Simultaneous classical communication and quantum key distribution using continuous variables*

Bing Qi

Simultaneous classical communication and quantum key distribution using continuous variable

Bing Qi[1, 2, *]

[1]*Quantum Information Science Group, Computational Sciences and Engineering Division,*
Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA
[2]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, TN 37996 - 1200, USA*

Presently, classical optical communication systems employing strong laser pulses and quantum key distribution (QKD) systems working at single-photon levels are very different communication modalities. Dedicated devices are commonly required to implement QKD. In this paper, we propose a scheme which allows classical communication and QKD to be implemented simultaneously using the same communication infrastructure. More specially, we propose a coherent communication scheme where both the bits for classical communication and the Gaussian distributed random numbers for QKD are encoded on the *same* weak coherent pulse, and decoded by the *same* coherent receiver. Simulation results based on practical system parameters show that both deterministic classical communication with a bit error rate of 10^{-9} and secure key distribution could be achieved over tens of kilometers single mode fibers. It is conceivable that in the future coherent optical communication network, QKD is operated in the background of classical communication at a minimal cost.[a]

PACS numbers: 03.67.Dd

I. INTRODUCTION

One of the most practical applications of quantum information science is the so-called quantum key distribution (QKD) protocol, which allows two remote parties, normally referred to as Alice and Bob, to generate a secure key through an insecure quantum channel [1–6]. The generated key can be further applied in other cryptographic protocols to enhance communication security.

In the first QKD protocol, the Bennett and Brassard 1984 (BB84) QKD protocol [1], information is carried by single-photon signals. Due to the channel loss and other implementation imperfections, those single-photon signals are detected in a probabilistic fashion with a relatively high quantum bit error rate (QBER) in the order of 10^{-2} [7]. This is in sharp contrast to a classical optical communication system, where information can be transmitted deterministically in an almost error-free fashion. Furthermore, specialized devices, such as single photons detectors, are typically required in QKD. This makes QKD a very different communication modality in comparison with classical communication.

More recently, continuous-variable (CV) QKD protocols based on optical coherent detection have been pro-

posed and demonstrated as viable solutions [8–11]. In an optical coherent receiver, a strong laser pulse called local oscillator (LO) is mixed with the incoming signal at a beam splitter. The resulting interference signal is strong enough and can be detected using highly efficient photo-diodes working at room temperature. The strong LO also acts as a natural and extremely selective filter, which can effectively suppress broadband noise photons generated in the communication channel. This intrinsic filtering function is especially useful when conducting QKD over a noisy channel, such as a lit fiber in a conventional fiber optic network [12, 13] or a free-space optical link [14].

One well-known CV-QKD protocol is the Gaussian-modulated coherent states (GMCS) protocol [10], which has been demonstrated over 100km telecom fiber [15] and in a real-world CV-QKD network [16]. The hardware required for implementing the GMCS QKD is surprisingly similar to that for classical coherent optical communication [17]. In fact, recent progresses in both communities have significantly reduced the gap between them. On one hand, the continuous improvement of detector performance and the development of forward-error-correction coding in classical coherent communication allows a bit error rate (BER) of 10^{-9} with only a few photons per bit [18]. On the other hand, CV-QKD protocols based on discrete modulation scheme, which are similar to the binary phase-shift keying (BPSK) and the quadrature phase-shift keying (QPSK) in classical communication, have been proposed [19, 20]. It is feasible to use the same communication infrastructure for either classical communication or QKD in a time-sharing manner.

In this paper, we go one step further by showing it is possible to conduct classical communication and QKD *simultaneously*. As a specific example, we propose a coherent communication scheme where both the bits for classi-

cal communication and the Gaussian distributed random numbers for GMCS QKD are encoded on the *same* weak coherent pulse, and decoded by the *same* coherent receiver. Such a scheme could be appealing in practice, where random numbers for QKD are superimposed on classical communication signals, and secure key distribution is conducted in the background of classical communication at a minimal cost.

Our protocol is a special case of the more general concept of simultaneous transmission of classical and quantum information [21, 22]. The trade-off relations for public communication, privacy communication and secure key generation have been derived in [22] assuming no feedback from the receiver to the sender. It could be interesting to extend the results in [22] to the GMCS QKD using reverse reconciliation.

This work is partly inspired by [23], where the authors propose improved schemes to implement CV-QKD using a *locally* generated LO [24–26]. One scheme proposed in [23] is to estimate the phase difference between two remote lasers by sending Gaussian modulated coherent states displaced in phase space. In our scheme, we encode classical information on the displacements of QKD signals.

This paper is organized as follows: in Section II, we present details of the proposed protocol. In Section III, we conduct numerical simulations based on practical system parameters. Finally, we conclude this paper with a discussion in Section IV.

II. DETAILS OF THE NEW PROTOCOL

For simplicity, in this paper we assume the BPSK scheme and the GMCS protocol are adopted in classical communication and QKD, correspondingly. The basic idea should be applicable in other encoding schemes.

A. Classical coherent communication using BPSK

In the BPSK modulation scheme, the classical binary information is encoded on the phase of a coherent state, and decoded by performing optical homodyne detection. More specifically, the bit value m_A ($m_A = 0, 1$) is encoded by $|e^{-im_A\pi}\alpha\rangle$, as shown in Fig.1(a). Without loss of generality, we assume α is a real number. The average photon number μ of the coherent state is given by $\mu = \alpha^2$.

We assume that the X-quadrature of the signal is measured by the receiver. The probability distribution of the measurement result x_c is shown in Fig.1(a) (right figure). The receiver can decode binary information using the sign of x_c, i.e., if $x_c > 0$ (< 0), the bit value is assigned as "0" ("1"). The BER of the BPSK scheme is determined by the measurement error variance σ and the
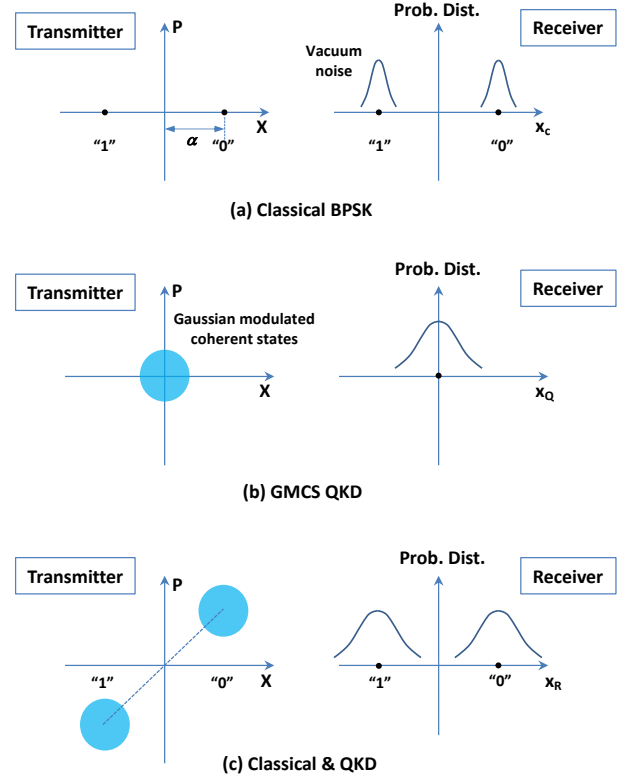

FIG. 1: Phase space representations of various coherent communication schemes. (a) Classical BPSK scheme. (b) GMCS QKD scheme. (c) The proposed scheme. The figures on the right show the probability distributions of X-quadrature measurement.

signal amplitude α, and is given by [17]

$$BER = \frac{1}{2}erfc(\frac{\sqrt{T_{ch}\eta}\alpha}{\sqrt{2}\sigma}) \qquad (1)$$

where T_{ch} is the channel transmittance, η is the detection efficiency, and erfc(*) denotes the complementary error function. If the homodyne detector is shot-noise limited (the technical noise is much lower than the vacuum noise), then σ is about 1/4. From (1), we need about 9 photons per bit at the receiver's end to achieve a BER of 10^{-9}.

B. GMCS QKD

In GMCS QKD, Alice prepares coherent states $|x_A + ip_A\rangle$ and sends them to Bob through a quantum channel. Here x_A and p_A are Gaussian random numbers with zero mean and a variance of $V_A N_0$, where $N_0 = 1/4$ denotes the shot-noise variance. In this paper, all the noise variances are defined in the shot-noise unit. At Bob's end, he can either perform optical homodyne detection to measure a randomly chosen quadrature [10], or perform

optical heterodyne detection to measure both quadratures simultaneously [27]. In this paper, our discussion is based on the homodyne detection scheme. The essential ideas can be extended to the other case. Fig.1(b) shows the phase space representation of Gaussian modulated coherent states. Given the system is shot-noise limited, the overall quadrature variance at the receiver's end is $(T_{ch}\eta V_A + 1)N_0$.

After quantum transmission stage, Bob announces which quadrature he measures for each incoming signal through an authenticated classical channel, and Alice only keeps the corresponding data. If the observed noise is below certain threshold, they can further work out a secure key by performing reconciliation and privacy amplification. See more details in Section III.

C. Simultaneous classical communication and QKD protocol

It is straightforward to combine the above two communication protocols. In this simultaneous classical communication and QKD scheme, Alice encodes her classical bit m_A and Gaussian random numbers $\{x_A, p_A\}$ on a coherent state $|(x_A + e^{-im_A\pi}\alpha) + i(p_A + e^{-im_A\pi}\alpha)\rangle$, as shown in Fig.1(c). Note in the GMCS QKD based on homodyne detection, Bob measures either X or P quadrature of each incoming signal. To achieve deterministic classical communication, the same classical bit m_A is encoded on both X and P quadrature. If heterodyne detection scheme is employed, then Alice only needs to encode m_A on one quadrature.

Assume Bob measures X-quadrature (P-quadrature) and his measurement result is x_R (p_R). Bob determines a classical bit m_B using the sign of x_R (p_R), i.e., if $x_R(p_R) > 0$, then the value of m_B is assigned as "0". Otherwise, the value of m_B is assigned as "1". To generate secure key, the measurement result will be rescaled and displaced based on the overall transmittance $T_{ch}\eta$ and the value of m_B as follows

$$x_B = \frac{x_R}{\sqrt{T_{ch}\eta}} + (2m_B - 1)\alpha$$
$$p_B = \frac{p_R}{\sqrt{T_{ch}\eta}} + (2m_B - 1)\alpha \qquad (2)$$

Alice and Bob can further 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.

Essentially, the states prepared by Alice are displaced Gaussian modulated coherent states, where the amount of displacement is determined by the classical bit m_A. Given a modulation variance V_A, the BER of classical communication can be reduced effectively by increasing the displacement α.

Next, we will show that the security proofs of the standard GMCS QKD can be applied to this new scheme. To illustrate the essential ideas, it is convenient to represent the classical communication and QKD using two separate
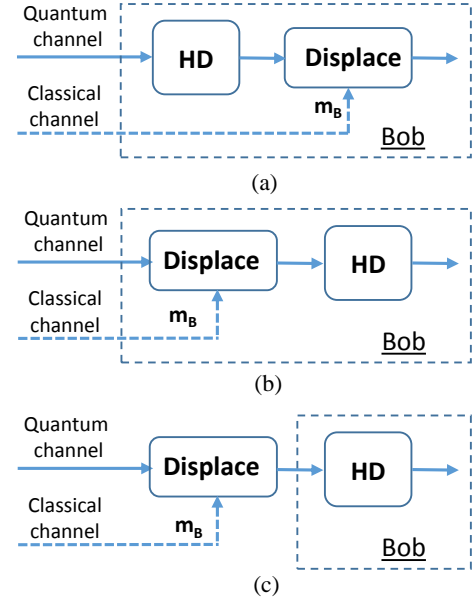

FIG. 2: Security models. HD–homodyne detection. (a) Our protocol; (b) A virtual QKD scheme equivalents to (a); (c) Standard GMCS QKD.

channels, and allow Eve to have full access and control of information transmitted through the classical channel, as shown in Fig.2 (a). In this picture, Bob performs a homodyne measurement on the incoming signal, then displaces his measurement results using classical information m_B (which could be provided by Eve). Equivalently, Bob could perform the displacement operation first, then perform the homodyne measurement, as shown in Fig.2 (b). Finally, if we move the displacement operation out of Bob's secure station and let Eve to have full control of it (see Fig.2 (c)), then the whole system reduces to the standard GMCS QKD, where Eve is allowed to manipulate the quantum signals transmitted through the channel at her will. Note, in the last step, we have given Eve additional power to control the displacement operation, so the security of the proposed scheme is at least as strong as the standard GMCS QKD.

In next section, we conduct numerical simulations to estimate the performance of the proposed scheme.

III. SIMULATION RESULTS

To evaluate the performance of the proposed scheme, we conduct numerical simulations using practical system parameters. On one hand, since the quantum signal is superimposed on a relatively strong classical signal, we expect that noises from the classical channel will be coupled into the quantum channel and reduce the QKD performance. On the other hand, the Gaussian modulation in QKD will also appear as a noise source in classical communication channel.

We first evaluate the performance of the classical communication. The main noise sources in classical channel are: (1) the vacuum noise with a variance of one; (2) the detector noise denoted by ν_{el}; and (3) the Gaussian modulation for QKD with a variance of V_A. All the above noises are defined in the shot-noise unit and are assumed to be independent Gaussian noises with zero mean. Note the first two are defined at the receiver's side, while the third is defined at the sender's side. As we will show below, to achieve a positive key rate in QKD, the excess noise due to phase instability and other modulation imperfections should be much smaller than the vacuum noise. So we neglect the phase noise in classical communication.

We assume the communication channel is optical fiber with an attenuation coefficient of γ. The channel transmittance is given by

$$T_{ch} = 10^{\frac{-\gamma L}{10}} \tag{3}$$

where L is the fiber length.

From (1), the BER of classical communication is given by

$$BER = \frac{1}{2} erfc(\frac{\sqrt{T_{ch}\eta}\alpha}{\sqrt{2(T_{ch}\eta V_A + 1 + \nu_{el})N_0}}) \tag{4}$$

To achieve a BER of 10^{-9} in the classical channel, the required displacement α is

$$\alpha = 4.24 \times \frac{\sqrt{T_{ch}\eta V_A + 1 + \nu_{el}}}{\sqrt{2T_{ch}\eta}}. \tag{5}$$

We conduct numerical simulation to calculate the required displacement α as a function of the fiber length using (5). Simulation parameters are $V_A = 4$, $\gamma = 0.2$ dB/km, $\eta = 0.5$, $\nu_{el} = 0.1$. The simulation results are shown in Fig.3.

Fig.3 shows that $\alpha^2 \geq (V_A + 1)N_0$ for a typical V_A in the range of 1 to 20. The presence of this relatively large displacement not only requires a large dynamic range of the detector, but also makes the QKD performance more sensitive to the phase noise. We will study these issues in details below.

The expected quadrature distribution at the receiver's end is shown in Fig.4, where $\alpha' = \sqrt{T_{ch}\eta}\alpha$ is the reduced displacement at receiver's end and $V_B = (T_{ch}\eta V_A + 1)N_0$ is the expected variance associated with the Gaussian modulation. Due to the finite dynamic ranges of electrical amplifiers and Analog to Digital Converter (ADC), a practical homodyne detector only has a limited linear response range $[-x_m, x_m]$, within which the output signal is propositional to the quadrature value of the input signal [28, 29]. For simplicity, we assume the output of the homodyne detector is either x_m or $-x_m$ if the input signal is beyond the linear range. The excess noise due to the finite measurement range of the detector is denoted
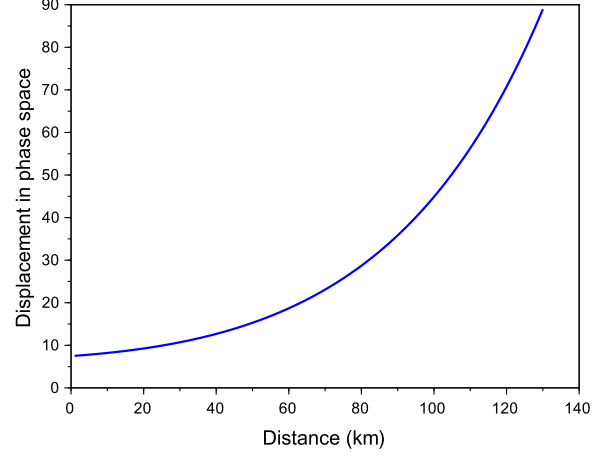

FIG. 3: Simulation results of the required displacement α to achieve a BER of 10^{-9} in the classical channel. Simulation parameters: $V_A = 4$, $\gamma = 0.2$ dB/km, $\eta = 0.5$, $\nu_{el} = 0.1$.

by ε_c, which is given by

$$\varepsilon_c = \frac{1}{N_0\sqrt{2\pi V_B}} \int_{-\infty}^{-x_m} (x + x_m)^2 e^{-\frac{(x-\alpha')^2}{2V_B}} dx$$
$$+ \frac{1}{N_0\sqrt{2\pi V_B}} \int_{x_m}^{\infty} (x - x_m)^2 e^{-\frac{(x-\alpha')^2}{2V_B}} dx. \tag{6}$$

Furthermore, due to the finite resolution of the ADC, we expect a quantization noise variance given by

$$\varepsilon_d = \frac{1}{N_0} \left[0.5 \times \frac{x_m - (-x_m)}{2^M} \right]^2 \tag{7}$$

where M is the number of bits of the ADC.

To estimate the magnitudes of ε_c and ε_d in a practical setup, we assume that the dynamic range of the homodyne detector is 30 dB, corresponding to a practical 10-bit ADC ($M = 10$). Other system parameters are assumed to be $V_A = 4$, $\gamma = 0.2$ dB/km, $\eta = 0.5$, and $x_m = 10$. Using (5)-(7), ε_c and ε_d have been determined to be 4.4×10^{-9} and 3.8×10^{-4}, which are negligible comparing with the electrical noise of the detector (typically in the order of 10^{-2} to 10^{-1}).

Next, we estimate the impact of phase noise which commonly exists in a coherent communication system. Under the assumption of $\alpha^2 \geq (V_A + 1)N_0$, the excess noise due to phase instability can be estimated by

$$\varepsilon_p = \frac{\alpha^2 \sigma_\phi}{N_0} \tag{8}$$

where σ_ϕ is the phase noise variance. Note σ_ϕ can include both the phase noise between the signal and the LO, and other modulation errors.
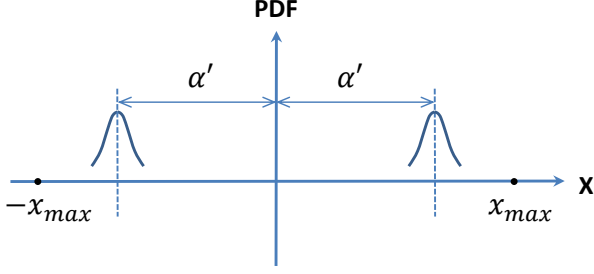
FIG. 4: The expected quadrature distribution at the receiver's end. $\alpha' = \sqrt{T_{ch}\eta}\alpha$; the variance of the Gaussian distribution is $V_B = (T_{ch}\eta V_A + 1)N_0$; the linear range of the homodyne detector is $[-x_m, x_m]$.

We define the overall excess noise outside of Bob's system as

$$\varepsilon = \varepsilon_p + \varepsilon_0 \qquad (9)$$

where ε_0 quantifies the excess noise independent of α. For more detailed studies on various noises in CV-QKD, see [23, 30–32].

To estimate the secure key rate of QKD, we adopt the "realistic" model [10] where one crucial assumption is that Eve cannot control the noise and loss inside Bob's system (ν_{el} and η). This "realistic" model has been widely adopted in long distance CV-QKD experiments [10, 11, 13, 15, 30, 31].

The asymptotic secure key rate, under the optimal collective attack, in the case of reverse reconciliation, is given by [31]

$$R = fI_{AB} - \chi_{BE} \qquad (10)$$

where I_{AB} is the Shannon mutual information between Alice and Bob; f is the efficiency of the reconciliation algorithm; χ_{BE} is the Holevo bound of the information between Eve and Bob. We remark a composable security proof against arbitrary attacks has been developed for GMCS QKD based on the heterodyne detection scheme [33]. Unfortunately, the existing security proof cannot produce a positive key rate for a reasonable data size [34]. Here, we adopt the security analysis given in [31] to facilitate the comparison with previous experimental results.

The mutual information between Alice and Bob is given by [10]

$$I_{AB} = \frac{1}{2}log_2\frac{V + \chi_{tot}}{1 + \chi_{tot}} \qquad (11)$$

The Holevo bound of the information between Eve and Bob is given by [31]

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right) \qquad (12)$$
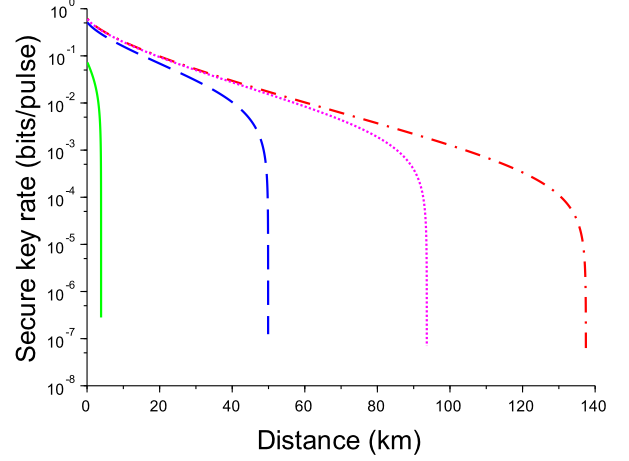
where $G(x) = (x+1)log_2(x+1) - xlog_2 x$

FIG. 5: Simulation results based on security analysis given in [31]. Simulation parameters: $\gamma = 0.2$ dB/km; $\varepsilon_0 = 0.01$; $\nu_{el} = 0.1$; $V_A = 4$; $\eta = 0.5$; $f = 0.95$; and $\sigma_\phi = 10^{-3}$ (solid line), 10^{-4} (dash line), 10^{-5} (dot line) and 10^{-6} (dash dot line).

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right] \qquad (13)$$

where

$$A = V^2(1 - 2T_{ch}) + 2T_{ch} + T_{ch}^2(V + \chi_{line})^2 \qquad (14)$$

$$B = T_{ch}^2(V\chi_{line} + 1)^2 \qquad (15)$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right] \qquad (16)$$

where

$$C = \frac{A\chi_{hom} + V\sqrt{B} + T_{ch}(V + \chi_{line})}{T_{ch}(V + \chi_{tot})} \qquad (17)$$

$$D = \sqrt{B}\frac{V + \sqrt{B}\chi_{hom}}{T_{ch}(V + \chi_{tot})} \qquad (18)$$

$$\lambda_5 = 1 \qquad (19)$$

System parameters in the above equations are defined as follows:

(a) $V = V_A + 1$.

(b) The total noise referred to the channel input $\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{T_{ch}}$.

(c) The total channel-added noise referred to the channel input $\chi_{line} = \frac{1}{T_{ch}} - 1 + \varepsilon$.

(d) The detector-added noise referred to Bob's input $\chi_{hom} = [1 - \eta + \nu_{el}]/\eta$.

We conduct numerical simulations of secure key rate at different phase noise variances. Other simulation parameters are: $\gamma = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $\nu_{el} = 0.1$, $\eta = 0.5$, $f = 0.95$, and $V_A = 4$. Fig. 5 shows the simulation results. The performance of the proposed scheme is heavily dependent on the phase noise of the system. The observed phase noises in previous CV-QKD experiments are in the orders of 10^{-3} [30], 10^{-4} [31], and 10^{-6} [15], suggesting simultaneous classical communication and QKD over tens of kilometer optical fiber is possible.

IV. DISCUSSION

One major roadblock to the wide applications of QKD is the high implementation cost. Presently, dedicated hardware are required to implement QKD protocols. In this paper, we show that by using optical coherent detection, classical communication and QKD could be implemented simultaneously on the same platform. Our simulation results suggest that the QKD performance is largely determined by the phase noise of the coherent communication system. To extend the distance of QKD, sophisticate phase stabilization scheme may be required.

In our simulation, an uncoded BPSK scheme is assumed for classical communication. In modern optical communication systems, forward error correction (FEC) schemes are commonly used to achieve high accuracy of data transmission with the minimum of optical power [35]. For example, by applying FEC coding, a BER of 10^{-9} was achieved at a signal power of 1.5 photons per pulse [18]. In comparison, an uncoded BPSK system requires at least 9 photons per pulse to achieve the same BER. As shown in (8), the excess noise due to the phase instability is proportional to the optical power in classical channel. By applying FEC coding, the excess noise in QKD can be further reduced. This can lead to a better secure key rate or a longer distance.

To apply our scheme in practice, there are important challenges to be addressed.

First, in our simulation, the secure key rate is calculated based on a security proof against collective attacks in the asymptotic limit of infinitely large data size. In practical applications, a composable security against arbitrary attacks is required. Unfortunately, the existing composable security proof techniques cannot produce a positive key rate for a reasonable data size [34]. This is a significant challenge not only to our scheme but also to all CV-QKD protocols based on coherent states. As remarked by the authors of [34], finding better security proofs allowing composable security for reasonable data size "is certainly the most pressing issue in the theoretical study of CVQKD".

Second, while today's classical communication systems can be operated at 10 to 100 GHz repetition rate, the highest repetition rate demonstrated in CV-QKD experiments is only 100 MHz [26]. To implement the simultaneous classical and quantum communication protocol, we either have to sacrifice the speed of the classical communication, or need to develop high-speed (above 10 GHz) shot-noise limited homodyne detectors. We remark that the speed of shot-noise limited homodyne detectors has been improved significantly over the years. A 1 GHZ shot-noise limited homodyne detector has been applied in a recently CV-QKD experiment [26]. We expect this trend will continue in the future and the gap between the repetition rates of classical and quantum communications may eventually disappear.

[1] C. H. Bennett and G. Brassard, *in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175-179.

[2] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

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

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

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

[6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, arXiv:1606.05853 (2016).

[7] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Phys. Rev. Lett.* **96**, 070502 (2006).

[8] T. C. Ralph, *Phys. Rev. A* **61**, 010303(R) (1999).

[9] M. Hillery, *Phys. Rev. A* **61**, 022309 (2000).

[10] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, *Nature* **421**, 238 (2003).

[11] P. Jouguet, S. Kunz-Jacques, A. Leverrier, Ph. Grangier, and E. Diamanti, *Nat. Photonics* **7**, 378 (2013).

[12] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, *New J. Phys.* **12**, 103042 (2010).

[13] R. Kumar, H. Qin, and R. Alléaume, *New J. Phys.* **17**, 043027 (2015).

[14] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G. Leuchs, *New J. Phys.* **16**, 113018 (2014).

[15] D. Huang, P. Huang, D. Lin, and G. Zeng, *Sci. Rep.* **6**, 19201 (2016).

[16] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, *Opt. Lett.* **41**, 3511 (2016).

[17] K. Kikuchi, *IEEE J. Lightw. Technol.* **34**, 157 (2016).

[18] M. L. C. Stevens, D. O. Robinson, B. S. Boroson, D. M. Kachelmyer, and A. L. Kachelmyer, *Opt. Exp.* **16**, 10412 (2008).

[19] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, *Phys. Rev. A* **79**, 012307 (2009).

[20] A. Leverrier and Ph. Grangier, *Phys. Rev. Lett.* **102**, 180504 (2009).

[21] I. Devetak and P. Shor, *Commun. Math. Phys.* **256**, 287 (2005).

[22] M. M. Wilde, P. Hayden, and S. Guha, *Phys. Rev. Lett.* **108**, 140501 (2012).

[23] A. Marie and R. Alléaume, arXiv:1605.03642 (2016).

[24] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, *Phys. Rev. X* **5**, 041009 (2015).

[25] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, *Phys. Rev. X* **5**, 041010 (2015).

[26] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, *Opt. Lett.* **40**, 3695 (2015).

[27] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).

[28] Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. I. Lvovsky, and L. Tian, *New J. Phys.* **13**, 013003 (2011).

[29] H. Qin, R. Kumar, and R. Alléaume, *Phys. Rev. A* **94**, 012325 (2016).

[30] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, *Phys. Rev. A* **76**, 052323 (2007).

[31] 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, *Phys. Rev. A* **76**, 042305 (2007).

[32] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, *Phys. Rev. A* **86**, 032309 (2012).

[33] A. Leverrier, *Phys. Rev. Lett.* **114**, 070501 (2015).

[34] E. Diamanti and A. Leverrier, *Entropy* **17**, 6072 (2015).

[35] F. Chang, K. Onohara, and T. Mizuochi, *IEEE Comm. Mag.* **48**, S48 (2010).