PHOTONICS Research

Continuous variable quantum key distribution with a shared partially characterized entangled source

Shanna Du,[1,2,†] Pu Wang,[1,2,3,†] Jianqiang Liu,[1,2] Yan Tian,[1,2] and Yongmin Li[1,2,*]

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
[3]School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China
*Corresponding author: yongmin@sxu.edu.cn

Received 19 September 2022; revised 11 January 2023; accepted 15 January 2023; posted 18 January 2023 (Doc. ID 475943); published 1 March 2023

Locking the sophisticated and expensive entanglement sources at the shared relay node is a promising choice for building a star-type quantum network with efficient use of quantum resources, where the involved parties only need to equip low-cost and simple homodyne detectors. Here, to our best knowledge, we demonstrate the first experimental continuous variable quantum key distribution with an entanglement source between the two users. We consider a practical partially characterized entangled source and establish the security analysis model of the protocol under realistic conditions. By applying a biased base technology, the higher key rate than that of the original protocol is achieved. The experimental results demonstrate that the distance between two users can reach up to 60 km over telecom single-mode fiber, implying the feasibility for high-rate and secure communication with a shared entangled source at metropolitan distances.

https://doi.org/10.1364/PRJ.475943

1. INTRODUCTION

Quantum key distribution (QKD) allows two distant parties to distill a common secret key by exploring the fundamental principles of quantum mechanics [1–3]. Different from the discrete-variable (DV) QKD schemes, the continuous-variable (CV) QKD [4–6] systems encode key information on the multiphoton quantum states and measure their quadratures using high-efficiency homodyne (heterodyne) detectors instead of single-photon detection technologies, which have potential higher secret key rates at metropolitan distances. In the last two decades, CV-QKD has received extensive attention [7,8], and remarkable progress has been achieved both theoretically and experimentally [9–25].

At present, most CV-QKD implementations are based on a one-way regime, where one of the two parties (transmitter) needs to establish a source, and the other (receiver) performs detection. Placing the entanglement source between two users offers an alternative route for secure communication with efficient use of quantum resources [26–28]. Here, we demonstrate the first experimental CV-QKD with entanglement source between the two users, which is suitable to develop an entanglement-based CV-QKD network, where the sophisticated and expensive entanglement source can be shared by multiple end users [29,30]. The initial concept was introduced in Ref. [26], proposing a scheme that allowed communicating parties to achieve a secure key when the entanglement originates from the middle and, hence, is well suited to construct a centric CV-QKD network with a shared entanglement source. However, the challenge occurs due to the assumption that the entangled source is perfectly pure and the homodyne detection is ideal (quantum efficiency of 100% and no dark noises), which is not suitable for the practical applications. Note that any realistic preparation process of Einstein–Podolsky–Rosen (EPR) states inevitably introduces losses and excess noises, and no pure EPR states can be produced in real scenarios.

In this work, we treat the entanglement source as a realistic mixed EPR source and take the trusted losses and electronic noises of the realistic detectors into account. We focus on a practical consideration of a partially characterized source, where the variances and correlations of the two output modes of the source are known, and the output modes keep the characteristics of Gaussian and independent and identical distribution (i.i.d.), which can be verified by testing the output of the prepared source. Note that the state preparation process does not need to be characterized. This means that an attacker (Eve) is able to acquire additional information by purifying the practical mixed source while maintaining the output characteristics of the source unchanged. A general security model under above conditions is established, and an improved strategy for the

secret key rate is proposed by using a biased base method. Finally, we experimentally demonstrate the protocol over long distance fibers, where the entanglement source is located at the relay node, and the distance between two users can reach up to 60 km, providing the possibility for the deployment of high-rate, cost-effective metropolitan quantum network.

2. PROTOCOL DESCRIPTION

The schematic of the protocol with entanglement source between the two users is illustrated in Fig. 1(a), which consists of two legitimate users, Alice and Bob, and a relay, Charlie, who prepares a mixed Gaussian EPR entangled state. Here, the actual physical implementation model of the state preparation process does not need to be characterized and can be regarded as a black box. The two modes of the EPR source are sent to Alice and Bob through two independent quantum channels and subsequently detected by homodyne detection. Due to the Gaussian and i.i.d. EPR source, according to the optimality of Gaussian attacks, the collective Gaussian attack is optimal for Eve. Therefore, we do not require the channel linearity assumption. By implementing parameter estimation, information reconciliation, and privacy amplification procedures, the secret keys can be extracted.

For convenience of security analysis, a purification scheme of the protocol is given in Fig. 1(b). Here, we assume the mixed EPR states are prepared by Eve, and that she can obtain additional information by purifying the mixed EPR source [14]. In order to mask her attack, the characteristics of the EPR states $\rho_{A_0B_0}$ remain intact. The two quantum channels are modeled by their transmissions T_A and T_B and mixed with thermal noises E_1 and E_2, which are extracted from a reservoir of entangled ancillae and have quantum correlations. This joint two-mode Gaussian attack is more powerful than two independent collective Gaussian attacks (see Appendix B for more details). At Alice's and Bob's sites, the realistic noisy detection is purified by a beam splitter with one of the input ports injected with a thermal state (one beam of an EPR state) followed by an ideal detector. The transformation of the beam splitter is employed to model the detection efficiency η_A (η_B), while the injected EPR beam is used to model the electronic noise ν_{elA} (ν_{elB}).

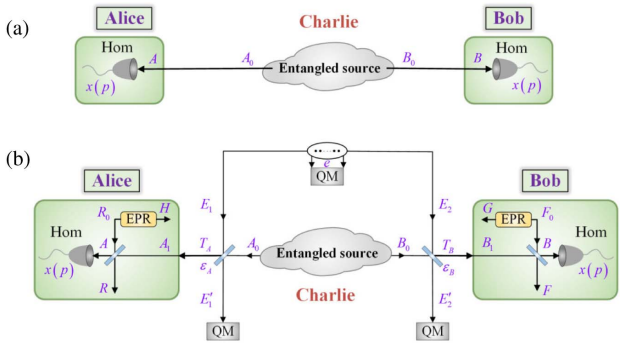

Fig. 1. Schematic illustration of CV-QKD protocol with partially characterized entangled source between the two users. (a) Prepare-and-measure (PM) scheme for protocol. (b) Equivalent purification scheme for protocol. Hom, homodyne detection; QM, quantum memory.

Based on the above purification schemes, the secret key rate can be estimated.

3. BIASED BASE

In the previous entanglement-based CV-QKD protocols, both Alice and Bob randomly measure the amplitude or phase quadrature of one of the entangled modes with an equal probability of 1/2. However, the secret key can only be extracted when both parties choose the same quadrature measurement base. Thus, they must discard half of the raw data after the base-sifting procedure, which results in waste of quantum state resources and low efficiency of the protocol. To improve the secret key rate, we present a biased-base scheme for entanglement-based CV-QKD similar to DV-QKD [31], in which Alice and Bob choose their measurement bases with nonuniform probability.

Suppose that Alice randomly chooses to implement a measurement in the phase and amplitude quadratures with probabilities P_A and $1-P_A$, respectively, and Bob measures the phase and amplitude quadratures with probabilities P_B and $1-P_B$, respectively. To ensure security, Alice and Bob must evaluate the key rate from two sifted measurement bases. The secret key rate against collective attacks with reverse reconciliation in the asymptotic limit is given by

$$K_{RR}^{\infty}=(1-P_A)(1-P_B)(\beta I_{AB}^{x}-\chi_{BE}^{x})+P_AP_B(\beta I_{AB}^{p}-\chi_{BE}^{p}), \tag{1}$$

where $(1-P_A)(1-P_B)$ and P_AP_B are the sifting efficiencies of the two bases. β is the reconciliation efficiency. I_{AB}^{x} (I_{AB}^{p}) denotes the Shannon mutual information between Alice's and Bob's data on the amplitude (phase) quadrature. χ_{BE}^{x} and χ_{BE}^{p} denote the Holevo bound for the amplitude and phase quadratures, respectively, putting the upper limit on the information available to Eve on Bob's sifted key. Using the purification treatment, $\chi_{BE}^{x(p)}$ can be obtained by

$$\chi_{BE}^{x(p)}=S(\rho_E)-S(\rho_{E/B}^{x(p)})=S(\rho_{A_1B_1})-S(\rho_{A_1FG/B}^{x(p)}), \tag{2}$$

where $S(\rho)$ is the von Neumann entropy, which can be directly calculated from the symplectic eigenvalues of the covariance matrix of quantum states (see Appendix A for more details).

The key rate can be improved by optimizing the total sifting efficiency $P_AP_B+(1-P_A)(1-P_B)$, where $P_A,P_B\in(0,1)$. When the probabilities P_A and P_B are equal to 1 or 0, the total sifting efficiency reaches the maximum value. Note that P_A and P_B cannot be set to 1 or 0, or the covariance matrix cannot be accurately estimated due to the lack of nonobserved quadrature data. To ensure security, the unknown parameters of the covariance matrix must be constrained by the Heisenberg uncertainty principle as the manipulation in the unidimensional CV-QKD protocol [32], which results in a significant degradation of the key rate. In our experiment, we chose $P_A=P_B=P=0.9$, which indicates that the phase quadratures are selected to be observed for most of the time. Within this framework, the key rate generated is 64% higher than that of the original unbiased base protocol (see Appendix E for more details).

4. EXPERIMENTAL DEMONSTRATION

A. Experimental Setup

In our experiment, we implement the protocol with an asymmetric configuration, meaning that Charlie is located close to one of the users, which provides better performance compared with the near-symmetric channels (see Appendix D for details). Note that such asymmetric configurations find widespread applications in practical QKD network setups [17,33].

A schematic of our experimental setup is shown in Fig. 2. The EPR entanglement source is placed at Charlie's site, which consists of a nonlinear resonator with a periodically poled $KTiOPO_4$ crystal inside. The nonlinear resonator is bidirectionally pumped by a 532 nm laser [34]. In the clockwise direction, the resonator operates above threshold and outputs bright downconversion fields that serve as the local oscillators (LOs) of Alice's and Bob's balanced homodyne detectors (BHD1 and BHD2), whereas in the anticlockwise direction, the resonator operates below threshold and generates the EPR entangled state (see Appendix G for more details).

The key rate depends on the two-mode squeezing and antisqueezing levels of the entangled state. However, higher two-mode squeezing does not necessarily mean higher key rate, especially at long distances, because higher two-mode squeezing is usually accompanied by a higher excess noise in anti-squeezing, which degrades the purity of the EPR states that can be exploited by Eve. To improve the key rate, a high-purity EPR state is prepared by suppressing the intracavity loss and improving the escape efficiency of the nonlinear resonator. Furthermore, the pump power of the nonlinear resonator is optimized to generate an EPR source with squeezing and antisqueezing levels of −7.1 and 9.6 dB, respectively. In this case, the key rate is maximized within a transmission distance of 80 km (from Charlie to Bob L_B) when the distance between Alice and Charlie is close to 0 km (see Appendix D for more details).

The two modes of the EPR state and the corresponding LOs are separated by two dichroic beam splitters, and the mode at 810 nm is sent to Alice, whereas the other mode at 1550 nm is coupled into single-mode polarization-maintaining fiber devices. The LO beam at 1550 nm is converted into pulsed light with a 50 kHz repetition rate and 8.5 μs pulse width by an amplitude modulator (AM). It is delayed by a 1.8 km single-mode fiber and combined with the signal mode on a polarization beam splitter (PBS). Then, the polarization-multiplexing and time-division-multiplexing LO and signal beams are sent to Bob via a telecom single-mode fiber. In this way, the photon leakage and nonlinear scattering noise of the intense LO beam are suppressed.

At Alice's site, we only couple the LO beam into the fiber-pigtailed phase modulator (PM) to randomly switch the measurement bases between the phase and amplitude quadrature. The signal beam propagates in free space and combines with the output LO beam from the collimator at a PBS. Then, the two beams interfere at a 50:50 beam splitter consisting of a half-wave plate and a PBS, and the output modes are detected by BHD1.

At Bob's site, the signal and LO beams at 1550 nm output from the long-distance fiber are polarization-demultiplexed by a polarization controller (PC) and PBS. The signal mode is delayed by the same length of fiber as that of the LO at Charlie's site to ensure the time synchronization between the signal and the LO. When the length of the transmission fiber is more than 40 km, an erbium-doped fiber amplifier followed by an optical filter (the full width at half-maximum is 160 pm) and an optical attenuator are employed to boost the LO power, so as to ensure that the signal-to-noise ratio of BHD2 is above 10 dB.

B. Switching Measurement Bases

Figure 3 shows a time-sequence diagram of the signal modes and measurement base pulses in our experiment. The orange and pink lines represent the signal modes measured at Alice's

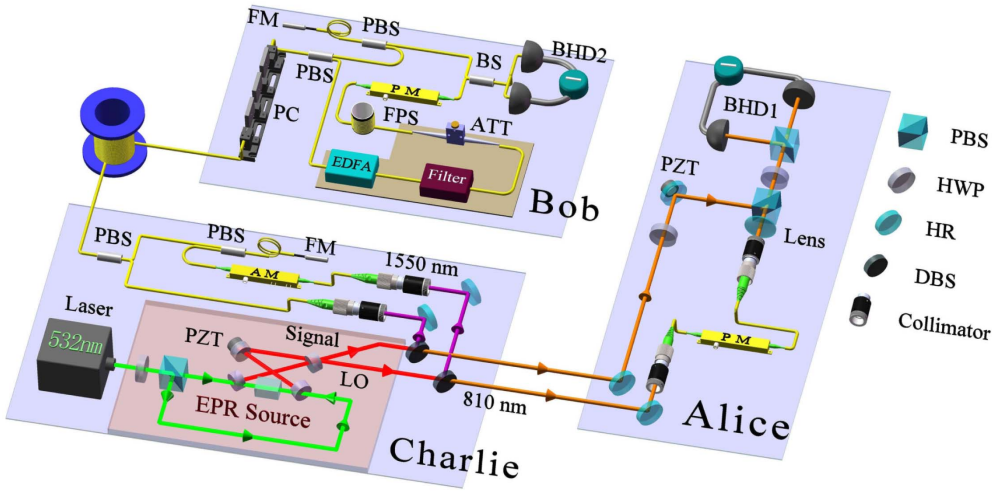

Fig. 2. Schematic drawing of the experimental setup. Charlie prepares a two-color EPR entangled state and sends one mode (810 nm) to Alice and the other mode (1550 nm) to Bob. The two users randomly measure the amplitude or phase quadrature of the received signal mode with BHDs. PZT, piezoelectric-transducer; AM, amplitude modulator; PM, phase modulator; FM, Faraday mirror; PBS, polarization beam splitter; DBS, dichroic beam splitter; HR, mirror with high reflection; HWP, half-wave plate; PC, polarization controller; EDFA, erbium-doped fiber amplifier; ATT, attenuator; FPS, fiber phase shifter; BS, 50:50 beam splitter.

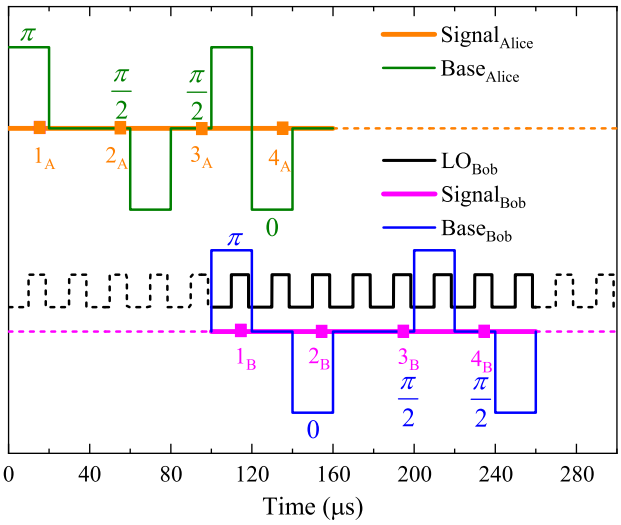

Fig. 3. Time-sequence diagram of signal modes and measurement base pulses. It shows the relative timing relationship between the signal mode and its corresponding measurement base pulses.

and Bob's sites, respectively. The solid squares indicate four pairs of entangled quantum states generated from the EPR entangled source at the same time; more precisely, $(1_A, 1_B)$, $(2_A, 2_B)$, $(3_A, 3_B)$, and $(4_A, 4_B)$. The time span of each quantum state is 6 μs. Bob's quantum state has a delay of approximately 100 μs relative to Alice's quantum state, which arises from the delay of 20 km of telecom single-mode fiber. The black line represents the pulsed LO that is synchronized with signal mode at Bob's site. The green and blue lines represent the measurement base voltage pulses that Alice and Bob have independently chosen.

To ensure that both users share the same phase reference frame and implement the correct quadrature measurement, we use a piezoelectric-transducer and a fiber phase shifter to compensate the slow phase drift between the LO and signal beams and lock their relative phase to $\pi/2$. Then, the electric pulses of the random and independent measurement bases are applied to the high-speed PM, so as to realize the random switching between the phase and amplitude quadratures. During the operation of the QKD system, the clocks of pulse-chopping, measurement bases, and quadrature sampling of Alice, Bob, and Charlie are strictly synchronized.

Particular attention must be paid to the introduction of excess noises, which seriously affect QKD performance. The base-switching pulses will affect the error signal of the slow drift phase and reduce the locking accuracy, which further disturbs the normal measurement of BHD. To measure the phase quadrature, zero voltage is applied to PM for the first 20 μs, followed by a $jV_{\pi/2}$ $(j = +, -)$ voltage of 20 μs. For measurement of the amplitude quadrature, we first actuate the PM with voltage of $jV_{\pi/2}$ for 20 μs and then switch the voltage to 0 for another 20 μs. The sign of the current voltage $jV^{n}_{\pi/2}$ is opposite to that of the previous voltage $jV^{n-1}_{\pi/2}$ with $j = +$ for $n = 1$. In this case, the high-frequency phase variation component caused by the bases switching can be averaged within a maximum period of 80 μs. In addition, a 5 kHz low-pass filter is used to filter the high-frequency phase variation component in the error signal before it is fed into the phase lock loop, so as to ensure that the locking accuracy remains intact with and without the measurement bases [18].

C. Experimental Results

Figure 4(a) depicts the experimental and theoretical security key rates versus the transmission distance from Charlie to Bob (L_B), where three different transmission distances from Charlie to Alice ($L_A = 0$, 1, and 2 km) are investigated. Here, L_A is simulated by inserting a neutral attenuator into the signal path. The experimental parameters used to estimate the key rate are shown in Table 1 (see Appendices C and G for more details).

Figure 4(b) shows the quantum correlation outcomes of the amplitude quadrature (x_A, x_B) and phase quadrature (p_A, p_B) simultaneously observed by Alice and Bob at $L_A = 2$ km and $L_B = 20$ km. From the experimental data, we can determine the EPR criterion to be $\sqrt{V^{x}_{A|B} \cdot V^{p}_{A|B}} = 0.935 < 1$, which clearly verifies the quadrature entanglement of the two modes shared between Alice and Bob.

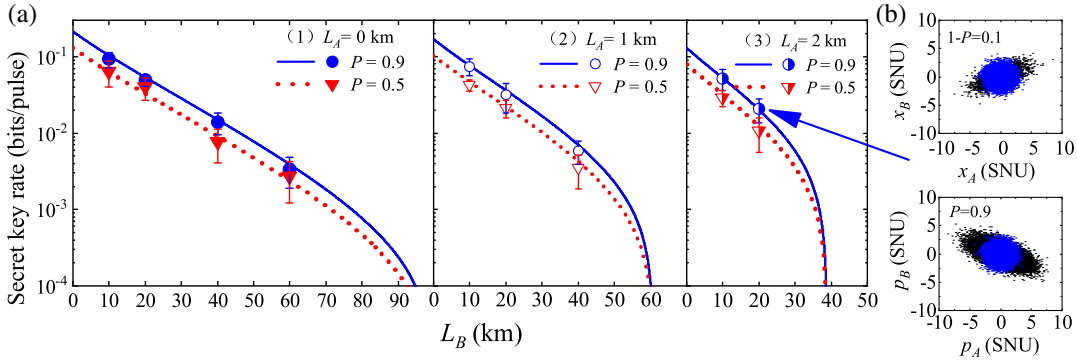

Fig. 4. Key rates for different distances and quantum correlation of the distributed EPR states. (a) Security key rates versus transmission distance from Charlie to Bob (L_B) for different (equivalent) transmission distances from Charlie to Alice (L_A) of 0, 1, and 2 km. Solid and dashed lines represent the theoretical simulation with the p base choosing probabilities of $P = 0.9$ and 0.5, respectively. Circles and triangles represent experimental measurement data. (b) Under conditions of $L_A = 2$ km and $L_B = 20$ km, the quantum correlation between Alice's and Bob's amplitude quadrature $(1 - P = 0.1)$ and phase quadrature $(P = 0.9)$.

Table 1. List of Experimental Parameters

Parameter	Symbol	Value
Reconciliation efficiency	β	0.95
Alice's excess noise	ε_A	0.001
Bob's excess noise	ε_B	0.01
Alice's electronic noise	ν_{elA}	0.02
Bob's electronic noise	ν_{elB}	0.05
Alice's detection efficiency	η_A	0.884
Bob's detection efficiency	η_B	0.506

We implement the protocol for three situations: (1) $L_A = 0$ km, and L_B varying from 10 to 60 km; (2) $L_A = 1$ km, and L_B varying from 10 to 40 km; (3) $L_A = 2$ km, and L_B varying from 10 to 20 km. Two biased-base choices of 0.9/0.1 (phase quadrature/amplitude quadrature) and 0.5/0.5 are demonstrated. The biased base of 0.9/0.1 increases the key rate significantly, i.e., by an amount of 64% compared with the unbiased base 0.5/0.5, which confirms our theoretical analysis of the optimal basis-selection ratio.

5. CONCLUSIONS AND OUTLOOK

The CV-QKD with the entanglement source between two users has the best performance at an asymmetric configuration; that is, one of the QKD users is closer to the entanglement source. This protocol is applicable to a number of star-type quantum networks with asymmetric configuration in practice, such as the quantum cryptography government network shown in Fig. 5, in which the private communication between each department of the civic center (Alice) and remote district government (Bob) can be established. More precisely, the sophisticated and expensive entangled source can be located in the civic center, so that each department of the civic center is very close to it. Computer-controlled optical switches can be used to connect the departments of the civic center and remote district government according to a user's request in this network. Once the connection between a pair of users is established, the entangled beams are sent to them via quantum channels. In this case, the departments of the civic center can share secret keys with the remote district government using the protocol.

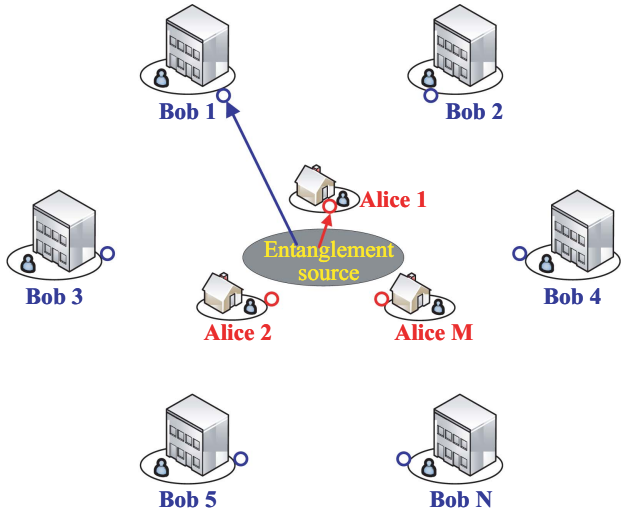

Fig. 5. Star-type quantum network. The entanglement source is placed at a common network node and is shared by multiple end users.

We have demonstrated the first CV-QKD with partially characterized EPR entangled states as the common relay node. To increase the efficiency of the scheme, we proposed and demonstrated the biased base strategy, which significantly improves the key rate compared with the original unbiased protocol. We remark that this can be extended to the finite-size scenario [35] (see Appendix E). Our work contributes an important step to the establishment of a CV-QKD quantum network with shared entanglement source, in which users only need to employ inexpensive detection equipment. More precisely, the output modes of the EPR source between the two users can be connected to $1 \times M$ and $1 \times N$ optical switches with nearby and distant users, respectively. By controlling the optical switch using a computer, each nearby user connected to one mode of the source can share the secure key with any distant user connected to the other mode of the source. It forms an M to N quantum network with entanglement source sharing.

The performance of our experimental system can be improved by further optimization. For instance, one can increase the propagation efficiency from the source to the nearest receiver Alice from 97% to 99%, optimize the interference efficiency to 99% and quantum efficiency of the photodiode to 99%. Similarly, the detection efficiency of Bob can be improved to 0.6 by welding all optical fiber devices to reduce the connector loss. For the entangled source, the escape efficiency can be increased to 0.95 by increasing the transmittance of the output coupling mirror and reducing the intracavity loss. Through the above optimizations, the distribution distance from the source to Alice can increase to 5 km with $L_B = 25$ km.

In our protocol, the entangled source is assumed to be partially characterized and the receiver is trusted. If the source is completely uncharacterized or untrusted, the non-Gaussian attack can be carried out by Eve to gain more information. The performance improvement of the protocol against this attack is worthy to be explored. For a completely characterized and trusted source, Eve can only attack the two quantum channels. In this case, the performance of the entanglement-in-the-middle protocol can be improved significantly (see Appendix F). For instance, the distribution distance can be increased to $L_A = L_B = 8$ km or $L_A = 5$ km and $L_B = 60$ km, effectively extending the distance in the symmetric and asymmetric quantum channels.

At present, a number of attacks against the receiver have been found, including saturation attack [36], blinding attack [37], calibration attack [38], and LO intensity attack [39]. However, these loopholes can be effectively eliminated by employing proper countermeasures [7,8]. For instance, one solution against these attacks is to add a real-time monitoring module for the LO power and the shot noise. The locally LO (LLO) scheme is also a useful countermeasure to prevent LO attacks [40,41]. In future work, we will employ the LLO scheme and implement real-time shot-noise measurement to guarantee the practical security at the receiver side.

Further research contains several directions. First, the user's detection equipment can be integrated into photonic and electronic chips to form a miniaturized and convenient QKD network [42,43]. Second, the protocol may be extended to a fully connected quantum network architecture via wavelength-division multiplexing technologies [44]. In addition, the protocol is limited to asymmetric situations at present for good performance, where one user is located relatively closer to the relay. For symmetric case, our QKD system can reach $L_A = L_B = 5$ km. Extending the distance of the protocol in a symmetric case is an issue to be addressed in the future to meet the wider applications.

Although our work focuses on the proof-of-principle experimental demonstration, the stability of the experimental system is critical to support the long-term use of future quantum networks. The main issue to solve is the development of an integrated, miniaturized, and stable entanglement source that supports long-term stable operation. The other key issue is that the implementation of all control and data-processing tasks of the system should be fully automated without human interaction.

APPENDIX A: THEORETICAL SECRET KEY RATE

In the asymptotic limit, the secret key rate of the protocol against collective attacks is given by

$$K_{RR}^{\infty} = P_A P_B(\beta I_{AB}^{x} - \chi_{BE}^{x}) + (1 - P_A)(1 - P_B)(\beta I_{AB}^{p} - \chi_{BE}^{p}). \tag{A1}$$

The Shannon mutual information between Alice and Bob for two quadratures x and p can be written as

$$I_{AB}^{x} = \frac{1}{2}\log_2 \frac{V_A^x}{V_{A/B}^x} = \frac{1}{2}\log_2 \frac{V_A^x}{V_A^x - (C_{AB}^x)^2/V_B^x},$$
$$I_{AB}^{p} = \frac{1}{2}\log_2 \frac{V_A^p}{V_{A/B}^p} = \frac{1}{2}\log_2 \frac{V_A^p}{V_A^p - (C_{AB}^p)^2/V_B^p}, \tag{A2}$$

where $V_A^{x(p)}$, $V_B^{x(p)}$, and $C_{AB}^{x(p)}$ represent the amplitude (phase) variance of Alice's sifted data, the amplitude (phase) variance of Bob's sifted data, and the covariance of Alice's and Bob's data, respectively. The upper bound of the information that Eve can steal under collective attacks is quantized by the Holevo bound $\chi_{BE}^{x(p)}$:

$$\chi_{BE}^{x(p)} = S(\rho_E) - S(\rho_{E/B}^{x(p)}). \tag{A3}$$

Assuming that Eve can purify the states shared between Alice and Bob and the detection process is believable, the Holevo bound $\chi_{BE}^{x(p)}$ can be rewritten as

$$\chi_{BE}^{x(p)} = S(\rho_{A_1B_1}) - S(\rho_{A_1FG/B}^{x(p)}), \tag{A4}$$

where $S(\rho_{A_1B_1})$ and $S(\rho_{A_1FG/B}^{x(p)})$ are the von Neumann entropy of the quantum states $\rho_{A_1B_1}$ and $\rho_{A_1FG/B}^{x(p)}$, which can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ and $\lambda_{3,4,5}^{x(p)}$ of the covariance matrix $\gamma_{A_1B_1}$ and $\gamma_{A_1FG/B}^{x(p)}$. The symplectic eigenvalues are obtained by finding the (standard) eigenvalues of the matrix $i\Omega\gamma$, where Ω is defined as

$$\Omega = \bigoplus_{j=1}^{k} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{A5}$$

where k takes 2 or 3, depending on the number of modes of the covariance matrix. Then, the Holevo bound $\chi_{BE}^{x(p)}$ becomes

$$\chi_{BE}^{x(p)} = \sum_{i=1}^{2} f(\lambda_i) - \sum_{i=3}^{5} f(\lambda_i^{x(p)}), \tag{A6}$$

where $f(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$.

The initial prepared EPR entangled state $\gamma_{A_0B_0}$ has the form

$$\gamma_{A_0B_0} = \begin{bmatrix} V_{A_0} I & C_{A_0B_0}\sigma_z \\ C_{A_0B_0}\sigma_z & V_{B_0} I \end{bmatrix}, \tag{A7}$$

where I is the identity matrix and $\sigma_z = \mathrm{diag}(1, -1)$. The variances of Alice's and Bob's modes and their correlation are given by

$$V_{A_0} = V_{B_0} = \frac{1}{2}(1/s + s + \Delta V_0),$$
$$C_{A_0B_0} = \frac{1}{2}(1/s - s + \Delta V_0),$$
$$\langle(\hat{x}_{A_0} - \hat{x}_{B_0})^2\rangle = \langle(\hat{p}_{A_0} + \hat{p}_{B_0})^2\rangle = 2s, \tag{A8}$$

where s is the degree of two-mode squeezing, and ΔV_0 is the excess noise of the antisqueezed quadrature. After the EPR states are sent to Alice and Bob through two quantum channels, the covariance matrix $\gamma_{A_1B_1}$ is obtained, which is expressed as

$$\gamma_{A_1B_1} = \begin{bmatrix} V_{A_1}^x & 0 & C_{A_1B_1}^x & 0 \\ 0 & V_{A_1}^p & 0 & C_{A_1B_1}^p \\ C_{A_1B_1}^x & 0 & V_{B_1}^x & 0 \\ 0 & C_{A_1B_1}^p & 0 & V_{B_1}^p \end{bmatrix}, \tag{A9}$$

and

$$V_{A_1}^x = V_{A_1}^p = V_{A_1} = T_A(V_{A_0} + \varepsilon_A) + 1 - T_A,$$
$$V_{B_1}^x = V_{B_1}^p = V_{B_1}$$
$$= T_B[V_{B_0}\eta_S + (1 - \eta_S) + \varepsilon_B] + 1 - T_B,$$
$$C_{A_1B_1}^x = \sqrt{\eta_S T_A T_B}\, C_{A_0B_0} + g\sqrt{1 - T_A}\sqrt{1 - T_B},$$
$$C_{A_1B_1}^p = -\sqrt{\eta_S T_A T_B}\, C_{A_0B_0} + g'\sqrt{1 - T_A}\sqrt{1 - T_B}, \tag{A10}$$

where two quantum channels are characterized by the transmissions T_A and T_B and excess noises ε_A and ε_B, respectively, and η_s denotes the loss of optical components before the channel. Here, we consider the joint two-mode Gaussian attack [17]. g and g' represent the correlations between the two quantum channels. Specifically, Eve's two ancillary modes E_1 and E_2 are extracted from a reservoir of entangled states and have the covariance matrix of the form [17]

$$\gamma_{E_1E_2} = \begin{bmatrix} \omega_A I & G \\ G & \omega_B I \end{bmatrix}, \qquad G = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix}, \tag{A11}$$

where ω_A and ω_B are the variances of the thermal noise introduced by E_1 and E_2, respectively, and $\omega_A = \varepsilon_A T_A/(1 - T_A) + 1$, $\omega_B = \varepsilon_B T_B/(1 - T_B) + 1$. The choices of g and g' must satisfy the Heisenberg uncertainty principle.

When $g = g' = 0$, the joint two-mode Gaussian attack degenerates into two independent Gaussian attacks.

In our protocol, Alice and Bob perform homodyne measurement; thus, the covariance matrix $\gamma^{x(p)}_{A_1FG/B}$ can be calculated by

$$\gamma^{x(p)}_{A_1FG/B} = \gamma_{A_1FG} - \sigma_{A_1FG;B}(X\gamma_B X)^{\mathrm{MP}}\sigma^T_{A_1FG;B}, \tag{A12}$$

where $X = \mathrm{diag}(1,0)$ or $X = \mathrm{diag}(0,1)$ when Bob's projective measurement is in amplitude or phase quadrature. MP denotes the Moore–Penrose inverse of a matrix. γ_{A_1FG}, $\sigma_{A_1FG;B}$, and γ_B are the submatrices of the covariance matrix γ_{A_1FGB}, which has the form

$$\gamma_{A_1FGB} = \begin{bmatrix} \gamma_{A_1FG} & \sigma_{A_1FG;B} \\ \sigma^T_{A_1FG;B} & \gamma_B \end{bmatrix}. \tag{A13}$$

This matrix can be obtained by applying a beam splitter transformation on the covariance matrix $\gamma_{A_1B_1}$ together with γ_{F_0G}.

Furthermore, using the transformation of the beam splitters at Alice's and Bob's sites for $\gamma_{A_1B_1}$, we obtain the covariance matrix γ_{AB} with the form

$$\gamma_{AB} = \begin{bmatrix} V^x_A & 0 & C^x_{AB} & 0 \\ 0 & V^p_A & 0 & C^p_{AB} \\ C^x_{AB} & 0 & V^x_B & 0 \\ 0 & C^p_{AB} & 0 & V^p_B \end{bmatrix}, \tag{A14}$$

where

$$\begin{aligned} V^x_A &= V^p_A = \eta_A V_{A_1} + 1 - \eta_A + v_{elA}, \\ V^x_B &= V^p_B = \eta_B V_{B_1} + 1 - \eta_B + v_{elB}, \\ C^x_{AB} &= \sqrt{\eta_A\eta_B}C^x_{A_1B_1}, \qquad C^p_{AB} = \sqrt{\eta_A\eta_B}C^p_{A_1B_1}. \end{aligned} \tag{A15}$$

Here, η_A (η_B) and v_{elA} (v_{elB}) are the detection efficiency and electronic noise of Alice (Bob). Inserting Eqs. (A14) and (A15) into Eq. (A2), the mutual information $I^{x(p)}_{AB}$ can be obtained.

APPENDIX B: MINIMIZATION OF THE KEY RATE

In Appendix A, we consider a realistic Gaussian attack against two quantum channels, i.e., joint two-mode Gaussian attack. It is important to note that the key rate depends on the correlation parameters (g, g') of the joint two-mode Gaussian attack via the correlation coefficient $C^{x(p)}_{A_1B_1}$. To obtain the secure key rate, we need to minimize the rate over all accessible values in the correlation plane (g, g'). In CV-MDI-QKD [17], it is found that the optimal correlated attack that Eve can perform is the "negative EPR attack" in which

$$\begin{aligned} &g' = -g = \phi, \\ &\phi = \min\left\{\sqrt{(\omega_A - 1)(\omega_B + 1)}, \sqrt{(\omega_A + 1)(\omega_B - 1)}\right\}. \end{aligned} \tag{B1}$$

However, the case is different for our protocol. The condition of $g' = -g = \phi$ does not indicate Eve's strongest attack. In this section, we analyze the optimal attack that Eve can perform.

First, we derive the analytical expression for the ideal key rate of the protocol by assuming the ideal detection and data reconciliation. The mutual information between Alice and Bob can be rewritten as

$$\begin{aligned} I^x_{AB} &= \frac{1}{2}\log_2\frac{V_{A_1}V_{B_1}}{V_{A_1}V_{B_1} - (C^x_{A_1B_1})^2}, \\ I^p_{AB} &= \frac{1}{2}\log_2\frac{V_{A_1}V_{B_1}}{V_{A_1}V_{B_1} - (C^p_{A_1B_1})^2}. \end{aligned} \tag{B2}$$

The Holevo bound $\chi^{x(p)}_{BE}$ can be simplified to

$$\begin{aligned} \chi^x_{BE} &= f(\lambda_1) + f(\lambda_2) - f(\lambda^x_3), \\ \chi^p_{BE} &= f(\lambda_1) + f(\lambda_2) - f(\lambda^p_3), \end{aligned} \tag{B3}$$

where

$$\begin{aligned} &\lambda_1 = \sqrt{\frac{\xi_1 + \xi_2}{2}}, \quad \lambda_2 = \sqrt{\frac{\xi_1 - \xi_2}{2}}, \quad \xi_1 = V^2_{A_1} + V^2_{B_1} + 2C^x_{A_1B_1}C^p_{A_1B_1}, \\ &\xi_2 = \sqrt{(V^2_{A_1} - V^2_{B_1})^2 + 4(V^2_{A_1} + V^2_{B_1})C^x_{A_1B_1}C^p_{A_1B_1} + 4V_{A_1}V_{B_1}[(C^x_{A_1B_1})^2 + (C^p_{A_1B_1})^2]}, \end{aligned} \tag{B4}$$

and

$$\begin{aligned} \lambda^x_3 &= \sqrt{V^2_{A_1} - \frac{V_{A_1}(C^x_{A_1B_1})^2}{V_{B_1}}}, \\ \lambda^p_3 &= \sqrt{V^2_{A_1} - \frac{V_{A_1}(C^p_{A_1B_1})^2}{V_{B_1}}}. \end{aligned} \tag{B5}$$

The key rate is

$$\begin{aligned} k_{\mathrm{tot}} &= P_AP_Bk^x_{AB} + (1 - P_A)(1 - P_B)k^p_{AB} \\ &= P_AP_B\beta I^x_{AB} + (1 - P_A)(1 - P_B)\beta I^p_{AB} \\ &\quad - P_AP_B[f(\lambda_1) + f(\lambda_2) - f(\lambda^x_3)] \\ &\quad - (1 - P_A)(1 - P_B)[f(\lambda_1) + f(\lambda_2) - f(\lambda^p_3)]. \end{aligned} \tag{B6}$$

When $P_A = P_B = 1/2$, the key rate can be simplified to

$$k_{\mathrm{tot}} = \frac{\beta(I^x_{AB} + I^p_{AB})}{4} - \frac{f(\lambda_1) + f(\lambda_2)}{2} + \frac{f(\lambda^x_3) + f(\lambda^p_3)}{4}. \tag{B7}$$

We can find that the key rate is invariant under permutation $g' = -g$, which means that the key rate is symmetric about the bisector $g' = -g$. Similar to CV-MDI-QKD, combining the symmetry and convexity of the accessible sets (g, g') allows one to restrict its minimization to the accessible points along the bisector $g' = -g$. Then, the optimal coherent attack can be obtained by $g' = -g = \phi$.

However, for the proposed biased base scheme, we find that the key rate changes under permutation of $g' = -g$. Thus, the key rate is asymmetric about the bisector $g' = -g$. In Fig. 6, we

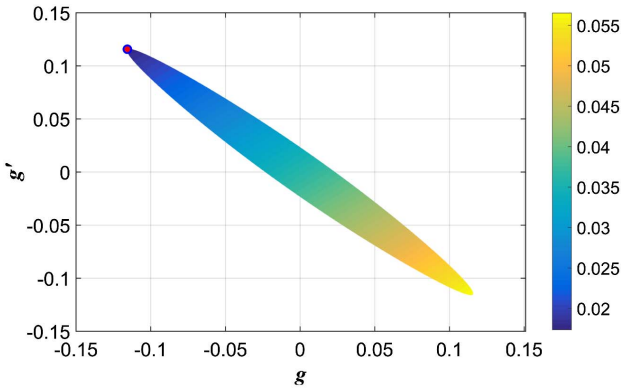

Fig. 6. Accessible points and key rate in the correlation plane (g, g') for $L_A = 1$ km and $L_B = 20$ km. The other parameters are set to $\beta = 0.95$, $\varepsilon_A = 0.001$, $\varepsilon_B = 0.01$, $\eta_A = 0.884$, $\eta_B = 0.506$, $\nu_{elA} = 0.02$, $\nu_{elB} = 0.05$, and $P_A = P_B = 0.9$.

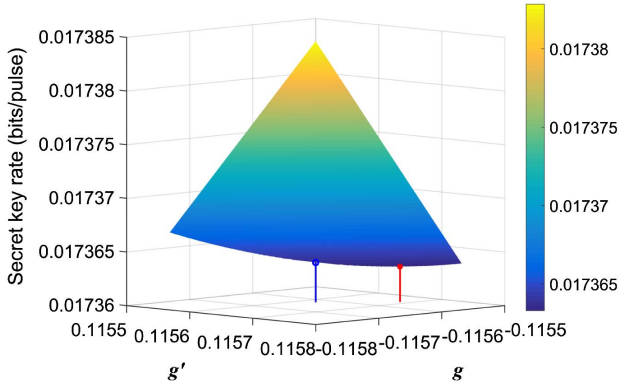

Fig. 7. Zoom of top-left corner of Fig. 6.

give the corresponding accessible region of the correlation (g, g') and achievable key rate at the fixed channel parameters. Note that the correlation region (g, g') is symmetric with respect to the bisector $g' = -g$. However, the key rate is not symmetric about $g' = -g$ due to the asymmetric base. The key rate decreases gradually toward the top-left corner of the correlation plane, but the extreme top-left point, that is, $g' = -g = \phi$, does not mean the minimum key rate that can be achieved. Such a phenomenon can be clearly observed in Fig. 7, which is a 3D graphical representation of the dependence of key rate on the (g, g') (top-left corner of Fig. 6). The blue line and circle represent $g' = -g = \phi$ and the corresponding key rate, respectively. The red dot and line represent the minimum key rate and the corresponding values of (g, g'), respectively. The worst (g, g') corresponding to Eve's optimal attack depends on the selection probability of the basis. For theoretical analysis, the minimum secret key rate can be obtained by scanning all values of (g, g') in the accessible physical region.

APPENDIX C: EXPERIMENTAL SECRET KEY RATE

The experimental key rate is estimated using the covariance matrix γ_{AB} with the form

$$\gamma_{AB} = \begin{bmatrix} V_A^x & 0 & C_{AB}^x & 0 \\ 0 & V_A^p & 0 & C_{AB}^p \\ C_{AB}^x & 0 & V_B^x & 0 \\ 0 & C_{AB}^p & 0 & V_B^p \end{bmatrix}. \tag{C1}$$

The relevant parameters for the reconstructed covariance matrix are the variances and covariances of the quadratures of Alice and Bob, which can be directly estimated by either Alice or Bob.

Supposing that Alice and Bob choose m_x and m_p raw keys for the parameter estimation of the amplitude and phase quadratures, respectively, the estimators can be given by

$$\begin{aligned} \hat{V}_A^x &= \frac{1}{m_x}\sum_{i=1}^{m_x} x_{Ai}^2, \qquad \hat{V}_B^x = \frac{1}{m_x}\sum_{i=1}^{m_x} x_{Bi}^2, \\ \hat{C}_{AB}^x &= \frac{1}{m_x}\sum_{i=1}^{m_x} x_{Ai}x_{Bi}, \quad \hat{V}_A^p = \frac{1}{m_p}\sum_{i=1}^{m_p} p_{Ai}^2, \\ \hat{V}_B^p &= \frac{1}{m_p}\sum_{i=1}^{m_p} p_{Bi}^2, \qquad \hat{C}_{AB}^p = \frac{1}{m_p}\sum_{i=1}^{m_p} p_{Ai}p_{Bi}. \end{aligned} \tag{C2}$$

Then, the Shannon mutual information between Alice and Bob can be obtained by

$$\begin{aligned} I_{AB}^x &= \frac{1}{2}\log_2\frac{\hat{V}_A^x}{\hat{V}_{A|B}^x} = \frac{1}{2}\log_2\frac{\hat{V}_A^x}{\hat{V}_A^x - (\hat{C}_{AB}^x)^2/\hat{V}_B^x}, \\ I_{AB}^p &= \frac{1}{2}\log_2\frac{\hat{V}_A^p}{\hat{V}_{A|B}^p} = \frac{1}{2}\log_2\frac{\hat{V}_A^p}{\hat{V}_A^p - (\hat{C}_{AB}^p)^2/\hat{V}_B^p}. \end{aligned} \tag{C3}$$

The elements of the covariance matrix $\gamma_{A_1B_1}$ can be obtained by using the relations

$$\begin{aligned} \hat{V}_{A_1}^x &= 1 + \frac{\hat{V}_A^x - 1 - v_{elA}}{\eta_A}, \qquad \hat{V}_{A_1}^p = 1 + \frac{\hat{V}_A^p - 1 - v_{elA}}{\eta_A}, \\ \hat{V}_{B_1}^x &= 1 + \frac{\hat{V}_B^x - 1 - v_{elB}}{\eta_B}, \qquad \hat{V}_{B_1}^p = 1 + \frac{\hat{V}_B^p - 1 - v_{elB}}{\eta_B}, \\ \hat{C}_{A_1B_1}^x &= \hat{C}_{AB}^x/\sqrt{\eta_A\eta_B}, \qquad \hat{C}_{A_1B_1}^p = \hat{C}_{AB}^p/\sqrt{\eta_A\eta_B}. \end{aligned} \tag{C4}$$

$\gamma_{A_1FG/B}^{x(p)}$ can be derived by applying the transformation of beam splitter and projective measurement. Finally, the Holevo bound $\chi_{BE}^{x(p)}$ can be calculated by

$$\chi_{BE}^{x(p)} = S(\rho_{A_1B_1}) - S(\rho_{A_1FG/B}^{x(p)}). \tag{C5}$$

APPENDIX D: PERFORMANCE DEPENDENCE OF THE PROTOCOL ON THE EPR STATES

The two-mode squeezing and antisqueezing levels can be evaluated by simultaneously measuring either the amplitude (x_{dA}, x_{dB}) or phase (p_{dA}, p_{dB}) quadrature of the EPR source with balanced homodyne detection. From the definitions of squeezing and antisqueezing of the two-mode entangled states

$$\begin{aligned} \langle(\hat{x}_{dA} - \hat{x}_{dB})^2\rangle &= \langle(\hat{p}_{dA} + \hat{p}_{dB})^2\rangle = 2s, \\ \langle(\hat{x}_{dA} + \hat{x}_{dB})^2\rangle &= \langle(\hat{p}_{dA} - \hat{p}_{dB})^2\rangle = 2s_{\text{anti}}, \end{aligned} \tag{D1}$$

we have

$$s=\frac{1}{2}(V_{dA}+V_{dB}-2C_{dAdB}),$$
$$s_{\text{anti}}=\frac{1}{2}(V_{dA}+V_{dB}+2C_{dAdB}), \quad \textbf{(D2)}$$

where s and s_{anti} represent the squeezing and antisqueezing. V_{dA} and V_{dB} are the variances of Alice's and Bob's measured data, respectively, and C_{dAdB} is their correlation, which contains the electronic noise and limited detection efficiency of the practical homodyne detector. Hence, the initial two-mode squeezing and antisqueezing levels can be approximately inferred by modifying s and s_{anti} to

$$s=\frac{1}{2}\left[\frac{V_{dA}-\nu_{eldA}-(1-\eta_{dA})}{\eta_{dA}}+\frac{V_{dB}-\nu_{eldB}-(1-\eta_{dB})}{\eta_{dB}}-\frac{2C_{dAdB}}{\sqrt{\eta_{dA}\eta_{dB}}}\right],$$
$$s_{\text{anti}}=\frac{1}{2}\left[\frac{V_{dA}-\nu_{eldA}-(1-\eta_{dA})}{\eta_{dA}}+\frac{V_{dB}-\nu_{eldB}-(1-\eta_{dB})}{\eta_{dB}}+\frac{2C_{dAdB}}{\sqrt{\eta_{dA}\eta_{dB}}}\right], \quad \textbf{(D3)}$$

where ν_{eldA}, ν_{eldB}, η_{dA}, and η_{dB} are the electronic noises and detection efficiencies of two homodyne detectors. The noise of the antisqueezing is $\Delta V_0 = s_{\text{anti}} - 1/s$.

To fully investigate the dependence of protocol on the entanglement degree of the EPR states, we experimentally prepare the two-mode entangled state with different levels of squeezing and antisqueezing. In Fig. 8, we simulate the asymptotic secret key rate versus transmission distance for EPR states with the experimental squeezing and antisqueezing values. Figure 8(a) represents the situation where the distance between Alice and Charlie is close to 0 km, and Fig. 8(b) simulates a 1 km of channel loss between Alice and Charlie. It is clear that the key rate can be significantly improved by raising the efficiency of Alice's detector, because high efficiency increases the mutual information between Alice and Bob while keeping the knowledge of Eve about Bob's results unchanged.

From Fig. 8, we find the higher two-mode squeezing does not necessarily mean higher key rate, especially at the long distance; further, stronger squeezing is usually accompanied by a higher excess noise level of the antisqueezed quadrature, which is detrimental to QKD. The EPR source with −5.6 dB of squeezing has the longer achievable transmission distance, and a −7.1 dB squeezing EPR source is able to achieve the higher key rate in the low- and medium-loss regions. In the experiment, we employ a −7.1 dB squeezing EPR source to meet the realistic application of the protocol in the asymmetric configurations, namely, a 0, 0.2, and 0.4 dB loss between Alice and Charlie.

In Fig. 9, we plot the maximum achievable transmission distance of the protocol as a function of the distance from Charlie to Alice under realistic conditions. The parameters for the simulation are −7.1 dB of squeezing and 9.6 dB of antisqueezing, $\beta = 0.95$, $\varepsilon_A = 0.001$, $\varepsilon_B = 0.01$, $\eta_A = 0.884$, $\eta_s = 0.81$, $\eta_B = 0.506$, $\nu_{elA} = 0.02$, and $\nu_{elB} = 0.05$. We can find that (for the reverse reconciliation) the protocol has better performance when Charlie's position is close to Alice.

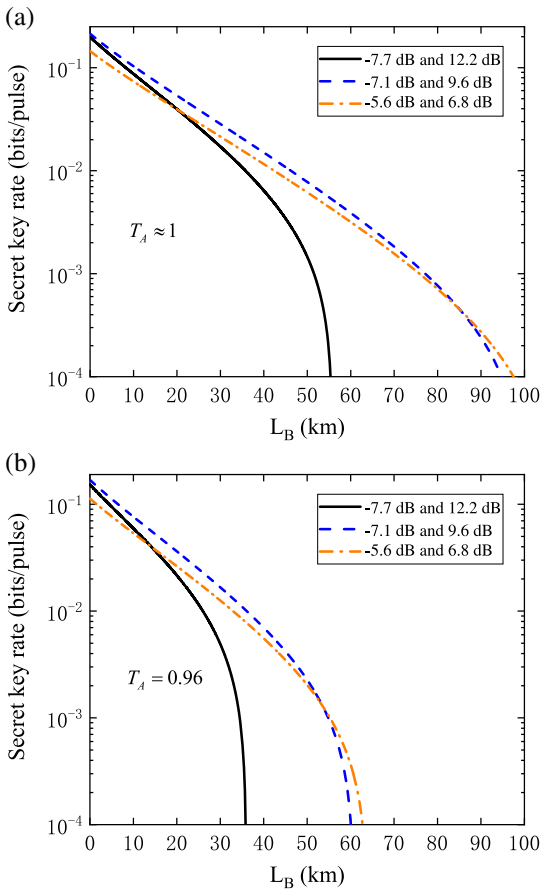

Fig. 8. Secret key rate versus transmission distance in the asymptotic case. The simulation parameters are set to $\beta = 0.95$, $\varepsilon_A = 0.001$, $\varepsilon_B = 0.01$, $\eta_A = 0.884$, $\eta_s = 0.81$, $\eta_B = 0.506$, $\nu_{elA} = 0.02$, and $\nu_{elB} = 0.05$.

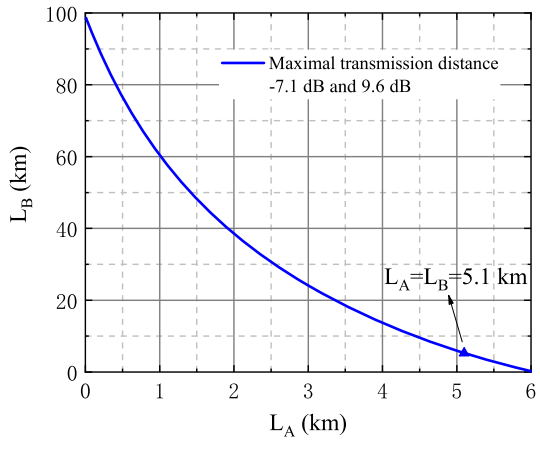

Fig. 9. Maximum transmission distance from Charlie to Bob (L_B) versus the distance from Charlie to Alice (L_A).

APPENDIX E: IMPROVING THE SECRET KEY RATE VIA A BIASED BASE METHOD

In the asymptotic limit, since the covariance matrix related to the calculation of the key rate can always be accurately

estimated, and the prepared entanglement source is approximately symmetrical, the key generation rate with biased base can be written as

$$\begin{aligned} K^{\infty} &= P_A P_B(\beta I^x_{AB} - \chi^x_{BE}) \\ &\quad + (1-P_A)(1-P_B)(\beta I^p_{AB} - \chi^p_{BE}) \\ &\approx [P_A P_B + (1-P_A)(1-P_B)](\beta I_{AB} - \chi_{BE}). \end{aligned} \tag{E1}$$

Obviously, the key rate can be improved by optimizing the total sifted efficiency $P_A P_B + (1-P_A)(1-P_B)$, where $P_A, P_B \in (0,1)$. When the probabilities P_A and P_B are close to 1 or 0, the total sifted efficiency approaches the maximum value. In our experimental implementation, the biased-base probabilities are set to $P_A = P_B = 0.9$, which indicates that the phase quadratures are selected to be observed for most of the time. In this case, the key rate generated is 64% higher than that of the original unbiased base protocol.

In CV-QKD, there are two detection methods for the quantum signals: homodyne detection and heterodyne detection. The heterodyne detection does not need to randomly switch the measurement bases; instead, it measures two quadratures at the same time. Therefore, all the data can be used to extract the key; however, it will inevitably introduce vacuum noises. The homodyne detection detects only a quadrature by randomly switching the measurement bases. The secret key can only be extracted when both parties choose the same measurement bases. Thus, in the original unbiased base scheme, half of the raw data have to be discarded, which results in the waste of quantum state resources and low efficiency of the protocol. By changing the switching ratio of bases, the total base sifted efficiency and the key rate can be significantly increased.

As shown in Fig. 10, we compare the key rates for the three different protocols. The black solid lines indicate the original case where Alice and Bob both perform homodyne detection with equal base choice ratio of 0.5/0.5, which is equivalent to the squeezed states protocol with homodyne detection and reverse reconciliation. The blue dashed lines indicate the case where Alice performs homodyne detection and Bob performs heterodyne detection, which is equivalent to the squeezed states protocol with heterodyne detection and reverse reconciliation. The red dashed lines indicate the case where Alice and Bob both perform homodyne detection with biased-base choices of 0.9/0.1. The simulation parameters are set to be the same as those in Fig. 4 (or Table 1) of the main text. We can see that the proposed biased-base scheme can achieve a higher key rate at most of the distribution distance. The heterodyne detection, instead of homodyne detection at Bob's side, can only increase the transmission distance a little. Note that the case where both Alice and Bob perform heterodyne detection, which is equivalent to the coherent states protocol and heterodyne detection, is not shown here as there is no positive key rate.

In the finite-size regime, when statistical fluctuations of the measured key data are taken into consideration and supposing that the total number of signals exchanged between Alice and Bob is N, the secret key rate for the biased base scheme is written as [35]

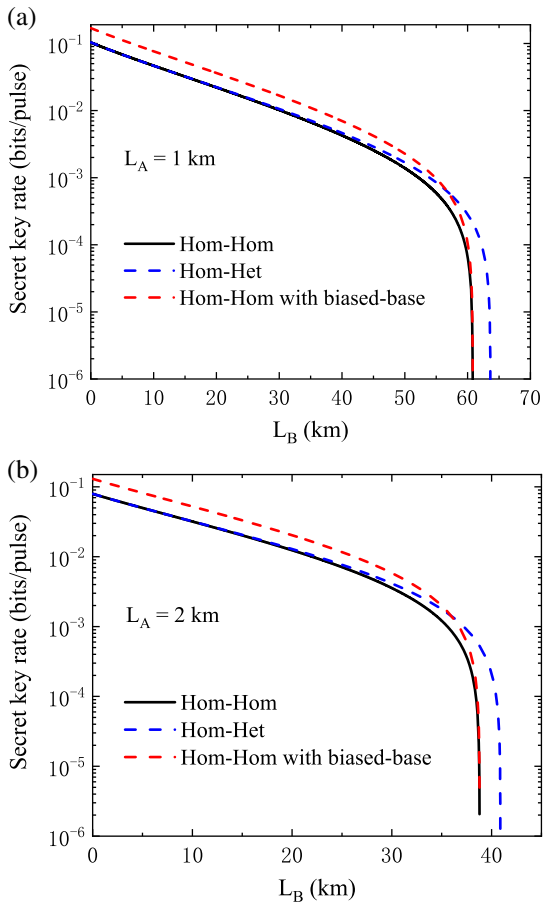

Fig. 10. Secret key rate versus the transmission distance for three different protocols. The simulation parameters are set to $\beta = 0.95$, $\varepsilon_A = 0.001$, $\varepsilon_B = 0.01$, $\eta_A = 0.884$, $\eta_s = 0.81$, $\eta_B = 0.506$, $\nu_{elA} = 0.02$, and $\nu_{elB} = 0.05$.

$$\begin{aligned} K^x &= (1-P_A)(1-P_B)\frac{n_x}{N_x}[\beta I^{x(\delta_{PE})}_{AB} - \chi^{x(\delta_{PE})}_{BE} - \Delta(n_x)], \\ K^p &= P_A P_B \frac{n_p}{N_p}[\beta I^{p(\delta_{PE})}_{AB} - \chi^{p(\delta_{PE})}_{BE} - \Delta(n_p)], \\ K^{\text{finite}} &= \max\{K^x, 0\} + \max\{K^p, 0\}, \end{aligned} \tag{E2}$$

where $N_x = (1-P_A)(1-P_B)N$ and $N_p = P_A P_B N$ are the number of sifted signals in the x and p quadratures, respectively, in which n_x and n_p signals are used to extract the secret keys, and the remaining $m_x = N_x - n_x$ and $m_p = N_p - n_p$ signals are used for parameter estimation. δ_{PE} is the security parameter, which quantifies the failure probability of the parameter estimation process. $\Delta(n_x)$ and $\Delta(n_p)$ are the correction terms related to the privacy amplification in two quadratures x and p. Because of the statistical fluctuations, the covariance matrix used to estimate the secret key rate can no longer be obtained accurately. There is a trade-off between the base choice probability and accuracy of the parameter estimation. In this case, it is of vital importance to find the optimal bias between the two quadrature bases to maximize key rate.

APPENDIX F: COMPLETELY CHARACTERIZED SOURCE

When the entangled source is considered to be completely characterized and trusted, Eve can only attack the two quantum channels. As shown in Fig. 11, the mixed EPR source can be purified by a four-mode state. Suppose that Charlie initially generates two independent pure EPR states (EPR1 and EPR2), which are injected into a Mach–Zehnder interferometer where two quadrature squeezers (SQZ1 and SQZ2) are inserted. By setting the suitable parameters, any Gaussian two-mode state $\rho_{A_0B_0}$ can be prepared. The four-mode state $\rho_{A_0B_0CD}$ is pure.

Then, the information that Eve can steal, the Holevo bound $\chi_{BE}^{x(p)}$, becomes

$$\chi_{BE}^{x(p)} = S(\rho_E) - S(\rho_{E/B}^{x(p)}) = S(\rho_{A_1B_1CD}) - S(\rho_{A_1CDFG/B}^{x(p)}). \tag{F1}$$

In Fig. 12, we show the maximum achievable transmission distance of the protocol considering the completely characterized entangled source. In this scenario, the protocol has better performance compared with that of the partially characterized source. For the symmetric case, the maximum transmission distance can reach up to $L_A = L_B = 8.2$ km. When $L_A = L_B = 8$ km, a key rate of 0.005 bits/pulse can be achieved. When $L_A = L_B = 5$ km, a key rate of 0.096 bits/pulse is obtained. For the asymmetric case, such as $L_A = 7$, $L_B = 14$, $L_A = 5$, and $L_B = 20$ km, key rates of 0.007 and 0.024 bits/pulse can be achieved, respectively. The reachable distribution distance is suitable to build a CV-QKD network with a shared source in a city's government service center or central business district.

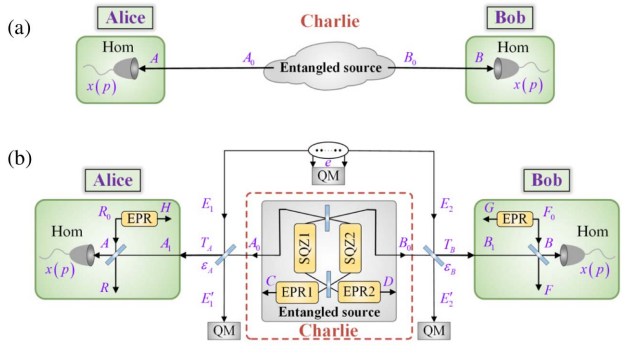

Fig. 11. PM and EB schemes of CV-QKD protocol with completely characterized entangled source. Hom, homodyne detection; SQZ, quadrature squeezer; QM, quantum memory.

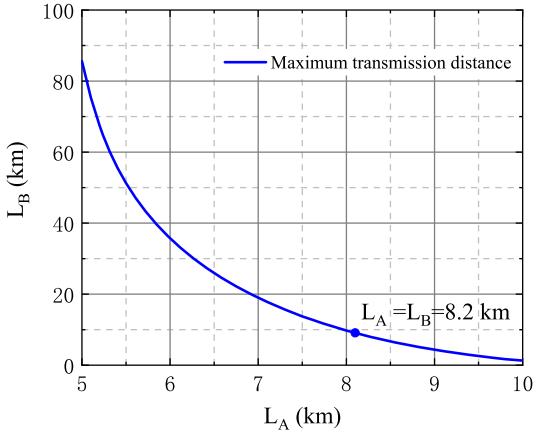

Fig. 12. Maximum transmission distance from Charlie to Bob (L_B) versus the distance from Charlie to Alice (L_A) for completely characterized entangled source with two-mode squeezing and antisqueezing of –7.1 and 9.6 dB. The simulation parameters are set to $\beta = 0.95$, $\varepsilon_B = 0.01$, $\eta_A = 0.884$, $\eta_B = 0.506$, $\nu_{elA} = 0.02$, and $\nu_{elB} = 0.05$.

APPENDIX G: EXPERIMENTAL DETAILS AND RESULTS

In the CV-QKD experiment based on EPR entangled states, Charlie prepares a two-color EPR entangled state and sends one mode (810 nm) to Alice and the other mode (1550 nm) to Bob. Then, Alice and Bob randomly measure the amplitude or phase quadrature of the received EPR mode with the balanced homodyne detectors (BHDs). The quantum state has a time span of 6 μs and repetition rate of 50 kHz. The output signals of two BHDs are sampled by high-speed acquisition cards with a sampling rate of 50 MHz. Due to the large difference of the propagation paths for the two modes of the EPR state, the recorded data of Alice and Bob are required to be synchronized accurately. Because the interval of the sampling data points is 0.02 μs, which is much smaller than the duration of a quantum signal, we can realize the synchronization by aligning the two user's data directly. The recorded 300 data points for each quantum state mix with a sinusoidal signal at 3.5 MHz and low-pass filtered with a cutoff frequency of 0.5 MHz digitally. The digital low-pass filter we use is a 200-tap finite impulse response (FIR) filter. The filtered data are added up to obtain the quadrature value of the quantum state, which is located at the sideband frequency of 3.5 MHz with a bandwidth of 1 MHz.

For measurement of the amplitude and phase quadratures, we need to apply voltages of $\pm V_{\pi/2}$ to the PM. Particular attention should be paid to the processes of signal modulation and detection. First, the voltage of the base pulses applied to the PM exists in oscillation at the rising and falling edges and may cause deviations of the measurement bases. Second, the sudden change of relative phase between the signal and LO makes the output signal from the BHDs oscillate, especially for Alice's measured outcomes, where the LO and signal mode are continuous-wave. Notice that this effect can be avoided for Bob by setting the rising and falling edges of the base pulses at the extinction regions of pulsed LO at 1550 nm (Fig. 3 of the main text). To handle the above issues, we set the signal mode in the second half of the base-switching pulse to make it far away from the rising and falling edges. Another method we adopted to suppress the influence of the oscillation on the BHD measurement results is to reduce the LO power properly.

Bob's excess noise mentioned in Table 1 of the main text mainly comes from three parts. The first part is the imperfect phase-locking accuracy between the LO beam and signal light, which contributes to 0.002 shot-noise unit (SNU) excess noise. The second part is the scattered noise photons due to the depolarized guided acoustic Brillouin scattering of the LO light in

Table 2. Original Data of the Data Point in Fig. 4(a) ($P = 0.9$)

L_A	0 km				1 km			2 km	
L_B	10 km	20 km	40 km	60 km	10 km	20 km	40 km	10 km	20 km
V_A^x	4.215	3.968	4.106	4.277	3.663	3.944	4.169	3.860	3.822
V_B^x	1.937	1.519	1.239	1.090	1.816	1.576	1.237	1.957	1.555
C_{AB}^x	2.106	1.529	1.039	0.646	1.846	1.590	1.059	2.015	1.533
V_A^p	4.275	4.468	4.398	4.226	3.741	4.020	4.353	4.147	4.066
V_B^p	1.858	1.534	1.245	1.066	1.848	1.512	1.255	1.909	1.497
C_{AB}^p	−2.053	−1.650	−1.118	−0.580	−1.891	−1.523	−1.103	−2.059	−1.509
K	0.0961	0.0477	0.0126	0.0038	0.0718	0.0283	0.0053	0.0543	0.0235

Table 3. Original Data of the Data Point in Fig. 4(a) ($P = 0.5$)

L_A	0 km				1 km			2 km	
L_B	10 km	20 km	40 km	60 km	10 km	20 km	40 km	10 km	20 km
V_A^x	4.309	3.902	4.187	3.976	3.533	3.870	4.031	3.300	3.686
V_B^x	1.851	1.531	1.297	1.079	1.786	1.542	1.243	1.837	1.522
C_{AB}^x	2.059	1.560	1.155	0.594	1.770	1.544	1.044	1.760	1.446
V_A^p	4.223	4.286	4.760	3.933	3.736	4.116	4.355	3.915	3.791
V_B^p	1.913	1.518	1.213	1.069	1.808	1.550	1.246	1.970	1.437
C_{AB}^p	−2.079	−1.588	−1.100	−0.566	−1.847	−1.590	−1.099	−2.044	−1.388
K	0.0602	0.0402	0.0076	0.0026	0.0363	0.0205	0.0042	0.0261	0.0124

a long-distance single-mode optical fiber, which induces an excess noise level about 0.001 SNU. The third part comes from the experimental system noise including stability of the EPR entanglement source and the calibration of the SNU, and the resulting excess noise is about 0.007 SNU. Other excess noise sources such as the leakage of LO light and the spontaneous Raman noise are suppressed to a negligible level by using the time multiplexing and polarization multiplexing of LO and signal light.

Tables 2 and 3 show the original data of the data point in Fig. 4(a) of the main text, where $V_{A(B)}^x$ represents the measured values of the amplitude quadrature normalized to shot noise unit, $V_{A(B)}^p$ represents the normalized value of phase quadrature, and $C_{AB}^{x(p)}$ and K denote the covariance and secret key rate calculated from the above measured values, respectively.

Funding. National Natural Science Foundation of China (62175138); National Key Research and Development Program of China (2016YFA0301403); Shanxi 1331KSC.

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

†These authors contributed equally to this paper.

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
2. 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**, 1301–1350 (2009).
3. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).
4. S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).
5. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
6. E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," NPJ Quantum Inf. **2**, 16025 (2016).
7. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
8. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
9. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).
10. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
11. 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).
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, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
13. 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).
14. 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).

15. 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**, 378–381 (2013).
16. H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, "Measurement-based noiseless linear amplification for quantum communication," Nat. Photonics **8**, 333–338 (2014).
17. 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," Nat. Photonics **9**, 397–402 (2015).
18. 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).
19. 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**, 634–642 (2016).
20. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett. **41**, 3511–3514 (2016).
21. X. Wang, W. Liu, P. Wang, and Y. Li, "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution," Phys. Rev. A **95**, 062330 (2017).
22. S. Du, Y. Tian, and Y. Li, "Impact of four-wave-mixing noise from dense wavelength-division-multiplexing systems on entangled-state continuous-variable quantum key distribution," Phys. Rev. Appl. **14**, 024013 (2020).
23. B. Qi, H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, and N. A. Peters, "Experimental passive-state preparation for continuous-variable quantum communications," Phys. Rev. Appl. **13**, 054065 (2020).
24. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
25. Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, "Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber," Optica **9**, 492–500 (2022).
26. C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," Phys. Rev. A **87**, 022308 (2013).
27. Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction," Phys. Rev. A **95**, 032304 (2017).
28. Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, "Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source," Phys. Rev. A **102**, 032604 (2020).
29. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69–72 (2013).
30. R. Ursin and R. Hughes, "Sharing quantum secrets," Nature **501**, 37–38 (2013).
31. H.-K. Lo, H. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J. Cryptol. **18**, 133–165 (2005).
32. V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**, 062337 (2015).
33. H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," Phys. Rev. Lett. **122**, 160501 (2019).
34. X. Guo, C. Xie, and Y. Li, "Generation and homodyne detection of continuous-variable entangled optical beams with a large wavelength difference," Phys. Rev. A **84**, 020301 (2011).
35. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
36. H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: saturation attack on practical continuous-variable quantum key distribution," Phys. Rev. A **94**, 012325 (2016).
37. H. Qin, R. Kumar, V. Makarov, and R. Alléaume, "Homodyne-detector-blinding attack in continuous-variable quantum key distribution," Phys. Rev. A **98**, 012312 (2018).
38. P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Phys. Rev. A **87**, 062313 (2013).
39. X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems," Phys. Rev. A **88**, 022339 (2013).
40. D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**, 041010 (2015).
41. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).
42. G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**, 839–842 (2019).
43. C. Bruynsteen, M. Vanhoecke, J. Bauwelinck, and X. Yin, "Integrated balanced homodyne photonic-electronic detector for beyond 20 GHz shot-noise-limited measurements," Optica **8**, 1146–1152 (2021).
44. S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," Nature **564**, 225–228 (2018).