# Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection

Bing Qi,[1,2,*] Pavel Lougovski,[1] Raphael Pooser,[1,2] Warren Grice,[1] and Miljko Bobrek[3]

[1]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6418, USA*

[2]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996-1200, USA*

[3]*RF, Communications, and Intelligent Systems Group, Electrical and Electronics Systems Research Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6006, USA*

(Received 2 March 2015; published 21 October 2015)

Continuous-variable quantum key distribution (CV-QKD) protocols based on coherent detection have been studied extensively in both theory and experiment. In all the existing implementations of CV-QKD, both the quantum signal and the local oscillator (LO) are generated from the same laser and propagate through the insecure quantum channel. This arrangement may open security loopholes and limit the potential applications of CV-QKD. In this paper, we propose and demonstrate a pilot-aided feedforward data recovery scheme that enables reliable coherent detection using a "locally" generated LO. Using two independent commercial laser sources and a spool of 25-km optical fiber, we construct a coherent communication system. The variance of the phase noise introduced by the proposed scheme is measured to be 0.04 (rad$^2$), which is small enough to enable secure key distribution. This technology also opens the door for other quantum communication protocols, such as the recently proposed measurement-device-independent CV-QKD, where independent light sources are employed by different users.

DOI: 10.1103/PhysRevX.5.041009 Subject Areas: Optics, Quantum Information

## I. INTRODUCTION

Quantum key distribution (QKD) allows two authenticated parties, normally referred to as Alice and Bob, to generate a secure key through an insecure quantum channel controlled by an eavesdropper, Eve [1–5]. Based on fundamental laws in quantum mechanics, idealized QKD protocols have been proved to be unconditionally secure against adversaries with unlimited computing power and technological capabilities [6–8].

Both discrete-variable (DV) QKD protocols based on single photon detection [1,2] and continuous-variable (CV) QKD protocols based on coherent detection [9–11] have been demonstrated as viable solutions in practice. One well-known CV-QKD protocol is the Gaussian-modulated coherent state (GMCS) protocol [11], which has been demonstrated through an 80-km optical fiber link recently [12]. One important advantage of the GMCS QKD is its robustness against incoherent background noise. The strong local oscillator (LO) employed in coherent detection also acts as a natural and extremely selective filter, which can suppress noise photons effectively. This intrinsic filtering function makes CV-QKD an appealing solution for secure key distribution over a noisy channel, such as a lit fiber in a conventional fiber optic network [13–15] or a free-space optical link [16].

However, all existing implementations of CV-QKD based on coherent detection contain a serious weakness: To reduce the phase noise, both the signal and the LO are generated from the same laser and propagate through the insecure quantum channel [11,12,16,17]. This arrangement has several limitations. First of all, it allows Eve to access both the quantum signal and the LO. Eve may launch sophisticated attacks by manipulating the LO, as demonstrated in recent studies [18–21]. Second, sending a strong LO through a lossy channel can drastically reduce the efficiency of QKD in certain applications. For example, to achieve a shot-noise-limited coherent detection, the required photon number in the LO is typically above $10^8$ photons per pulse at the receiver's end [11,12,17]. With a 1-GHz pulse repetition rate and a channel loss of 20 dB, the required LO power at the input of the quantum channel is about 1.2 W (at 1550 nm). If optical fiber is used as the quantum channel, noise photons generated by the strong LO inside the optical fiber may significantly reduce QKD efficiency and multiplexing capacity. Third, the LO is typically 7 or 8 orders of magnitude brighter than the quantum signal; complicated multiplexing and

*qib1@ornl.gov

demultiplexing schemes are required to effectively separate the LO from the quantum signal at the receiver's end. Note that the second and third problems discussed above might be mitigated by sending a weak LO from Alice and applying optical amplification at Bob's side. However, it is important to take into account the noise introduced by the optical amplifier in this case.

In brief, in CV-QKD, it is desirable to generate the LO "locally" using an independent laser source at the receiver's end. Unfortunately, such a scheme has never been implemented in practice. The main challenge is how to effectively establish a reliable phase reference between Alice and Bob. While various techniques, such as feedforward carrier recovery [22], optical phase-locked loops [23], and optical injection phase-locked loops [24], have been developed in classical coherent communication, these techniques are not suitable in QKD where the quantum signal is extremely weak and the tolerable phase noise is low. Furthermore, to prevent Eve from manipulating the LO, the LO laser should be isolated from outside both optically and electrically.

In this paper, we solve the above long-outstanding problem by proposing and demonstrating a pilot-aided feedforward data recovery scheme, which enables reliable coherent detection using a "locally" generated LO. This scheme is built upon the observation that in the GMCS QKD, Bob does not need to perform the measurement in the "correct basis." In fact, Bob can perform the measurement in an arbitrarily rotated basis as along as the basis information (the phase reference) is available afterwards. With this postmeasurement basis information, either Alice or Bob can rotate data at hand and generate correlated data with the other. We demonstrate the above scheme in a coherent communication system constructed by a spool of 25-km optical fiber and two independent commercial laser sources operated at free-running mode. The observed phase-noise variance is 0.04 ($\mathrm{rad}^2$), which is small enough to enable secure key distribution. This technology also opens the door for other novel quantum communication protocols, such as the measurement-device-independent (MDI) CV-QKD protocol [25–27], where independent light sources are employed by different users.

This paper is organized as follows: In Sec. II, we conduct a theoretical analysis of the proposed scheme. In Sec. III, we present the details of proof-of-principle experiments. We conclude this paper with a discussion in Sec. IV.

## II. THEORETICAL ANALYSIS

In GMCS QKD, Alice draws two random numbers $X_A$ and $P_A$ from a set of Gaussian random numbers (with a mean of zero and a variance of $V_A N_0$), prepares a coherent state $|X_A + iP_A\rangle$ accordingly, and sends it to Bob. Here, $N_0 = 1/4$ denotes the shot-noise variance. At Bob's end, he can perform either optical homodyne detection or optical heterodyne detection.

In GMCS QKD protocol based on homodyne detection [11], Bob randomly chooses to measure either the amplitude quadrature ($X$) or phase quadrature ($P$) of the incoming signal. Later on, he announces which quadrature he measures for each incoming signal through an authenticated public channel, and Alice only keeps the corresponding data. In GMCS QKD based on heterodyne detection [28], Bob first splits the incoming signal into two with a 50:50 beam splitter. He then measures $X$ at one output port and $P$ at the other. In this case, Alice keeps all her quadrature data.

After the quantum transmission stage, Alice shares a set of correlated Gaussian random variables (called the "raw key") with Bob. Alice and Bob compare a random sample of the raw key through an authenticated classical channel to estimate the transmittance and excess noise of the quantum channel. If the observed excess noise is small enough, they can further work out a secure key.

In the above description, we have implicitly assumed that Alice and Bob share a phase reference, so Bob can perform the required quadrature measurement. If the LO is generated for an independent laser source, how can Alice and Bob establish a phase reference in this case?.

In this section, we present a pilot-aided phase estimation scheme that allows Alice and Bob to measure the phase relation between two independent lasers in real time. Using this phase information, either Alice or Bob can rotate the data at hand in the postprocessing stage ("quadrature remapping") and establish correlation with the other. In principle, our scheme can be applied to both CV-QKD with homodyne detection and the one with heterodyne detection. In this paper, we focus on the case of heterodyne detection. For an independent and related work, see Ref. [29].

### A. CV-QKD using the quadrature remapping scheme

In a phase-coding DV-QKD protocol, it is also crucial to control the phase between a signal pulse and a reference pulse when performing interferometric measurement. In fact, a DV-QKD protocol using a strong phase-reference pulse has been proposed in Ref. [30]. In this scheme, Alice sends Bob a quantum signal together with a strong phase-reference pulse generated from the same laser. At Bob's side, he interferes the strong phase-reference pulse with a sampling beam from his LO laser to determine the phase difference between the two lasers, corrects this phase difference by introducing a phase shift to his LO laser, and then performs an interferometric measurement on the quantum signal using the phase-corrected LO pulse. However, the above scheme has not been demonstrated yet, possibly because of the following reasons: First, the phase difference between two remote independent lasers is expected to fluctuate rapidly; this makes real-time phase-feedback control very challenging. Second, different types of detectors are required for phase measurement and quantum signal detection; this increases the complexity

of the overall system. As we show below, the above two challenges can be overcome in a CV-QKD protocol.

Suppose in a CV-QKD system based on heterodyne detection, both the signal laser and the LO laser are operated in free-running mode. Without loss of generality, for each transmission, we can choose the phase of the signal laser as the phase reference ($\phi_S = 0$). When Bob performs conjugated homodyne detection, the phase $\phi$ of his LO laser can be treated as a random variable. Bob's measurement results $(X_B, P_B)$ are given by (after scaling with the channel transmittance)

$$\begin{aligned} X_B &= X_A \cos\phi + P_A \sin\phi + N_X, \\ P_B &= -X_A \sin\phi + P_A \cos\phi + N_P, \end{aligned} \tag{1}$$

where $N_X$ and $N_P$ are assumed to be independent and identically distributed (i.i.d.) Gaussian noises with zero mean.

If Alice and Bob can determine $\phi$ after Bob has performed his measurement, one of them (for example, Bob) can use this postmeasurement phase information to correct his data by performing the following rotation:

$$\begin{aligned} X'_B &= X_B \cos\phi - P_B \sin\phi, \\ P'_B &= X_B \sin\phi + P_B \cos\phi. \end{aligned} \tag{2}$$

From Eqs. (1) and (2), it is easy to show

$$\begin{aligned} X'_B &= X_A + N'_X, \\ P'_B &= P_A + N'_P, \end{aligned} \tag{3}$$

where the noise terms in the rotated data are given by

$$\begin{aligned} N'_X &= N_X \cos\phi - N_P \sin\phi, \\ N'_P &= N_X \sin\phi + N_P \cos\phi. \end{aligned} \tag{4}$$

Given $N_X$ and $N_P$ are i.i.d. Gaussian noises, it is easy to see that $N'_X$ and $N'_P$ are also independent Gaussian noises with the same variance as $N_X$ and $N_P$. This suggests that the rotation process will not introduce additional noise if the phase $\phi$ can be determined precisely.

The above "quadrature remapping" scheme allows Alice and Bob to establish correlated data without using a complicated phase-feedback-control system, thus removing the first challenge listed at the beginning of this section. Next, we present a scheme that allows Alice and Bob to determine $\phi$ under *realistic* scenarios using the *same* detector for quantum signal detection, thus removing the second challenge listed above.

### B. Pilot-aided phase recovery scheme

If the drift of phase $\phi$ is slow enough such that within a frame time of $\Delta T$ (within which the phase $\phi$ can be treated as a constant), many rounds of quantum transmission can be conducted, then the following scheme can be applied to estimate the phase $\phi$. After the quantum transmission stage, for each frame, Alice can randomly choose a subset of the transmitted signals as calibration pulses and announce the encoded data through an authenticated channel. Using the corresponding measurement results at hand, Bob can estimate phase $\phi$ for this frame using Eq. (1). Since Alice's signals are at quantum level, each individual calibration pulse cannot provide a precise estimation of the phase $\phi$. However, by averaging the results acquired from a large number of calibration pulses, the phase noise can be reduced effectively. This scheme was first proposed and implemented in Ref. [17] to reduce the noise associated with the slow phase drift of a fiber interferometer in GMCS QKD.

Unfortunately, the above scheme is not practical when the quantum signals and the LOs are generated from independent laser sources. On one hand, the phase difference between two practical lasers fluctuates rapidly because of the laser frequency instability and the phase noise associated with the finite laser linewidth; on the other hand, the maximum transmission rate of CV-QKD is limited by the bandwidth of the shot-noise-limited optical coherent detector. As such, we cannot acquire an accurate estimation of $\phi$ by measuring quantum signals.

To solve the above problem, we proposed a pilot-aided feedforward data recovery scheme [31]. The basic idea is as follows. For each quantum transmission, Alice sends out both a quantum signal and a relatively strong phase-reference pulse generated from the same laser. The quantum signal carries Alice's random numbers, as in the case of conventional CV-QKD. The reference pulse, on the other hand, is not modulated. These two pulses propagate through the same quantum channel to the measurement device, where Bob performs conjugate homodyne detection on both of them using LOs generated from the LO laser. Note, to avoid detector saturation, Bob can use a relatively weak LO to measure the reference pulse.

The measurement results from the phase-reference pulse $(X_R, P_R)$ can be used to determine $\phi$ using

$$\phi = -\tan^{-1}\frac{P_R}{X_R}, \tag{5}$$

where the minus sign is due to the definition of phase reference. By using a relatively strong reference pulse, Bob can acquire an accurate estimation of $\phi$ and use this phase information to implement the quadrature remapping scheme.

In this paper, we study a simple implementation of the above scheme, where Alice sends out quantum signals and reference pulses alternately and periodically, as shown in Fig. 1. We remark that if the drift of phase $\phi$ is slow enough

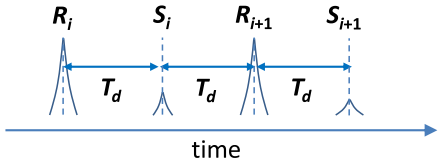


FIG. 1. Distribution of quantum signals ($S$) and reference pulses ($R$).

compared with the transmission rate of QKD, it is possible to use fewer reference pulses to improve QKD efficiency.

In Fig. 1, a quantum signal $S_i$ and the corresponding reference pulse $R_i$ are measured at different times with a time delay of $T_d$. If the frequency difference of the two lasers $(f_1 - f_2)$ is a constant and can be precisely determined, we can estimate phase $\phi_{S,i}$ at the time when $S_i$ is measured from the phase measurement result of $R_i$ by simply adding a constant phase shift of $2\pi(f_1 - f_2)T_d$. In practice, however, both lasers present slow frequency drift over time. Here, we use a simple scheme to estimate $\phi_{S,i}$. Since the signal pulse $S_i$ is in the middle of two reference pulses $R_i$ and $R_{i+1}$, we can estimate $\phi_{S,i}$ from the phase measurement results on $R_i$ and $R_{i+1}$ as

$$\bar{\phi}_{S,i} = \frac{\phi_{R,i} + \phi_{R,i+1}}{2}. \tag{6}$$

Note the above equation can also be written as

$$\bar{\phi}_{S,i} = \phi_{R,i} + 2\pi\bar{f}_d T_d, \tag{7}$$

where $\bar{f}_d = (\phi_{R,i+1} - \phi_{R,i}/4\pi T_d)$ can be interpreted as the frequency difference of the two lasers within the short time interval between two adjacent reference pulses.

While similar to classical intradyne detection, a key difference in our scheme separates phase recovery of a quantum signal from that of a classical one. A phase reference cannot be recovered reliably from a quantum signal, while it can in the classical case, meaning that the reference pulses here must be used to estimate that phase of the LO and quantum signal during the time window in which the quantum signal arrives. This places additional stringent requirements on relative laser noise compared to the classical case.

### C. Security analysis

In this section, we show that the existing security proofs of conventional CV-QKD [32–34] (built upon the assumption that Eve can only access the quantum signals) can be applied in our scheme directly.

First, the phase-reference pulses are only used to provide (classical) phase information; they are not directly used in the coherent detection of the quantum signals. In fact, in our scheme, Eve can never access the LO itself. Note, a standard assumption in CV-QKD is that Eve can have full knowledge of the phase reference used in quantum state preparation or coherent detection, so the reference pulses will not give Eve any additional information. Eve can certainly interfere with the phase recovery process by manipulating the phase-reference pulses when they propagate through the quantum channel. This could result in an increased phase noise, and the secure key rate will be reduced. This is one type of denial-of-service attack, which can be applied to any QKD protocols. From Eve's point of view, whatever can be achieved by manipulating the reference pulses can also be achieved by manipulating the quantum signals directly. In brief, sending phase-reference pulses through the quantum channel will not cause any security problem.

Next, we show that the security of the CV-QKD protocol using the quadrature remapping scheme is equivalent to that of the conventional CV-QKD protocol. To illustrate the essential ideas, it is convenient to represent the phase recovery scheme by a separate classical communication channel that can be fully controlled by Eve. Figure 2(a) is a schematic diagram of Bob's system in our new QKD scheme. In this picture, Bob performs a heterodyne measurement on the incoming quantum signal and then rotates his measurement results using the phase $\phi$ estimated through the classical communication channel. In Ref. [35], the authors proved that a unitary phase rotation commutes with heterodyne detection. More specifically, Bob can either rotate the optical phase of the quantum signal first and then perform heterodyne detection, or he can perform heterodyne detection first and then rotate the classical measurement results in the postprocessing stage. So, the protocol shown in Fig. 2(a) is equivalent to the virtual QKD

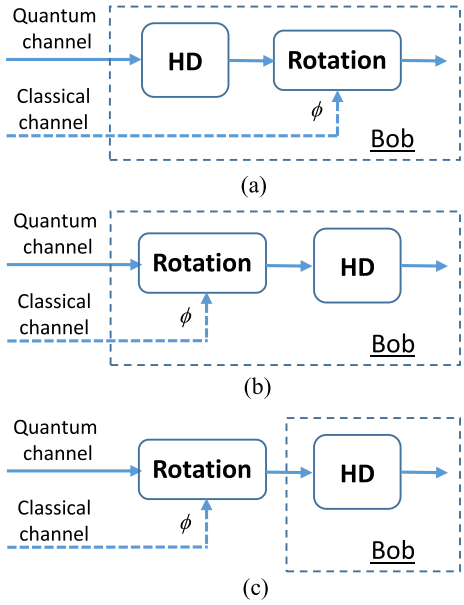


FIG. 2. Security models. HD–heterodyne detection. (a) CV-QKD protocol using quadrature remapping scheme. (b) A virtual QKD scheme equivalent to (a). (c) Conventional QKD scheme.

protocol shown in Fig. 2(b). Since the classical phase estimation channel can be controlled by Eve, we can move the phase rotation operator out of Bob's secure station and let Eve have full control of it, as shown in Fig. 2(c). Note the QKD protocol shown in Fig. 2(c) is exactly the conventional CV-QKD based on heterodyne detection, where Eve is allowed to manipulate the quantum signals transmitted through the channel at her will. So, the security of our new QKD scheme is equivalent to that of the conventional CV-QKD protocol.

While we do not need to develop a new security proof for the proposed QKD scheme, to achieve a high secure key rate, it is important to reduce the noise of the phase recovery process. From Eq. (2), the uncertainty of $\phi$ will be translated into an excess noise in $(X'_B, P'_B)$ (after scaling with the channel transmittance) as

$$\varepsilon_\phi = V_A \sigma_\phi, \tag{8}$$

where $V_A$ is Alice's modulation variance and $\sigma_\phi$ is the noise variance in determining phase $\phi$. This extra noise $\varepsilon_\phi$ will reduce the secure key generation rate. It is thus very important to minimize the phase noise $\sigma_\phi$.

In the next section, we study the performance of the proposed phase recovery scheme under a realistic scenario.

## III. PROOF-OF-PRINCIPLE DEMONSTRATION

### A. Noise model

There are two major noise sources in determining phase $\phi$ using Eq. (6). The first one is the measurement noise when Bob tries to determine $\phi_{R,i}$ ($\phi_{R,i+1}$) of the reference pulses $R_i$ ($R_{i+1}$). This noise could be significant when the reference pulses become extremely weak; thus, the contribution of shot noise cannot be ignored. However, in practice, we can use a relatively strong reference pulse to reduce the contribution of the shot noise. For example, if the average photon number of the reference pulse (at Bob's heterodyne detector) is 1000, given the detection efficiency of the heterodyne detector is 50%, the phase noise variance due to the shot noise is about 0.001, which is negligible in practice (see details in Appendix A). In this paper, we simply ignore this noise contribution.

The second noise source is the quantum phase noise of the laser, which originates from the amplified spontaneous emission. More specifically, even if we know the phase of the reference pulse, we still cannot determine the phase of the signal pulse precisely since they are generated at different times. The spontaneous emitted photons generated within the above time interval contribute a fundamental phase noise. Since the laser phase noise cannot be reduced by simply increasing the amplitude of the reference pulse, it is the main noise source in our scheme.

Define the laser phase at time $t = 0$ as $\theta_0$. The phase noise $\Delta\theta(t)$ quantifies the deviation of the laser phase at time $t$ from $\theta_0 + 2\pi f t$ (the phase expected from an ideal sine wave), where $f$ is the central frequency of the laser. $\Delta\theta(t)$ can be modeled as a Gaussian random variable with a mean of zero and a variance of [36]

$$\langle(\Delta\theta(t))^2\rangle = \frac{2t}{\tau_c}. \tag{9}$$

Here, $\tau_c$ is the coherence time of the laser. For a laser with Lorentzian line shape, $\tau_c$ is related to its linewidth $\Delta f$ by [36]

$$\tau_c \simeq \frac{1}{\pi \Delta f}. \tag{10}$$

As shown in Appendix A, given that the phase noise of the signal laser and that of the LO laser are $\langle(\Delta\theta_S(t))^2\rangle$ and $\langle(\Delta\theta_L(t))^2\rangle$, respectively, the noise variance of our phase estimation scheme [Eq. (6)] is described by

$$\sigma_\phi = \frac{1}{2}\{\langle(\Delta\theta_S(T_d))^2\rangle + \langle(\Delta\theta_L(T_d))^2\rangle\}, \tag{11}$$

where $T_d$ is the time delay between the signal pulse and the reference pulse (see Fig. 1).

### B. Experimental setup

We demonstrate the pilot-aided feedforward data recovery scheme using commercial off-the-shelf devices. The experimental setup is shown in Fig. 3. Two commercial frequency-stabilized continuous wave (cw) lasers at Telecom wavelength (Clarity-NLL-1542-HP from Wavelength Reference) are employed as the signal and the LO laser. Both lasers are operated at a free-running mode with no optical or electrical connections between them. The central frequency difference between the two lasers can stay within 10 MHz without doing any feedback controls. A LiNbO3 waveguide intensity modulator (EOSpace) is used to generate 8-ns laser pulses at a repetition rate of 50 MHz. Since half of the laser pulses are used as phase references, the equivalent data transmission rate in our experiment is 25 MHz. A LiNbO3 waveguide phase

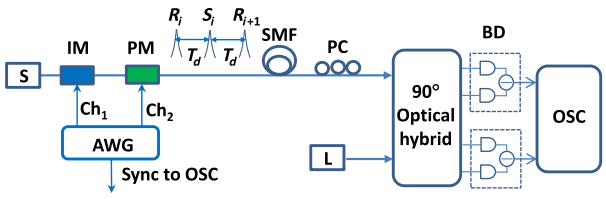


FIG. 3. Experimental setup. S is the signal laser, L is the LO laser, IM is the optical intensity modulator, PM is the optical phase modulator, AWG is the arbitrary waveform generator, SMF is the 25-km single -mode fiber spool, PC is the polarization controller, BD is the balanced photodetector, and OSC is the oscilloscope.

modulator (EOSpace) is used to modulate the phase of the signal pulses.

Both the signal pulses and the reference pulses propagate through a spool of 25-km single-mode fiber before arriving at the measurement device. A commercial 90° optical hybrid (Optoplex) and two 350-MHz balanced amplified photodetectors (Thorlabs) are employed to measure both $X$ quadrature and $P$ quadrature of the incoming pulses. The 90° optical hybrid is a passive device featuring a compact design. No temperature control is required to stabilize its internal interferometers. The outputs of the two balanced photodetectors are sampled by a broadband oscilloscope at a 1-GHz sampling rate. For simplicity, the LO laser is operated at the cw mode. A waveform generator with a bandwidth of 120 MHz provides the modulation signals to both the intensity and the phase modulator, as well as a synchronization signal to the oscilloscope.

### C. Experimental results

To evaluate the effectiveness of the phase recovery scheme, we conduct a phase-encoding coherent communication experiment using a binary pattern of "01010101…," where bit 0 is represented by no phase shift and bit 1 by a phase shift of 1.65 rad. The phase modulator shown in Fig. 3 is used to encode binary phase information on the signal pulses. The amplitude of the signal pulse is the same as that of the reference pulse. At the receiver's end, the average photon number per pulse is about $10^5$, which is significantly lower than that of the LO used in a typical GMCS QKD experiment. Note, in this experiment, to determine the noise of the phase recovery scheme, strong signal pulses are employed to provide "true" values of the phases to be estimated.

In total, 25000 signal pulses and 25000 reference pulses are transmitted. For each pulse received by Bob, its phase is calculated from the measured quadrature values $\{X, P\}$ using Eq. (5). The phase measurement results from the signal pulses $\{\phi_{S,i}^{(\mathrm{raw})}, i = 1, 2, \ldots, 25000\}$ are shown in Figs. 4(a) and 4(b). Because of the random phase change between the signal laser and the LO laser, the measured phases are randomly distributed within $[0, 2\pi)$, regardless of the encoded phase information.

From the phase measurement results of the reference pulses $\{\phi_{R,i}, i = 1, 2, \ldots, 25000\}$, we recover a phase reference $\bar{\phi}_{S,i}$ for each signal pulse using Eq. (6), and we correct the raw measurement results by

$$\phi_{S,i}^{(\mathrm{cor})} = \phi_{S,i}^{(\mathrm{raw})} + \bar{\phi}_{S,i}. \tag{12}$$

The corrected phase measurement results $\{\phi_{S,i}^{(\mathrm{cor})}, i = 1, 2, \ldots, 25000\}$ are shown in Figs. 4(c) and 4(d). After the phase correction, the measurement results for bit 0 and bit 1 are clearly separated.

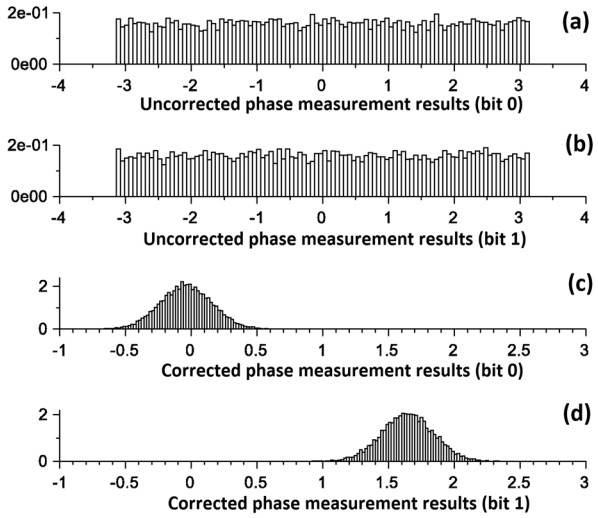


FIG. 4. Histograms of the phase measurement results. (a) The measurement results corresponding to bit 0 (before phase correction). (b) The measurement results corresponding to bit 1 (before phase correction). (c) The measurement results corresponding to bit 0 (after phase correction). (d) The measurement results corresponding to bit 1 (after phase correction).

The variances of the residual phase noise (the difference between $\phi_{S,i}^{(\mathrm{cor})}$ and the phase information encoded by Alice) have been determined to be $0.040 \pm 0.001$ (for bit 0) and $0.039 \pm 0.001$ (for bit 1), respectively.

Note in the above experiment, relatively strong reference pulses have been employed. While this will not introduce any security problem, in practice, it may be more convenient to use weak reference pulses. We conduct experiments to determine phase noise variance $\sigma_\phi$ using reference pulses with different average photon numbers (10000,1000,100). The measured phase noise variances are $(0.039 \pm 0.001, 0.040 \pm 0.001, 0.054 \pm 0.001)$. These results show that the phase recovery scheme works well even with reference pulses containing only a thousand photons.

As we have discussed in the previous section, the main noise source in our setup is laser phase noise associated with its finite linewidth. We conduct experiments to determine the phase noise of each laser. For $T_d = 20$ ns (which corresponds to the 50-MHz pulse repetition rate in the above experiments), the phase noise of the two lasers has been determined to be $0.035 \pm 0.001$ and $0.044 \pm 0.001$ (see details in Appendix A). From Eq. (11), the expected noise of the phase recovery scheme is $\sigma_\phi = 0.040 \pm 0.001$, which matches with the experimental results very well. To further reduce the noise $\sigma_\phi$, we can either use a smaller time delay $T_d$ (which is ultimately limited by the detector bandwidth) or choose lasers with a narrower linewidth.

As another demonstration of the phase recovery scheme, we conduct an experiment by using the phase reference recovered from the reference pulses to remap quadrature

values measured with weak quantum signals. In this experiment, no phase information is encoded on the signal pulses. The average photon number of each reference pulse at the receiver's end is about 1000, while that of each signal pulse is 66. Figure 5 shows the quadrature values $(X, P)$ of the signal pulses in phase space (sample size is 24000). The figure on the left shows the raw measurement results, where the phase is randomly distributed in $[0, 2\pi)$, as expected. The figure on the right shows the results after performing quadrature remapping. More specifically, we first recover a phase reference $\bar{\phi}_{S,i}$ for each signal pulse using Eq. (6) and then rotate the raw data using Eq. (2). The quadrature values have been scaled by taking into account the 3-dB loss due to heterodyne detection and the 50% overall efficiency of the detection system. The noise variance in the $X$ quadrature (right figure) has been determined to be 1.83 in shot-noise units. This result suggests the excess noise of the detector (including noise from the balanced photodetector and the oscilloscope) is about 0.83 in shot-noise units. Note, because of the residual phase noise of the phase recovery scheme, the distribution shown in the right figure is not symmetric: The variance of the $P$ quadrature $(\Delta_P)$ is larger than that of the $X$ quadrature $(\Delta_X)$. The phase noise $\sigma_\phi$ in the above experiment can be estimated by $\sigma_\phi = (\Delta_P - \Delta_X)/X_0^2$, where $X_0$ is the mean value of the $X$ quadrature. The experimental result is $(0.034 \pm 0.01)$, which is consistent with the noise variance estimated with strong signal pulses. This shows that the proposed phase recovery scheme works well in both the classical and the quantum domain. Note the uncertainty in this measurement is higher than that in previous experiments since we estimate a small quantity $(\sigma_\phi)$ from the difference of two relatively large quantities ($\Delta_P$ and $\Delta_X$).

Given the noise of the phase recovery scheme, we can use Eq. (8) to determine the additional excess noise contributed by this scheme and estimate the secure key rate using the existing security proof of GMCS QKD. In Appendix B, we present simulation results based on practical system parameters. Under the "realistic" model [11] where Eve cannot control the noise and loss of Bob's detector, the secure key could be generated over a distance of 120 km through telecom fiber in the asymptotic case, where the finite-data-size effect is ignored. To estimate the finite-data-size effect, we also conduct simulations using the most recent composable security proof of CV-QKD [34]. We remark that the above realistic model has been widely adopted in CV-QKD experiments [11,12,15,17].

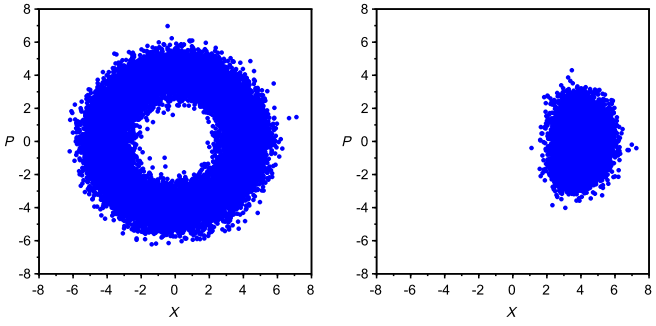


FIG. 5. The measured quadrature values in phase space. Left panel: before quadrature remapping; right panel: after quadrature remapping (no phase information is encoded in this experiment).

## IV. DISCUSSION

A long-outstanding problem in CV-QKD based on coherent detection is how to generate the LO "locally." In all the existing implementations of CV-QKD, both the quantum signal and the LO are generated from the same laser and propagate through the insecure quantum channel. This arrangement may open security loopholes and also limit the potential applications of CV-QKD.

In this paper, we solve the above problem by proposing and demonstrating a pilot-aided feedforward data recovery scheme that allows reliable coherent detection using a locally generated LO. This scheme also greatly simplifies the CV-QKD design by getting rid of the cumbersome unbalanced fiber interferometers and the associated phase stabilization system. Proof-of-principle experiments based on commercial off-the-shelf components show that the noise due to the proposed scheme is tolerable in CV-QKD. To further reduce the noise, laser sources with a smaller linewidth can be applied.

We remark that the measurement device employed in our experiment is essentially an intradyne detection scheme that has been applied in classical coherent communication for carrier phase recovery [37,38]. It is thus convenient to name our new scheme "intradyne" CV-QKD, while the conventional scheme is called "self-homodyne" CV-QKD [39]. However, there are several important differences between the classical and the quantum case. First, in classical communication, the signals are strong and the modulation scheme (such as BPSK and QPSK) is relatively simple. This allows carrier phase recovery from the signals directly. In GMCS QKD, the quantum signals are extremely weak (typically contain a few photons or less), and the modulation scheme is more complicated; the carrier phase cannot be recovered from the quantum signals reliably. As shown in Appendix A, the contribution of shot noise becomes significant when the photon number is below 100. Thus, it is necessary to employ relatively strong reference pulses. Second, the transmission rate of a classical communication system can reach 100 GHz, while the transmission rate of a state-of-the-art GMCS QKD system is below 100 MHz. This places a more stringent requirement on laser phase noise in the quantum system. Third, a classical digital communication system can tolerate higher phase noise than the CV-QKD. In brief, it is much more challenging to recover the carrier phase in quantum communication.

Although a complete CV-QKD experiment using the proposed scheme is not presented in this paper, all the components required to implement such a system, including broadband shot-noise-limited homodyne detectors [40–42], have been well developed. In fact, the structure of the proposed QKD system is much simpler compared to the conventional scheme [12].

We remark that a similar CV-QKD scheme has been independently proposed by Soh *et al.* [29]. In Ref. [29], Soh *et al.* study the expected secure key rate of their protocol under a passive channel, taking into account the effects of quantum noise on the reference pulse; they show in what limit the reference pulse scheme achieves the same performance as the standard scheme (where a LO is transmitted). They further conduct a proof-of-principle QKD experiment in the presence of strong phase noise between Alice's signal pulses and Bob's LO pulses generated from the same laser. Note in Ref. [29], the authors adopt a more conservative "paranoid" model [11], where the imperfections inside Bob's system can be controlled by Eve. Security analysis based on this model leads to more pessimistic predictions on the QKD performance, as in the case of conventional CV-QKD [11]. In our study, we establish the security of the proposed QKD protocol by showing that it is equivalent to the conventional GMCS QKD protocol; thus, the well-established security proof can be applied directly. Our proof-of-principle demonstration focuses on establishing a reliable phase reference between two independent lasers over a 25-km optical fiber link, a practical scenario that the proposed protocol is designed for. We expect that our scheme will be widely adopted in CV-QKD. This technology also opens the door for other quantum communication protocols, such as the MDI-CV-QKD protocol.

## ACKNOWLEDGMENTS

We would like to thank Hoi-Kwong Lo and Paul Jouguet for very helpful discussions. This work was performed at Oak Ridge National Laboratory, operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725. The authors acknowledge support from the Laboratory Directed Research and Development Program.

## APPENDIX A: NOISE IN PHASE RECOVERY SCHEME

In this Appendix, we first derive Eq. (11), which quantifies the contribution of laser phase noise to the noise variance of the phase recovery scheme. Then, we present details of experiments where the phase noise of each laser is measured. Finally, we consider the case when the shot noise associated with the reference pulses cannot be ignored.

For simplicity, we consider the case where the phases of two reference pulses measured at times $t_0$ and $t_2$ are used to estimate the phase difference of the signal laser and the LO laser at time $t_1$, as shown in Fig. 6.

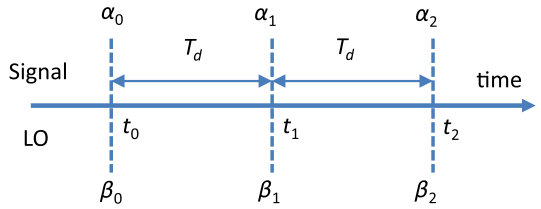


FIG. 6. Phase noise analysis.

Assume that the phases of the signal laser and the LO laser at time $\{t_0, t_1, t_2\}$ are $\{\alpha_0, \alpha_1, \alpha_2; \beta_0, \beta_1, \beta_2\}$, correspondingly. The phase differences of the two lasers at the above times are given by

$$\begin{aligned} \phi_0 &= \beta_0 - \alpha_0, \\ \phi_1 &= \beta_1 - \alpha_1, \\ \phi_2 &= \beta_2 - \alpha_2. \end{aligned} \tag{A1}$$

The phases of the signal laser at different times are related by

$$\begin{aligned} \alpha_1 &= \alpha_0 + 2\pi f_S T_d + N_{S,1}, \\ \alpha_2 &= \alpha_1 + 2\pi f_S T_d + N_{S,2}, \end{aligned} \tag{A2}$$

where $f_S$ is the central frequency of the signal laser. $N_{S,1}$ and $N_{S,2}$ are independent Gaussian noises with a mean of zero and a variance of $\langle(\Delta\theta_S(T_d))^2\rangle$.

Similarly, the phases of the LO laser are related by

$$\begin{aligned} \beta_1 &= \beta_0 + 2\pi f_L T_d + N_{L,1}, \\ \beta_2 &= \beta_1 + 2\pi f_L T_d + N_{L,2}, \end{aligned} \tag{A3}$$

where $f_L$ is the central frequency of the LO laser. $N_{L,1}$ and $N_{L,2}$ are independent Gaussian noises with a mean of zero and a variance of $\langle(\Delta\theta_L(T_d))^2\rangle$.

We assume that $\phi_0$ and $\phi_2$ can be determined precisely by using strong reference pulses. From Eq. (6) and using Eqs. (A1)–(A3), phase $\phi_1$ can be estimated by

$$\overline{\phi_1} = \frac{\phi_0 + \phi_2}{2} = \phi_1 + \frac{N_{S,1} + N_{L,2} - N_{S,2} - N_{L,1}}{2}. \tag{A4}$$

Since all the above noise terms in Eq. (A4) are independent from each other, it is easy to show that the noise variance of the phase recovery scheme is given by

$$\sigma_{\phi_1} = \langle(\overline{\phi_1} - \phi_1)^2\rangle = \frac{1}{2}\{\langle(\Delta\theta_S(T_d))^2\rangle + \langle(\Delta\theta_L(T_d))^2\rangle\}. \tag{A5}$$

This result is Eq. (11) in the main text.

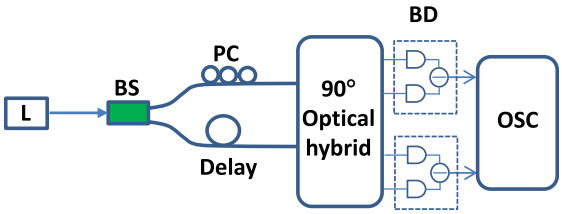


FIG. 7. Experimental setup for determining laser phase noise. L stands for laser, BS is for fiber beam splitter, PC is for polarization controller, BD is for balanced photodetector, and OSC is for oscilloscope.

We conduct experiments to determine the laser phase noise $\langle(\Delta\theta_S(T_d))^2\rangle$ and $\langle(\Delta\theta_L(T_d))^2\rangle$. The experimental setup is shown in Fig. 7. The cw output of a laser is split into two beams by a symmetric fiber splitter. After the two beams pass through two separate fiber links, the phase difference between the two beams is measured with a 90° optical hybrid, two balanced photodetectors, and an oscilloscope.

Given that the time delay difference between the two fiber links is $T_d$, we can determine the phase noise $\langle(\Delta\theta(T_d))^2\rangle$ of each laser directly. The phase noise of both the signal laser and the LO laser are measured at time delay $T_d = (5\text{ ns}, 20\text{ ns}, 25\text{ ns})$. The experimental results are shown in Fig. 8. As expected from Eq. (9), the observed laser phase noise linearly depends on $T_d$. At $T_d = 20$ ns, the phase noises of the two lasers have been determined to be $0.035 \pm 0.001$ and $0.044 \pm 0.001$.

Finally, we consider the case when the shot noise associated with the reference pulses cannot be ignored, so $\phi_0$ and $\phi_2$ in Eq. (A4) cannot be determined precisely. Assume that the average photon number of the reference pulse (at the receiver's end) is $n_{\text{ref}}$ and the overall detection efficiency is $\eta$. Then, the noise variance in $\phi_0$ and $\phi_2$ due to the shot noise is given by

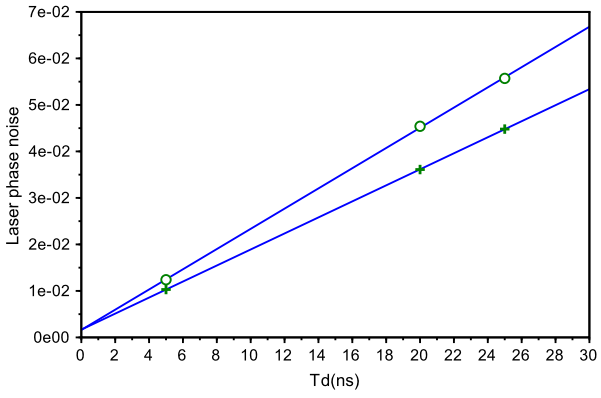


FIG. 8. Measured laser phase noise at different time delay $T_d$. The "open circle" shows the LO laser, and the "plus" is the signal laser.

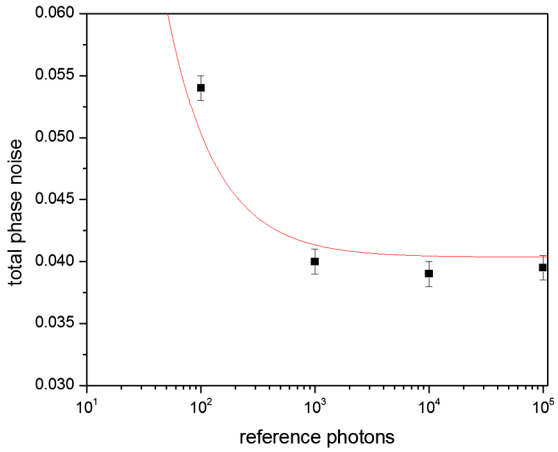


FIG. 9. Dependence of the phase noise variance on the average photon number of the reference pulse. The solid line shows simulation results using Eq. (A7). The square dots are experimental results.

$$\sigma_{\phi_0} = \sigma_{\phi_2} = \frac{2N_0}{\eta n_{\text{ref}}}, \tag{A6}$$

where $N_0 = 1/4$ denotes the shot-noise variance and the factor 2 is due to heterodyne detection.

Using Eqs. (A4) and (A5), the overall noise variance of the phase recovery scheme is given by

$$\sigma_{\phi_1} = \frac{1}{2}\{\langle(\Delta\theta_S(T_d))^2\rangle + \langle(\Delta\theta_L(T_d))^2\rangle\} + \frac{2N_0}{\eta n_{\text{ref}}}. \tag{A7}$$

The dependence of the phase noise variance on the average photon number of the reference pulse is plotted in Fig. 9. When the photon number is above 1000, the overall noise is dominated by the laser phase noise; when the photon number is below 100, the shot noise plays a significant role.

## APPENDIX B: SIMULATION OF SECURE KEY RATE

The security of one-way GMCS QKD has been well established. Here, our simulations are based on secure key rate formulas given in Ref. [43].

The secure key rate under the optimal collective attack, in the case of reverse reconciliation, is given by

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

where $I_{AB}$ is the Shannon mutual information shared between Alice and Bob, $f$ is the efficiency of the reconciliation algorithm, and $\chi_{BE}$ is the Holevo bound of the information between Eve and Bob.

The mutual information between Alice and Bob is given by

$$I_{AB} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \tag{B2}$$

The Holevo bound of the information between Eve and Bob is given by

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{B3}$$

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

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{B4}$$

where

$$A = V^2(1-2T) + 2T + T^2(V + \chi_{\text{line}})^2, \tag{B5}$$

$$B = T^2(V\chi_{\text{line}} + 1)^2, \tag{B6}$$

$$\lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \tag{B7}$$

where

$$C = \frac{1}{(T(V + \chi_{\text{tot}}))^2}[A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \times (V\sqrt{B} + T(V + \chi_{\text{line}})) + 2T(V^2 - 1)], \tag{B8}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{B9}$$

$$\lambda_5 = 1. \tag{B10}$$

System parameters in the above equations are defined as follows.

(1) $V = V_A + 1$, where $V_A$ is Alice's modulation variance.

(2) The total noise referred to the channel input $\chi_{\text{tot}} = \chi_{\text{line}} + (\chi_{\text{het}}/T)$, where $T$ is the channel transmittance. If we assume the quantum channel between Alice and Bob is optical fiber with an attenuation coefficient of $\alpha$, then the channel transmittance is given by $T = 10^{-\alpha L/10}$, where $L$ is the fiber length.

(3) The total channel-added noise referred to the channel input $\chi_{\text{line}} = (1/T) - 1 + \varepsilon$, where $\varepsilon$ is the excess noise outside of Bob's system. We assume that $\varepsilon$ is mainly due to the imperfection of the LO phase recovery scheme

$$\varepsilon = V_A\sigma_\phi, \tag{B11}$$

where $\sigma_\phi$ is the noise variance associated with the LO phase recovery scheme.

(4) The detection-added noise referred to Bob's input $\chi_{\text{het}} = [1 + (1-\eta) + 2\nu_{el}]/\eta$, where $\nu_{el}$ and $\eta$ are detector noise and detector efficiency, respectively.

We conduct numerical simulation using realistic parameters as summarized below: $\alpha = 0.2$ dB/km, $\nu_{el} = 0.1$, $\sigma_\phi = 0.04$, $\eta = 0.5$, $f = 0.95$, and $V_A = 1$. Figure 10 shows the simulation result in the asymptotic case. The simulation result shows that the proposed LO phase recovery scheme can be applied to achieve efficient QKD.

Note that the secure key rates depicted in Fig. 10 are obtained under the assumption of an infinite number of pulses sent from Alice to Bob. However, experimentally one is always limited to a finite-size data sample. To estimate the effect of finite data on the secure key rate, we also conduct simulation using the most recent composable security proof [34]. It can be shown [see Eq. (C13) in supplemental materials of Ref. [34]] that the secure key rate under the optimal collective attack is

$$R = (1 - \epsilon_{\text{rob}})\left(\beta I_{AB} - f(\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}) - \frac{1}{2n}\left[\Delta_{\text{AEP}} - \Delta_{\text{ent}} - 2\log_2\frac{1}{2\bar{\epsilon}}\right]\right), \tag{B12}$$

where $I_{AB}$ is the Shannon mutual information shared between Alice and Bob given in Eq. (B2), $\beta$ is the efficiency of the reconciliation algorithm, $f$ is the upper bound of the Holevo information $\chi_{BE}$ between Eve and Bob calculated in the supplemental materials of Ref. [34] [Eqs. (B2), (C9)–(C11)], $\epsilon_{\text{rob}}$ is the protocol robustness parameter, $\Delta_{\text{ent}} = \log_2(1/\epsilon) - \sqrt{8n\log_2^2(4n)\log_2(1/\epsilon)}$,

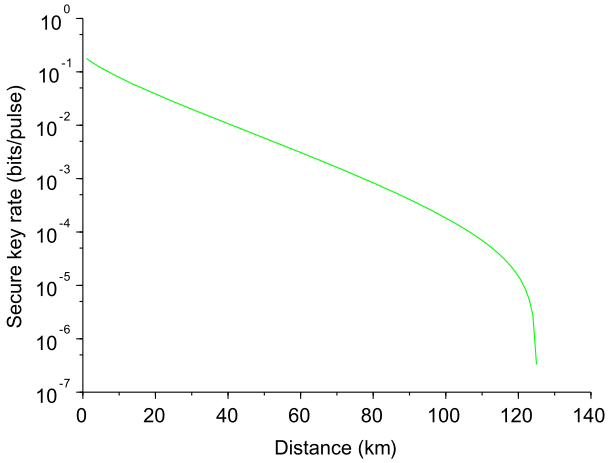


FIG. 10. Simulation results based on the security analysis given in Ref. [43]. Simulation parameters are as follows: $\alpha = 0.2$ dB/km, $\nu_{el} = 0.1$, $\sigma_\phi = 0.04$, $\eta = 0.5$, $f = 0.95$, and $V_A = 1$. We consider the asymptotic case where the finite data size effect is ignored.

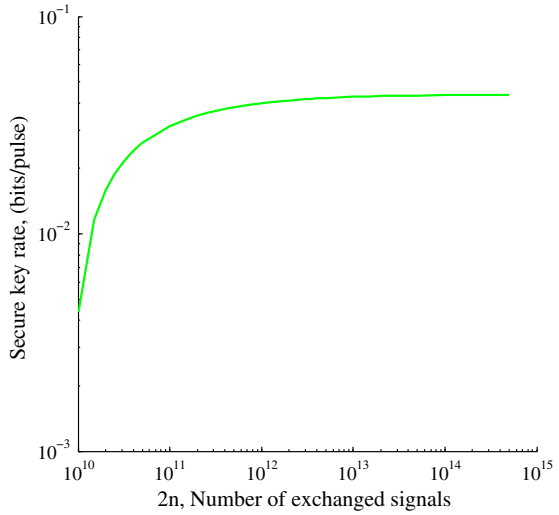


FIG. 11. Secure key rate simulation results for a finite number of pulses.

and $\Delta_{\text{ent}} = \sqrt{2n}[(d+1)^2 + 4(d+1)\log_2(2/\epsilon_{\text{sm}}^2) + 2\log_2(2/\epsilon^2\epsilon_{\text{sm}})] - 4\epsilon_{\text{sm}}d/\epsilon$. For our simulations, following Ref. [34], we choose protocol parameters such that the protocol is $\epsilon$ secure against collective attacks with $\epsilon = 10^{-20}$ and $\epsilon_{\text{cor}}$ correct with $\epsilon_{\text{cor}} \leq 10^{-2}$ by setting $\epsilon_{\text{sm}} = \bar{\epsilon} = 10^{-21}$, $\epsilon_{\text{PE}} = \epsilon_{\text{cor}} = \epsilon_{\text{ent}} = 10^{-41}$. We also assume that the discretization parameter $d = 5$; i.e., each measurement result is placed in one of five bins. Similarly to the asymptotic secure key rate simulations, we set the physical parameters as $\alpha = 0.2$ dB/km, $\sigma_\phi = 0.04$, and $V_A = 1$ and the reconciliation efficiency as $\beta = 0.95$. In Fig. 11, we plot the simulated secure key rate as a function of the number of pulses transmitted for a fixed fiber length $L = 10$ km assuming noiseless detectors ($\nu_{el} = 0$, $\eta = 0.5$). The simulation results indicate that a usable secure key can be generated by sending $\approx 10^{11}$ pulses, which is achievable with a CV-QKD system operated at a rate of tens of MHz.


[1] C. H. Bennett and G. Brassard, "*Quantum Cryptography: Public Key Distribution and Coin Tossing*," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

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

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

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The Security of Practical Quantum Key Distribution*, Rev. Mod. Phys. **81**, 1301 (2009).

[5] H.-K. Lo, M. Curty, and K. Tamaki, *Secure Quantum Key Distribution*, Nat. Photonics **8**, 595 (2014).

[6] D. Mayers, *Unconditional Security in Quantum Cryptography*, J. ACM **48**, 351 (2001).

[7] H.-K. Lo and H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, Science **283**, 2050 (1999).

[8] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85**, 441 (2000).

[9] T. C. Ralph, *Continuous Variable Quantum Cryptography*, Phys. Rev. A **61**, 010303(R) (1999).

[10] M. Hillery, *Quantum Cryptography with Squeezed States*, Phys. Rev. A **61**, 022309 (2000).

[11] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, *Quantum Key Distribution Using Gaussian-Modulated Coherent States*, Nature (London) **421**, 238 (2003).

[12] 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).

[13] 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).

[14] P. Jouguet, S. Kunz-Jacques, R. Kumar, H. Qin, R. Gabet, E. Diamanti, and R. Alléaume, *Experimental Demonstration of the Coexistence of Continuous-Variable Quantum Key Distribution with an Intense DWDM Classical Channel*, *Annual Conference on Quantum Cryptography (QCRYPT), Waterloo, Canada, 2013*.

[15] R. Kumar, H. Qin, and R. Alléaume, *Coexistence of Continuous Variable QKD with Intense DWDM Classical Channels*, New J. Phys. **17**, 043027 (2015).

[16] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G. Leuchs, *Atmospheric Continuous-Variable Quantum Communication*, New J. Phys. **16**, 113018 (2014).

[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] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, *Wavelength Attack on Practical Continuous-Variable Quantum-Key-Distribution System with a Heterodyne Protocol*, Phys. Rev. A **87**, 052309 (2013).

[19] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, *Quantum Hacking of a Continuous-Variable Quantum-Key-Distribution System Using a Wavelength Attack*, Phys. Rev. A **87**, 062329 (2013).

[20] 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).

[21] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Quantum Hacking on Quantum Key Distribution Using Homodyne Detection*, Phys. Rev. A **89**, 032304 (2014).

[22] E. Ip and J. M. Kahn, *Feedforward Carrier Recovery for Coherent Optical Communications*, IEEE J. Lightw. Technol. **25**, 2675 (2007).

[23] H.-C. Park, M. Lu, E. Bloch, T. Reed, Z. Griffith, L. Johansson, L. Coldren, and M. Rodwell, 40 Gbit/s *Coherent Optical Receiver Using a Costas Loop*, Opt. Express **20**, B197 (2012).

[24] M. J. Fice, A. Chiuchiarelli, E. Ciaramella, and A. J. Seeds, *Homodyne Coherent Optical Receiver Using an Optical Injection Phase-Lock Loop*, IEEE J. Lightw. Technol. **29**, 1152 (2011).

[25] 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 (2015).

[26] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, *Continuous-Variable Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **89**, 052301 (2014).

[27] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, *Gaussian-Modulated Coherent-State Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **89**, 042335 (2014).

[28] 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).

[29] 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*, following Article, Phys. Rev. X **5**, 041010 (2015).

[30] M. Koashi, *Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse*, Phys. Rev. Lett. **93**, 120501 (2004).

[31] B. Qi, *Pilot-Aided Feedforward Data Recovery in Optical Coherent Communications*, U.S. Patent Application No. 14/849,757 (10 September 2015).

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

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

[34] A. Leverrier, *Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States*, Phys. Rev. Lett. **114**, 070501 (2015).

[35] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, *Security of Continuous-Variable Quantum Key Distribution Against General Attacks*, Phys. Rev. Lett. **110**, 030502 (2013).

[36] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications*, 6th ed. (Oxford University Press, New York, 2007).

[37] F. Derr, *Coherent Optical QPSK Intradyne System: Concept and Digital Receiver Realization*, IEEE J. Lightw. Technol. **10**, 1290 (1992).

[38] R. Noé, *Phase Noise-Tolerant Synchronous QPSK/BPSK Baseband-Type Intradyne Receiver Concept with Feedforward Carrier Recovery*, IEEE J. Lightw. Technol. **23**, 802 (2005).

[39] We thank an anonymous reviewer for suggesting the use of the terms "intradyne" CV-QKD and "self-homodyne" CV-QKD to distinguish our new scheme from the conventional GMCS QKD scheme.

[40] R. Okubo, M. Hirano, Y. Zhang, and T. Hirano, *Pulse-Resolved Measurement of Quadrature Phase Amplitudes of Squeezed Pulse Trains at a Repetition Rate of 76 MHz*, Opt. Lett. **33**, 1458 (2008).

[41] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, *A Balanced Homodyne Detector for High-Rate Gaussian-Modulated Coherent-State Quantum Key Distribution*, New J. Phys. **13**, 013003 (2011).

[42] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. H. Huntington, and A. I. Lvovsky, *Versatile Wideband Balanced Detector for Quantum Optical Homodyne Tomography*, Opt. Commun. **285**, 5259 (2012).

[43] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and Ph. Grangier, *Improvement of Continuous-Variable Quantum Key Distribution Systems by Using Optical Preamplifiers*, J. Phys. B **42**, 114014 (2009).