Experimental Passive-State Preparation for Continuous-Variable Quantum Communications

Bing Qi,[1,2,*] Hyrum Gunther,[3] Philip G. Evans,[1] Brian P. Williams,[1] Ryan M. Camacho,[3] and Nicholas A. Peters[1,4]

[1] *Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*

[2] *Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996, USA*

[3] *Department of Electrical and Computer Engineering, Brigham Young University, Provo, Utah 84602, USA*

[4] *Center for Interdisciplinary Research and Graduate Education, The University of Tennessee, Knoxville, Tennessee 37996, USA*

(Received 21 January 2020; revised manuscript received 15 April 2020; accepted 7 May 2020; published 26 May 2020)

In the Gaussian-modulated coherent state quantum key distribution (QKD) protocol, the sender first generates Gaussian-distributed random numbers and then encodes them on weak laser pulses *actively* by performing amplitude and phase modulations. Recently, an equivalent *passive* QKD scheme has been proposed by exploring the intrinsic field fluctuations of a thermal source [B. Qi, P. G. Evans, and W. P. Grice, Phys. Rev. A **97**, 012317 (2018)]. This passive QKD scheme is especially appealing for chip-scale implementation since no active modulation is required. In this paper, we conduct an experimental study of the passively encoded QKD scheme using an off-the-shelf amplified spontaneous emission source operated in continuous-wave mode. Our results show that the excess noise introduced by the passive state preparation scheme can be effectively suppressed by applying optical attenuation and a secure key can be generated over metro-area distances.

DOI: 10.1103/PhysRevApplied.13.054065

I. INTRODUCTION

Quantum key distribution (QKD) allows two remote users (Alice and Bob) to establish a secure key by transmitting quantum states through an untrusted channel [1–4]. The generated secure key can be further applied in various cryptographic protocols to achieve long-term proven security against adversaries with unlimited computational power.

QKD protocols are commonly divided into two families based on encoding schemes: discrete-variable (DV) QKD or continuous-variable (CV) QKD. In contrast, classical optical communications are typically grouped into two categories based on detection schemes: direct detection or coherent detection. In principle, the combination of both encoding (DV or CV) and detection (direct or coherent) could lead to four families of QKD protocols. Among them, DV-QKD with direction detection (single-photon detection) [5,6] and CV-QKD with coherent detection (optical homodyne detection) [7–9] are dominant, although other protocols, such as CV-QKD using single-photon detection [10], do exist. For simplicity, in this paper we use the term CV-QKD to refer to CV-QKD using coherent detection.

CV-QKD's most distinguishing feature is coherent detection. It enables high-speed optical homodyne detection with no dead time, which could give high secure-key rates over short distances. Further, the intrinsic filtering provided by the local oscillator in a coherent receiver can effectively suppress background noise and enable QKD through conventional dense wavelength-division-multiplexed fiber networks in the presence of strong classical traffic [11–13]. The similarity between a CV-QKD system and a classical coherent communication system opens the door for simultaneous quantum and classical communications [14] with a technological pathway toward fully integrated on-chip photonic implementation [15]. The integration of CV-QKD on a chip may have several benefits. It allows for the integration of multiple photonic functions into a single compact circuit. In particular, the phase-sensitive optical circuits commonly used for CV-QKD can be made more robust to temperature-induced phase drifts by reducing path-length differences on chip. Furthermore, silicon photonic devices are compatible with complementary-metal-oxide-semiconductor (CMOS) processes that enable monolithic integration of electronics and photonics, potentially leading to significant cost

*qib1@ornl.gov

 © 2020 American Physical Society

reduction that would enable the widespread utilization of QKD.

One important CV-QKD protocol is the Gaussian-modulated-coherent-states (GMCS) QKD protocol [9], which has been implemented with standard off-the-shelf telecom components, such as laser sources, optical homodyne detectors, and optical intensity and phase modulators [16–20]. In the GMCS protocol, Alice first generates Gaussian-distributed random numbers x_A and p_A and then prepares a coherent state $|x_A + ip_A\rangle$, sent to Bob through a channel controlled by the adversary (Eve). The quantum state preparation is commonly implemented *actively* using amplitude and phase modulation. High-speed modulation with high extinction is extremely challenging in chip-scale silicon photonics. While on-chip modulation with an extinction ratio above 65 dB has been demonstrated recently [21], the high-speed on-chip modulators required for active QKD encoding add significant cost, manufacturing time, and complexity and are the principal source of loss in most integrated photonic circuits. Therefore, the potential to remove the modulators used for encoding may yield significant reductions in cost, manufacturing time, and on-chip loss.

One could simplify the chip-scale implementation by adopting a passive CV-QKD protocol, where the amplitude and phase modulators in GMCS QKD are replaced by a thermal source, beam splitters, optical attenuators, and homodyne detectors [22]. As we show in Ref. [22], given that Alice's QKD transmitter is trusted, the passive CV-QKD protocol is equivalent to GMCS QKD. This means that the well-established security proofs for GMCS QKD can be applied to passive CV-QKD directly. More recently, this passive state preparation scheme has also been extended to measurement-device-independent CV-QKD [23]. It could also be applied in other CV quantum communication protocols, such as quantum secret sharing [24] and quantum digital signatures [25].

In this paper, we conduct experimental studies of passive CV-QKD using a practical multimode thermal source. As we show below, the excess noise due to the passive state preparation scheme can be effectively suppressed by Alice applying optical attenuation and a secure key can be generated over metro-area distances using an off-the-shelf amplified spontaneous emission source operated in continuous-wave (cw) mode.

This paper is organized as follows. In Sec. II, we review the passive CV-QKD protocol and compare it with conventional GMCS QKD [9,26] as well as entanglement-based CV-QKD using a two-mode squeezed vacuum state [27]. In Sec. III, we present our experimental setup and develop a corresponding noise model. In Sec. IV, we present the experimental results. Finally, we conclude this paper with a brief summary in Sec. V.

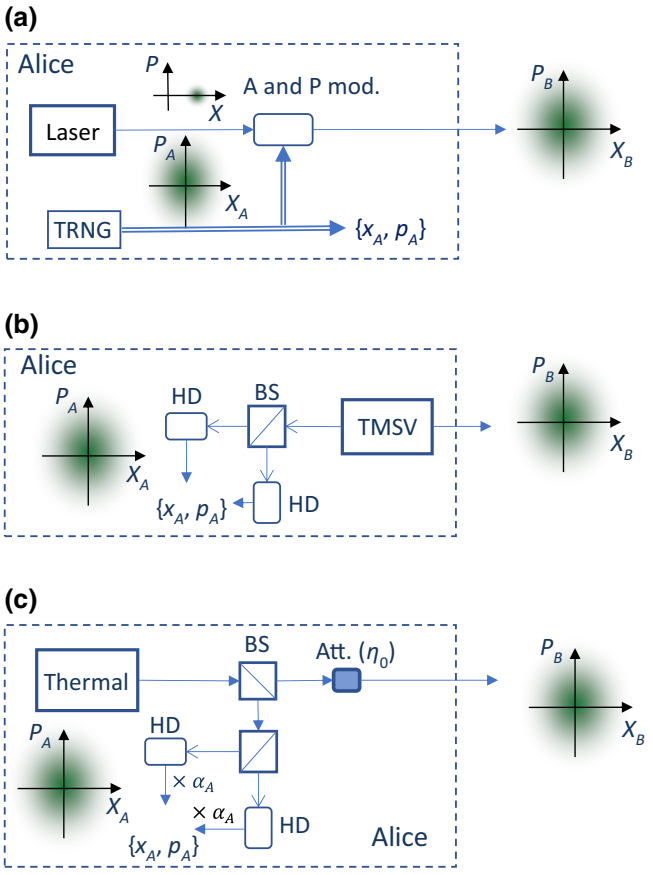

FIG. 1. Three equivalent quantum state preparation schemes. (a) The Gaussian-modulated coherent states (GMCS) QKD [9]. TRNG, true random-number generator; A&P mod., amplitude and phase modulators. (b) Entanglement-based CV-QKD [27]. TMSV, two-mode squeezed vacuum state; HD, homodyne detector; BS, beam splitter. (c) Passive CV-QKD [22]. Att., optical attenuator.

II. THE PROTOCOL AND ITS SECURITY

In the GMCS QKD protocol [9], Alice generates Gaussian-distributed random numbers x_A and p_A using a trusted random-number generator, prepares a coherent state $|x_A + ip_A\rangle$ accordingly, and transmits it to Bob, as shown in Fig. 1(a). At Bob's end, he can either measure a randomly chosen quadrature of the incoming quantum state by conducting single homodyne detection [9] or measure both quadratures simultaneously by conducting conjugate homodyne detection (which is called the heterodyne protocol) [26]. Alice and Bob further estimate channel-induced noise and other QKD parameters by comparing a subset of their data through an authenticated classical channel. This allows them to upper bound the information that could be gained by a third party, Eve. Given that the correlation between Alice's and Bob's data is above a certain threshold, they can perform reconciliation and privacy amplification to generate a final secure key.

There are different reconciliation algorithms in GMCS QKD. In this paper, we consider the heterodyne protocol [26] using reverse reconciliation [9], where Alice tries to determine Bob's measurement results from her data. In this case, a secure key can be generated as long as the mutual information between Alice and Bob is larger than the information Eve could have on Bob's measurement results. More details about GMCS QKD can be found in recent reviews [28,29].

Note that from Eve's point of view, the quantum state from Alice is a mixture of all possible coherent states, which is simply a thermal state with an average photon number $n_0 = V_A/2$, where V_A is Alice's modulation variance. We remark that throughout this paper, all the noise variances and modulation variances are defined in shot-noise units. There are different ways (corresponding to different QKD protocols) for Alice to prepare the outgoing thermal state, as shown in Fig. 1. As long as Alice's QKD transmitter is within a trusted location, Eve cannot tell which protocol is actually carried out by Alice. This suggests that all these QKD protocols are equivalent in terms of security. In fact, the security of GMCS QKD is commonly analyzed based on an entanglement-based CV-QKD protocol using a two-mode squeezed vacuum state [27], as shown in Fig. 1(b). In this entanglement-based protocol, by performing conjugate homodyne detection on one mode of a properly chosen two-mode squeezed vacuum state, Alice acquires Gaussian-distributed random numbers x_A and p_A with the desired variance of V_A. In the meantime, Alice transmits the other mode, which is projected to a coherent state $|x_A + ip_A\rangle$, in her perspective, to Bob through the quantum channel. From Eve's point of view, since she has no information about x_A and p_A, the state from Alice is thermal, as in the case of GMCS QKD.

In passive CV-QKD [22], the intrinsic field fluctuations of a thermal source are utilized to generate a secure key, as shown in Fig. 1(c). In this protocol, Alice splits the output of a thermal source into two spatial modes using a beam splitter. One mode is sent to Bob after being attenuated using an optical attenuator, while the other mode will be measured locally by Alice using conjugate homodyne detection. Alice further numerically scales down her measurement results by a factor of α_A, acquiring Gaussian-distributed random numbers x_A and p_A, her estimation of the quadrature values of the outgoing mode (for details about how to determine the optimal α_A, see Sec. III). By choosing a proper combination of source intensity and optical attenuation, the quadrature variance of the outgoing mode can be set to the desired value V_A. Again, from Eve's point of view, she cannot distinguish the quantum state sent in passive CV-QKD from the one in GMCS QKD (or, for that matter, entanglement-based CV-QKD), so all three protocols are equivalent in terms of security. We remark that the combination of the balanced beam splitter and the optical attenuator in Fig. 1(c) can be replaced by a single unbalanced beam splitter with a suitable splitting ratio. The latter configuration can lead to a more efficient use of the thermal source.

While the security is not dependent on which of the above schemes is employed, the secure-key rate is sensitive to the excess noise generated in the quantum state preparation process. Since the quantum states sent by Alice are identical in the three schemes, so is the information that Eve could gain on Bob's measurement results. The mutual information between Alice and Bob directly connects to Alice's uncertainties on the quadrature values of the outgoing mode. In GMCS QKD (and the above entanglement-based CV-QKD), the minimum uncertainty Alice could achieve on either quadrature of the outgoing mode is equal to one, as determined by the uncertainty principle in quantum mechanics. In Appendix A, we present a detailed noise model of the passive CV-QKD protocol and show that Alice's uncertainty on the outgoing mode is given by

$$\Delta = \frac{2V_A(\upsilon_a + 1)}{V_A\eta_a + 2\eta_0(\upsilon_a + 1)}\eta_0 + 1, \tag{1}$$

where η_0 is the transmittance of the optical attenuator and η_a and υ_a are the efficiency and noise variance of Alice's detector, respectively [see Eq. (A5) in Appendix A].

From Eq. (1), the excess noise due to the passive state preparation scheme (which equals $\Delta - 1$) can be effectively suppressed by introducing optical attenuation at Alice (while keeping V_A at the desired value). Equation (1) suggests that regardless of the amount of detector noise, as η_0 approaches zero, so does the excess noise. In practice, this is convenient, since Alice's detector does not need to be shot-noise limited. To further illustrate the role of the optical attenuation, in Appendix A we explicitly show that under the beam-splitting attack, the information advantage between Alice and Bob, when compared to that between Eve and Bob, can be improved by introducing optical loss at Alice.

In practice, η_0 cannot be zero; otherwise, to have a nonzero average photon number in the outgoing mode, the intensity of the thermal source has to be infinite. Security proofs of practical CV-QKD, taking into account the excess noise contributed by both Alice and Bob, are well developed [28,29]. In the next section, we present our experimental setup, develop a corresponding noise model, and quantify the QKD performance using the established security proof.

III. EXPERIMENTAL SETUP AND NOISE MODEL

The experimental setup is shown in Fig. 2. A fiber amplifier (PriTel, Inc.), operated in cw mode (amplified spontaneous emission: ASE in Fig. 2) with vacuum-state input, is employed as a broadband thermal source. Previous studies have shown that the output from an unseeded fiber amplifier is thermal [22,30–32]. To select a single

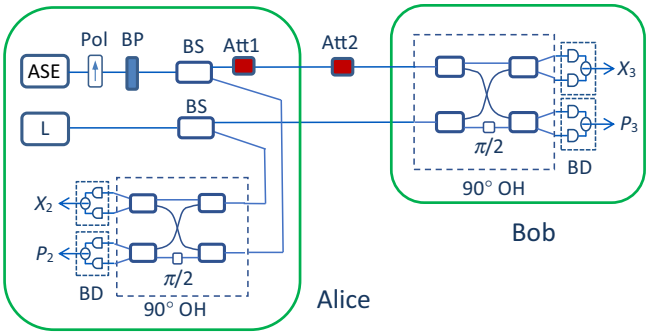

FIG. 2. The experimental setup. ASE, broadband amplified spontaneous emission source; L, narrow-band laser source as local oscillator; BP, optical band-pass filter; BS, balanced beam splitter; Pol, fiber polarizer; Att1, Att2, variable optical attenuators; 90° OH, 90° optical hybrid; BD, balanced photodetector.

polarization mode, a fiber pigtailed polarizer (Pol in Fig. 2) is placed right after the light source. Since the spectral bandwidth of the source is about 30 nm, a 0.8-nm optical band-pass filter centered at 1542 nm (BP in Fig. 2) is employed to reduce the optical power of unused light. Note that the actual bandwidth of this filter is not crucial, since the optical coherent detection is mode selective: only photons in the same spectral-temporal and polarization mode as the local oscillator will be detected. Nevertheless, the optical power of unused modes should be suppressed so that they are well below the power of the local oscillator.

The filtered thermal light is split by a balanced beam splitter into two modes: one is sent to Bob after passing through an optical attenuator while the other is measured locally by Alice using conjugate homodyne detection. Note that there are two optical attenuators shown in Fig. 2: Att1 represents a "trusted" attenuator inside Alice's system, which cannot be controlled by Eve. It provides the desired attenuation η_0 shown in Eq. (1); Att2 represents the channel loss, which is fully controlled by Eve. In this proof-of-principle experiment, a single optical attenuator is employed to provide the combined attenuation of Att1 and Att2.

A cw laser source with a central wavelength of 1542 nm (Clarity-NLL-1542-HP from Wavelength Reference) is employed to provide local oscillators for both Alice's and Bob's conjugate homodyne detection systems. For long-distance applications, instead of transmitting a local oscillator from Alice to Bob, it is more appropriate to generate Bob's local oscillator locally [33–35]. The conjugate homodyne detection is implemented using a 90° optical hybrid and two balanced photodetectors. Limited by the detectors available, different types of balanced photodetectors are employed in Alice's and Bob's systems. The corresponding bandwidths are 100 MHz (Alice) and 75 MHz (Bob). The outputs of all the balanced photodetectors are sampled by a real-time oscilloscope.

One important deviation of the setup shown in Fig. 2 from the ideal passive QKD protocol discussed in the previous section is that a multimode (rather than a single-mode) thermal source is employed in the actual experiment. On the one hand, this modification greatly simplifies the implementation, since it is experimentally challenging to prepare a single-mode thermal state; on the other, the existence of unused modes could contribute additional noise, as we discuss below.

Within the integration time of the homodyne detector, the output of the light source (even after the 0.8-nm spectral filter) contains many spectral-temporal modes of independent thermal states. To generate correlated keys, Alice and Bob have to measure the same mode. In practice, the modes measured by Alice and Bob (which are determined by the modes of their local oscillators) may not be perfectly overlapped. We define the mode measured by Bob as mode $|B\rangle$. The mode measured by Alice may be decomposed as

$$|A\rangle = a|B\rangle + b|B'\rangle, \tag{2}$$

where $|B'\rangle$ represents the mode orthogonal to mode $|B\rangle$ and $|a|^2 + |b|^2 = 1$. Without loss of generality, we assume that the mode-overlap coefficient a is a real number.

For simplicity, we only consider the X quadrature below. The P quadrature can be studied in a similar way. The X quadrature of the outgoing mode (see Fig. 3) is given by

$$x_1 = \sqrt{\frac{\eta_0}{2}}x_{\rm in} - \sqrt{\frac{\eta_0}{2}}x_{v1} - \sqrt{1-\eta_0}x_{v3}, \tag{3}$$

where $x_{\rm in}$ is the X quadrature of mode $|B\rangle$ of the source, η_0 is the transmittance of the optical attenuator, and x_{v1} and x_{v3} represent vacuum noises introduced by beam splitter 1 and the optical attenuator, respectively.

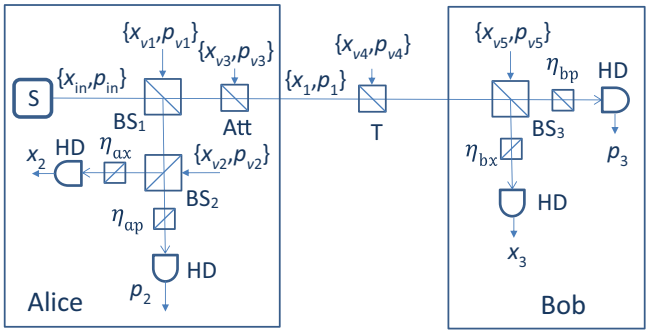

FIG. 3. The noise model of the experimental setup. S, thermal source; BS_{1-3}, balanced beam splitter; Att, optical attenuator; HD, homodyne detector; T, a beam splitter emulating channel loss; $\eta_{\rm ax}$, $\eta_{\rm bx}$, $\eta_{\rm ap}$, and $\eta_{\rm bp}$, beam splitters emulating losses of homodyne detectors.

Similarly, Alice's measurement result of the X quadrature is given by

$$x_2 = \frac{\sqrt{\eta_{\rm ax}}}{2}(a x_{\rm in} + b x'_{\rm in}) + \frac{\sqrt{\eta_{\rm ax}}}{2}(a x_{v1} + b x'_{v1}) + \sqrt{\frac{\eta_{\rm ax}}{2}} x_{v2} - \sqrt{1-\eta_{\rm ax}} x_{\rm va} + E_{\rm ax}, \tag{4}$$

where $\eta_{\rm ax}$ and $E_{\rm ax}$ are the efficiency and noise of Alice's homodyne detector for X-quadrature measurement; $x'_{\rm in}$ is the X quadrature of mode $|B'\rangle$ of the source; x'_{v1} is the vacuum noise in mode $|B'\rangle$ from beam splitter 1; x_{v2} and $x_{\rm va}$ are vacuum noises associated with beam splitter 2 and $\eta_{\rm ax}$.

Given x_2, Alice's optimal estimation of x_1 is

$$x_{\rm opt} = \alpha_A x_2, \tag{5}$$

where $\alpha_A = \langle x_1 x_2\rangle / \langle x_2^2\rangle$ [36,37].

Using Eqs. (3) and (4), we can determine α_A as

$$\alpha_A = \frac{n_0 a \sqrt{2\eta_0 \eta_{\rm ax}}}{n_0 \eta_{\rm ax} + 2\upsilon_{\rm ax} + 2}, \tag{6}$$

where n_0 is the average photon number per mode from the source and $\upsilon_{\rm ax} = \langle E_{\rm ax}^2\rangle$ is the detector-noise variance. The relation $\langle x_{\rm in}^2\rangle = \langle (x'_{\rm in})^2\rangle = 2n_0 + 1$, which is a good approximation for the broadband light source used in our experiment, is used in the above derivation.

Using Eqs. (3)–(6), Alice's uncertainty on x_1 given her measurement result of x_2 can be determined as

$$V_{x1|x2} = \langle (x_1 - \alpha_A x_2)^2\rangle = \frac{2V_A\eta_0(\upsilon_{\rm ax}+1) + V_A^2\eta_{\rm ax}(1-a^2)}{V_A\eta_{\rm ax} + 2\eta_0(\upsilon_{\rm ax}+1)} + 1, \tag{7}$$

where $V_A = \eta_0 n_0$ is the equivalent modulation variance of the outgoing mode.

The excess noise due to the passive state preparation scheme is $\varepsilon_A = V_{x1|x2} - 1$, which can be determined from Eq. (7) as

$$\varepsilon_A = \frac{2V_A\eta_0(\upsilon_{\rm ax}+1) + V_A^2\eta_{\rm ax}(1-a^2)}{V_A\eta_{\rm ax} + 2\eta_0(\upsilon_{\rm ax}+1)}. \tag{8}$$

Once the QKD excess noise has been appropriately quantified, we can apply the standard security proof for GMCS QKD to calculate the secure-key rate. In the next section, we experimentally determine the mode mismatch a and other system parameters to evaluate the performance of our system.

IV. EXPERIMENTAL RESULTS

In the experiment, both the broadband light source and the local oscillator are operated in cw mode. A 2-GHz-bandwidth real-time oscilloscope is employed to sample the outputs of Alice's and Bob's detectors. The modes sampled by Alice and Bob are determined by lengths of optical paths and also the electrical frequency responses of the optical homodyne detectors. Due to experimental imperfections, the modes measured by Alice and Bob are not perfectly overlapped, i.e., $a < 1$. To determine a, we calculate the correlation between Alice's and Bob's measurement results at different output photon numbers.

Alice's X-quadrature measurement result, x_2, is given by Eq. (4). Similarly, when no optical attenuation is applied ($\eta_0 = 1$, $T = 1$, see Fig. 3), Bob's X-quadrature measurement result, x_3, is given by

$$x_3 = \frac{\sqrt{\eta_{\rm bx}}}{2} x_{\rm in} - \frac{\sqrt{\eta_{\rm bx}}}{2} x_{v1} + \sqrt{\frac{\eta_{\rm bx}}{2}} x_{v5} - \sqrt{1-\eta_{\rm bx}} x_{\rm vb} + E_{\rm bx}, \tag{9}$$

where $\eta_{\rm bx}$ and $E_{\rm bx}$ are the efficiency and noise of Bob's homodyne detector for X-quadrature measurement; x_{v5} and $x_{\rm vb}$ are vacuum noises associated with beam splitter 3 and $\eta_{\rm bx}$ (see Fig. 3).

Using Eqs. (4) and (9), it is easy to show that

$$\langle x_2^2\rangle = \frac{\eta_{\rm ax}}{2} n_0 + \upsilon_{\rm ax} + 1, \tag{10}$$

$$\langle x_3^2\rangle = \frac{\eta_{\rm bx}}{2} n_0 + \upsilon_{\rm bx} + 1, \tag{11}$$

$$\langle x_2 x_3\rangle = \frac{\sqrt{\eta_{\rm ax}\eta_{\rm bx}}}{2} n_0 a. \tag{12}$$

From Eqs. (10)–(12), the correlation coefficient between x_2 and x_3 is given by

$$\mathrm{Corr} = \frac{\langle x_2 x_3\rangle}{\sqrt{\langle x_2^2\rangle \langle x_3^2\rangle}} = \frac{n_0\sqrt{\eta_{\rm ax}\eta_{\rm bx}}}{\sqrt{(\eta_{\rm ax} n_0 + 2\upsilon_{\rm ax} + 2)(\eta_{\rm bx} n_0 + 2\upsilon_{\rm bx} + 2)}} a. \tag{13}$$

Equation (13) shows that as n_0 approaches infinity, the correlation coefficient approaches the mode-overlap coefficient a. Thus, we can determine a experimentally by measuring the correlation between Alice's and Bob's measurement results at a high output photon number.

We adjust n_0 by changing the pump power of the fiber amplifier and calculate the correlation coefficient from experimental data. In this experiment, no optical attention is applied ($\eta_{\rm tot} = \eta_0 T = 1$). The local oscillator power is 2 mW. The detection efficiency and noise variance of Alice's and Bob's conjugate homodyne detectors are $\eta_{\rm ax} = 0.43 \pm 0.01$, $\eta_{\rm ap} = 0.38 \pm 0.01$, $\eta_{\rm bx} = 0.54 \pm 0.01$, $\eta_{\rm bp} = 0.51 \pm 0.01$, $\upsilon_{\rm ax} = 0.17 \pm 0.01$, $\upsilon_{\rm ap} = 0.19 \pm 0.01$, $\upsilon_{\rm bx} = 0.24 \pm 0.01$, and $\upsilon_{\rm ap} = 0.23 \pm 0.01$. At each photon level, we collect 500 000 data samples, which are

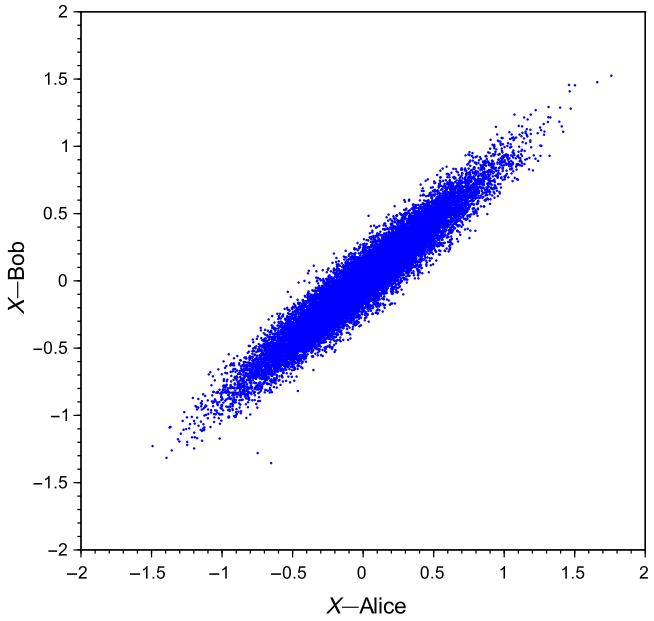

FIG. 4. The raw data of Alice's and Bob's X-quadrature measurement results ($n_0 = 880$ and no optical attenuation applied).

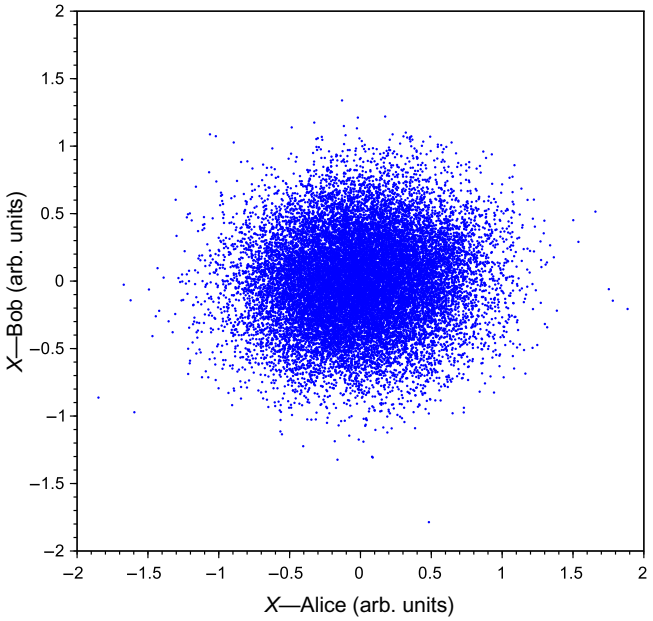

FIG. 6. The raw data of Alice's and Bob's X-quadrature measurement results ($n_0 = 900$ and $\eta_{\text{tot}} = -42.2$ dB).

further divided into ten 50 000-data sets. The correlation coefficient is calculated for each data set.

Figure 4 shows the raw data of Alice's and Bob's X-quadrature measurement results when the average photon number per mode from the source is $n_0 = 880$. Figure 5 shows the correlation coefficient of Alice's and Bob's X-quadrature measurement results at different n_0 (the error bars represent one standard deviation). The solid line is a curve fit using Eq. (13) with $a = 0.96$ and the detector parameters given above. The theory and experimental results match well.

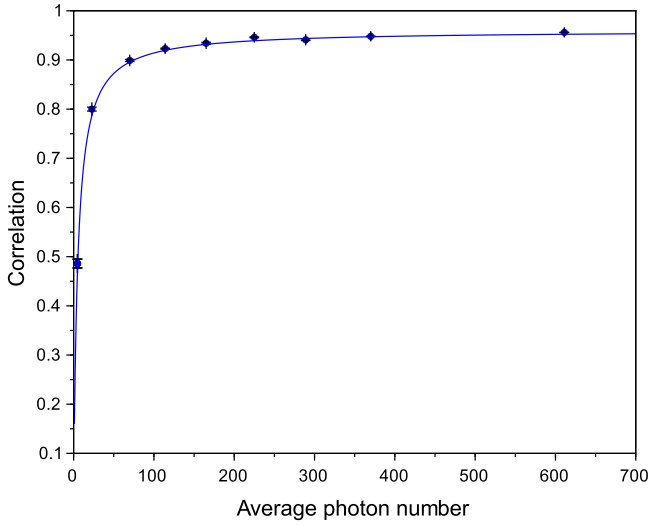

FIG. 5. The correlation coefficient of Alice's and Bob's X-quadrature measurement results at different output photon numbers of the light source. The blue dots represent experimental results (the error bars represent one standard deviation). The solid line is a fitting curve using Eq. (13) with $a = 0.96$.

To further justify the above noise model, we conduct experiments using a constant n_0 of 900 and different optical attenuation η_{tot}. This experiment can also be modeled using Eq. (13), with η_{bx} replaced by $\eta_{\text{tot}}\eta_{\text{bx}}$. Note that when the optical loss is very high, the correlation between Alice's and Bob's data is barely visible from the raw data, as evidenced by the case of $\eta_{\text{tot}} = -42.2$ dB shown in Fig. 6. Nevertheless, by calculating the correlation coefficient from the raw data and comparing it with the theoretical prediction, the proposed noise model is well justified, as shown in Fig. 7.

As we show in Ref. [22], the well-established security proof of GMCS QKD can be applied to passive CV-QKD, as long as Alice's excess noise is properly quantified using Eq. (8). We calculate the secure key as a function of the channel length using the experimentally determined system parameters. Here, we assume that the quantum channel is a single-mode fiber with an attenuation coefficient of $\gamma = 0.2$ dB/km. As shown in Fig. 8, a practical distance above 80 km could be achieved. The QKD distance could be further extended by improving the mode-overlap factor a. Details of the secure-key formulas are summarized in Appendix B.

To compare the simulated secure-key rates with the experimental results shown in Fig. 7, we use Eq. (A11) in Appendix A to determine the mutual information between Alice and Bob from the experimentally determined correlation coefficient as $I_{AB} = \log_2\left[1/(1 - \text{Corr}^2)\right]$. Two data

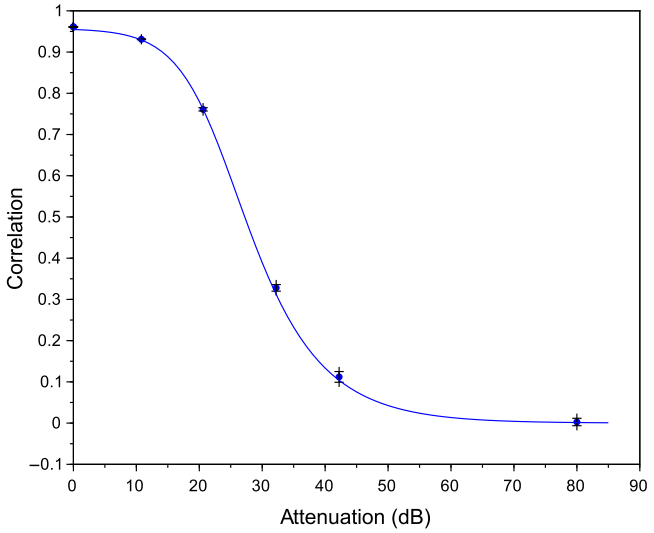

FIG. 7. The correlation coefficient of Alice's and Bob's X-quadrature measurement results as a function of the optical attenuation $\eta_{\rm tot} = \eta_0 T$. The blue dots represent experimental results (the error bars represent one standard deviation). The solid line is a fit curve based on Eq. (13) by replacing $\eta_{\rm bx}$ with $\eta_{\rm tot}\eta_{\rm bx}$.

points shown in Fig. 7, corresponding to $\eta_{\rm tot} = -32.1$ dB and -42.2 dB, are used in the calculation. Since only one attenuator is applied in the experiment, we artificially divide the total attenuation $\eta_{\rm tot}$ into Alice's attenuation η_0 and channel transmittance T as $\{\eta_0 = 0.0009, T = 0.69\}$ (for $\eta_{\rm tot} = -32.1$ dB) and $\{\eta_0 = 0.0004, T = 0.15\}$ (for $\eta_{\rm tot} = -42.2$ dB). The calculated secure-key rates are shown in Fig. 8 as two points, with error bars determined by one standard deviation of the correlation coefficient.

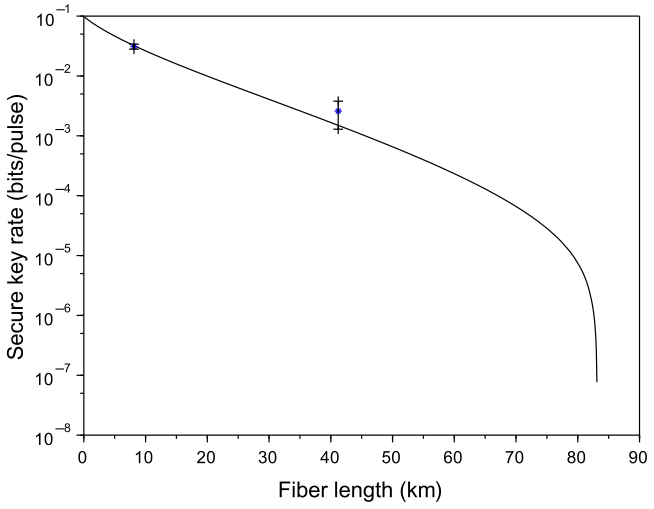

FIG. 8. The secure-key rate as a function of channel loss. Simulation parameters: $a = 0.96$, $n_0 = 900$, $\eta_{\rm ax} = 0.43$, $\eta_{\rm ap} = 0.38$, $\eta_{\rm bx} = 0.54$, $\eta_{\rm bp} = 0.51$, $\upsilon_{\rm ax} = 0.17$, $\upsilon_{\rm ap} = 0.19$, $\upsilon_{\rm bx} = 0.24$, and $\upsilon_{\rm ap} = 0.23$. The efficiency of the reconciliation algorithm is $f = 0.95$ (see details in Appendix B). The two data points are secure-key rates calculated using the experimental results shown in Fig. 7 (the error bars are determined by one standard deviation of the correlation coefficient).

V. SUMMARY

One common question on the passive CV-QKD scheme is whether we can trust the randomness from a thermal source. It is a common practice to apply a quantum random-number generator [38,39] in prepare-and-measure QKD for state preparation and/or measurement-basis selection. As we discuss in Ref. [32], while quantum randomness is ultimately connected to quantum superposition states, in the fully trusted device scenario, the quantum state received by the detector does not need to be a pure state. One illustrative example is the first quantum random-number generator, where electrons from a radioactive source such as ^{90}Sr are detected by a Geiger-Müller tube at random times [40,41]. In this process, while the whole system (the radioactive nuclei and electrons) is in a pure state, the state received by the detector is a mixture of zero-electron and one-electron emission states. True randomness can be generated as long as Eve cannot access (or control) the radioactive source. Similar arguments can also be applied to randomness generated from spontaneous emission using a thermal source.

The security of QKD is only as good as its underlying assumptions [42]. In this paper, we adopt a commonly used assumption in QKD that the QKD systems employed by Alice and Bob are fully trusted and cannot be accessed by Eve. In practice, any real-life QKD systems cannot be perfect. It is thus important to scrutinize all of the implementation details to identify potential side channels and develop the corresponding countermeasures. The investigation of loopholes and countermeasures in practical QKD systems plays a complementary role to security proofs.

In summary, we conduct experimental studies on the recently proposed passive CV-QKD protocol [22], which is appealing for chip-scale implementation. When implemented with a practical multimode thermal source, one important issue is how to determine the excess noise contributed by photons in the unwanted modes. In this paper, we develop a noise model based on a practical setup and conduct experiments to verify the above model using a commercial off-the-shelf amplified spontaneous emission source. Our results suggest that passive CV-QKD could be a cost-effective solution for metro-area QKD.

ACKNOWLEDGMENTS

This work was performed at Oak Ridge National Laboratory (ORNL). ORNL is managed by UT-Battelle, LLC, under Contract No. DE-AC05-00OR22725 for the DOE. We acknowledge support from the DOE Office of Cybersecurity Energy Security and Emergency Response (CESER)

through the Cybersecurity for Energy Delivery Systems (CEDS) program.

The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive paid-up irrevocable worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for U.S. Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan [43].

APPENDIX A: DETAILED NOISE MODEL ANALYSIS

In this appendix, we present a detailed noise model of the passive CV-QKD scheme, taking into account the imperfections of practical homodyne detectors. To gain some intuition on its security, we also study the well-known beam-splitting attack where Eve replaces the lossy quantum channel by a beam splitter with a suitable transmittance and measures both the X quadrature and P quadrature of the reflected light, as shown in Fig. 9. Note that in our model, we assume that Eve's detectors are perfect while Alice's and Bob's detectors are lossy and noisy.

For simplicity, we only consider the X quadrature below. The P quadrature can be studied in a similar way. The X quadrature of the optical-mode output from Alice (see Fig. 9) is given by

$$x_1 = \sqrt{\frac{\eta_0}{2}}x_{\rm in} - \sqrt{\frac{\eta_0}{2}}x_{v1} - \sqrt{1-\eta_0}x_{v3}, \tag{A1}$$

where $x_{\rm in}$ is the X quadrature of the output of the source, η_0 is the transmittance of the optical attenuator, and x_{v1} and x_{v3} represent vacuum noises introduced by beam splitter 1 and the optical attenuator, respectively (see Fig. 9). Note that the variance of the vacuum noise is 1 in shot-noise units, i.e., $\langle x_{v1}^2\rangle = \langle x_{v3}^2\rangle = 1$.

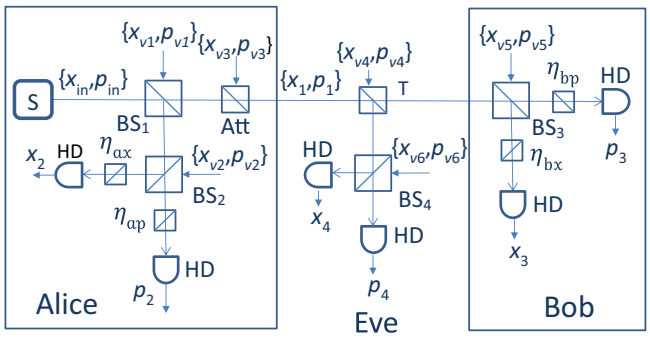

FIG. 9. The detailed noise model under the beam-splitting attack. S, thermal source; BS_{1-4}, balanced beam splitter; Att, optical attenuator; HD, homodyne detector; T, a beam splitter emulating channel loss; $\eta_{\rm ax}$, $\eta_{\rm bx}$, $\eta_{\rm ap}$, $\eta_{\rm bp}$, beam splitters emulating losses of homodyne detectors.

Given that the source outputs a thermal state with an average photon number of n_0, it is easy to show that the outgoing mode from Alice is also a thermal state with an average photon number of $\eta_0 n_0/2$. The output state from Alice in the passive CV-QKD is identical to that of GMCS QKD using active modulation with a modulation variance of

$$V_A = \eta_0 n_0. \tag{A2}$$

As we discuss in Sec. II, the secure-key rate of CV-QKD is sensitive to excess noises. It is thus important to quantify how much excess noise is introduced by the passive state preparation scheme.

As shown in Fig. 9, Alice splits the output of the source into two modes using a balanced beam splitter and measures the X quadrature and P quadrature of the local mode. Alice's X-quadrature measurement result is

$$\begin{aligned} x_2 = {} & \frac{\sqrt{\eta_{\rm ax}}}{2}x_{\rm in} + \frac{\sqrt{\eta_{\rm ax}}}{2}x_{v1} \\ & + \sqrt{\frac{\eta_{\rm ax}}{2}}x_{v2} - \sqrt{1-\eta_{\rm ax}}x_{\rm va} + E_{\rm ax}, \end{aligned} \tag{A3}$$

where $\eta_{\rm ax}$ and $E_{\rm ax}$ are the efficiency and noise of Alice's homodyne detector for X-quadrature measurement and x_{v2} and $x_{\rm va}$ are vacuum noises associated with beam splitter 2 and $\eta_{\rm ax}$.

Given x_2, Alice's optimal estimation of x_1 is $x_{\rm opt} = \alpha_0 x_2$, where $\alpha_0 = \langle x_1 x_2\rangle/\langle x_2^2\rangle$ [36,37].

Using Eqs. (A1) and (A3), we can determine α_0 as

$$\alpha_0 = \frac{n_0\sqrt{2\eta_0\eta_{\rm ax}}}{n_0\eta_{\rm ax} + 2\upsilon_{\rm ax} + 2}. \tag{A4}$$

In the above derivation, we define the detector-noise variance as $\upsilon_{\rm ax} = \langle E_{\rm ax}^2\rangle$. We also use the relation of $\langle x_{\rm in}^2\rangle = 2n_0 + 1$, which is true for a thermal state.

Alice's uncertainty on x_1 given her measurement result of x_2 is $\Delta = V_{x1|x2} = \langle (x_1 - \alpha_0 x_2)^2\rangle$. Using Eqs. (A1)–(A4), we can determine the excess noise of state preparation as

$$\varepsilon_A = \Delta - 1 = \frac{2V_A(\upsilon_{\rm ax}+1)}{V_A\eta_{\rm ax} + 2\eta_0(\upsilon_{\rm ax}+1)}\eta_0. \tag{A5}$$

Equation (A5) suggests that the excess noise of the passive state preparation scheme can be effectively reduced by introducing large optical attenuation at Alice (i.e., $\eta_0 \ll 1$). Note that to keep a desired variance V_A of the outgoing mode, a large n_0 is required from the source to compensate a small η_0.

To further illustrate the role of the optical attenuation, we calculate the mutual information between Alice and Bob (I_{AB}), and the one between Eve and Bob (I_{BE}), under the beam-splitting attack. We emphasis that in this paper, we consider the CV-QKD protocol using heterodyne detection and reverse reconciliation, where Bob measures both the X quadrature and the P quadrature of the incoming mode, and Alice tries to guess Bob's measurement results from her data. This is in contrast to the direct reconciliation protocol, where Bob tries to determine Alice's data.

As shown in Fig. 9, a lossy channel with a transmittance of T can be modeled by a beam splitter with an appropriate splitting ratio. In the beam-splitting attack, the transmitted and reflected mode are detected by Bob and Eve, respectively.

From Fig. 9, Bob's X-quadrature measurement result is given by

$$x_3 = \frac{\sqrt{\eta_0 T\eta_{\rm bx}}}{2}x_{\rm in} - \frac{\sqrt{\eta_0 T\eta_{\rm bx}}}{2}x_{v1} - \sqrt{\frac{(1-\eta_0)T\eta_{\rm bx}}{2}}x_{v3} - \sqrt{\frac{(1-T)\eta_{\rm bx}}{2}}x_{v4} + \sqrt{\frac{\eta_{\rm bx}}{2}}x_{v5} - \sqrt{1-\eta_{\rm bx}}x_{\rm vb} + E_{\rm bx}, \tag{A6}$$

where $\eta_{\rm bx}$ and $E_{\rm bx}$ are the efficiency and noise of Bob's homodyne detector for X-quadrature measurement, $x_{\rm vb}$ represents vacuum noise associated with $\eta_{\rm bx}$, and vacuum noises introduced by other components are shown in Fig. 9.

Similarly, Eve's X-quadrature measurement result is given by

$$x_4 = \frac{\sqrt{\eta_0(1-T)}}{2}x_{\rm in} - \frac{\sqrt{\eta_0(1-T)}}{2}x_{v1} - \sqrt{\frac{(1-\eta_0)(1-T)}{2}}x_{v3} + \sqrt{\frac{T}{2}}x_{v4} + \frac{1}{\sqrt{2}}x_{v6}. \tag{A7}$$

In reverse reconciliation, Alice tries to guess Bob's measurement result x_3 given her own measurement result x_2. Alice's optimal estimation of x_3 is $x_A = \alpha_1 x_2$, where $\alpha_1 = \langle x_3 x_2\rangle/\langle x_2^2\rangle$. From Eqs. (A3) and (A6), Alice's conditional variance on Bob's measurement result $V_{B|A}$ can be determined as

$$V_{B|A} = \langle (x_3 - \alpha_1 x_2)^2\rangle = \langle x_3^2\rangle - \frac{\langle x_2 x_3\rangle^2}{\langle x_2^2\rangle} = \frac{V_A T\eta_{\rm bx}(\upsilon_{\rm ax}+1)}{\frac{\eta_{\rm ax}}{\eta_0}V_A + 2\upsilon_{\rm ax} + 2} + \upsilon_{\rm bx} + 1. \tag{A8}$$

Since a secure key could be generated from both X and P, the mutual information between Alice and Bob is given by

$$I_{AB} = \log_2\left(\frac{V_B}{V_{B|A}}\right), \tag{A9}$$

where Bob's X-quadrature variance V_B is given by

$$V_B = \langle x_3^2\rangle = \frac{V_A T\eta_{\rm bx}}{2} + \upsilon_{\rm bx} + 1. \tag{A10}$$

Note that by using Eqs. (A8) and (A10), we can write Eq. (A9) as

$$I_{AB} = \log_2\left(\frac{1}{1-{\rm Corr}^2}\right), \tag{A11}$$

where ${\rm Corr} = \langle x_2 x_3\rangle/\sqrt{\langle x_2^2\rangle\langle x_3^2\rangle}$ is the correlation coefficient. Equation (A11) allows us to use the experimentally determined correlation coefficient to estimate the mutual information between Alice and Bob.

Following a similar procedure, Eve's conditional variance on Bob's measurement result and the mutual information between Eve and Bob can be determined as

$$V_{B|E} = \frac{V_A T\eta_{\rm bx}}{V_A(1-T)+2} + \upsilon_{\rm bx} + 1 \tag{A12}$$

and

$$I_{BE} = \log_2\left(\frac{V_B}{V_{B|E}}\right). \tag{A13}$$

From Eqs. (A8) to (A13), for a given V_A, we can effectively suppress $V_{B|A}$ and thus increase I_{AB} by reducing the value of η_0. In contrast, I_{BE} is independent of the value of η_0. This shows that the information advantage between Alice and Bob over that between Eve and Bob can be improved by introducing optical loss at Alice.

In principle, a secure key could be generated as long as $V_{B|A} < V_{B|E}$. The corresponding constraint on η_0 can be determined from Eqs. (A8) and (A12) as

$$\eta_0 < \frac{\eta_{\rm ax}}{(\upsilon_{\rm ax}+1)(1-T)}. \tag{A14}$$

APPENDIX B: SECURE-KEY-RATE CALCULATION

The asymptotic secure-key rate of GMCS QKD, in the case of reverse reconciliation, is given by Refs. [16,44]:

$$R = fI_{AB} - \chi_{BE}, \tag{B1}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, f is the efficiency of the reconciliation algorithm, and χ_{BE} is the Holevo bound on Eve's information about Bob's secure key.

For an optical fiber link with an attenuation coefficient of γ, the channel transmittance is given by

$$T = 10^{(-\gamma L)/10}, \tag{B2}$$

where L is the fiber length in kilometers.

In the case of conjugate homodyne detection, the X-quadrature noise added by Bob's detector (referred to Bob's input) is given [43] by

$$\chi_{\text{het}} = [1 + (1 - \eta_{\text{bx}}) + 2\upsilon_{\text{bx}}]/\eta_{\text{bx}}. \tag{B3}$$

The channel-added noise (referred to the channel input) is given by

$$\chi_{\text{line}} = \frac{1}{T} - 1 + \varepsilon_A, \tag{B4}$$

where ε_A is defined in Eq. (8) in the main text.

The overall noise is given by

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}. \tag{B5}$$

Since both quadratures can be used to generate a secure key, the mutual information between Alice and Bob can be determined by

$$I_{AB} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{B6}$$

where $V = V_A + 1$.

To estimate χ_{BE}, we assume that Eve cannot control the imperfections in Bob's system. This noise model has been widely used in CV-QKD experiments [9,12,16–20]. Under this model, the Holevo bound of the information between Eve and Bob is given [16] by

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{B7}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$,

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{B8}$$

where

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2, \tag{B9}$$

$$B = T^2(V\chi_{\text{line}} + 1)^2, \tag{B10}$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \tag{B11}$$

where

$$C = \frac{1}{[T(V + \chi_{\text{tot}})]^2}\{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \times [V\sqrt{B} + T(V + \chi_{\text{line}})] + 2T(V^2 - 1)\}, \tag{B12}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{B13}$$

$$\lambda_5 = 1. \tag{B14}$$

We remark that in this paper, all the excess noise generated at Alice is assumed to be caused by Eve's attack. This is a very conservative assumption. An alternative way to deal with the excess noise is to develop a suitable "trusted" noise model [45], which may lead to a better secure-key rate.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (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 (2009).

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

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

[5] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), p. 175.

[6] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[7] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

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

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

[10] B. Qi, Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation, Opt. Lett. **31**, 2795 (2006).

[11] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, Feasibility of quantum key distribution through 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 (2015).

[13] T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, *et al.*, Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels, Commun. Phys. **2**, 9 (2019).

[14] B. Qi, Simultaneous quantum and classical communication using continuous variable, Phys. Rev. A **94**, 042340 (2016).
[15] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, *et al.*, An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nat. Photonics **13**, 839 (2019).
[16] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, *et al.*, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).
[17] 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).
[18] P. Jouguet, S. Kunz-Jacques, A. Leverrier, Ph. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).
[19] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).
[20] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).
[21] S. Liu, H. Cai, C. T. DeRose, P. Davids, A. Pomerene, A. L. Starbuck, D. C. Trotter, R. Camacho, J. Urayama, and A. Lentine, High speed ultra-broadband amplitude modulators with ultrahigh extinction >65 dB, Opt. Express **25**, 11254 (2017).
[22] B. Qi, P. G. Evans, and W. P. Grice, Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution, Phys. Rev. A **97**, 012317 (2018).
[23] D. Bai, P. Huang, H. Ma, T. Wang, and G. Zeng, Passive-state preparation in continuous-variable measurement-device-independent quantum key distribution, J. Phys. B **52**, 135502 (2019).
[24] W. P. Grice and B. Qi, Quantum secret sharing using weak coherent states, Phys. Rev. A **100**, 022339 (2019).
[25] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, Free-Space Quantum Signatures Using Heterodyne Measurements, Phys. Rev. Lett. **117**, 100503 (2016).
[26] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography without Switching, Phys. Rev. Lett. **93**, 170504 (2004).
[27] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Inf. Comput. **3**, 535 (2003).
[28] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).
[29] F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations, Adv. Quantum Technol. **1**, 1800011 (2018).
[30] W. S. Wong, H. A. Haus, L. A. Jiang, P. B. Hansen, and M. Margalit, Photon statistics of amplified spontaneous emission noise in a 10-Gbit/s optically preamplified direct-detection receiver, Opt. Lett. **23**, 1832 (1998).
[31] P. Voss, M. Vasilyev, D. Levandovsky, T.-G. Noh, and P. Kumar, Photon statistics of single-mode zeros and ones from an erbium-doped fiber amplifier measured by means of homodyne tomography, IEEE Photon. Technol. Lett. **12**, 1340 (2000).
[32] B. Qi, True randomness from an incoherent source, Rev. Sci. Instrum. **88**, 113101 (2017).
[33] 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).
[34] 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).
[35] D. Huang, D. K. Lin, P. Huang, and G. H. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).
[36] J.-Ph. Poizat, J.-F. Roch, and Ph. Grangier, Characterization of quantum non-demolition measurements in optics, Ann. Phys. (Paris) **19**, 265 (1994).
[37] Ph. Grangier, J.-A. Levenson, and J.-Ph. Poizat, Quantum non-demolition measurements in optics, Nature **396**, 537 (1998).
[38] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Inf. **2**, 16021 (2016).
[39] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).
[40] M. Isida and Y. Ikeda, Random number generator, Ann. Inst. Stat. Math. **8**, 119 (1956).
[41] H. Schmidt, Quantum-mechanical random-number generator, J. Appl. Phys. **41**, 462 (1970).
[42] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).
[43] http://energy.gov/downloads/doe-public-access-plan.
[44] S. Fossier, E. Diamanti, T. Debuisschert, R. TualleBrouri, and Ph. Grangier, Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers, J. Phys. B **42**, 114014 (2009).
[45] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: A threat and a defense, Entropy **18**, 20 (2016).