Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol

Duan Huang,[1] Peng Huang,[1,*] Tao Wang,[1] Huasheng Li,[1] Yingming Zhou,[1] and Guihua Zeng[1,2,†]

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

[2] *College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China*

(Received 25 April 2016; published 6 September 2016)

We propose and experimentally demonstrate a continuous-variable quantum key distribution (CV-QKD) protocol using dual-phase-modulated coherent states. We show that the modulation scheme of our protocol works equivalently to that of the Gaussian-modulated coherent-states (GMCS) protocol, but shows better experimental feasibility in the plug-and-play configuration. Besides, it waives the necessity of propagation of a local oscillator (LO) between legitimate users and generates a real local LO for quantum measurement. Our protocol is proposed independent of the one-way GMCS QKD without sending a LO [Opt. Lett. **40**, 3695 (2015); Phys. Rev. X **5**, 041009 (2015); **5**, 041010 (2015)]. In those recent works, the system stability will suffer the impact of polarization drifts induced by environmental perturbations, and two independent frequency-locked laser sources are necessary to achieve reliable coherent detection. In the proposed protocol, these previous problems can be resolved. We derive the security bounds for our protocol against collective attacks, and we also perform a proof-of-principle experiment to confirm the utility of our proposal in real-life applications. Such an efficient scheme provides a way of removing the security loopholes associated with the transmitting LO, which have been a notoriously hard problem in continuous-variable quantum communication.

DOI: 10.1103/PhysRevA.94.032305

I. INTRODUCTION

Quantum key distribution (QKD) is the best-known application of quantum information, which promises to achieve the Holy Grail of cryptography; unconditional secure communication in the real world [1–4]. Several landmark accomplishments have been achieved in both discrete-variable (DV) QKD [1,2] and continuous-variable (CV) QKD [3,4]. The main motivation for dealing with CV-QKD, however, originates from its tantalizing promise of providing higher key distribution rates compared with its DV counterpart [5–7]. In recent years, numerous experiments of CV-QKD in the laboratory [8–15] as well as in the field [16–19] focused on the distribution of quantum states through an optical-fiber channel or an atmospheric channel. In most of these experiments, the one-way Gaussian-modulated coherent-states (GMCS) protocol was implemented [6]. In the state-of-art experiments of GMCS CV-QKD, quantum signals were randomly modulated in two quadratures of coherent states (X and P or equivalently the amplitude and phase) and then transmitted together with a strong local oscillator (LO) over a single-fiber channel by using time- and polarization-multiplexing techniques [8–10]. The security of the protocol has been proved, in principle, secure against collective eavesdropping attacks, which are optimal in both the asymptotic case [20–22] and the finite-size regime [23–25].

However, the impact of nonlocal arrangement of LO has often been overlooked in the previous experiments. In practice, limited by the intrinsic photon loss in the quantum channel, the LO power would be insufficient to operate well within the shot-noise limit for quantum measurement under long-distance conditions [8,9]. Moreover, almost all of the reported attacks, such as wavelength attacks [26,27], saturation attacks [28], calibration attacks [29], and LO fluctuation attacks [30], were related with the security loopholes of LO. Recently, several groups introduced CV-QKD schemes without sending a LO which can be locally generated by using an independent laser source at the receiver's side [31–33]. Nevertheless, in the real-life implementations of those schemes, the security and performance would be reduced because of the frequency instabilities of two independent laser sources (arguably the most critical part of the implementation), the fiber length fluctuations, and the polarization drifts induced by environmental perturbations.

Considering the drawbacks of the one-way GMCS protocol without sending a LO, another approach to generate a local LO for quantum state measurement is to use a single laser source for the legitimate users, and it was called the *plug-and-play* configuration in quantum cryptography. A preliminary experiment of plug-and-play CV-QKD using single-phase-modulated coherent states has shown the experimental feasibility on the polarization self-compensation [14]. Instead of utilizing polarization-sensitive amplitude modulation, they can take advantage of the polarization-insensitive properties of a phase modulator so that the coherent-state preparation would not be affected by the polarization drifts of fiber channel. Unfortunately, this candidate protocol shows much higher sensitivity to excess noise compared with symmetrically modulated (amplitude and phase) GMCS QKD [34,35].

On the other hand, the plug-and-play symmetrically modulated GMCS QKD using a real local LO has never been seriously studied before. This might be due in part to the fact that almost all of the reported CV-QKD experiments were focusing on the one-way GMCS protocol during the past decade. Another primary reason is that the plug-and-play protocols

[*] huang.peng@sjtu.edu.cn

[†] ghzeng@sjtu.edu.cn

suffer the Trojan-horse attack [36,37], and the secure distance is limited by the Rayleigh scattering [38]. Previous studies have presented the quantitative security analysis on a general class of plug-and-play DV-QKD protocol with unknown and untrusted sources [39]. Recently, several works focused on the study of one-way CV-QKD in which the imperfection of Gaussian coherent-states generation and modulation can be ascribed to a neutral source noise model, since the untrusted source noise model would overestimate Eve's power and leads to an untight security bound [40–44]. However, a complete unconditional security proof of plug-and-play CV-QKD with an untrusted source has never been rigorously proved. Thus, to avoid compromising the security and performance, the existing and underlying practical vulnerabilities should be resolved.

In this paper, we propose and experimentally demonstrate a plug-and-play CV-QKD protocol based on dual-phase-modulated coherent states (DPMCS). It differs from our previous proposed CV-QKD without sending a LO [31], but relies on the distribution of a Gaussian key that is obtained by continuously modulating the phase of coherent light pulses at Bob's side and subsequently performing homodyne detection at Alice's side. We show that the dual-phase-modulation scheme works equivalently to symmetrically modulated (amplitude and phase) Gaussian-state protocols. The receiver Alice keeps the classical light of LO in our implementation so that shot-noise-limited homodyne detection becomes more flexible by modifying the real local LO power even in the presence of strong optical losses. Compared with the one-way GMCS protocol with nonlocal or local arrangement of LO, our DPMCS protocol benefits from the plug-and-play scheme so that we can waive the necessity of two independent laser sources and compensate the polarization drifts automatically. In the security analysis of the proposed protocol, we take into account the untrusted source, a long-standing open question of plug-and-play CV-QKD. A complete proof of its unconditional security against collective attacks is presented. Besides, we demonstrate these feasibilities of our proposed DPMCS protocol without sending a LO by performing a 1-MHz proof-of-principle experiment over a 20-km standard single-mode-fiber (SMF) spool with a loss of 0.2 dB/km. The practical limitations of our experiment on the secure distance are essentially technical and appear to be due mostly to the sampling length which is necessary to ensure the composable security.

The paper is organized as follows. In Sec. II, we first describe the basic one-way GMCS protocol, then extend to plug-and-play GMCS protocol, and finally present our plug-and-play DPMCS protocol. We show that our proposed plug-and-play DPMCS protocol is actually equivalent to the one-way GMCS protocol, but shows better polarization stability in the plug-and-play configuration. In Sec. III, we analyze the security of the proposed plug-and-play DPMCS protocol with untrusted source. First, we introduce the model of prepare-and-measurement scheme for the new protocol, and then, based on the equivalent entanglement-based scheme, we can calculate the amount of leaked information. In Sec. IV, we describe a specific proof-of-principle experiment based on the DPMCS protocol and report the experimental results. We then conclude the paper in Sec. V.

II. EXTENDING ONE-WAY GMCS PROTOCOL TO PLUG-AND-PLAY DPMCS PROTOCOL

A. One-way GMCS QKD protocol

Figure 1(a) shows the standard prepare-and-measure description of the one-way GMCS QKD protocol [5–7]. Alice prepares a coherent state $|\psi\rangle$, in practice, the amplitude and phase of which are modulated by an amplitude modulator (AM) and a phase modulator (PM), respectively. The modulation values obey Gaussian distribution centered at zero and of variance V_A in the units of shot-noise variance N_0. The modulated coherent states are then sent to Bob through a quantum channel together with a strong LO, which provides the required phase reference. Particularly, the quantum channel typically features a transmission efficiency $T = 10^{-\alpha L/10}$ over a standard optical fiber with a constant loss coefficient α and channel length L. The excess noise ξ_c of the quantum channel is assumed to be ascribed to the eavesdropper's intervention. Therefore, the noise variance referred to Bob's input, expressed in shot-noise units, is $\chi_c = 1 + T\xi_c$. When Bob receives the Gaussian-modulated coherent states and LO, he randomly measures either one of the two quadratures with homodyne detector or both quadratures with heterodyne detector. More

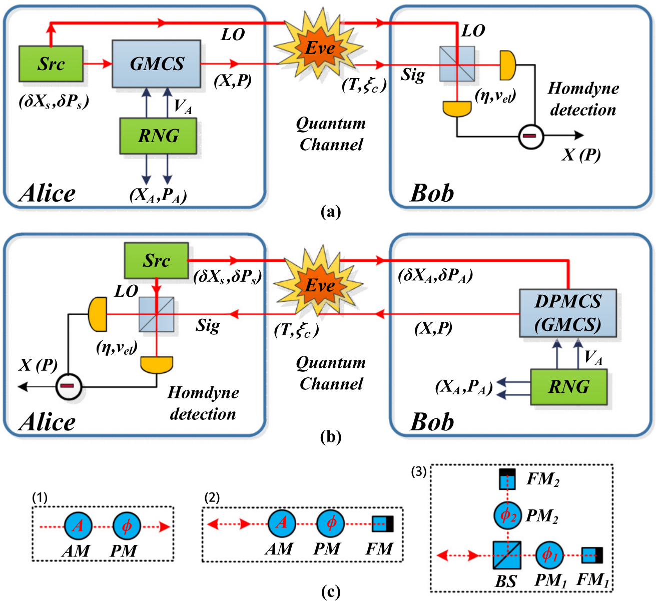

FIG. 1. (a) One-way GMCS protocol. (b) Plug-and-play DPMCS (GMCS) protocol. (c) Modulation schemes: (1) Gaussian modulation by coding of an AM and a PM in forward direction, (2) Gaussian modulation by coding of an AM and a PM in backward direction, (3) Gaussian modulation by coding of two PMs in backward direction. In the one-way GMCS protocol, Alice generally utilizes an amplitude modulator and a phase modulator to encode the key information which features a centered Gaussian distribution. In our proposed protocol, Alice generates a classical light and sends it to Bob; Bob uses a dual-phase-modulation scheme to encode the information. This arrangement takes advantage of the polarization-insensitive properties of phase modulators so that the coherent-state preparation would not be affected by the polarization drifts of the fiber channel. AM, amplitude modulator; PM, phase modulator; BS, beam splitter; FM, Faraday mirror; RNG, random number generator.

exactly, in a homodyne (or heterodyne) protocol, a detector usually features an electronic noise υ_{el} and an efficiency η. Therefore, in such a practical homodyne protocol, the total noise referred to the channel input can be expressed as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T$, where $\chi_{\text{line}} = \chi_c/T - 1$, $\chi_h = [(1-\eta) + \upsilon_{el}]/\eta$ [45]. Finally, the mutual information of Alice and Bob I_{AB} can be derived from the achievable signal-to-noise ratio (SNR) using Shannon's equation:

$$I_{AB} = \frac{1}{2}\log_2(1+\text{SNR}) = \frac{1}{2}\log_2\left(\frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}\right). \quad (1)$$

To extract a shared secret key from I_{AB} and establish private correlations, Alice and Bob must estimate the experimental parameters, especially the excess noise ξ_c and shot-noise variance N_0, by broadcasting and comparing a part of their random bits so that the leaked information to Eve χ_{BE} is bounded, and then the Shannon secret key rate can be given by

$$K = \beta I_{AB} - \chi_{BE}, \quad (2)$$

where β corresponds to the classical reconciliation efficiency. It is important to note that the security proofs show that the derived tight bound for the secret key rate in the case of collective attacks remains asymptotically valid for arbitrary coherent attacks, which are the most powerful attacks allowed by quantum mechanics [45]. Therefore, the results that we derived in this paper for collective attacks are valid for coherent attacks as well.

B. Extending one-way GMCS protocol to plug-and-play GMCS protocol

In this section, we extend CV-QKD from the one-way GMCS protocol to a plug-and-play GMCS protocol without sending a LO. In the above one-way GMCS protocol, Alice owns all of the physical resources for the preparation of quantum states, and their sole purpose is the encoding of Gaussian secret information. However, in previous one-way CV-QKD configurations [9,10,13], Alice needs to employ time- and polarization-multiplexing techniques to send the Gaussian quantum signal and the orthogonal polarization LO in the same fiber channel. Hence, during the process, a potential eavesdropper can easily perform intercept-resend attacks by exploiting the security loopholes of LO [26–30], especially the LO intensity fluctuation, which is associated with a key experimental parameter, i.e., the shot-noise variance N_0.

We are now interested in a scenario where some of physical resources for the preparation of quantum states are distributed from Bob's side, and Alice keeps the locally generated LO for quantum states measurement. Let us explicitly construct such a CV-QKD protocol using the schematic shown in Fig. 1(b). The protocol proceeds as follows. (i) Alice generates a strong classical light as a locally generated LO and sends a classical light to Bob through a quantum channel which is usually referred to a standard fiber link. (ii) Bob encodes a random N-bit sequence $s_1, s_2, s_3, ...s_N$ on the weak coherent signal by using Gaussian modulation. (iii) After possible intervention by a potential eavesdropper, Alice receives the quantum signal. (iv) Alice utilizes the locally generated LO and randomly measures one of the quadratures of quantum states so that she can get a real outcome X that is correlated with the encoded signal X_B. (v) Alice and Bob finally possess two correlated variables X and X_B. After the classical reconciliation, they are able to bound the Shannon secret information K.

What is remarkable here is that the above plug-and-play GMCS protocol is similar to the one-way GMCS protocol, because the classical signal sent from Alice to Bob does not contain any Gaussian-modulated information. However, none of the experiment on the plug-and-play GMCS protocol without sending a LO has demonstrated in recent years. In fact, the concept of plug-and-play GMCS protocol without sending a LO has never been introduced before. This is because there exist some difficulties on the security analysis and experimental realization for the candidate protocol.

C. Extending plug-and-play GMCS protocol to plug-and-play DPMCS protocol

For the understanding of the basic idea of our plug-and-play DPMCS protocol, we need to deepen our analysis on the feasibility of Bob's encoding strategy and Alice's decoding strategy based on the plug-and-play GMCS protocol. First, we present the feasibility study of the encoding strategy. So far, the most studied CV systems rely on Gaussian states, Gaussian operations, and Gaussian measurement, owing to their experimental feasibility and the relative simplicity of their mathematical description [4]. Intuitively, as shown in Fig. 1(c)(2), the above idea can be implemented simply by employing an AM and a PM to prepare a Gaussian coherent state at Bob's side, which will be directly reflected to the receiver Alice by a Faraday mirror [14]. Unfortunately, in practice, most of AMs, especially the widely used LiNbO$_3$ modulators, are polarization sensitive and features a polarizer, which means the portion of the light that is not aligned in the correct orientation cannot be transmitted [46].

For simplicity, we assume that the AM's Jones matrix $\mathbf{J}_{AM}$ is oriented in the x directions of the electromagnetic field. The equivalent attenuation coefficient in the x direction is ϱ, which depends on the modulation voltages, while the equivalent attenuation coefficient in the y direction is ζ, which is approaching zero. Therefore, the Jones matrices of AM in the x and y directions are given by

$$\mathbf{J}_{AM_x} = \begin{bmatrix} \varrho & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbf{J}_{AM_y} = \begin{bmatrix} 0 & 0 \\ 0 & \zeta \end{bmatrix}. \quad (3)$$

The most important advantage of the plug-and-play Faraday QKD system is that it can automatically compensate for any birefringence effect in fiber. Generally, the Faraday rotation angle $\theta = 45^\circ$, and the Jones matrix of faraday mirror (FM) can be written as [47]

$$\begin{aligned} \text{FM}(\theta) &= \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ -\sin(2\theta) & -\cos(2\theta) \end{bmatrix} \\ &= \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}. \end{aligned} \quad (4)$$

When the input coherent states return from the FM without any modulation device, their polarizations are orthogonal to that of their initial state. It can be proved that in such an ideal situation, the configuration shown in Fig. 1(c)(3) can compensate the birefringence of medium automatically. The complete Jones matrix of the rotated element will be

$$\mathbf{T}_{FM} = \mathbf{T}(-\theta^{'})\mathrm{FM}(\theta)\mathbf{T}(\theta^{'}) = e^{i(\varphi)}\mathrm{FM}(\theta), \tag{5}$$

where $\varphi = \varphi_o + \varphi_e$, φ_o and φ_e are the propagation phases of ordinary and extraordinary rays, respectively, $\theta^{'}$ is the rotation angle between the reference basis and the eigenmode basis of the birefringence medium, and $\mathbf{T}(-\theta^{'})$ and $\mathbf{T}(\theta^{'})$ are the Jones matrices of birefringence medium when the signal photons go forward and backward of the single-mode delay lines, which are given by

$$\begin{aligned}\mathbf{T}(\pm\theta^{'}) = &\begin{bmatrix}\cos(\theta^{'}) & \mp\sin(\theta^{'})\\ \pm\sin(\theta^{'}) & \cos(\theta^{'})\end{bmatrix}\begin{bmatrix}e^{i\varphi_o} & 0\\ 0 & e^{i\varphi_e}\end{bmatrix}\\ &\times\begin{bmatrix}\cos(\theta^{'}) & \pm\sin(\theta^{'})\\ \mp\sin(\theta^{'}) & \cos(\theta^{'})\end{bmatrix}.\end{aligned} \tag{6}$$

Therefore, considering the polarization-altering properties of AM ($\zeta \approx 0$), the complete Jones matrix $\mathbf{T}_0 = \mathbf{T}_{AM+PM+FM}$ in a round trip is

$$\mathbf{T}_0 = \mathbf{T}(-\theta^{'})\mathbf{J}_{AM_x}\mathbf{J}_{PM_x}\mathrm{FM}(\theta)\mathbf{J}_{PM_y}\mathbf{J}_{AM_y}\mathbf{T}(\theta^{'}) \approx 0. \tag{7}$$

Equation (7) indicates an extreme situation in which the Gaussian modulation is completely disturbed by the polarization properties of AM. However, it might not be immediately clear whether there is an impact of the polarization properties of AM in the plug-and-play GMCS since none of the experiments have demonstrated it before. However, in a practical plug-and-play CV-QKD experiment, it is reasonable for us to assume that this arrangement may introduce huge extra loss (equivalently large excess noise in parameter estimation) because of the polarization drifts of the fiber channel.

In Fig. 1(c)(3), we resolve the problem and present a dual-phase-modulation scheme to prepare Gaussian coherent states. In fact, we can find that previous studies of plug-and-play DV-QKD systems are implemented with a single polarization-independent PM which features low losses in a round trip [47]. It is easy to write the transformation matrices of the dual-phase modulation scheme,

$$\begin{aligned}\mathbf{T}_{PM_1+FM_1} &= \mathbf{T}(-\theta^{'})\mathbf{J}_{PM_{1x}}\mathrm{FM}(\theta)\mathbf{J}_{PM_{1y}}\mathbf{T}(\theta^{'})\\ &= \varsigma_1 e^{i(\varphi_1)}\mathrm{FM}(\theta),\\ \mathbf{T}_{PM_2+FM_2} &= \mathbf{T}(-\theta^{'})\mathbf{J}_{PM_{2x}}\mathrm{FM}(\theta)\mathbf{J}_{PM_{2y}}\mathbf{T}(\theta^{'})\\ &= \varsigma_2 e^{i(\varphi_2)}\mathrm{FM}(\theta),\end{aligned} \tag{8}$$

where ς_1 and ς_2 are the equivalent attenuation coefficient of PM_1 and PM_2 respectively; φ_1 and φ_2 are electronically modulated phases of PM_1 and PM_2, respectively. Here we suppose the input Jones vector is $\widetilde{E}_{\mathrm{in}}$; the beam of light passes through a 50:50 beam splitter (BS) and is reflected by a FM. After a round trip, the output of dual-phase modulation $\widetilde{E}_{\mathrm{out}}$ can be expressed as follows:

$$\widetilde{E}_{\mathrm{out}} = \tfrac{1}{2}(\varsigma_1\widetilde{E}_{\mathrm{in}}e^{i(\varphi_1)} + \varsigma_2\widetilde{E}_{\mathrm{in}}e^{i(\varphi_2)})\mathrm{FM}(\theta). \tag{9}$$

In an ideal dual-phase modulation system with perfect optical components, we can get the same insertion loss in the two arms, $\varsigma \approx \varsigma_1 \approx \varsigma_2$. Thus, the output of dual-phase modulation in Eq. (9) can be simplified as

$$\widetilde{E}_{\mathrm{out}} = \varsigma\widetilde{E}_{\mathrm{in}}\exp\left[\frac{i(\varphi_1+\varphi_2)}{2}\right]\cos\left(\frac{\varphi_1-\varphi_2}{2}\right)\mathrm{FM}(\theta). \tag{10}$$

Equation (10) indicates an ideal Gaussian modulation by using two polarization-independent PMs instead of a polarization-dependent AM and a PM. In other words, the proposed modulation scheme of the DPMCS protocol works equivalently to that of the GMCS protocol. This also means that the polarization angle of returned quantum signal in our plug-and-play dual-phase modulation system will keep stable even if the polarization characteristics of the quantum channel vary randomly.

III. SECURITY ANALYSIS OF PLUG-AND-PLAY DPMCS QKD PROTOCOL

Based on the framework of plug-and-play DPMCS QKD protocol, the optical source transmitted from Alice to Bob becomes the most important battlefield for the Eve and legitimate parties. In fact, the source of the plug-and-play CV-QKD protocol is equivalently controlled by Eve. In this section, we explore the security of the proposed protocol with an untrusted source under realistic conditions of a lossy and noisy quantum channel and detector. First, we introduce the models of prepare-and-measurement scheme for the new protocol. Then we show that the entanglement-based scheme is equivalent to the prepare-and-measurement scheme. This equivalence is at the heart of security proofs for this type of CV-QKD protocols and it has been explained in detail in Refs. [45,48]. Since it might be no longer correct to assume that the prepared Gaussian state is a pure state, as is commonly assumed in standard security proof, we show that the secret key rate and secure distances can still be bounded with the consideration of the untrusted source.

A. Model description

Figure 2 shows the prepare-and-measure scheme of the plug-and-play DPMCS protocol. The source of light in our plug-and-play protocol is transmitted from Alice to Bob.

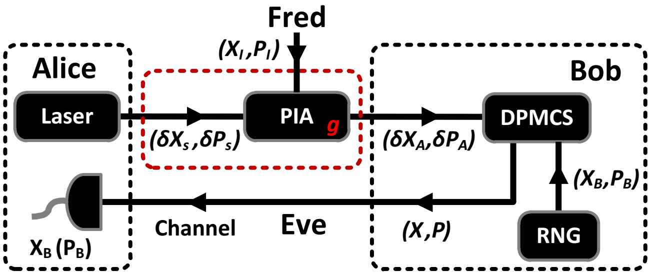

FIG. 2. The prepare-and-measure scheme of the plug-and-play DPMCS protocol with untrusted coherent source. A practical phase-insensitive amplifier (PIA) is placed at the channel. The PIA is a nondegenerate optical parametric amplifier, which amplifies symmetrically both quadratures, but such an amplification process will inevitably increase the noise induced by the coupling of the signal input to the internal modes of the amplifier [45].

Under the realistic assumption that Fred can control the classical source, the main consequence of this intervention is that it will inevitably increase a fundamental excess noise, because one cannot suppress the excess noise by increasing the variance of original source and then attenuating the state. In this scenario, we characterize the untrusted source noise by introducing a phase-insensitive amplifier (PIA). Such an unknown source can be viewed as a combination of an ideal coherent source with quadratures of $(\delta X_s,\delta P_s)$ which satisfy $\langle(\delta X_s)^2\rangle = \langle(\delta P_s)^2\rangle = 1$ (in shot-noise units), a PIA with a gain of g ($g \geqslant 1$), and an idle input of (X_I,P_I), which is ideally in a vacuum state or a realistic state with a noise variance of V_I. These serve the purpose of modeling Eve's intervention in the source, and the introduction of the amplifier models is because of their importance for various practical and technological applications including optical communication systems. The quadratures $(\delta X_A,\delta P_A)$ of an untrusted coherent state transmitted from Alice can be described as

$$\begin{aligned}\delta X_A &= \sqrt{g}\delta X_s + \sqrt{g-1}\delta X_I,\\ \delta P_A &= \sqrt{g}\delta P_s + \sqrt{g-1}\delta P_I.\end{aligned}\tag{11}$$

Therefore, the quadratures of the dual-phase-modulated coherent state sent from Bob to Alice are

$$\begin{aligned}X &= X_B + \delta X_A,\\ P &= P_B + \delta P_A.\end{aligned}\tag{12}$$

The modulated random numbers satisfy the Gaussian distribution, and the variances of X and P are

$$\langle X^2\rangle = \langle P^2\rangle = V + \xi_s,\tag{13}$$

where $V = V_B + 1$ and $\xi_s = g - 1 + (g-1)V_I$. The conditional variances $V_{X|X_B}$ and $V_{P|P_B}$ are

$$\begin{aligned}V_{X|X_B} &= \langle X^2\rangle - \frac{\langle XX_B\rangle^2}{\langle X_B^2\rangle} = \xi_s + 1,\\ V_{P|P_B} &= \langle P^2\rangle - \frac{\langle PP_B\rangle^2}{\langle P_B^2\rangle} = \xi_s + 1.\end{aligned}\tag{14}$$

The entanglement-based scheme of our DPMCS protocol with homodyne or heterodyne detections is illustrated in Fig. 3. Here we should remark that the entanglement-based scheme is kept equivalent to a standard prepare-and-measure scheme for the GMCS protocol, and the optimality of a Gaussian attack in the entanglement-based scheme is guaranteed under the general collective attack. In our equivalent entanglement-based scheme, Fred prepares a three-mode entanglement state $|\Psi_{ABF}\rangle$. The quadratures (X',P') and (X,P) denote the state (mode B) kept by Bob and the state (mode A_0) sent to Alice. We assume they satisfy the following relations:

$$\langle X^2\rangle = \langle P^2\rangle = V + \xi_s, \langle X'^2\rangle = \langle P'^2\rangle = V.\tag{15}$$

According to the uncertainty relation [48], we can have

$$|\langle XX'\rangle^2| \leqslant V(V+\xi_s) - \frac{V}{V+\xi_s}.\tag{16}$$

Because the ABF system might not be maximally entangled, the correlation between A_0 and B might not achieve the limit in Eq. (16). Therefore, it can be reasonably assumed that

$$|\langle XX'\rangle^2| = \sqrt{V^2-1}, \quad |\langle PP'\rangle^2| = -\sqrt{V^2-1}.\tag{17}$$

In the entanglement-based scheme, if Bob chooses to enable a heterodyne detection on X' and P' (mode B) simultaneously, we can get

$$X' = X' - \delta X'_B, \quad P' = P' - \delta P'_B,\tag{18}$$

where $\langle(\delta X'_B)\rangle^2 = \langle(\delta P'_B)\rangle^2 = 1$. Bob gets the estimation of (X,P), denoted by (X_B,P_B), which satisfy

$$X_A = \sqrt{\frac{V-1}{V+1}}X'_A, \quad P_A = \sqrt{\frac{V-1}{V+1}}P'_A.\tag{19}$$

We have $\langle X_B^2\rangle = \langle P_B^2\rangle = V_B$ and $V_{X|X_B} = V_{P|P_B} = \xi_s + 1$, which are results identical to those of the prepare-and-measure scheme scheme. In the prepare-and-measure scheme, the added noise induced by an imperfect homodyne detector (or heterodyne detector) refers to the receiver's input as $\chi_h = [(1-\eta) + \upsilon_{el}]/\eta$. The entanglement-based scheme is modeled by a beam splitter with a transmission efficiency of η and coupled with an Einstein-Podolsky-Rosen (EPR) state ρ_{H_0G} featuring a variance of υ_d, so the added noise is $(1-\eta)\upsilon_d/\eta$. In order to make the detection-added noise of the entanglement-based scheme equal $\eta\chi_h$, the variance υ_d should be $\upsilon_d = \eta\chi_h/(1-\eta) = (1-\eta+\upsilon_{el})/(1-\eta)$. Therefore, when we assume that the EPR source and Bob's detection are hidden in the black box, the eavesdropper cannot distinguish which scheme (prepare-and-measure scheme or entanglement-based scheme) is applied.

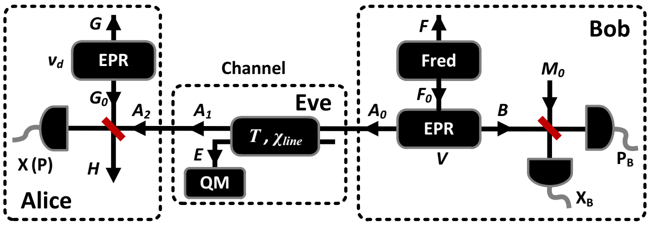

FIG. 3. The equivalent entanglement-based scheme of the DPMCS protocol. Eve can control the transmission efficiency T and channel-added noise χ_{line}. Though Eve does not have access to the apparatus of legitimate users, the source is equivalently controlled by Eve in the plug-and-play architecture. Therefore, in this entanglement-based scheme, Fred is not a neutral party. To derive a tight security bound, Fred is assumed to be controlled by Eve.

B. Security against collective attacks

In this section, we consider the security of the DPMCS CV-QKD protocol with reverse reconciliation. For simplicity, we consider the secret key rate when Alice performs homodyne detection. In order to derive a tight security bound, the model assumes that Fred can be controlled by Eve, which means Eve may acquire extra information. Similar to the GMCS protocol, the secret key rate can be calculated as

$$K' = \beta I_{AB} - \chi_{AE},\tag{20}$$

where χ_{AE} is the maximum information available to Eve on Alice's key. In the DPMCS protocol, the Shannon mutual information between Alice and Bob I_{AB} is derived from Alice's measured variance $V_A = \eta T(V + \xi_s + \chi_{\text{tot}})$ and the conditional variance $V_{A|B} = \eta T(1+\xi_s+\chi_{\text{tot}})$, where $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T$ is the same as the GMCS protocol. Using Shannon's equation, the mutual information can be expressed as

$$I_{AB} = \frac{1}{2}\log_2\frac{V_A}{V_{A|B}} = \frac{1}{2}\log_2\frac{V+\xi_s+\chi_{\text{tot}}}{1+\xi_s+\chi_{\text{tot}}}. \tag{21}$$

Eve's information on Alice's key is bounded by the Holevo quantity

$$\chi_{AE} = S(\rho_E) - \int dm_A p(m_A) S(\rho_E^{m_A}), \tag{22}$$

where S is the von Neumann entropy of the quantum state ρ, $\rho_E^{m_A}$ is the Eve's state conditional on Alice's measurement result, m_A represents the measurement of Alice (and in the homodyne detection, it can take the form $m_A = x_A$), and $p(m_A)$ is the probability density of the measurement [49]. Since Eve can purify the system FBA_1, we get $S(\rho_E) = S(\rho_{FBA_1})$. After Alice's measurement (purifies the system FBEHG), the global pure state collapses to ρ_{FBEHG}, and we get $S(\rho_E^{m_A}) = S(\rho_{FBHG})$. We can find that $S(\rho_E^{m_A})$ or $(S(\rho_{FBHG})$ is independent of m_A for the Gaussian protocols. Then Eve's maximum information can be bounded by

$$\chi_{AE} = S(\rho_{FBA_1}) - S(\rho_{FBHG}^{m_A}). \tag{23}$$

However, because of the eavesdropper's intervention, the Bob's prepared state ρ_{BFA_0} might not be a pure state, and the optimality of Gaussian attacks has not been proved under this condition. In other words, we cannot bound the maximal information that Eve could gain by exploiting the optical source, arguably the most critical part of the security analysis. Fortunately, if we assume that ρ_{BFEA_0} is a pure state, we can achieve a lowest bound of K' when ρ_{BFA_0} is a Gaussian state [20–22]. Thus, it is enough to consider Gaussian states in the derivation of a lower bound of the secret key rate, and the expressions for the above equation can be further simplified as [40,45]

$$\chi_{AE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{24}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix γ_{FBA_1} characterizing the state ρ_{FBA_1}, and $\lambda_{1,2,3}$ can be expressed as

$$\lambda_{1,2}^2 = \tfrac{1}{2}(A \pm \sqrt{A^2 - 4B}), \tag{25}$$

where

$$A = V^2 - 2T(V^2-1) + T^2(V+\xi_s+\chi_{\text{line}})^2,$$
$$B = T^2[1 + V(\xi_s + \chi_{\text{line}})]^2, \tag{26}$$

and $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix γ_{FBHG} characterizing the state $\rho_{FBHG}^{m_A}$, and $\lambda_{4,5,6,7}$ can be expressed as

$$\lambda_{3'4}^2 = \tfrac{1}{2}(C \pm \sqrt{C^2 - 4D}), \lambda_5 = 1, \tag{27}$$

where

$$C = \frac{A\chi_h + V\sqrt{B} + T(V+\xi_s+\chi_{\text{line}})}{T(V+\xi_s+\chi_{\text{tot}})},$$
$$D = \frac{\sqrt{B}V + B\chi_h}{T(V+\xi_s+\chi_{\text{tot}})}. \tag{28}$$

Based on Eqs. (21), (24), (25), (26), (27), and (28), we can calculate the asymptotic lower bound of the secret key rate in Eq. (20) against collective attacks.

C. Theoretical security simulation and practical security analysis

The theoretical security simulation result is shown in Fig. 4. We apply the results derived in the above and several practical parameters of the previous GMCS CV experiments that intervene in these equations in order to compare their performance for different configurations. The parameters V_B, ξ_c, η, υ_{el}, and β are fixed in the simulations. The noise variance V_I of the PIA is set to 1 (in shot-noise units). The security bound to the imperfect coherent source is weighted by the parameter g. From a practical point of view, it is interesting to directly compare the performance of the secret key rate K' in different imperfect source scenarios. For the reasonable parameters $g = 0$ (zero noise gain), 0.001, and 0.01, we observe that the key rates are slightly affected by the noise of the coherent source. Practically, it is easy to understand that if the states Alice sent turn noisy (in the presence of Fred's interaction), the secret key rate and maximum secure distance will be reduced. Fortunately, the source noise weighted by g can be carefully measured with a practical detector at Bob's side.

Here let us discuss some practical countermeasures for the reported attacks. Consider the case of the Trojan-horse attacks [36,37]. When Alice sends strong classical pulses to Bob, Eve is able to freely manipulate these pluses, or she may even replace them with her own sophisticatedly prepared

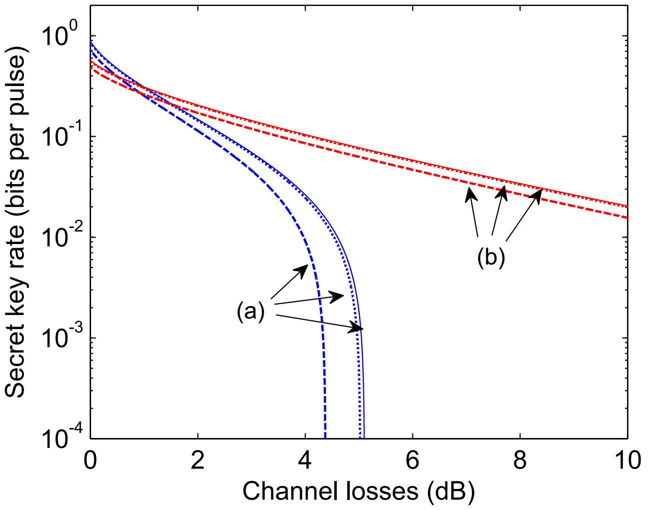

FIG. 4. Secret key generation rate as a function of channel losses for the DPMCS protocol with homodyne detection and a phase-insensitive amplifier in the case of collective eavesdropping attacks. The blue curves correspond to the fixed parameters: (a) $V_B = 20$, $\xi_c = 0.04$, $\eta = 0.5$, $\upsilon_{el} = 0.01$, and $\beta = 0.9$, which are achievable in the experiments of Refs. [11–13], and the red curves corresponds to the fixed parameters; (b) $V_B = 4$, $\xi_c = 0.01$, $\eta = 0.5$, $\upsilon_{el} = 0.01$, and $\beta = 0.97$, which are achievable in the recent experiments of Refs. [8–10]. From right to left, the solid, dotted, and dashed (blue or red) lines represent the key rate for $g = 0$, 0.001, and 0.01.

bright pulse to Bob and split the corresponding output pulses from Bob. In order to limit these kind of attacks, filters should be inserted at Bob's side to enable single-mode assumption in the plug-and-play CV-QKD system. Second, the "modulation door" should be open only during encoding time, i.e., activating the phase modulator only when optical pulses are there. We remark that the "time door" may challenge current modulation techniques because of the limited bandwidth, so that Eve may exploit the finite rising or falling edge of modulated pulses and then implement phase-remapping attacks [50,51]. Previous work has also shown that Bob can use a classical detector to monitor the input pulses to combat this kind of intercept-resend attack. Therefore, we assume that the designer of the plug-and-play CV-QKD has examined each of the above points. However, obviously the most important one is that we should compute the maximal information that Eve could gain by exploiting the optical source. In other words, we should calculate the amount of leaked information so that we can compute how much additional privacy amplification is required to successfully defeat such kinds of attacks.

Fortunately, we could find some ways to calculate the source noise and improve the secret key rate. First, we note that previous studies of the imperfect source noise effects on the GMCS QKD have shown results similar to our own, since the source noise in coherent-state generation and Gaussian signal preparation would also undermine the secret key rate [40–44]. They considered Fred as a neutral-party model who cannot be controlled by Eve, and the key rate of the neutral model can be improved using a passive source monitoring approach to bound the leaked information induced by Eve's manipulation [41]. However, in our untrusted model, the modulation noise is also ascribed to Eve for simplicity. Therefore, the system's performance might be improved by designing a bidirectional monitoring apparatus at Bob's side so that the modulation noise is bounded. Besides, researchers also studied the CV-QKD using thermal (or noisy) Gaussian resource states [52–54]. Though the preparation noise at the sender's station becomes significantly noisy (even 10^4 times greater than the variance of the vacuum mode), there still exist secret keys with direct reconciliation. This is because, provided the channel losses do not exceed 50%, the security of quantum cryptography is not dependent on the channel transmission and is therefore incredibly robust against significant levels of impurity of sender states. In our theoretical security model, we consider the reverse reconciliation and a pure coherent state sent from Alice to Bob so that the secure distance could break the 3-dB limit [5,6]. If we take into account the imperfect generation of coherent states, i.e., a coherent laser source with nonignorable phase noises [55], it is necessary to carefully characterize such kind of source noise by using a monitoring apparatus at Alice's side.

IV. EXPERIMENT

A. Experimental setup

Figure 5 shows the configuration of a proof-of-principle CV-QKD experiment based on the plug-and-play DPMCS protocol. At Alice's side, a continuous-wave (cw) output from a center wavelength of a 1550.12-nm laser splits into two portions with an intensity ratio of 99:1, a fraction (1%) of which is attenuated and sent to Bob; the other portion (99%) is used as a locally generated LO. The linewidth of the cw laser is 1.5 kHz, and the short-term stability of the laser is less than 4 MHz per hour. The small portion of cw light is transformed into a 1-MHz clock pulse train by a $\mathrm{LiNbO_3}$ AM. We generate optical pulses with a full width at half maximum (FWHM) of 200 ns. The length of fiber spool is 20 km and the measured loss of the fiber link is 0.2 dB/km. At Bob's side, the optical pulses transmitted from the quantum channel are split into two groups again, a fraction of which is used to monitor the input pulses using a photodiode (PD) that is important to defeat the phase-remapping attacks [51] and the pulse-shape attacks [56], the other of which goes through the BS and Gaussian modulated by two PMs, as we described in Sec. II C. A small amount of modulated signal is detected by a PD and used to monitor the modulation variance in real time. A variable optical attenuator is used by Bob to attenuate modulated pulses to an optimized variance of $V_B N_0$. In the plug-and-play protocol, the forward and backward propagation gives perfect polarization stability, but the 45° FM will impose a 90° rotation on the polarization of input coherent states. The delay fiber line at Bob's side compensates the difference of fiber length for two phase-modulation paths. The classical optical pulses and quantum signal pulses propagate through the quantum channel with orthogonal polarizations and different directions, and they are also delayed in time. At Alice's side, the LO pulses are transmitted through a PBS and reflected by a FM, which provides a 90° polarization rotation on LO's polarization. Besides, Alice can measure randomly X_0 or $X_{\pi/2}$ to select one of the two quadratures of quantum states by

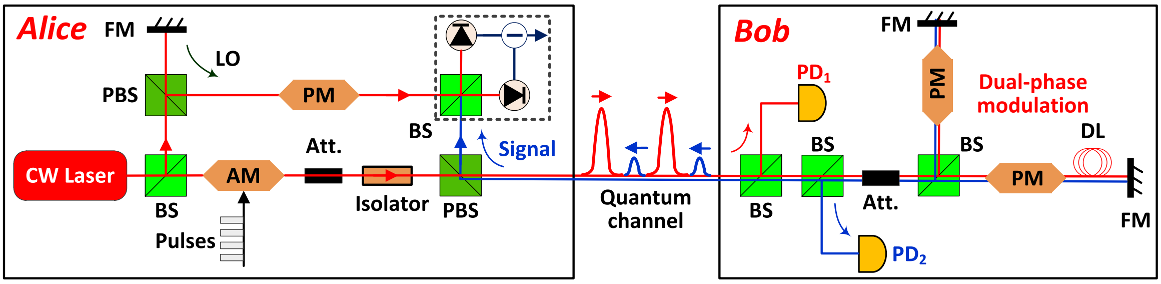

FIG. 5. Experimental setup of plug-and-play CV-QKD using dual-phase modulated coherent states. cw laser, continuous-wave laser; BS, beam splitter; AM, amplitude modulator; Att., attenuator; PM, phase modulator; PBS, polarizing beam splitter; DL, delay line; FM, faraday mirror; PD, photodetector.

using a PM located on a LO path. The optical quantum states reflected through a PBS will interfere with the LO, and a shot-noise-limited homodyne detector is used to measure these quantum states.

In laboratory circumstances, this preliminary experiment does not insert wavelength filters at both sides that could pose risks as explained in at the beginning of Sec. III, but we should stress that it is one of the most suitable countermeasures against Trojan-horse-type attacks in the further field test of plug-and-play CV-QKD. Besides, as we discussed in Sec. III C, a watchdog detector countermeasure should also be inserted at Alice's side in the next step to monitor the stability of the laser source. This is because the laser source noise can be treated as the noise introduced by a neutral party instead of an untrusted party; thus, this arrangement could further improve the system performance. We note that a self-referenced phase-compensation scheme is necessary to align Alice's and Bob's measurement bases [31–33], since there exists an unavoidable phase drift due to environmental perturbations on the well-established fiber spool. The security of the phase-compensation scheme using classical phase-reference pulses was carefully discussed in these independent works. Finally, raw bits of data are then processed into the error reconciliation and privacy amplification using public communication.

B. Polarization measurement

In a typical coexistence architecture of CV-QKD based on polarization-multiplexing techniques [10], the noise photons in the quantum channel are mainly contributed by the in-band leakage photons from the strong classical light of LO [8,9,13]. In fact, almost all of the recently reported CV-QKD experiments [8–10] employed manual polarization controllers or dynamic polarization controllers. As we described above, the LO is locally generated at receiver's side in the proposed plug-and-play DPMCS protocol, so that we no longer need polarization stabilization for LO signals.

Now we focus on the polarization properties of the distributed quantum states. Figure 6 shows the polarization traces on the Poincaré sphere measured with a polarization analyzer (PSGA-101, General Photonics). Limited by the dynamic power range of our analyzer (−40 to +2 dB m), the attenuators at both sides are adjusted to get a minimum attenuation value. Each point on the Poincaré sphere represents a unique polarization state. It takes 3 h and 30 min to measure the polarization drifts at Bob's side and Alice's side, respectively. If we consider the use of the one-way GMCS QKD protocol without active polarization stabilization, such an arrangement of CV-QKD system would inevitably produce a slow polarization drift that occurs in the transmission-fiber spool because of mechanical strains or temperature changes [see Fig. 6(a)]. What is remarkable here is that the above technological challenge of polarization stabilization is also encountered in the recent studies of CV-QKD without sending a LO [31–33]. Different from our recent work [31], the present experiment not only compensates the polarization drift by taking advantage of plug-and-play Faraday QKD protocol [see Fig. 6(b)], but also generates a local LO at the receiver's side.

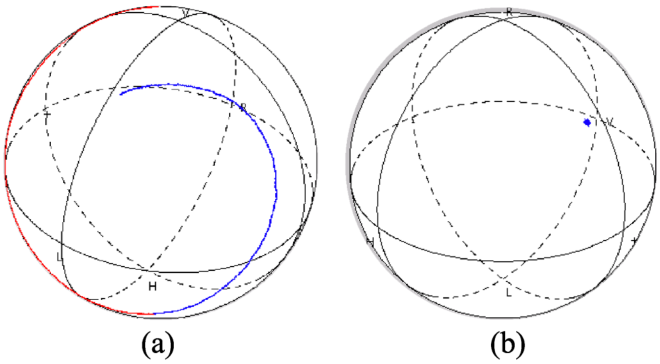

FIG. 6. (a) Polarization traces measured at the input of Bob's apparatus. (b) Polarization traces measured at Alice's side (between the input of homodyne detector and the output of PBS; see Fig. 5).

C. Rayleigh backscattering estimation

In the plug-and-play CV-QKD experiment, we need to consider the effects of Rayleigh backscattering of the quantum channel itself. Recently, researchers have shown that spontaneous anti-Stokes Raman scattering is the dominant source of noise in the one-way dense-wavelength-division-multiplexing (DWDM) CV-QKD configuration [9,57]. These results revealed that CV-QKD can benefit from a built-in single-mode filtering (coherent detection) and therefore this QKD protocol can be less affected by DWDM-induced noise photons than the reported DV-QKD systems. However, in the proposed plug-and-play DPMCS protocol we solved some technical and security problems; the plug-and-play structure introduces some other problems of its own: The coherent detection of quantum states at Alice's side would suffer Rayleigh scattering by fiber refractive index inhomogeneities. Because this reflected light is of the same frequency as the initial laser source, the "in-band" photons cannot be filtered or attenuated. The excess noise ξ_{RB} (refer to Bob's side) induced by Rayleigh backscattering photons $\langle N_{RB}\rangle$ can be expressed as

$$\xi_{RB} = 2\langle N_{RB}\rangle/(\eta T). \tag{29}$$

Here we consider an infinite fiber used as a QKD link, which features a length L (km) and a fiber loss α (dB/km). The channel transmission efficiency $T = 10^{-\alpha L/10}$. The insertion loss inside Bob (round-trip) is denoted as η_B. The backscattered photons $\langle N_{RB}\rangle$ per second P_B can be given by [38]

$$P_B = \beta(1 - 10^{-2\alpha L/10})\mu R/\eta_B T, \tag{30}$$

where β represents the Rayleigh backscattering coefficient which means a fraction of forward-propagated light backscattered into the fiber spatial model, $\mu = V_B/2$ is the mean number of photons per pulse emitted from Bob's side, and R is the system repetition rate. If we assume that the electronic integral time (rise and fall time) of Alice's homodyne detector is δt, the excess noise contributed by the quantum channel itself is

$$\xi_{RB} = \frac{2P_B\eta\delta t}{\eta T} = \frac{\beta(1 - 10^{-2\alpha L/10})V_B R\delta t}{\eta_B 10^{-2\alpha L/10}}. \tag{31}$$

In this preliminary experiment, we use a standard SMF-28e+ optical-fiber spool (Corning) [58], and the given Rayleigh backscattering coefficient β is -80 dB at 1550 nm. To estimate the scattering effects in this plug-and-play CV-QKD experiment, we use some achievable parameters: $\beta = -80\,\text{dB}$, $\alpha = 0.2\,\text{dB/km}$, $L = 20\,\text{km}$, $V_B = 4$, $R = 1\,\text{MHz}$, $\delta t = 1\,\mu\text{s}$, and $\eta_B = 20\,\text{dB}$. According to Eq. (31), the excess noise ξ_{RB} induced by Rayleigh backscattering could be controlled in the order of 0.02. While in the previous experiments [9,57] the excess noise induced by Raman scattering can be reduced to 10^{-5} by using an attenuated transmission optical power. From a more practical point of view, we could find some ways to further reduce the excess noise ξ_{RB}. Intuitively, we can reduce the integral time δt by using a wideband shot-noise-limited homodyne detector and preparing optical pulses with a narrow FWHM. For example, if we control the FWHM within 10 ns and use a gigahertz bandwidth homodyne detector [9,59], we can reduce the excess noise ξ_{RB} by two orders of magnitude. Reducing the insertion loss η_B might be another solution since it could enable us to decrease the transmission optical power of Alice. In our proposed protocol, we employ polarization-independent PM instead of polarization-dependent AM so that the η_B keeps in a stable and low level. However, because of the risk of Eve using Trojan-horse attacks, η_B should not be arbitrarily small [38].

D. Excess noise measurement

The parameter estimation is a completely standard procedure, in particular, the excess-noise measurement is arguably the most crucial step of CV-QKD. In the plug-and-play system, Alice sends some information to Bob so that he can compute a confidence region for the covariance matrix in the derivation of the secret key rate [25]. Therefore, in order to pass the parameter estimation test, one should apply a trade-off between the expected secret key rate and the robustness. In practice, it is necessary for us to determine the excess noise of quantum channel ξ_c. For the previous one-way GMCS protocol, we can consider a normal linear model for Alice and Bob's correlated variables $(x_i, y_i)_{i=1,2,\ldots,m}$, and $y = \sqrt{\eta T}x + z$, where z follows a centered normal distribution with a variance of $\sigma^2 = N_0 + \eta T \xi_c + \upsilon_{el}$. Using these independent estimators, we can calculate the ξ_c and then compute a secret key rate. However, the excess-noise estimation becomes slightly more complex in our experiment, since we have discussed an untrusted source model that should be added in the plug-and-play configuration (see Sec. III).

Here we mainly take into account the potential technical imperfections that are not due to Eve but might be considered as untrusted sources. In our preliminary experiment, the excess noise due to the untrusted sources is expected to be

$$\xi_s = \xi_s^{Eve} + \xi_{\text{laser}} + \xi_{\text{pulse}} + \xi_{\text{modulation}}, \tag{32}$$

where ξ_s^{Eve}, ξ_{laser}, ξ_{pulse}, and $\xi_{\text{modulation}}$ represent the excess noise induced by Eve's intervention in the source, laser diode phase noise, pulses modulation at Alice's side, dual-phase-modulation at Bob's side, respectively. It is clear that all of these noise sources could be manipulated by Eve if they are not well calibrated. We emphasize that there might exist some other noise sources potentially accessible to Eve, but all of them should be calculated from the final raw data. In this "paranoid mode," we can estimate and control the magnitude of excess noise induced by technical imperfection. This experiment implemented with an external pulse-modulation scheme at Alice's side based on a narrow-linewidth cw laser, which features a lower phase noise compared with the pulsed distributed feedback laser (DFB). In previous studies, the signal modulation was based on noisy pulsed DFB, and the total measured excess noise was $\xi_{\text{tot}} = 0.06N_0$ for a modulation variance $V_A = 40N_0$ and decreases proportionally for lower modulation variances [55,60]. In our case, the modulation variance is around 4. Therefore, a typical value for the noise variances $\xi_{\text{laser}} + \xi_{\text{pulse}}$ and $\xi_{\text{modulation}}$ would be around $0.01N_0$.

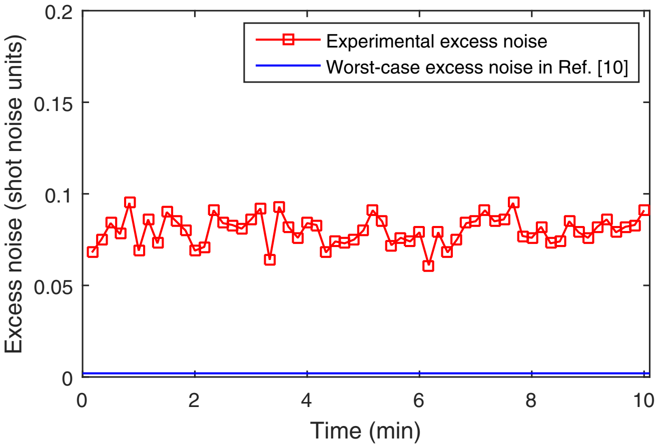

FIG. 7. Experimental excess noise measured at Alice's side (red squares). The blue line corresponds to the worst-case excess noise reported in Ref. [10].

Figure 7 shows the experimental excess noise measured on blocks of size 1×10^7. These excess noise points represent the system noises that might be controlled by Eve, including the source noise, the noise induced by Rayleigh backscattering, and so on. They also illustrate the stability of our system. Here we need to clarify that the apparently useless portion of experimental data frame should be directly discarded in the sifted key distillation, since these raw data blocks might have been hacked by an eavesdropper. In our 20-km plug-and-play CV-QKD experiment, the measured excess noise is around 0.08, which is higher than most of the previous experiments, i.e., the reported values of excess noise ξ_c were 0.056 [13] and 0.04 [16]. In the state-of-art 53-km one-way CV-QKD experiment, the reported worst-case excess noise was less than 0.002 [10]. This is due in part to the fact that the imperfect frequency stabilization of laser source and the variation of transmission delay would make it difficult to compensate the fast phase drifts between the LO and the quantum signal. The security study of the excess noise induced by the imperfect phase compensation is discussed in our recent works [8,61]. We note that several groups have reported the phase-compensation scheme for CV-QKD [8,32,33]. However, it still provides significant experimental challenges to overcome fast phase drifts under a low-SNR situation not only for the present plug-and-play protocol but also for recent

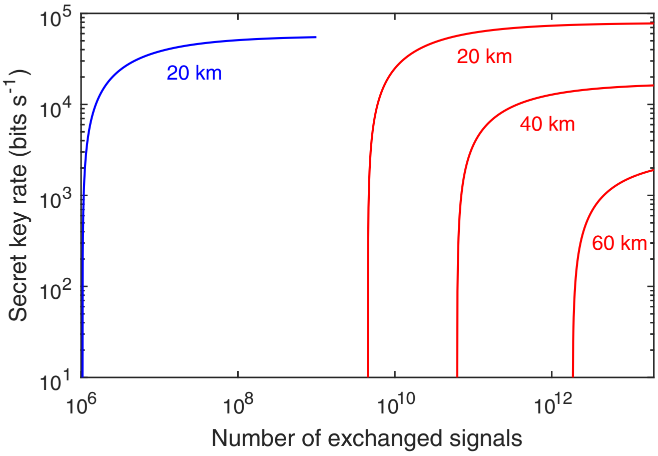

FIG. 8. Security thresholds based on the uncertainty principle (blue line) and the composable security framework (red line). From left to right, the transmittance of the quantum channel corresponds to distances of 20 km (blue), 20 km (red), 40 km (red), and 60 km (red) with a typical loss of 0.2 dB/km. The blue line corresponds to the secret key rates calculated from the proof-of-principle experiment based on the same finite-size security of previous experiment [10,23]. Red lines correspond to the respective asymptotic expected secret key rates in different finite-size blocks of exchanged signals [25]. The modulation variance V_B is 4; the excess noise ξ is 0.08; the reconciliation efficiency β is 0.97; the robustness parameter ϵ_{rob} is less than 10^{-2}; the security parameter ϵ is 10^{-20}.

independent one-way protocols without sending a LO [31–33]. Another important reason is that in the plug-and-play structure, the system has to suffer a Rayleigh backscattering effect. Though the present QKD does not coexist with other copropagating classical channels, the backscattering noisy photons produce more excess noise than that of Raman scattering. Further improvement of the experiment should focus on the optimization of system parameters so that the excess noise can be controlled within a lower level.

E. Security thresholds in the composable security framework

The secret key rate of our proof-of-principle experiment is based on the assumption of collective attacks. We note that in the composable security framework [25], the secret key rate is asymptotically equal to the one assuming a Gaussian attack and it is quite different from the case for the proof based on the uncertainty principle [23], which was employed in the previous state-of-the-art CV-QKD experiment [10]. Indeed, the security threshold calculated in this rigorous framework becomes much tighter and it also puts forward higher requirements of the number of exchanged signals.

In Fig. 8, we calculated security thresholds based on the uncertainty principle (blue line) and the composable security framework (red lines). We plot the secret key rate as a function of the number of exchanged signals. For simplicity, the simulation parameters for the expected key rates in long-distance conditions are fixed as our 20-km experiment. However, it is also worth mentioning that achieving a good reconciliation efficiency β at any SNR is necessary for us to work with a wider range of modulation variance V_B. Our previous work demonstrated a high-performance Low Density Parity Check (LDPC) code (an efficiency of 97%) [62] for a one-way 50-MHz GMCS QKD experiment [9]. Therefore, in this simulation, it is reasonable for us to assume that we can perform the reconciliation step at any distance. Besides, in our experiment, the realistic finite-size data block of exchanged signals is between 10^6 and 10^9 (see blue line), which allows us to achieve a secure distance up to 20 km.

An important issue concerning the secret key rate and secure distance is that the parameter estimation procedure requires a large amount of exchange signals in not only the conventional one-way CV-QKD protocol but also our plug-and-play protocol. This is because the efficiency of the CV protocols will decrease with the increasing of the exchanged bits that are sacrificed. In order to achieve a distance of 60 km, a number of exchanged signals between 10^{13} and 10^{14} is necessary. We note that our protocol is much simpler than pervious protocols to realize a 100-MHz shot-noise-limited homodyne detection, since it does not need to continue increasing the sender's transmitting power according to the growing demand of secure distance. It means that larger blocks are also practical over a longer period of sampling time for further high-speed CV-QKD.

V. CONCLUSION

We proposed a dual-phase-modulated coherent-states QKD protocol, and we also experimentally demonstrated such a plug-and-play protocol over a 20-km fiber channel. In this protocol, a legitimate sender can use the polarization-insensitive dual-phase modulation to prepare Gaussian states so that this intrinsically stable protocol preserves the simplicity and security of one-way Gaussian cryptographic protocols. In particular, a long outstanding problem associated with the transmitted LO is solved because we can benefit from the plug-and-play scheme in which a real local LO will be generated from the same laser of quantum signal at the receiver's side, and does not need to propagate through the insecure quantum channel. Besides, in our previous high-speed experiment, one of the limitations of the secure distance is that the gigahertz quantum detectors require sufficient LO power to operate well within the shot-noise limit [9]. Therefore, compared with previous one-way CV-QKD schemes, we can find that this arrangement could not only remove all of the security loopholes related with the transmitted LO, but also provide greater flexibility of high-speed shot-noise-limited measurement by controlling the optical power of the local LO. Therefore, this scheme might be very suited for gigahertz CV-QKD in the future.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61170228, No. 61332019, No. 61471239, and No. 61501290), the National Program On Key Research Project of China (Grant No. 2016YFA0302600), and the Hi-Tech Research and Development Program of China (Grant No. 2013AA122901).

[1] H. K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] L. B. Samuel and V. L. Peter, Rev. Mod. Phys. **77**, 513 (2005).
[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[7] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[8] D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, Sci. Rep. **6**, 19201 (2016).
[9] D. Huang, D. K. Lin, P. Huang, C. Wang, W. Q. Liu, S. H. Fang, and G. H. Zeng, Opt. Express **23**, 17511 (2015).
[10] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).
[11] Q. D. Xuan, Z. S. Zhang, and P. L. Voss, Opt. Express **17**, 24244 (2009).
[12] 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, Phys. Rev. A **76**, 042305 (2007).
[13] B. Qi, L. L. Huang, L. Qian, and H. K. Lo, Phys. Rev. A **76**, 052323 (2007).
[14] M. Legre, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **6**, 326 (2006).
[15] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nat. Commun. **6**, 8795 (2015).
[16] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle–Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).
[17] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle–Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express **20**, 14030 (2012).
[18] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).
[19] D. Huang, P. Huang, H. S. Li, T. Wang, Y. M. Zhou, and G. H. Zeng, Opt. Lett. **41**, 3511 (2016).
[20] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[21] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[22] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[23] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[24] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[25] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[26] J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **87**, 062329 (2013).
[27] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **87**, 052309 (2013).
[28] H. Qin, R. Kumar, and R. Alléaume, Proc. SPIE **8899**, 88990N (2013).
[29] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[30] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **88**, 022339 (2013).
[31] D. Huang, D. K. Lin, P. Huang, and G. H. Zeng, Opt. Lett. **40**, 3695 (2015).
[32] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).
[33] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).
[34] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[35] T. Gehring, C. S. Jacobsen, and U. L. Andersen, arXiv:1507.01003v2.
[36] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[37] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).
[38] D. Subacius, A. Zavriyev, and A. Trifonov, Appl. Phys. Lett. **86**, 011103 (2005).
[39] Y. Zhao, B. Qi, and H. K. Lo, Phys. Rev. A **77**, 052327 (2008).
[40] P. Huang, G. Q. He, and G. H. Zeng, Int. J. Theor. Phys. **52**, 1572 (2013).
[41] Y. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).
[42] Y. Shen, J. Yang, and H. Guo, J. Phys. B **42**, 235506 (2009).
[43] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[44] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[45] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).
[46] Photoline, Technical notes of $\mathrm{LiNbO_3}$ modulators, http://www.photonics.ixblue.com/technical-notes/faq.
[47] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005).
[48] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[49] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).
[50] C.-H. Fred Fung, B. Qi, K. Tamaki, and H. K. Lo, Phys. Rev. A **75**, 032314 (2007).
[51] F. H. Xu, B. Qi, and H. K. Lo, New J. Phys. **12**, 113026 (2010).
[52] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
[53] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[54] C. S. Jacobsen, T. Gehring, and U. L. Andersen, Entropy **17**, 4654 (2015).
[55] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).
[56] S. H. Sun, F. H. Xu, M. S. Jiang, X. C. Ma, H. K. Lo, and L. M. Liang, Phys. Rev. A **92**, 022304 (2015).
[57] R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015).
[58] Corning, SMF-28e+ optcial fiber, http://www.corning.com/worldwide/en/products/communication-networks/products/fiber/optical-fiber-products.html.
[59] D. Huang, J. Fang, C. Wang, P. Huang, and G. H. Zeng, Chin. Phys. Lett. **30**, 114209 (2013).
[60] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **72**, 050303 (2005).
[61] P. Huang, D. K. Lin, D. Huang, and G. H. Zeng, Int. J. Theor. Phys. **54**, 2613 (2015).
[62] D. K. Lin, D. Huang, P. Huang, J. Y. Peng, and G. H. Zeng, Int. J. Quantum Inf. **13**, 1550010 (2015).