Noise Analysis of Simultaneous Quantum Key Distribution and Classical Communication Scheme Using a True Local Oscillator

Bing Qi[1,2,*] and Charles Ci Wen Lim[1,3,4,†]

[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, National University of Singapore, 117583 Singapore, Singapore*
[4]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*

(Received 30 August 2017; revised manuscript received 19 December 2017; published 7 May 2018)

Recently, we proposed a simultaneous quantum and classical communication (SQCC) protocol where random numbers for quantum key distribution and bits for classical communication are encoded on the *same* weak coherent pulse and decoded by the same coherent receiver. Such a scheme could be appealing in practice since a single coherent communication system can be used for multiple purposes. However, previous studies show that the SQCC protocol can tolerate only very small phase noise. This makes it incompatible with the coherent communication scheme using a true local oscillator (LO), which presents a relatively high phase noise due to the fact that the signal and the LO are generated from two independent lasers. We improve the phase noise tolerance of the SQCC scheme using a true LO by adopting a refined noise model where phase noises originating from different sources are treated differently: on the one hand, phase noise associated with the coherent receiver may be regarded as *trusted* noise since the detector can be calibrated locally and the photon statistics of the detected signals can be determined from the measurement results; on the other hand, phase noise due to the instability of fiber interferometers may be regarded as *untrusted* noise since its randomness (from the adversary's point of view) is hard to justify. Simulation results show the tolerable phase noise in this refined noise model is significantly higher than that in the previous study, where all of the phase noises are assumed to be untrusted. We conduct an experiment to show that the required phase stability can be achieved in a coherent communication system using a true LO.

DOI: 10.1103/PhysRevApplied.9.054008

I. INTRODUCTION

Quantum key distribution (QKD) allows two remote parties, traditionally called Alice and Bob, to generate a secure key through an insecure quantum channel fully controlled by an adversary (Eve) [1–6]. The secure key can be further applied in other cryptographic protocols to enhance communication security.

One of the major roadblocks in the wide adoption of QKD is the high cost: dedicated communication infrastructures (such as dark fibers) and expensive devices (such as single-photon detectors) are commonly required in today's commercial QKD systems. It is thus imperative to come up with cost-effective QKD solutions. Recently, in light of the similarity between continuous-variable (CV) QKD based on coherent detection [7] and classical coherent communication, we proposed a simultaneous quantum and classical communication (SQCC) protocol where Gaussian distributed random numbers for QKD and bits for classical communication are encoded on the *same* weak coherent pulse and decoded by the same coherent receiver [8]. Since a single coherent communication system can be used for both classical communication and QKD, it can effectively reduce the cost of QKD itself.

However, previous studies show the SQCC protocol can tolerate only very small phase noise [8]. This is mainly due to the cross talk between the QKD signal and the classical communication signal: on the one hand, the random QKD signal appears as an additional noise source in the classical communication. To ensure the classical bit error rate (BER) is below a given threshold, a larger modulation amplitude of the classical signal would be required compared to

*qib1@ornl.gov
†elelimc@nus.edu.sg

the case of conducting classical communication alone. On the other hand, since the QKD signal is superimposed on the classical signal, the variance of excess noise due to phase fluctuation is proportional to the power of the classical signal. A larger modulation amplitude of the classical signal will result in a higher excess noise in QKD, hence resulting in a poorer performance. To achieve high-performance classical communication and QKD at the same time, the tolerable phase noise variance is less than 10^{-4} rad^2 in the previous study [8]. Experimentally, phase noise below 10^{-4} rad^2 has been demonstrated in CV-QKD experiments using a distributed local oscillator (LO), where the LO for coherent detection is generated from Alice's signal laser and distributed to Bob through an insecure quantum channel [9–13]. However, it could be difficult to achieve such a small phase noise in CV QKD using a *true* LO, where the LO is generated by Bob using an independent laser source. Note that CV QKD using a true LO is very appealing in practice due to its simple design and enhanced security [14–18].

Can we relax the requirement of very low phase noise in the SQCC protocol? In QKD, Alice and Bob can quantify the information gained by Eve from the observed noise and other system parameters: a higher noise level implies more information gained by Eve thus a lower secure key rate. One conservative approach to deal with noise in QKD is to assume that all of the observed noises are due to Eve's attack. This approach may overestimate Eve's information since practical QKD systems present *intrinsic* noises not necessarily controllable by Eve. An alternative approach is to assume that certain intrinsic noises well protected from Eve are *trusted* in the security proof. This approach can typically lead to a better QKD performance. For example, the trusted detector noise model has been widely adopted in long-distance CV-QKD experiments [7,9–12,19]. More recently, the trusted source noise model was also studied in CV QKD [20–24].

In this paper, we improve the phase noise tolerance of the SQCC scheme using a true LO by adopting a refined noise model where phase noises originating from different sources are treated differently: on the one hand, phase noise associated with the coherent receiver may be regarded as trusted noise since the detector can be calibrated locally and the photon statistics of the detected signals can be determined from the measurement results. This assumption is consistent with the commonly adopted assumption of trusted detector noise in practical CV QKD; on the other hand, phase noise due to the instability of fiber interferometers are regarded as *untrusted* noise since its randomness (from Eve's point of view) is hard to justify. We conduct numerical simulations of the SQCC protocol using a true LO based on the above noise model. Simulation results show the tolerable phase noise in this refined noise model is significantly higher than that in the previous study, where all of the phase noise is assumed to be untrusted. Based on a design proposed in Ref. [25], we conduct an experiment to show the required phase stability can be achieved in a coherent communication system using a true LO generated on Bob's end. Our findings suggest that the SQCC protocol could be a viable solution in practice.

This paper is organized as follows: In Sec. II, we present details of the SQCC protocol based on conjugate homodyne detection. In Sec. III, we develop the noise model of the SQCC using a true LO and present simulation results based on practical system parameters. In Sec. IV, we conduct an experiment to show that the required phase stability can be achieved in a coherent communication system using a true LO. Finally, we conclude this paper with a discussion in Sec. V.

II. PROTOCOLS

The QKD protocol adpoted in this paper is the Gaussian-modulated coherent states (GMCS) protocol [7] based on conjugate homodyne detection [26]. We further assume that the QKD protocol is implemented with a true LO generated by Bob, as proposed in Ref. [14]. Since conjugate homodyne detection allows Bob to measure both the X quadrature and the P quadrature simultaneously, we adopt the quadrature phase-shift keying (QPSK) modulation for classical communication. This setup is quantitatively different from Ref. [8], where binary phase-shift keying modulation is used for classical communication.

A. Classical QPSK scheme

In QPSK, Alice encodes two classical bits, m_A and n_A, into the X quadrature and the P quadrature of a coherent state, given by

$$|\psi\rangle = |(e^{-im_A\pi} + ie^{-in_A\pi})\alpha\rangle, \tag{1}$$

where α is assumed to be a real number. The average photon number μ of the coherent state $|\psi\rangle$ is given by $\mu = 2\alpha^2$.

Bob measures both the X quadrature and the P quadrature of the incoming signal and uses the signs of the measurement results to decode m_A and n_A; i.e., if the measured quadrature value is positive (negative), the corresponding classical bit is assigned as 0 (1).

B. The GMCS QKD based on conjugate homodyne detection

In GMCS QKD based on conjugate homodyne detection [26], Alice prepares a coherent state $|x_A + ip_A\rangle$, where x_A and p_A are Gaussian random numbers with zero mean and a variance of $V_A N_0$. Here, $N_0 = 1/4$ denotes the shot-noise variance. In this paper, all of the noise variances are defined in the shot-noise unit. On Bob's end, he performs conjugate homodyne detection to measure both the X and P quadratures simultaneously. After repeating the above quantum state transmission and detection process many times, Alice and Bob perform data postprocessing. Through an authenticated classical channel, Alice and Bob compare a subset of their data to

estimate the transmission efficiency and the noise variance for each quadrature. If the observed noise is below a certain threshold, Alice and Bob can further work out a secure key by performing reconciliation and privacy amplification. See Sec. III for additional details.

C. The SQCC protocol

In the SQCC protocol, Alice encodes her classical bits $\{m_A, n_A\}$ and Gaussian random numbers $\{x_A, p_A\}$ on a coherent state $|(x_A + e^{-im_A\pi}\alpha) + i(p_A + e^{-in_A\pi}\alpha)\rangle$ and transmits it to Bob, who performs conjugate homodyne detection to measure both the X and P quadratures simultaneously.

Bob determines the classical bits $\{m_B, n_B\}$ from the signs of his measurement results $\{x_R, p_R\}$: if $x_R(p_R) > 0$, then the bit value of $m_B(n_B)$ is assigned as 0. Otherwise, the bit value is assigned as 1. To decode Alice's random numbers for QKD, Bob processes his measurement results using on the overall transmittance $T\eta$ and the classical bits $\{m_B, n_B\}$ determined above:

$$x_B = \sqrt{\frac{2}{T\eta}}x_R + (2m_B - 1)\alpha,$$
$$p_B = \sqrt{\frac{2}{T\eta}}p_R + (2n_B - 1)\alpha, \tag{2}$$

where T is the channel transmittance, η is the detector efficiency, and the factor $\sqrt{2}$ is due to conjugate homodyne detection.

Alice and Bob can further perform data postprocessing and work out a secure key from raw keys $\{x_A, x_B\}$ and $\{p_A, p_B\}$, just as in the case of conventional GMCS QKD [7]. The phase-space representations of the above three protocols are shown in Fig. 1.

D. CV QKD using a true LO

In all of the protocols discussed above, a LO is needed in coherent detection. In most existing implementations of CV QKD, to reduce the phase noise, both the signal and the LO are generated by Alice from the same laser and sent through the insecure quantum channel [7,9–13,19]. This arrangement, however, may allow Eve to launch sophisticated attacks by manipulating the LO [27–31]. It also requires complicated multiplexing and demultiplexing schemes to effectively separate the strong LO from the weak quantum signal at the receiver's end. To solve the above problems, CV QKD using a true LO generated at Bob's side was developed [14,15]. The scheme presented in Ref. [14] works as follows: for each transmission, Alice sends out both a quantum signal and a phase reference pulse generated from the same laser. The quantum signal carries Alice's random numbers, while the phase reference pulse is not modulated. On Bob's end, he performs conjugate homodyne detection on both the quantum signal and the

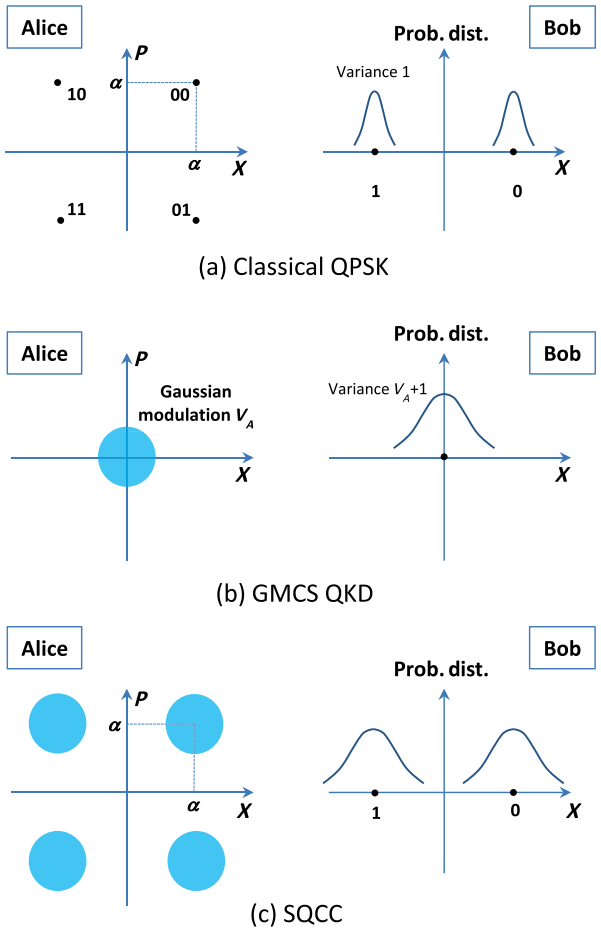

FIG. 1. Phase-space representations of various coherent communication schemes. (a) Classical QPSK scheme. (b) The GMCS QKD scheme. (c) The SQCC protocol. The figures on the right show the probability distributions of X-quadrature measurement.

phase reference pulse using two separate LOs generated from his own LO laser. The measurement results from the phase reference pulse are used to recover the phase relation ϕ between the two lasers. Using this phase information, Bob can classically correct his measurement results of the quantum signal in the postprocessing stage by performing the following rotation:

$$x'_R = x_R\cos\phi - p_R\sin\phi,$$
$$p'_R = x_R\sin\phi + p_R\cos\phi. \tag{3}$$

Various schemes have been proposed to implement CV QKD using a true LO. In Ref. [14], the QKD signal and the phase reference pulse were generated by using an amplitude modulator to modulate the output of a continuous-wave (cw) laser twice, as shown in Fig. 2(a). Two LO pulses are generated from Bob's laser in the same way. Given that Bob's detector noise is much smaller than the shot noise, the main phase noise of this scheme can be estimated by [14]

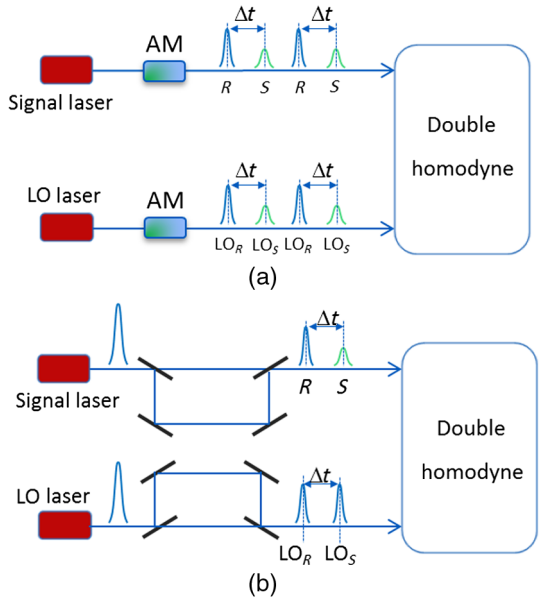

FIG. 2. Two different ways to generate phase reference pulses in CV QKD using a true LO. (a) The QKD signal (S) and the phase reference pulse (R) are generated from a continuous-wave laser by using an amplitude modulator (AM) [14]. (b) The QKD signal and the phase reference pulse are split from a common laser pulse using a path-unbalanced interferometer [25].

$$\sigma = \frac{\Delta t}{\tau_1} + \frac{\Delta t}{\tau_2} + \frac{2N_0}{\eta n_{\mathrm{ref}}}, \tag{4}$$

where Δt is the time delay between the signal pulse and the phase reference pulse, τ_1 (τ_2) is the coherent time of the signal (LO) laser, and n_{ref} is the average photon number of the phase reference pulse on Bob's side.

We define $\sigma_B = [(2N_0)/(\eta n_{\mathrm{ref}})]$. It represents the shot-noise contribution and, in principle, can be suppressed by using a strong phase reference pulse. The first two terms on the rhs of Eq. (4) are fundamental phase noises associated with the finite linewidth of the lasers, which can be reduced by decreasing the time delay Δt or using lasers with a longer coherent time (narrower linewidth).

In Ref. [25], Marie and Alléaume proposed a modified scheme where the signal pulse and the phase reference pulse are split from a common pulse using a path-unbalanced interferometer, as shown in Fig. 2(b). Since this scheme can effectively remove the phase noise contributed by the lasers, the residual phase noise is mainly determined by the last term on the rhs of Eq. (4) and the phase instability of the path-unbalanced interferometers. We adopt this modified scheme in this paper.

III. NOISE ANALYSIS

The performance of the SQCC protocol depends on the noises presented in the system. In this section, we first present the noise model adopted in this paper, followed by calculations of the BER in classical communication, the secure key rate in QKD, and simulation results based on realistic parameters.

A. Noise model

The main noise sources considered here are (1) phase noise in a coherent communication system using a true LO, (2) noise $\varepsilon_{\mathrm{le}}$ due to the leakage from the phase reference pulse to the signal, (3) detector noise denoted by υ_{el}, (4) signal-independent noise ε_0 from the channel and other unidentified or unprotected sources, and (5) vacuum noise. All of the noises are assumed to be Gaussian, and we use the same symbol to represent both the noise and its variance.

In this paper, we adopt the trusted detector noise model by assuming both the detector efficiency η and detector noise υ_{el} are well calibrated and out of Eve's control. By contrast, items (2) and (4) are untrusted noises and contribute to Eve's attack. Item (1) is more complicated and can be further separated into two terms: the phase noise σ_I due to the instability of the path-unbalanced interferometers [see Fig. 2(b)], and the phase noise σ_B given by the last term on the rhs of Eq. (4). As discussed in Ref. [25], previous experimental demonstrations of CV QKD using a distributed LO have shown that the phase noise σ_I associated with path-unbalanced interferometers can be very small. For example, phase noises on the order of 10^{-4}–10^{-5} rad^2 were demonstrated in Refs. [9,12]. By comparison, phase noise σ_B is typically much higher (10^{-3} rad^2, as we show in this paper).

One crucial assumption we make in this paper is that the phase noise σ_B is trusted. Since σ_B is determined by the detector and the photon number of the phase reference pulse received by Bob, to justify this assumption in practice, Bob may need to calibrate the detector and the phase reference pulse in the QKD process [32,33]. The detector calibration is also required in the trusted detector noise model and has been studied previously [30]. Here, we present a brief discussion on the calibration of the photon number of the phase reference pulse. As discussed in Sec. II D, to determine the phase relation between the LO laser and the signal laser, Bob performs conjugate homodyne detection to measure both the X quadrature and the P quadrature of the phase reference pulse. From his measurement results, Bob can also determine the photon statistics of phase reference pulses since, classically, the quantity $z = X^2 + Y^2$ is proportional to the intensity of the phase reference pulse [34]. So, the same measurement device for the LO phase recovery can also be used for phase reference pulse calibration. Given the finite photon number of the phase reference pulse, the corresponding phase noise essentially originates from vacuum noise, which is truly random to both the QKD users and Eve. We thus assume that σ_B is trusted noise.

Can we assume that the phase noise σ_I is also trusted? At first sight, since Eve cannot access the QKD system, it

seems reasonable to assume that σ_I cannot be manipulated by Eve. However, the unpredictability of this noise (from Eve's point of view) is hard to justify. If there are some internal patterns of the interferometer phase drift which are ignored by QKD users but known by Eve, she may compensate for this phase drift when the signal propagates through the channel and thus reduce the phase noise. In the meantime, she can attack the quantum signal to gain information, at the cost of introducing noise. If the total noise (including the reduced phased noise and the noise due to Eve's attack) equals the phase noise expected by the users (when Eve does not compensate for the phase drift in the channel), Eve's attack cannot be detected. For this reason, we assume that σ_I is untrusted.

The term $\varepsilon_{\mathrm{le}}$ quantifies the noise due to the leakage from the phase reference pulse to the signal. Since the effect of leakage is implementation specific, we conduct a detailed analysis in the Appendix based on the design to be presented in Sec. IV, where both time multiplexing and polarization multiplexing are employed to reduce the leakage. As shown in the Appendix, the excess noise contributed by the leakage referred to the input of the channel is given by

$$\varepsilon_{\mathrm{le}} = \frac{n_{\mathrm{ref}}\Delta t}{TN_0\tau_c} \times 10^{-(\xi_A/10)} \times 10^{-(\xi_P/10)}, \tag{5}$$

where Δt is the time delay between the signal pulse and the phase reference pulse, τ_c is the coherent time of Alice's laser, and ξ_A and ξ_P are the extinction ratios (in decibels) of the amplitude modulator and the polarization multiplexing scheme.

From Eq. (5), the excess noise $\varepsilon_{\mathrm{le}}$ can be effectively suppressed by improving the extinction ratio ξ_A or ξ_P. While amplitude modulators with a 65-dB extinction ratio have been demonstrated experimentally [35] and applied in a CV-QKD experiment [36], most standard commercial products can achieve an extinction ratio in the range of 20 to 50 dB. In the simulation below, we assume an extinction ratio of 30 dB for both amplitude modulation and polarization multiplexing.

B. Bit error rate in classical communication

In the SQCC protocol, the Gaussian modulation for QKD appears as a Gaussian noise for classical communication. Furthermore, the contribution of phase noises is proportional to the power of classical signal and can be described by $(\alpha^2/N_0)(\sigma_I + \sigma_B)$. The overall noise variance at the receiver's end is given by

$$N_{\mathrm{tot}} = \frac{1}{2}T\eta\left[V_A + \varepsilon_{\mathrm{le}} + \varepsilon_0 + \frac{\alpha^2}{N_0}(\sigma_I + \sigma_B)\right] + 1 + \upsilon_{\mathrm{el}}, \tag{6}$$

where the factor $\frac{1}{2}$ is due to conjugate homodyne detection since the received signal is split by Bob into two using a symmetric beam splitter.

We assume that the channel between Alice and Bob is telecom fiber with an attenuation coefficient of γ, which is assumed to be 0.2 dB/km. The channel transmittance is given by

$$T = 10^{(-\gamma L/10)}, \tag{7}$$

where L is the fiber length in kilometers.

Given that the signals transmitted by Alice are described by Eq. (1), the BER of the classical QPSK is given by

$$C_{\mathrm{BER}} = \frac{1}{2}\mathrm{erfc}\left(\frac{\sqrt{T\eta}\alpha}{\sqrt{4N_{\mathrm{tot}}N_0}}\right), \tag{8}$$

where $\mathrm{erfc}(\cdots)$ denotes the complementary error function.

To achieve a BER of C_{BER} in the classical communication, the required displacement α can be determined from Eqs. (6)–(8) as

$$\alpha = w\frac{\sqrt{T\eta(V_A + \varepsilon_{\mathrm{le}} + \varepsilon_0) + 2 + 2\upsilon_{\mathrm{el}}}}{\sqrt{T\eta(2 - 4w^2\sigma_I - 4w^2\sigma_B)}}, \tag{9}$$

where w is defined as

$$w = \mathrm{erf}^{-1}(1 - 2C_{\mathrm{BER}}). \tag{10}$$

Here $\mathrm{erf}^{-1}(\cdots)$ is the inverse error function.

We remark that to achieve a BER of 10^{-9} in classical communication, the maximum tolerable phase noise is $\sigma_I + \sigma_B = 0.0278$. This number is determined from Eq. (9) by requiring the denominator to be a real number.

C. Secure key rate in QKD

The asymptotic secure key rate of QKD, in the case of reverse reconciliation, is given by Refs. [9,37]:

$$R = fI_{AB} - \chi_{BE}, \tag{11}$$

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 between Eve and Bob.

As we have discussed above, we assume that the detector noise υ_{el} and the phase noise σ_B are trusted, while the phase noise σ_I, the excess noise due to leakage $\varepsilon_{\mathrm{le}}$, and the channel noise ε_0 are untrusted. Under this noise model, in the case of conjugate homodyne detection, the detector-added noise referred to Bob's input is given by

$$\chi_{\mathrm{het}} = (2 + 2\upsilon_{\mathrm{el}})/\eta - 1 + T\varepsilon_B, \tag{12}$$

where ε_B quantifies the excess noise due to the trusted phase noise referred to the channel input:

$$\varepsilon_B = \left(\frac{\alpha^2}{N_0} + V_A\right)\sigma_B. \tag{13}$$

The total channel-added noise (including all of the untrusted noise) referring to the channel input is given by

$$\chi_{\text{line}} = \frac{1}{T} - 1 + \varepsilon_{\text{le}} + \varepsilon_0 + \varepsilon_I + \frac{4\alpha^2}{N_0} C_{\text{BER}}, \tag{14}$$

where ε_I quantifies the excess noise due to untrusted phase noise and is given by $\varepsilon_I = [(\alpha^2/N_0) + V_A]\sigma_I$. The term $[(4\alpha^2)/N_0]C_{\text{BER}}$ quantifies the excess noise contributed by the BER in classical communication.

The overall noise referred to the channel input is given by

$$\chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}. \tag{15}$$

Since both quadratures are used for secure key generation, the mutual information between Alice and Bob is given by

$$I_{AB} = \log_2 \frac{V_A + 1 + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \tag{16}$$

The Holevo bound of the information between Eve and Bob is given by Ref. [9],

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{17}$$

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

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{18}$$

where

$$A = V^2(1-2T) + 2T + T^2(V + \chi_{\text{line}})^2, \tag{19}$$

$$B = T^2(V\chi_{\text{line}} + 1)^2, \tag{20}$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right], \tag{21}$$

where

$$C = \frac{1}{[T(V + \chi_{\text{tot}})]^2}\{A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \times [V\sqrt{B} + T(V + \chi_{\text{line}})] + 2T(V^2 - 1)\}, \tag{22}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{23}$$

$$\lambda_5 = 1. \tag{24}$$

D. Simulation results

We conduct numerical simulations of the secure key rate of QKD under the constraint of 10^{-9} BER in the classical communication. Other simulation parameters are $\gamma = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $v_{\text{el}} = 0.1$, $\eta = 0.5$, $f = 0.95$, $\Delta t = 50$ ns, $\tau_c = 1\,\mu$s, $\xi_A = \xi_P = 30$ dB, and $n_{\text{ref}} = 1000$. At each distance, the channel transmittance T can be determined using Eq. (7). From Eqs. (9) and (10), given T and that $C_{\text{BER}} = 10^{-9}$, the displacement α is determined by V_A and other system parameters. So the only free parameter needs to be optimized is the modulation variance V_A. We numerically optimize V_A at each distance to achieve the maximum secure key rate. Secure key rates are calculated at four different phase noise combinations: (1) $\sigma_I = 10^{-5}$, $\sigma_B = 10^{-3}$; (2) $\sigma_I = 10^{-5}$, $\sigma_B = 10^{-2}$; (3) $\sigma_I = 10^{-4}$, $\sigma_B = 10^{-3}$; and (4) $\sigma_I = 10^{-4}$, $\sigma_B = 10^{-2}$. Figure 3 shows the simulation results. As a comparison, we also calculate the secure key rate under the assumption that the phase noise σ_B is untrusted. Using the same system parameters, no secure key can be generated at any distance.

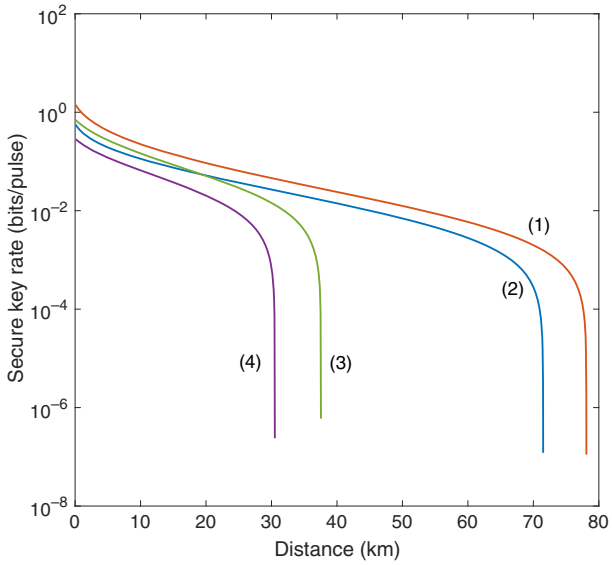

FIG. 3. Simulation results of secure key rate under the constraint of 10^{-9} BER in the classical communication. The simulation parameters are $\gamma = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $v_{\text{el}} = 0.1$, $\eta = 0.5$, $f = 0.95$, $\Delta t = 50$ ns, $\tau_c = 1\,\mu$s, $\xi_A = \xi_P = 30$ dB, and $n_{\text{ref}} = 1000$. The modulation variance V_A is numerically optimized at each fiber length. The four curves presented correspond to the following phase noise combinations: (1) $\sigma_I = 10^{-5}$, $\sigma_B = 10^{-3}$; (2) $\sigma_I = 10^{-5}$, $\sigma_B = 10^{-2}$; (3) $\sigma_I = 10^{-4}$, $\sigma_B = 10^{-3}$; and (4) $\sigma_I = 10^{-4}$, $\sigma_B = 10^{-2}$. As a comparison, using the above system parameters, no secure key can be generated at any distance if the phase noise σ_B is untrusted.

IV. PHASE NOISE MEASUREMENT

We conduct an experiment to determine the phase noise in a coherent communication system using a true LO based on the phase recovery scheme proposed in Ref. [25]. A similar experiment was also conducted recently by Wang *et al.* [38].

The experimental setup is shown in Fig. 4. Two commercial frequency-stabilized cw lasers at telecom wavelength (Clarity-NLL-1542-HP from Wavelength Reference) are employed as the signal laser and the LO laser. Both lasers are operated at free-running mode with no optical or electrical connections between them. Two $LiNbO_3$ waveguide amplitude modulators (EOSPACE) are used to generate 10-ns laser pulses at a repetition rate of 10 MHz. At Alice's side, a polarization-maintaining fiber interferometer with a time-delay unbalance of 46.9 ns is employed to generate a phase-related pulse pair (signal and phase reference) from each incoming pulse. A specially designed bias-free amplitude and phase modulator (APM in Fig. 4) is placed inside the interferometer to control the amplitude and phase of the signal pulse. Details of the APM's design are presented in Fig. 5. Note that the signal pulse and the phase reference pulse are coupled into orthogonal polarization modes by using a polarization beam combiner (PBC_1 in Fig. 4). Such a design can improve the isolation between the two pulses. Both the signal pulse and the phase reference pulse propagate through a spool of 25-km single-mode fiber. At Bob's end, a commercial 90° optical hybrid (Optoplex) and two 350-MHz balanced amplified photodetectors (Thorlabs) are employed to measure both the X quadrature and the P quadrature of the two pulses from Alice. The two LOs used in the coherent detection are split from a common pulse generated by the LO laser. A tunable optical delay line (TDL in Fig. 4) is placed inside Bob's interferometer to match its time-delay difference to that of Alice's interferometer. By adjusting two polarization controllers (PC_2 and PC_3 in Fig. 4), the intensity of each LO pulse can be adjusted individually. Similar to the signal pulse and the reference pulse from Alice, the two LO pulses are also coupled into orthogonal polarization modes by a polarization beam combiner (PBC_2 in Fig. 4). Another polarization controller (PC_1 in Fig. 4) is used to match the polarization of Alice's pulse to that of the corresponding LO. Finally, the outputs of the two balanced photodetectors are sampled by a 12-bit data acquisition board (Texas Instruments).

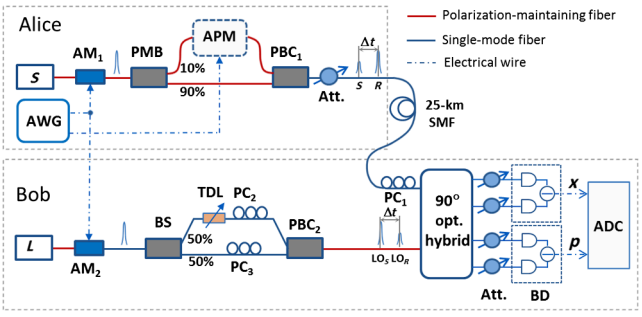

FIG. 4. Experimental setup. S, signal laser; L, LO laser; $AM_{1,2}$, amplitude modulator; APM, amplitude and phase modulator (see the details in Fig. 5); PMB, 90:10 polarization-maintaining fiber beam splitter; BS, 50:50 single-mode-fiber (SMF) beam splitter; TDL, tunable optical delay line; $PBC_{1,2}$, polarization beam combiner; PC_{1-3}, polarization controller; Att., tunable optical attenuator; AWG, arbitrary waveform generator; BD, balanced photodetector; ADC, analog-to-digital converter.

In high-speed QKD, $LiNbO_3$ waveguide modulators are commonly employed to implement amplitude and/or phase modulation. The bias voltage control is vital for an amplitude modulator since its bias point commonly drifts with time. Here, we achieve bias-free amplitude and phase modulation by placing a phase modulator asymmetrically inside a loop interferometer, as shown in Fig. 5. See a similar scheme in Ref. [39]. The basic idea is to introduce different phase shifts on lights traveling through the loop clockwise (CW pulse) or counterclockwise (CCW pulse). Note that, depending on the input optical signal (cw or pulsed) and the waveform of the electrical control signal on the phase modulator, this device can act as either an optical pulse generator or an amplitude and phase modulator. When the input is cw light, each control pulse on the phase modulator will generate a pair of output light pulses with a time delay given by $\Delta t = n(L_2 - L_1)/c$,

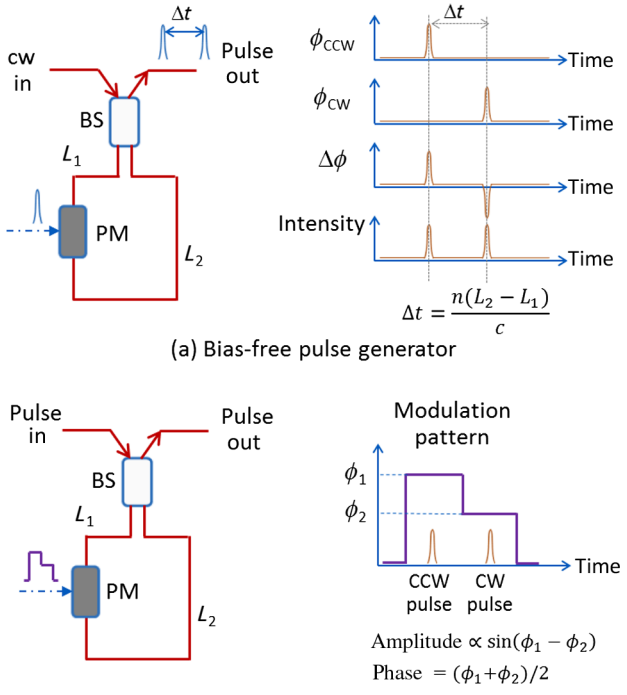

FIG. 5. Bias-free amplitude and phase modulator. BS, 50:50 polarization-maintaining fiber beam splitter; PM, phase modulator; CW, clockwise; CCW, counterclockwise. (a) When the input is cw light, the setup can act as a pulse generator. (b) When the input is pulsed light, the setup can act as an amplitude and phase modulator.

where $(L_2 - L_1)/2$ is the offset of the phase modulator from the middle point of the loop interferometer (which is about 1.8 m in our experiment), n is the refractive index of the optical fiber, and c is the speed of light in vacuum [see the details in Fig. 5(a)]. The temporal width of the output optical pulse is determined by the width of the control signal. When the input is pulsed light, bias-free amplitude and phase modulation can be achieved by controlling the waveform of the control signal to the phase modulator, as shown in Fig. 5(b). This design can be useful in other applications beyond QKD. In this experiment, we simply use it to adjust the photon number of the signal.

In CV QKD using a true LO [14], the measurement results of the phase reference pulse $(X_{\mathrm{ref}}, P_{\mathrm{ref}})$ are used to determine the phase difference between the signal laser and the LO laser using the relation

$$\phi = -\tan^{-1}\frac{P_{\mathrm{ref}}}{X_{\mathrm{ref}}}. \tag{25}$$

Once ϕ has been determined, Bob can correct his measurement results of the signal pulse by using Eq. (3). Here, we want to determine the phase noise of the above process. More specifically, we want to quantify the difference between the ϕ estimated by Bob and the true value of the phase difference ϕ_{tru} between the two lasers when the signal is measured. To acquire a precise estimation of ϕ_{tru}, we replace Alice's signals for the SQCC protocol QKD by strong (unmodulated) calibration pulses. In fact, to minimize the measurement noise associated with the calibration pulse, their intensity is even stronger than that of the phase reference pulse. In this experiment, we define the weak pulse going through the path with an amplitude and phase modulator (see Fig. 4) as the phase reference pulse, and the strong pulse going through the other path as the calibration pulse. We remark that no information is encoded in this experiment.

From the measurement results of the calibration pulse (X_c, P_c), we calculate

$$\phi_{\mathrm{tru}} = -\tan^{-1}\frac{P_c}{X_c}. \tag{26}$$

The phase error is defined as $\phi - \phi_{\mathrm{tru}}$. Experimentally, the variance of $\phi - \phi_{\mathrm{tru}}$ is determined to be $2.4 \pm 0.4 \times 10^{-3}$ rad^2 (when the average photon number of the phase reference pulse is 10^3), and $0.79 \pm 0.25 \times 10^{-3}$ rad^2 (when the average photon number of the phase reference pulse is 10^4). From Fig. 3, this phase noise is low enough to implement the SQCC protocol over practical distances.

V. DISCUSSION

CV QKD based on optical coherent detection is appealing in practice since it can be implemented with standard telecommunication technology [40]. The research in CV QKD is also aligned with the resurgence of classical optical coherent communication, which is the most promising solution to the dramatic growth of global communication traffic [41]. Studies in this paper show that it is feasible to use the same coherent communication system to conduct QKD and classical communication simultaneously, as long as the distance is within the reach of QKD.

To improve phase noise tolerance of the SQCC protocol and make it compatible with the CV-QKD scheme using a true LO, in this paper we adopt a refined noise model where phase noise due to the finite photon number of the phase reference pulse and the detector imperfection is assumed to be trusted. Systematic noise analysis is conducted. Simulation results show that the tolerable phase noise in this refined noise model is significantly higher than that in previous studies [8]. Experimentally, using a design proposed in Ref. [25], we demonstrate that the required phase stability can be achieved in practice.

While the results presented in this paper are encouraging, further research is needed to bring this technology into real life. As we show in this paper, a trusted noise model could significantly improve the QKD performance. However, it could also introduce potential security loopholes if Eve has a way to manipulate the phase noise, or if the QKD users overestimate the amount of trusted phase noise. It is thus important to implement local calibration systems at both Alice and Bob to monitor the relevant noise in real time.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their important comments on the trusted noise model and the noise associated with the leakage of the phase reference pulses. This work was performed at Oak Ridge National Laboratory (ORNL), operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725. The authors acknowledge support from the ORNL Laboratory Directed Research and Development Program. C. C. W. L. acknowledges support from National University of Singapore start-up Grant No. R-263-000-C781-133/731 and CQT Fellowship Grant No. R-710-000-027-135.

APPENDIX: LEAKAGE FROM PHASE REFERENCE PULSE

In this appendix, we study the leakage from the phase reference pulse to the signal based on the specific design presented in Sec. IV.

As shown in Fig. 4, Alice generates laser pulses from a cw laser source by using an optical amplitude modulator. Each laser pulse is further split into two (the phase reference pulse and the signal pulse) by using a path-unbalanced interferometer. The signal and the reference are coupled to orthogonal polarization modes to improve the isolation between them.

In practice, only a finite extinction ratio can be achieved in both amplitude modulation and polarization multiplexing. So there will be unavoidable leakage from the phase reference pulse to the signal pulse, as highlighted in Fig. 6.

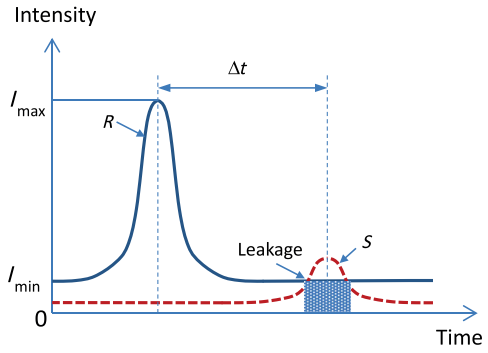

FIG. 6. Leakage from the phase reference pulse to the signal pulse due to the finite extinction ratio. R, phase reference pulse; S, signal pulse; Δt, time delay introduced by the path-unbalanced interferometer.

Given that the average photon number of the phase reference pulse on Bob's end is n_{ref}, the average photon number of the leakage on Alice's end is determined by

$$n_{\mathrm{le}} = \frac{n_{\mathrm{ref}}}{T} \times 10^{-(\xi_A/10)} \times 10^{-(\xi_P/10)}, \tag{A1}$$

where ξ_A and ξ_P are the extinction ratios (in decibels) of the amplitude modulator and the polarization multiplexing scheme, correspondingly.

If the leakage photon has a fixed phase relation with the phase reference pulse, then it introduces only a constant displacement in phase space, which can be determined from Bob's measurement results and removed in the postprocessing stage [10]. When taking into account the phase noise of the QKD system and the finite coherent time of the signal laser, the excess noise contributed by the leakage can be described by

$$\varepsilon_{\mathrm{le}} = \frac{n_{\mathrm{le}}}{2N_0}\sigma_{\mathrm{le}}, \tag{A2}$$

where σ_{le} quantifies the phase noise of the leakage.

In our setup, σ_{le} is determined mainly by the coherent time τ_c of the laser. Note that the phase reference pulse and the leakage are emitted at different times (with a time delay of Δt) by Alice's laser. The spontaneous emitted photons generated within the above time interval contribute a fundamental phase noise with a variance of $2\Delta t/\tau_c$. As shown in Ref. [14], the coherent time of our laser is about 1 μs. If Δt is about 50 ns (see Fig. 6), then the phase noise of the leakage contributed by the laser is about 0.1 rad^2, which is much larger than other phase noise in the QKD system.

Using $\sigma_{\mathrm{le}} = 2\Delta t/\tau_c$ and Eq. (A1), Eq. (A2) can be revised as

$$\varepsilon_{\mathrm{le}} = \frac{n_{\mathrm{ref}}\Delta t}{TN_0\tau_c} \times 10^{-(\xi_A/10)} \times 10^{-(\xi_P/10)}. \tag{A3}$$

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

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

[7] 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).

[8] B. Qi, Simultaneous classical communication and quantum key distribution using continuous variables, Phys. Rev. A **94**, 042340 (2016).

[9] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and Ph. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[10] 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).

[11] 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).

[12] 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).

[13] Y.-C. Zhang, Z. Li, Z. Chen *et al.*, Continuous-variable quantum key distribution over 50 km commercial fiber, arXiv:1709.04618.

[14] 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).

[15] 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).

[16] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, High-speed continuous-variable quantum key distribution without sending a local oscillator, Opt. Lett. **40**, 3695 (2015).

[17] S. Kleis, M. Rueckmann, and C. G. Schaeffer, Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals, Opt. Lett. **42**, 1588 (2017).

[18] R. Corvaja, Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection, Phys. Rev. A **95**, 022315 (2017).

[19] R. Kumar, H. Qin, and R. Alléaume, Coexistence of continuous variable QKD with intense DWDM classical channels, New J. Phys. **17**, 043027 (2015).

[20] V. C. Usenko and R. Filip, Feasibility of continuous-variable quantum key distribution with noisy coherent states, Phys. Rev. A **81**, 022318 (2010).

[21] Y. Shen, X. Peng, J. Yang, and H. Guo, Continuous-variable quantum key distribution with Gaussian source noise, Phys. Rev. A **83**, 052304 (2011).

[22] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Analysis of imperfections in practical continuous-variable quantum key distribution, Phys. Rev. A **86**, 032309 (2012).

[23] J. Yang, B. Xu, and H. Guo, Source monitoring for continuous-variable quantum key distribution, Phys. Rev. A **86**, 042314 (2012).

[24] V. C. Usenko and R. Filip, Trusted noise in continuous-variable quantum key distribution: A threat and a defense, Entropy **18**, 20 (2016).

[25] A. Marie and R. Alléaume, Self-coherent phase reference sharing for continuous-variable quantum key distribution, Phys. Rev. A **95**, 012316 (2017).

[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] H. Häseler, T. Moroder, and N. Lütkenhaus, Testing quantum devices: Practical entanglement verification in bipartite optical systems, Phys. Rev. A **77**, 032303 (2008).

[28] 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).

[29] 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).

[30] 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).

[31] 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).

[32] In Ref. [33], the authors discuss an interesting attack in CV QKD using a true LO where Eve intentionally increases the photon number of the phase reference pulse received by Bob. She can achieve this goal by conveying the phase reference pulse from Alice to Bob using a lossless channel. If Alice and Bob blindly apply the trusted phase noise model without monitoring the photon number of the phase reference pulse at Bob, they may overestimate the amount of trusted phase noise and leave room for Eve to hide her attack on the quantum signal. Of course, this attack does not work if Alice and Bob assume that all of the phase noises are untrusted, as in Refs. [14,15].

[33] S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, Reference-pulse attack on continuous-variable quantum key distribution with local local oscillator under trusted phase noise, arXiv:1709.10202.

[34] B. Qi, P. Lougovski, and B. P. Williams, Characterizing photon number statistics using conjugate optical homodyne detection, arXiv:1702.02558.

[35] 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).

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

[37] 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).

[38] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express **26**, 2794 (2018).

[39] M. L. Dennis, I. N. Duling, and W. K. Burns, Inherently bias drift free amplitude modulator, Electron. Lett. **32**, 547 (1996).

[40] E. Diamanti and A. Leverrier, Distributing secret keys with quantum continuous variables: Principle, security and implementations, Entropy **17**, 6072 (2015).

[41] E. Agrell *et al.*, Roadmap of optical communications, J. Opt. **18**, 063002 (2016).