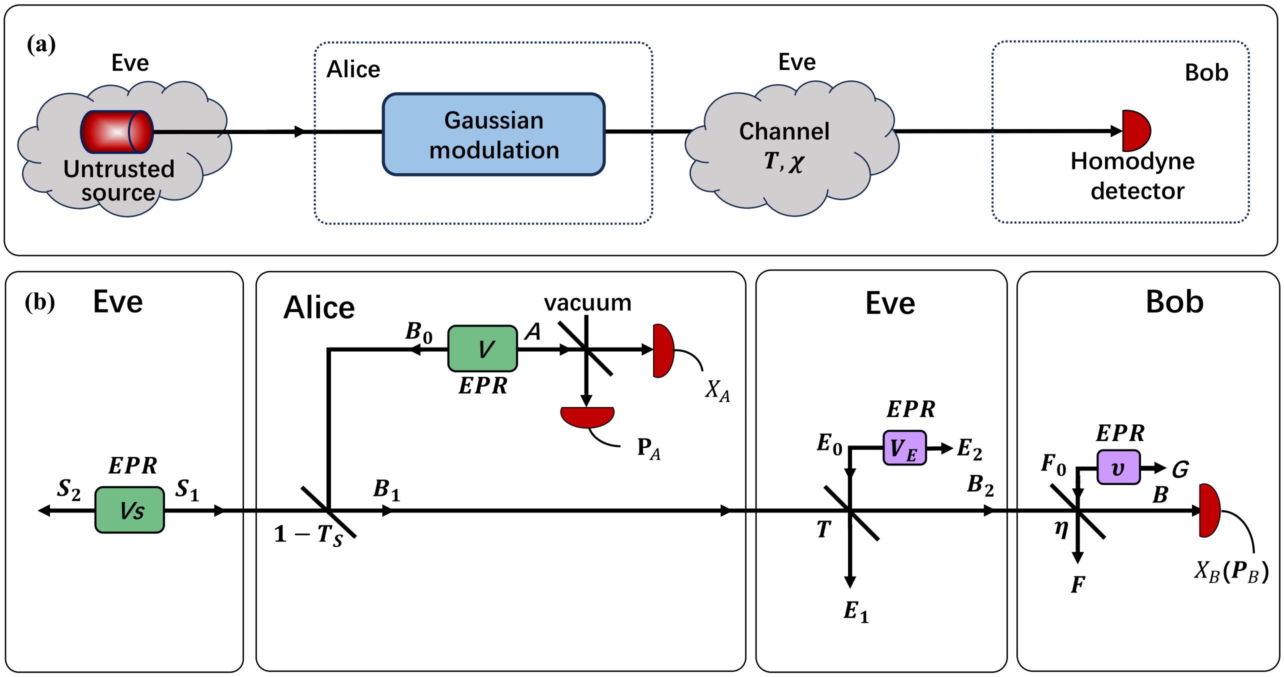

FIG. 8. (a) Simplified schematic for the prepare-and-measure model and (b) the corresponding entanglement-based model of the plug-and-play CV-QKD system with the untrusted source.

with $Y^{BS_3} = I_A \oplus S^{BS}_{B_2F_0} \oplus I_G$, where γ_{F_0G} is the covariance matrix of the EPR state used to model the detector's electronic noise with variance υ. The matrix γ_{F_0G} is given by

$$\gamma_{F_0G} = \begin{bmatrix} \upsilon\, \mathbb{I} & \sqrt{(\upsilon^2-1)}\, \sigma_Z \\ \sqrt{(\upsilon^2-1)}\, \sigma_Z & \upsilon\, \mathbb{I} \end{bmatrix}. \qquad \text{(A11)}$$

To calculate the final part of Eq. (A1), one needs to derive the covariance matrix $\gamma^{m_B}_{AFG}$. The matrix $\gamma^{m_B}_{AFG}$ can be determined from

$$\gamma^{m_B}_{AFG} = \gamma_{AFG} - \sigma^{\mathrm{T}}_{AFGB} H \sigma_{AFGB}. \qquad \text{(A12)}$$

The matrix γ_{AFG}, $\sigma^{\mathrm{T}}_{AFGB}$, and γ_B can be obtained by decomposition of the covariance matrix

$$\gamma_{AFGB} = \begin{bmatrix} \gamma_{AFG} & \sigma^{\mathrm{T}}_{AFGB} \\ \sigma_{AFGB} & \gamma_B \end{bmatrix}, \qquad \text{(A13)}$$

which can be derived from the transformation of the matrix γ_{ABFG} in Eq. (A10).

As a result, $S(\rho_{AB_2})$ can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of γ_{AB_2}, and $\mathrm{S}(\rho^{m_B}_{AFG})$ can be calculated from the symplectic eigenvalues $\lambda_{3,4,5}$ of $\gamma^{m_B}_{AFG}$. Thus, the Holevo quantity can be expressed as

$$\chi(B : E_1E_2S_1S_2) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right). \qquad \text{(A14)}$$

The remaining calculational steps for the asymptotic SKR for the plug-and-play CV-QKD with the untrusted source are the same as in Sec. III A.

APPENDIX B: THE TRUSTED SOURCE

For comparison, we further analyze the situation when the source noise is trusted, as shown in Fig. 9(a), and the corresponding entanglement-based model is shown in Fig. 9(b). In this case, the system S_1S_2 is out of Eve's control. The mutual information is the same as in Eq. (2), and the corresponding Holevo bound can be expressed as

$$\chi(B : E_1E_2) = S(\rho_E) - \int dm_B p(m_B) \mathrm{S}(\rho^{m_B}_E). \qquad \text{(B1)}$$

Since Eve is able to purify the system $S_1S_2AB_2$, and Bob's measurement purifies the system S_1S_2AFG, the Holevo bound can be written as

$$\chi(B : E_1E_2) = S(\rho_{S_1S_2AB_2}) - S(\rho^{m_B}_{S_1S_2AFG}). \qquad \text{(B2)}$$

Here, $S(\rho_{S_1S_2AB_2})$ can be calculated from the symplectic eigenvalues $\lambda_{1,2,3,4}$ of $\gamma_{S_1S_2AB_2}$, and $S(\rho^{m_B}_{S_1S_2AFG})$ can be calculated from the symplectic eigenvalues $\lambda_{5,6,7,8,9}$ of $\gamma^{m_B}_{S_1S_2AFG}$, which can be derived as

$$\gamma^{m_B}_{S_1S_2AFG} = \gamma_{S_1S_2AFG} - \sigma^{\mathrm{T}}_{S_1S_2AFGB} H \sigma_{S_1S_2AFGB}. \qquad \text{(B3)}$$

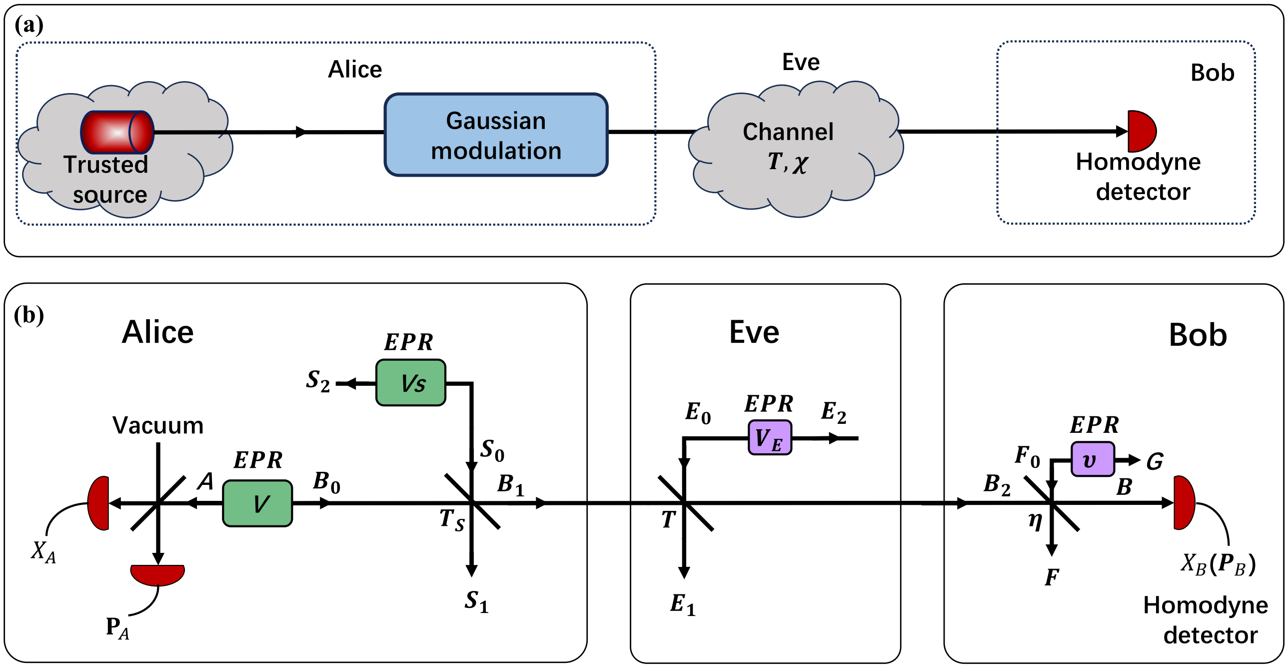

FIG. 9. (a) Simplified schematic for the prepare-and-measure model and (b) the corresponding entanglement-based model of the plug-and-play CV-QKD system with the trusted source.

The matrices $\gamma_{S_1S_2AFG}$, $\sigma_{S_1S_2AFGB}$, and γ_B can be determined from the decomposition of the covariance matrix:

$$\gamma_{S_1S_2AFGB} = \begin{bmatrix} \gamma_{S_1S_2AFG} & \sigma^{\mathrm{T}}_{S_1S_2AFGB} \\ \sigma_{S_1S_2AFGB} & \gamma_B \end{bmatrix}, \tag{B4}$$

which can be derived from the transformation of the matrix

$$\gamma_{S_1S_2ABFG} = (Y^{BS})^{\mathrm{T}}[\gamma_{S_1S_2AB_2} \oplus \gamma_{F_0G}]Y^{BS}, \tag{B5}$$

where $Y^{BS} = \mathbb{I}_{S_1} \oplus \mathbb{I}_{S_2} \oplus \mathbb{I}_A \oplus S^{BS}_{BF_0} \oplus \mathbb{I}_G$. Based on Eqs. (B3)–(B5), the matrix $\gamma^{mB}_{S_1S_2AFG}$ is obtained and its symplectic eigenvalues can be calculated. Thus, $\chi(B:E_1E_2)$ can be calculated as

$$\chi(B:E_1E_2) = \sum_{i=1}^{4} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=5}^{9} G\left(\frac{\lambda_i - 1}{2}\right). \tag{B6}$$

Therefore, the asymptotic SKR can be obtained.

APPENDIX C: HETERODYNE DETECTION

For the plug-and-play CV-QKD scheme with heterodyne detection, two quadratures are measured. The mutual between Alice and Bob is given by

$$I(A:B) = \log_2 \frac{V_B}{V_{B|A}}. \tag{C1}$$

The variance $\upsilon = 1 + 2\upsilon_{\mathrm{el}}/(1-\eta)$ and the symplectic matrix that represents the heterodyne measurement on mode B [see Eq. (13)] can be expressed as $H = (\gamma_B + II)^{-1}$. Based on the above changes, we calculate the secure key rate under different situations, as shown in Fig. 10. One can find that the simulation results of heterodyne detection in the given parameters are close to that of homodyne detection.

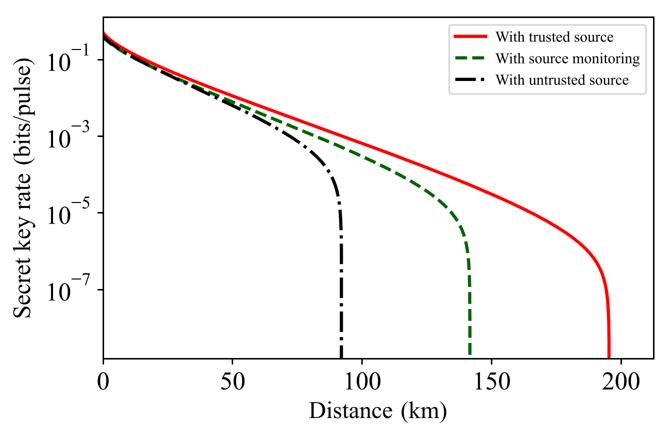

FIG. 10. Simulation secret key rate results with heterodyne detection for the plug-and-play CV-QKD scheme under the untrusted source model (black dash-dotted line), the source monitoring model (green dashed line), and the trusted source model (red solid line). The source noises are set at $\varepsilon_M = 0.01$ and $\varepsilon_S^{\mathrm{Eve}} = 0.02$.

[1] F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).
[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).
[3] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, Appl. Phys. Rev. **11**, 1 (2024).
[4] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature **421**, 238 (2003).
[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).
[6] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).
[7] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection, Phys. Rev. X **5**, 041009 (2015).
[8] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, Phys. Rev. X **5**, 041010 (2015).
[9] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).
[10] Y. C. Zhang, Z. Y. Chen, S. Pirandola, X. Y. Wang, C. Zhou, B. J. Chu, Y. J. Zhao, B. J. 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).
[11] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. Solar Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).
[12] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber, Opt. Lett. **48**, 1766 (2023).
[13] A. A. Hajomer, I. Derkach, N. Jain, H. M. Chin, U. L. Andersen, and T. Gehring, Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator, Sci. Adv. **10**, eadi9474 (2024).
[14] H. Wang, Y. D. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. L. Liu, C. L. Zhang, Y. C. Zhang, and B. J. 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).
[15] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, Y. Zhang, J. Yang, T. Zhang, W. Huang, and B. Xu, Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area, Commun. Phys. **5**, 162 (2022).
[16] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system, Opt. Lett. **47**, 3307 (2022).
[17] Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, High-performance long-distance discrete-modulation continuous-variable quantum key distribution, Opt. Lett. **48**, 2953 (2023).
[18] 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).
[19] Y. Zhang, *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).
[20] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics **13**, 839 (2019).
[21] Y. Bian, Y. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, High-rate point-to-multipoint quantum key distribution using coherent states, arXiv:2302.02391 (2023).
[22] Y. Pan, Y. Bian, H. Wang, J. Dou, Y. Shao, Y. Pi, T. Ye, J. Yang, Y. Li, W. Huang, S. Yu, Y. Zhang, and B. Xu, in *49th European Conference on Optical Communication, ECOC* (IET, Hybrid Conference, Glasgow, UK, 2023).
[23] Y. Xu, T. Wang, H. Zhao, P. Huang, and G. Zeng, Round-trip multi-band quantum access network, Photonics Res. **11**, 1449 (2023).
[24] Y. Huang, T. Shen, X. Wang, Z. Chen, B. Xu, S. Yu, and H. Guo, Realizing a downstream-access network using continuous-variable quantum key distribution, Phys. Rev. Appl. **16**, 064051 (2021).
[25] X. Wang, Z. Chen, Z. Li, D. Qi, S. Yu, and H. Guo, Experimental upstream transmission of continuous variable quantum key distribution access network, Opt. Lett. **48** (12), 3327 (2023).
[26] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, Phys. Rev. Lett. **114**, 070501 (2015).
[27] A. Leverrier, Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction, Phys. Rev. Lett. **118**, 200501 (2017).
[28] 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).
[29] S. Pirandola, Limits and security of free-space quantum communications, Phys. Rev. Res. **3**, 013279 (2021).
[30] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems, Phys. Rev. A **88**, 022339 (2013).
[31] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han,

Quantum hacking on quantum key distribution using homodyne detection, Phys. Rev. A **89**, 032304 (2014).

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

[33] 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).

[34] Y. Shao, H. Wang, Y. Pi, W. Huang, Y. Li, J. Liu, J. Yang, Y. Zhang, and B. Xu, Phase noise model for continuous-variable quantum key distribution using a local local oscillator, Phys. Rev. A **104**, 032608 (2021).

[35] Y. Shao, Y. Li, H. Wang, Y. Pan, Y. Pi, Y. Zhang, W. Huang, and B. Xu, Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator, Phys. Rev. A **105**, 032601 (2022).

[36] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, PRX Quantum **3**, 040307 (2022).

[37] Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, Continuousmode quantum key distribution with digital signal processing, npj Quantum Inf. **9**, 28 (2023).

[38] 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).

[39] D. Huang, P. Huang, T. Wang, H. S. Li, Y. M. Zhou, and G. H. Zeng, Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol, Phys. Rev. A **94**, 032305 (2016).

[40] Q. Liao, H. Liu, Y. Gong, Z. Wang, Q. Peng, and Y. Guo, Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation, Opt. Express **30**, 3876 (2022).

[41] R. Valivarthi, S. Etcheverry, J. Aldama, F. Zwiehoff, and V. Pruneri, Plug-and-play continuous-variable quantum key distribution for metropolitan networks, Opt. Express **28**, 14547 (2020).

[42] R. Goncharov, D. Kirichenko, I. Vorontsova, I. Filipov, Y. Adam, B. Pervushin, B. Nasedkin, E. Samsonov, and V. Egorov, Security of plug-and-play continuous-variable quantum key distribution, J. Opt. Technol. **89** (7), 430 (2022).

[43] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[44] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems, IEEE J. Sel. Top. Quantum Electron. **21** (3), 168 (2015).

[45] B. Xu, X. Peng, and H. Guo, Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system, Phys. Rev. A **82**, 042301 (2010).

[46] X. Peng, B. Xu, and H. Guo, Passive-scheme analysis for solving the untrusted source problem in quantum key distribution, Phys. Rev. A **81**, 042320 (2010).

[47] X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, Experimental quantum-key distribution with an untrusted source, Opt. Lett. **33**, 2077 (2008).

[48] V. C. Usenko and R. Filip, Feasibility of continuous-variable quantum key distribution with noisy coherent states, Phys. Rev. A **81**, 022318 (2010).

[49] Y. Shen, X. Peng, J. Yang, and H. Guo, Continuous-variable quantum key distribution with Gaussian source noise, Phys. Rev. A **83**, 052304 (2011).

[50] J. Yang, B. J. Xu, and H. Guo, Source monitoring for continuous-variable quantum key distribution, Phys. Rev. A **86**, 042314 (2012).

[51] B. Chu, Y. Zhang, Y. Huang, S. Yu, Z. Chen, and H. Guo, Practical source monitoring for continuous-variable quantum key distribution, Quantum Sci. Technol. **6**, 025012 (2021).

[52] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: a threat and a defense, Entropy **18**, 20 (2016).

[53] Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, Practical security of continuous-variable quantum key distribution with reduced optical attenuation, Phys. Rev. A **100**, 012313 (2019).

[54] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations, Adv. Quantum Technol. **1**, 1800011 (2018).

[55] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[56] C. Weedbrook, S. Pirandola, and T. C. Ralph, Continuous-variable quantum key distribution using thermal states, Phys. Rev. A **86**, 022318 (2012).

[57] I. Derkach, V. C. Usenko, and R. Filip, Preventing side-channel effects in continuous-variable quantum key distribution, Phys. Rev. A **93**, 032309 (2016).

[58] I. Derkach, V. C. Usenko, and R. Filip, Continuous-variable quantum key distribution with a leakage from state preparation, Phys. Rev. A **96**, 062309 (2017).