Editors' Suggestion

Long-Distance Continuous-Variable Quantum Key Distribution with Entangled States

Ning Wang,[1,2] Shanna Du,[1,2] Wenyuan Liu,[1,2] Xuyang Wang,[1,2] Yongmin Li,[1,2,*] and Kunchi Peng[1,2]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, P. R. China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, P. R. China*

(Received 19 June 2018; revised manuscript received 5 September 2018; published 12 December 2018)

We experimentally demonstrate long-distance continuous-variable quantum key distribution over a 50-km standard optical fiber based on continuous-variable Einstein-Podolsky-Rosen entangled states. The entanglement survives despite being distributed over a high-loss optical fiber channel. At a channel excess noise level of 0.01 shot-noise units, we achieve an asymptotic secret key rate of 0.03 bit per sample, which is superior to the optimized coherent-state protocol. The superiority is even more evident at a high-channel excess noise level of 0.1 shot-noise units. Our work paves the way toward practical applications of continuous-variable quantum key distribution under high amounts of excess channel noise.

DOI: 10.1103/PhysRevApplied.10.064028

I. INTRODUCTION

Quantum entanglement, distributed among distant parties, plays a key role in quantum information processing. It serves as key resources in quantum teleportation, quantum key distribution (QKD), etc. [1,2]. Relying on the fundamental laws of quantum physics, QKD allows remote users to share an information-theoretically secure random bit string, which can be used as a secret key [3–6]. Combined with the one-time pad strategy, secure private communication can be achieved, which is necessary in a variety of domains [5].

Continuous-variable (CV) QKD encodes the key information in the quadratures of a light field and uses coherent detection techniques, such as homodyne (or heterodyne) detection [7–9]. Its advantages over qubit-based QKD protocols include cost-effective detection technique instead of dedicated single-photon-counting technology, higher key rates at metropolitan distances [10], and superior ability to coexist with classical signals in optical networks [11–13]. For practical implementations, a number of CV QKD protocols have been proposed and demonstrated [8–36] based on coherent states, squeezed states, and Einstein-Podolsky-Rosen (EPR) entangled states. Compared to the coherent-state protocol, the squeezed-state protocol is more robust against channel excess noises and can tolerate higher channel loss [22,23]. By using CV EPR sources, the modulated-entangled-states QKD protocol [24] and one-sided device-independent QKD protocol [29,30] have recently been proposed and demonstrated. However, these previous proofs of principle used short-distance free space as the quantum channel, and the optical loss of the transmission channel was modeled by a variable attenuator or an equivalent theoretical beam splitter.

In this article, we report the first long-distance CV QKD over a standard single-mode fiber based on a CV EPR entangled state. To this end, a two-color CV EPR state is prepared, and one beam of the EPR state at 0.8 μm is kept and measured at the side of the first participant (Alice), whereas the other one (Bob) uses a telecommunications wavelength of 1.5 μm, distributed over a 50-km single-mode fiber. By operating the EPR source in parametric deamplification and optimizing the relevant parameters, we suppress the carrier power of the EPR state to the level of 1 μW, which is low enough to avoid the undesired nonlinear scattering effects in optical fibers [37–39]. In addition, by developing polarization and time-multiplexing techniques, we can suppress the adverse effect of the intense local oscillator on the signal field during propagation along the same fiber. Using these approaches, CV EPR entanglement is successfully distributed over the long optical fiber with very low excess noise. We further demonstrate that CV QKD is feasible based on these distributed entangled states, with performance superior to the coherent-state protocol.

II. THEORETICAL ANALYSIS OF THE PROTOCOL

Figure 1(a) shows our QKD scheme with a mixed two-mode Gaussian entangled state, i.e., a mixed EPR state. The impure EPR states arise from the fact that any realistic preparation process of the EPR states inevitably introduces some linear losses (t_1, t_2) and excess noise (ξ_1, ξ_2) [2],

*liyongminwj@163.com

and perfect pure-EPR states do not exist in real scenarios. After preparing the EPR states, Alice keeps one partite of each state and sends the other partite to Bob via an insecure quantum channel, which is fully controlled by the third participant, Eve. This channel is characterized by the channel transmittance η and excess noise ε. Both Alice and Bob randomly measure the quadrature x or p of their respective modes by homodyne detection with respective detection efficiencies η_A and η_B. After the measurements, the measurement bases are announced via an authenticated classical channel, and only those samples measured in the same quadratures are retained. For the reverse reconciliation protocol considered here, Bob sends the syndrome of his data to Alice, and Alice corrects her data to be identical to that of Bob. Finally, Alice and Bob perform the privacy amplification step using two universal hash functions and extract the final secure key.

In the asymptotic limit of infinitely long exchanged signals, it is sufficient to consider the collective attack to ensure the security of our QKD protocol [40–43]. The corresponding secret key rate is given by

$$\Delta I = \beta I_{AB} - \chi_{BE}. \tag{1}$$

Here, β represents the data reconciliation efficiency, χ_{BE} represents the Holevo quantity between Bob's data and Eve's quantum states, and I_{AB} represents the Shannon mutual information between the measurement results of Alice and Bob, given by

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}} = \frac{1}{2}\log_2 \frac{V_A}{V_A - C_{AB}^2/V_B}, \tag{2}$$

where V_A and V_B are the variances of the quadratures measured by Alice and Bob, respectively. $V_{A|B}$ denotes the conditional variance, while C_{AB} denotes the correlation coefficient between Alice's and Bob's measured quadratures.

Consider a mixed two-mode Gaussian entangled state generated from a nondegenerate optical parametrical amplifier (NOPA). The variance of the modes' quadratures and the correlation coefficient and quantum correlation between the modes' quadratures are, respectively,

$$\begin{aligned} V_{A_0} = V_{B_0} &= \frac{1}{2}(1/s + s) + n_E, \\ C_{A_0B_0} = \langle \hat{x}_{A_0}\hat{x}_{B_0}\rangle = \langle \hat{p}_{A_0}\hat{p}_{B_0}\rangle &= \frac{1}{2}(1/s - s) + n_E, \\ \left\langle (\hat{x}_{A_0} - \hat{x}_{B_0})^2 \right\rangle = \left\langle (\hat{p}_{A_0} + \hat{p}_{B_0})^2 \right\rangle &= 2s, \end{aligned} \tag{3}$$

where s is the two-mode squeezing and n_E represents the excess noise of the antisqueezed quadrature. We assume the quantum channel is characterized by the transmittance η and excess noise ε; in this case, the variances of the quadratures measured by Alice and Bob are

$$V_A = \eta_A V_{A_0} + 1 - \eta_A, \quad V_B = G(V_{B_0} + \chi_{\text{tot}}), \tag{4}$$

where $G = \eta\eta_B$ is the total transmittance and

$$\begin{aligned} \chi_{\text{tot}} &= \chi_{\text{line}} + \chi_{\text{hom}}/\eta, \quad \chi_{\text{line}} = 1/\eta - 1 + \varepsilon, \\ \chi_{\text{hom}} &= (1 + \upsilon_{\text{el}})/\eta_B - 1. \end{aligned} \tag{5}$$

Here, χ_{tot} denotes the total added noise for the channel input site; χ_{line} denotes the channel added noise for the channel input site, which includes two parts: the noise due to linear losses (vacuum noise) and the excess noise ε; χ_{hom} denotes the added noise of the realistic homodyne detector for Bob's input site; and η_B and υ_{el} are the efficiency and electronic noise of the measurement apparatus. The correlation coefficient between Alice's and Bob's measured quadratures is

$$C_{AB} = \sqrt{\eta_A G}\, C_{A_0B_0} = \sqrt{\eta_A G}\left[\frac{1}{2}(1/s - s) + n_E\right]. \tag{6}$$

In order to facilitate the theoretical calculation of the secret key rate, the two-mode mixed EPR state is purified to a four-mode entangled state [24,44]. To this end, two independent EPR states are injected into a Mach-Zehnder interferometer in which two quadrature squeezers are located, as shown in Fig. 1(b). By setting six parameters, namely, the variances of the two EPR states (V_1, V_2), the transmittances of the two beam splitters (T_1, T_2), and the squeezing parameters of the squeezers (r_1, r_2), any two-mode Gaussian state AB_0 generated in our experiment can be represented by, and purified into, a four-mode entangled state $CDAB_0$.

We assume that the covariance matrix of the two-mode Gaussian states AB_0 generated in our experiment is given by

$$\gamma_{AB_0} = \begin{pmatrix} \gamma_A & \sigma_{AB_0} \\ \sigma_{AB_0}^T & \gamma_{B_0} \end{pmatrix} = \begin{pmatrix} V_A^x & 0 & C_{AB_0}^x & 0 \\ 0 & V_A^p & 0 & C_{AB_0}^p \\ C_{AB_0}^x & 0 & V_{B_0}^x & 0 \\ 0 & C_{AB_0}^p & 0 & V_{B_0}^p \end{pmatrix}. \tag{7}$$

The impure two-mode Gaussian states AB_0 can be purified by considering them to be part of a four-mode pure state $CDAB_0$. The covariance matrix γ_{CAB_0D} of the four-mode

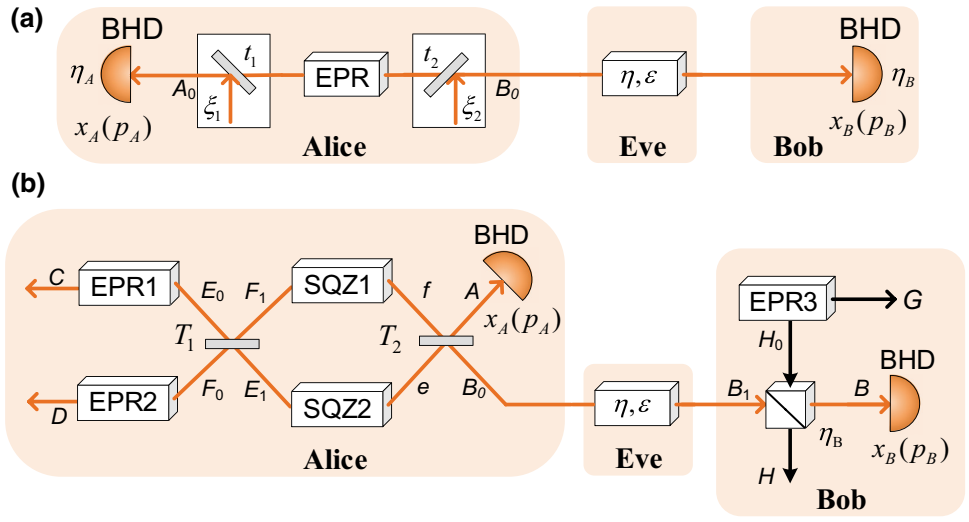

FIG. 1. Schematic diagram of the CV QKD protocol with entangled states. (a) The original protocol where Alice prepares a mixed two-mode entangled state. (b) The equivalent protocol where Alice purifies her mixed state to a four-mode pure state.

state can be obtained by using the following transformation:

$$\gamma_{CE_1F_1D} = Y_{BS1} \cdot \gamma_{CE_0F_0D} \cdot Y_{BS1}^T, \ \gamma_{CefD} = Y_S \cdot \gamma_{CE_1F_1D} \cdot Y_S^T,$$
$$\gamma_{CAB_0D} = Y_{BS2} \cdot \gamma_{CefD} \cdot Y_{BS2}^T, \tag{8}$$

where

$$Y_{BS1} = I_C \oplus S_{E_0F_0}^{E_1F_1} \oplus I_D, \quad Y_{BS2} = I_C \oplus S_{E_1F_1}^{ef} \oplus I_D,$$
$$Y_S = I_C \oplus S_{E_1} \oplus S_{F_1} \oplus I_D. \tag{9}$$

Here, I_C and I_D are the identity matrices, $S_{E_0F_0}^{E_1F_1}$ and $S_{E_1F_1}^{ef}$ are the beam splitter transformation matrices, and S_{E_1} and S_{F_1} are single-mode squeezing matrices [45]. In order to determine the related purification parameters V_1, V_2, T_1, T_2, r_1, and r_2, we refer to the solutions of the following set of six equations:

$$\gamma_{CAB_0D}[3,3] = V_A^x, \quad \gamma_{CAB_0D}[4,4] = V_A^p,$$
$$\gamma_{CAB_0D}[5,5] = V_{B_0}^x,$$
$$\gamma_{CAB_0D}[6,6] = V_{B_0}^p, \quad \gamma_{CAB_0D}[5,3] = C_{AB_0}^x,$$
$$\gamma_{CAB_0D}[6,4] = C_{AB_0}^p, \tag{10}$$

where $\gamma_{CAB_0D}[i,j]$ represents the matrix element in the ith row and jth column, which is a function of the six purification parameters $f_{i,j}(V_1, V_2, T_1, T_2, r_1, r_2)$, as described by Eq. (8). At this stage, all the elements of the matrix γ_{CAB_0D} are known, and the matrix γ_{CDAB_0} of the four-mode pure state $CDAB_0$ can be obtained by rearranging the lines and columns of the matrix γ_{CAB_0D}:

$$\gamma_{CDAB_0} = \begin{pmatrix} \gamma_C & \sigma_{CD} & \sigma_{CA} & \sigma_{CB_0} \\ \sigma_{CD}^T & \gamma_D & \sigma_{DA} & \sigma_{DB_0} \\ \sigma_{CA}^T & \sigma_{DA}^T & \gamma_A & \sigma_{AB_0} \\ \sigma_{CB_0}^T & \sigma_{DB_0}^T & \sigma_{AB_0}^T & \gamma_{B_0} \end{pmatrix}. \tag{11}$$

The mode B_0 is sent to Bob via an unsafe quantum channel (characterized by the transmittance η and excess noise ε). We can write the covariance matrix γ_{CDAB_1} by using the relationship

$$\gamma_{B_1} = \eta(\gamma_{B_0} + \chi_{\text{line}} I), \ \sigma_{AB_1} = \sqrt{\eta}\sigma_{AB_0}, \ \sigma_{DB_1} = \sqrt{\eta}\sigma_{DB_0},$$
$$\sigma_{CB_1} = \sqrt{\eta}\sigma_{CB_0}. \tag{12}$$

Here, I is the identity matrix. The mode B_1 received by Bob is detected by a realistic homodyne detector with electronic noise υ_{el} and quantum efficiency η_B. This imperfect detection can be modeled by applying a beam splitter transformation $S_{B_1H_0}^{BH}$ to the modes B_1 and H_0, where the transmittance of the beam splitter η_B models the efficiency of the detector and the thermal state H_0 with variance N_0 simulates the electronic noise υ_{el} of the detector. Thus, the covariance matrix γ_{CDABHG} of the six-mode state $CDABHG$ is given by

$$\gamma_{CDABHG} = Y[\gamma_{CDAB_1} \oplus \gamma_{H_0G}]Y^T, \tag{13}$$

where $Y = (I_{CDA} \oplus S_{B_1H_0}^{BH} \oplus I_G)$, I_{CDA} and I_G are the identity matrices, $S_{B_1H_0}^{BH}$ represents the beam splitter transformation matrix, and γ_{H_0G} is the covariance matrix of the EPR source H_0G.

The optimality of Gaussian attacks [40–42] provides a powerful tool to estimate the Holevo quantity using the covariance matrix formalism. The Holevo quantity χ_{BE} between Bob's data and Eve's quantum states is given by

$$\chi_{BE} = S(\rho_E) - S(\rho_E^{x_B}), \tag{14}$$

where $S(\rho)$ denotes the von Neumann entropy of the quantum state ρ, and $\rho_E^{x_B}$ represents Eve's quantum state conditional on Bob's detection results. As states ρ_{CDAB_1E} and $\rho_{CDAEHG}^{x_B}$ are pure, $S(\rho_E) = S(\rho_{CDAB_1})$ and $S(\rho_E^{x_B}) =$

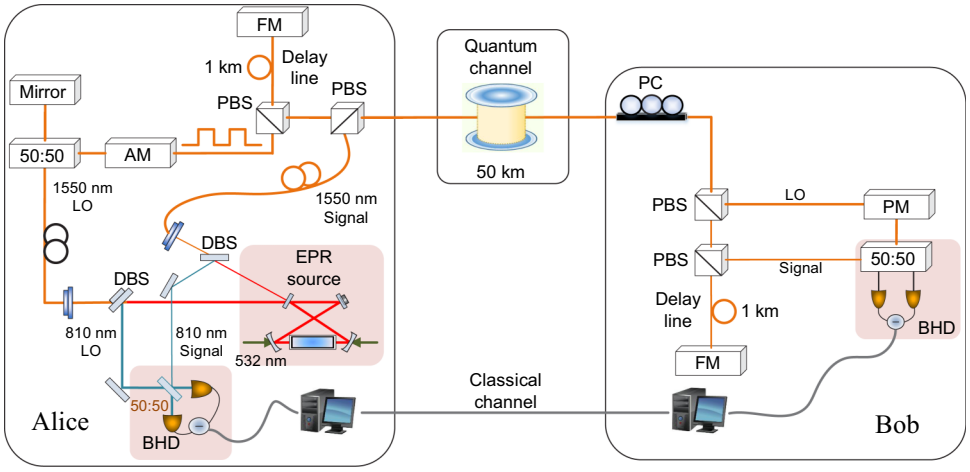

FIG. 2. Schematic of the experimental setup for continuous variable quantum key distribution with EPR states. Green line, 532-nm pump laser for the EPR source; red line, down-conversion fields; blue line, 810-nm signal (LO); orange line, 1550-nm signal (LO); DBS, dichroic beam splitter; FM, Faraday mirror; AM, amplitude modulator; PM, phase modulator; PBS, polarization beam splitters; BHD, balanced homodyne detector; PC, polarization controller.

$S(\rho^{x_B}_{CDAHG})$. Eq. (14) can be rewritten as

$$\chi_{BE} = S(\rho_{CDAB_1}) - S(\rho^{x_B}_{CDAHG}). \tag{15}$$

For the Gaussian states considered here, we have $S(\rho) = \sum_i G[(\lambda_i - 1)/2]$ with the bosonic entropic function $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. Here, λ_i represents the symplectic eigenvalues of the covariance matrix, which characterizes the state ρ.

The covariance matrix $\gamma^{x_B}_{CDAHG}$ describing the state $\rho^{x_B}_{CDAHG}$ conditional on Bob's detection results x_B is

$$\gamma^{x_B}_{CDAHG} = \gamma_{CDAHG} - \sigma_{CDAHG;B}(X\gamma_B X)^{MP}\sigma^T_{CDAHG;B}, \tag{16}$$

where

$$X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{17}$$

and MP stands for the Moore-Penrose matrix inverse. The matrices γ_{CDAHG}, γ_B, $\sigma_{CDAHG;B}$, and $\sigma^T_{CDAHG;B}$ are submatrices of the covariance matrix γ_{CDAHGB}

$$\gamma_{CDAHGB} = \begin{pmatrix} \gamma_{CDAHG} & \sigma_{CDAHG;B} \\ \sigma^T_{CDAHG;B} & \gamma_B \end{pmatrix}, \tag{18}$$

which can be obtained by permuting the elements of the matrix γ_{CDABHG} (13). At this stage, the Holevo quantity is given by

$$\chi_{BE} = \sum_{i=1}^{4} G[(\lambda_i - 1)/2] - \sum_{j=5}^{9} G[(\lambda_j - 1)/2], \tag{19}$$

where λ_i and λ_j are the symplectic eigenvalues of the covariance matrices γ_{CDAB_1} and $\gamma^{x_B}_{CDAHG}$, respectively. Here, the symplectic eigenvalues $\{\lambda_j\}$ can be obtained by finding the eigenvalues $\{\mp i\lambda_j\}$ of the matrix $\Omega\gamma$, where the symplectic form Ω is defined as

$$\Omega \equiv \oplus_{i=1}^{n}\omega, \quad \omega \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{20}$$

III. EXPERIMENTAL SETUP AND RESULTS

Figure 2 shows the schematic diagram of the experimental setup. A bright two-color continuous-wave EPR-entangled state, generated from a NOPA, is located at Alice's station. The NOPA consists of a bowtie-shaped cavity and a nonlinear periodically poled $KTiOPO_4$ (PPKTP) crystal. A 532-nm single-frequency laser is employed to pump the nonlinear resonator from two opposite directions. In one direction, the nonlinear resonator operates above threshold to produce bright down-conversion fields, which serve as local oscillators (LOs) for Alice's and Bob's homodyne detection and provide the seed field for the NOPA. In the other direction, the NOPA operates below threshold to generate the bright two-mode entangled state (see Ref. [46] for details of the EPR source). By operating the NOPA in parametric deamplification and optimizing the relevant parameters, the carrier power of the EPR state is effectively suppressed to around 1 μW, which is low enough to avoid the nonlinear scattering noise in a long-distance single-mode fiber.

Figure 3(a) illustrates typical quantum correlation outcomes when detecting either the amplitude quadrature (x_A, x_B) or the phase quadrature (p_A, p_B) of the EPR source with a balanced homodyne detector (BHD). The measurements are implemented at the sideband frequency of 3.5 MHz with a bandwidth of 500 kHz. Quadrature correlations (with a correlation coefficient of 0.95) are clearly visible between Alice's and Bob's measurement results when they simultaneously measure the same quadrature of their modes. From the measurement results, the two-mode squeezing and antisqueezing levels are 4.7 and 11.2 dB, respectively. The corresponding value of the EPR criterion [2] is $\sqrt{V^x_{A|B} \cdot V^p_{A|B}} = 0.65 < 1$, which indicates the generated two-mode state is indeed quadrature entangled.

One mode of the EPR source at 810 nm is kept by Alice herself and directed to a free-space BHD, where either the amplitude or phase quadrature is detected. The other mode, at the telecommunication wavelength of 1550 nm,

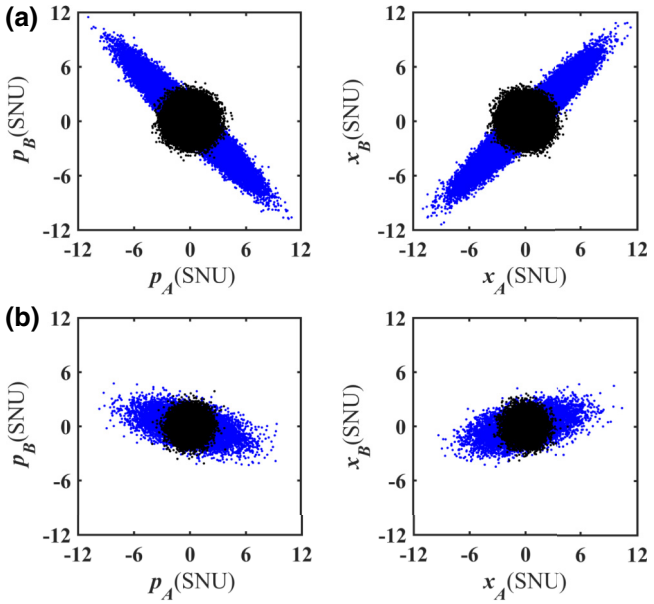

FIG. 3. Observed correlations between Alice's and Bob's amplitude quadrature x and phase quadrature p using balanced homodyne detection. The black points represent the correlations of vacuum states. The blue points represent the quadrature data of Alice and Bob, which are normalized to the noise standard deviation of a vacuum state. (a) Correlations of the initial EPR source. (b) Correlations between Alice's and Bob's quadrature data when one mode of the EPR source at the telecommunication wavelength of 1550 nm is sent to Bob via a 50.2-km standard single-mode fiber.

and its corresponding LO, are coupled into single-mode polarization-maintaining fiber devices (with coupling efficiency of 95%) and then injected into a 50.2-km standard single-mode fiber spool (placed on an optical table) through polarization multiplexing and time multiplexing. Here, the multiplexing approaches effectively suppress the excess noises resulting from the relatively intense LO field, including the leakage and the nonlinear optical scattering of the LO beam. The LO is first split by a 50:50 fiber beam splitter, and one output beam is reflected back to the NOPA for supplying the seed field. The other beam is modulated by a high-extinction-ratio (40 dB) Mach-Zehnder amplitude modulator (AM) with a pulse generator to produce a 10-μs width and 50-kHz repetition rate pulse train. The time multiplexing is implemented by a delay line composed of a 1-km single-mode fiber followed by a Faraday rotation mirror, which reflects the LO pulse with a polarization rotation of 90°, and therefore, eliminates undesired birefringence-induced polarization variation during the LO pulse propagation along the single-mode fiber delay line.

On Bob's side, a manual fiber-polarization controller recovers the precise polarization states of both the signal and the LO, with a polarization extinction ratio above 30 dB. In this case, the two optical fields are polarization demultiplexed by polarization beam splitters (PBSs). To ensure time overlapping of the signal and the time-delayed LO fields, another delay line is inserted in the signal's path. The optical-path-matched signal and LO interfere on a 50:50 fiber beam splitter, and the amplitude or phase quadrature of the signal is detected by using an all-fiber shot-noise limit BHD. The system is calibrated in advance to ensure the measured quadratures of Alice are in phase with those of Bob. To this end, the slow phase drifts between the signal and LO at both sides are compensated by piezoelectric-transducer-based phase shifters. To switch the measurement basis between the phase and amplitude quadrature, a phase shift of 0 or $\pi/2$ is applied randomly to each LO beam via by a high-speed waveguide electro-optical phase modulator. The error signal for the phase lock loop is extracted from the homodyne detector output, which is high-order low-pass filtered with a cut-off frequency of 2 kHz. In this way, the high-frequency phase variation components due to the high-speed phase modulator are averaged out.

A two-channel data acquisition card with a rate of 10 MHz samples Alice's and Bob's quadrature data. The data acquisition of the system is triggered by the pulse generator (which provides a driving signal for the AM to produce the pulsed LO beam), and an electronic delay is introduced to precisely synchronize the arrival times of the two entangled beams; in this way, maximum correlation is obtained between Alice's and Bob's data. For each signal mode with a 10-μs window, the 100 sampled data points are mixed down at 3.5 MHz and successively low-pass filtered using a 100-tap finite-impulse-response filter with a cut-off frequency of 500 kHz. The filtered data are then added together to yield a single value that defines the quadrature of the signal mode.

Alice's BHD has an electronic noise of $\upsilon_{\mathrm{el}} = 0.005$ and an efficiency of $\eta_A = 86\%$, which includes an optical propagation efficiency of 96%, photodiode quantum efficiency of 93%, and homodyne visibility of 98.5%. For Bob's BHD, the electronic noise is $\upsilon_{\mathrm{el}} = 0.09$ and the efficiency is $\eta_B = 55\%$ (optical propagation efficiency of 62%, quantum efficiency of the photon diodes of 89%, and homodyne visibility of 99.5%). Figure 3(b) plots a typical correlation outcome between Alice's and Bob's amplitudes and phase quadratures over a standard single-mode telecom fiber of 50.2 km. Quadrature correlations (with a correlation coefficient of 0.5) are clearly visible between Alice's and Bob's measurement results. From the measured data, the EPR criterion is determined to be $\sqrt{V^x_{A|B} \cdot V^p_{A|B}} = 0.982 < 1$, which states that the two-mode state shared between Alice and Bob is still quadrature entangled. The degradation of the quantum correlations is mainly caused by the linear loss introduced by the single-mode fiber, and the added excess noises are very small.

Using a subset of the raw data measured by Alice's and Bob's homodyne detection, the total excess noise and channel transmission of the QKD system are determined

to be 0.01 shot-noise units (SNU) and $\eta = 0.098$, respectively. In our system, five noise sources mainly contribute to the excess noise ε: the leakage of the LO pulse, the nonideal phase-locking between the LO beam and signal, the depolarized guided acoustic wave Brillouin scattering (GAWBS) of the LO beam, the spontaneous Raman scattering (SRS) of the LO, and the systematic excess noise. In the following, we analyze quantitatively the amount of excess noise due to each of these mechanisms.

Due to the direct utilization of the EPR protocol and the fact that no modulation is required, the excess noise arising from the modulation errors occurring in a preparation and measurement scheme does not exist here. Considering the total extinction ratio of 70 dB (including the extinction ratio of the LO pulse of 40 dB plus the polarization extinction ratio of 30 dB) and the average noise photon number of approximately 1 at the sideband 3–4 MHz, the excess noise due to the leakage of the LO pulse is approximately 10^{-7} photons, which is negligible. The phase-locking fluctuations between the LO and signal fields can cause variation in Bob's measurement basis and induce an excess noise of $\langle(\Delta\hat{x}')^2\rangle - \langle(\Delta\hat{x})^2\rangle \approx V_A^0\phi^2$, where ϕ is the standard deviation of the phase-locking fluctuations. In our system, the signal variance is $V_A^0 \approx 7.7$, and the deviation of the phase fluctuations is around 0.9°, which induces an excess noise level of approximately 0.002 SNU.

Another source of excess noise is the depolarized GAWBS noise, where a small portion of LO photons are scattered to the signal mode [37–39]. Notably, the polarization isolation assumption is invalid here because of depolarization scattering. However, the frequency bandwidth range (3–4 MHz) we use is well below the first depolarized GAWBS mode (approximately 20 MHz for our telecom single-mode fiber). There is still some residual scattering background noise in the low-frequency range. Such excess noise at the sideband 3–4 MHz is observed to be 9.2 SNU with only polarization multiplexing employed. However, this scattering noise is further suppressed by 40 dB due to the time multiplexing of the LO and the signal, which results in an ultimate excess noise level of approximately 0.001 SNU. The SRS of the LO is also an excess noise source for the QKD. For a 50-km standard telecom single-mode fiber, the induced excess noise due to the SRS is around 0.01 SNU, which is suppressed by the time-multiplexing technique and contributes to the excess noise with an amount of around 10^{-6} SNU. The systematic excess noise, including the stability of the EPR source and the calibration of the SNU, contributes to a typical excess noise level of 0.007 SNU.

Figure 4 plots the secret key rate achieved by our CV QKD system. A reconciliation efficiency of $\beta = 0.95$ is used. For a 50.2-km standard telecommunication fiber, using the channel parameter estimation results $\eta = 0.098$, $\varepsilon = 0.01$, and other experimentally determined parameters, we achieve a secret key rate of 0.03 bit per sample

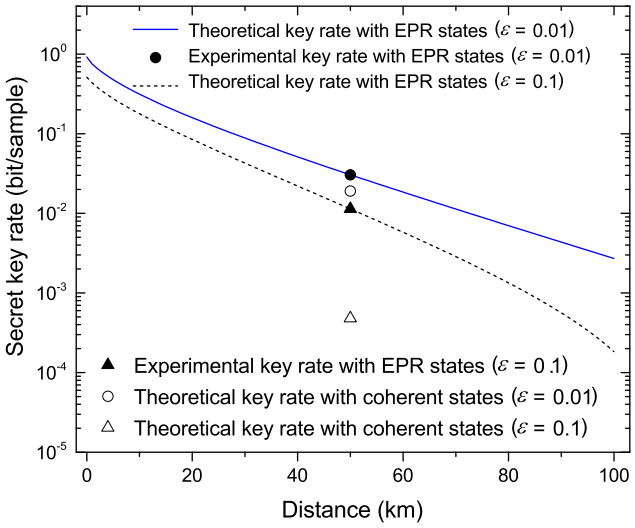

FIG. 4. Secret key rate produced by the CV QKD system. Two different levels of excess noises are investigated, $\varepsilon = 0.01$ and $\varepsilon = 0.1$.

for EPR states (the solid circle in the figure). For the same experimental parameters, if we instead employ a coherent-state-based protocol with optimized modulation variance ($V_A = 4.5$), the corresponding secret key rate is 0.019 bit per sample (empty circle). To investigate the performance of our QKD system under different excess noise levels, we add noise to Bob's data to simulate an excess noise level of $\varepsilon = 0.1$. In this case, the experimental key rate decreases to 0.01 bit per sample (solid triangle). In contrast, the secret key rate for a coherent-state-based protocol with optimized modulation variance ($V_A = 4.5$, other experimental parameters unchanged) drops dramatically to 4.8×10^{-4} bit per sample.

The solid and dashed lines show the theoretically predicted key rate as a function of different channel distances (standard fiber with an attenuation of 0.2 dB/km). From the above results, we conclude that the CV QKD system with EPR states performs better than the coherent-state based system; in particular, its superiority is more evident when the system's excess noise level is relatively high.

IV. CONCLUSION

In summary, we have experimentally demonstrated long-distance continuous-variable quantum key distribution over a 50-km standard optical fiber based on continuous-variable entangled states. The achieved secret key rate is higher than that of the coherent-state protocol, in particular in a high-channel excess noise environment. It has been shown that CV QKD possesses an outstanding ability to coexist with classical signals in optical networks [11–13]. Due to its robustness to the channel noise, the entanglement-based CV QKD protocol is well suited for a noisy channel and will further boost the multiplexing

capacity. Encouragingly, the performance of our current QKD system can be improved further by enhancing the degree of entanglement and bandwidth of the EPR source [47–49]. In this way, a high-speed, more robust QKD system can be achieved. On the other hand, our work paves the way toward practical applications of one-sided device-independent CV QKD using EPR states over long-distance fibers [29,30].

ACKNOWLEDGMENTS

This work is supported by the National Key R&D Program of China (Grant No. 2016YFA0301403); the National Natural Science Foundation of China (NSFC) (Grants No. 61378010 and No. 11774209); Shanxi 1331KSC; the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[2] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Colloquium: The Einstein-Podolsky-Rosen paradox: From concepts to applications, Rev. Mod. Phys. **81**, 1727 (2009).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

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

[5] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

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

[7] S. L. Braunstein and P. Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[8] X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Quantum information with Gaussian States, Phys. Rep. **448**, 1 (2007).

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

[10] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, High-bit-rate continuous-variable quantum key distribution, Phys. Rev. A **90**, 042329 (2014).

[11] B. Qi, W. Zhu, L. Qian, and H. K. Lo, Feasibility of quantum key distribution through a dense wavelength division multiplexing network, New J. Phys. **12**, 103042 (2010).

[12] R. Kumar, H. Qin, and R. Alléaume, Coexistence of continuous variable QKD with intense DWDM classical channels, New J. Phys. **17**, 043027 (2014).

[13] F. Karinou, H. H. Brunner, C. H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. Xie, M. Peev, and A. Poppe, Toward the integration of CV quantum key distribution in deployed optical networks, IEEE Photon. Technol. Lett. **30**, 650 (2018).

[14] 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).

[15] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light, Phys. Rev. Lett. **95**, 180503 (2005).

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

[17] 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).

[18] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous variable quantum cryptography using two-way quantum communication, Nat. Phys. **4**, 726 (2008).

[19] A. Leverrier and P. Grangier, Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation, Phys. Rev. Lett. **102**, 180504 (2009).

[20] Q. D. Xuan, Z. S. Zhang, and Paul L. Voss, A 24 km fiber-based discretely signaled continuous variable quantum key distribution system, Opt. Express **17**, 24244 (2009).

[21] X. L. Su, W. Z. Wang, Y. Wang, X. J. Jia, C. D. Xie, and K. C. Peng, Continuous variable quantum key distribution based on optical entangled states without signal modulation, Europhys. Lett. **87**, 20005 (2009).

[22] R. García-Patrón and N. J. Cerf, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Phys. Rev. Lett. **102**, 130501 (2009).

[23] V. C. Usenko and R. Filip, Squeezed-state quantum key distribution upon imperfect reconciliation, New J. Phys. **13**, 113007 (2011).

[24] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Continuous variable quantum key distribution with modulated entangled states, Nat. Commun. **3**, 1083 (2012).

[25] X. Y. Wang, Z. L. Bai, S. F. Wang, Y. M. Li, and K. C. Peng, Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise, Chin. Phys. Lett. **30**, 010305 (2013).

[26] 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).

[27] D. Huang, D. Lin, C. Wang, W. Q. Liu, S. H. Fang, J. Y. Peng, P. Huang, and G. H. Zeng, Continuous-variable quantum key distribution with 1 Mbps secure key rate, Opt. Express **23**, 17511 (2015).

[28] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, Nature Photonics **9**, 397 (2015).

[29] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, Nat. Commun. **6**, 8795 (2015).

[30] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution, Optica **3**, 634 (2016).

[31] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Single quadrature continuous-variable quantum key distribution, Quant. Inf. Comput. **16**, 1081 (2016).

[32] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[33] X. Y. Wang, W. Y. Liu, Pu Wang, and Y. M. Li, Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution, Phys. Rev. A **95**, 062330 (2017).

[34] X. Y. Zhang, Y. C. Zhang, Y. J. Zhao, X. Y. Wang, S. Yu, and H. Guo, Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **96**, 042334 (2017).

[35] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Phys. Rev. A **97**, 052327 (2018).

[36] B. Qi and C. C. W. Lim, Noise Analysis of Simultaneous Quantum Key Distribution and Classical Communication Scheme Using a True Local Oscillator, Phys. Rev. Appl. **9**, 054008 (2018).

[37] R. M. Shelby, M. D. Levenson, and P. W. bayer, Resovled Forward Brillouin Scattering in Optical Fibers, Phys. Rev. Lett. **54**, 939 (1985).

[38] R. M. Shelby, M. D. Levenson, S. H. Perlmutter, R. G. DeVoe, and D. F. Walls, Broad-Band Parametric Deamplification of Quantum Noise in an Optical Fiber, Phys. Rev. Lett. **57**, 691 (1986).

[39] Y. M. Li, N. Wang, X. Y. Wang, and Z. L. Bai, Influence of guided acoustic wave Brillouin scattering on excess noise in fiber-based continuous variable quantum key distribution, J. Opt. Soc. Am. B **31**, 2379 (2014).

[40] M. M. Wolf, G. Giedke, and J. I. Cirac, Extremality of Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).

[41] R. García-Patron and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[42] M. Navascues, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[43] R. Renner and J. I. Cirac, de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[44] S. L. Braunstein, Squeezing as an irreducible resource, Phys. Rev. A **71**, 055801 (2005).

[45] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevApplied.10.064028 for details of the relevant matrixes which are used to derive the secret key rate.

[46] X. M. Guo, J. J. Zhao, and Y. M. Li, Robust generation of bright two-color entangled optical beams from a phase-insensitive optical parametric amplifier, Appl. Phys. Lett. **100**, 091112 (2012).

[47] T. Eberle, V. Händchen, and R. Schnabel, Stable control of 10 dB two mode squeezed vacuum states of light, Opt. Express **21**, 11546 (2013).

[48] S. Ast, M. Mehmet, and R. Schnabel, High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity, Opt. Express **21**, 13572 (2013).

[49] Y. Y. Zhou, X. J. Jia, F. Li, C. D. Xie, and K. C. Peng, Experimental generation of 8.4 dB entangled state with an optical cavity involving a wedged type-II nonlinear crystal, Opt. Express **23**, 4952 (2015).