Generating the local oscillator “locally” in continuous-variable quantum key distribution based on coherent detection

Bing Qi,1,2 Pavel Lougovski,ı Raphael Pooser,1,2 Warren Grice,1 and Miljko Bobrek3

1Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, USA
2Department of Physics and Astronomy, The University of Tennessee, Knoxville, TN 37996 - 1200, USA
3RF, Communications, and Intelligent Systems Group, Electrical and Electronics Systems Research Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831-6006, USA

(Dated: March 3, 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 also limit the potential applications of CV-QKD. In this paper, we propose and demonstrate a pilot-aided feedforward data recovery scheme which 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 (MDI) CV-QKD where independent light sources are employed by different users.

PACS numbers: 03.67.Dd

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 a 80km 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.

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] [10]. This arrangement has several limitations. First of all, the above co-propagating scheme 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 [17–20]. 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] [15]. With a 1 GHz pulse repetition rate and a channel loss of 20 dB, the required LO power at input of the channel is about 1.2 W (at 1550 nm). 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 demultiplexing schemes are required to effectively separate the LO from the quantum signal at the receiver’s end.

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 [21], optical phase-locked loops [22], and optical injection phase-lock loop [23], 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 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 long as the basis information is available afterwards. With this post-measurement 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. If the observed excess noise is small enough, they can further work out a secure key. One widely adopted assumption in QKD is that the users cannot distinguish the noise due to Eve’s attack from the intrinsic noise of the QKD system. If the intrinsic noise of the QKD system is too high, then it is impossible to generate quantum keys with proven security.

One important source of excess noise in CV-QKD is the phase noise in coherent detection. High-precision coherent detection relies on the fixed phase relation between the signal laser and the LO laser. In practice, it is very difficult to lock the phase of these two lasers, especially when they are isolated from each other both optically and electrically. Fortunately, in GMCS QKD, Bob does not need to measure Alice’s signal in the “correct basis”. As long as they can know which basis is used by Bob, one of them can rotate the data at hand in the post-processing stage and establish correlation with the other party.

In our scheme, both the signal laser and the LO laser are operated at free-running mode. For convenience, we choose Alice’s signal laser as the phase reference. When Bob performs conjugate homodyne detections, the phase $\phi$ of the LO laser is a random number uniformly distributed between $[0, 2\pi)$. Obviously, Bob’s measurement results $(X_\phi, P_\phi)$ have no correlation with the random numbers $(X_A, P_A)$ encoded by Alice. However, if Alice and Bob have a method to determine $\phi$, then one of them (for example, Alice) can remap the data at hand during the post-processing process

$$X'_A = X_A \cos\phi + P_A \sin\phi$$
$$P'_A = -X_A \sin\phi + P_A \cos\phi$$

Under normal conditions (no Eve), $(X_\phi, P_\phi)$ and $(X'_A, P'_A)$ are correlated. Alice and Bob can further apply error correction and privacy amplification to work out a secure key, as in the conventional GMCS QKD. We remark that a similar “quadrature-remapping” scheme was first applied in [16] to remove the noise due to the slow phase drift of a fiber interferometer.

We developed a pilot-aided feedforward data recovery scheme [27] which allows Bob to determine the phase $\phi$ reliably. The basic idea is as follows. For each quantum transmission, Alice sends out a Gaussian modulated weak coherent state (signal pulse) and a relatively strong phase reference pulse generated from the same laser (the signal laser). These two pulses propagate through the same quantum channel to the measurement device, where Bob performs conjugate homodyne detections on both of them using LOs generated from the LO laser. The measurement results from the phase reference pulse $(X_R, P_R)$ can be used to determine $\phi$.

In practice, $\phi$ cannot be determined perfectly due to laser phase noise and measurement errors. From eq. (1), the uncertainty of $\phi$ will be translated into an excess noise in $(X'_A, P'_A)$ as

$$\varepsilon_\phi = V_A \sigma_\phi$$

where $V_A$ is Alice’s modulation variance, $\sigma_\phi$ is the noise variance in determining $\phi$. To achieve a high secure key rate, it is crucial to reduce $\sigma_\phi$.

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 $\theta_0 + 2\pi ft$ (the phase expected from an ideal sine wave), where $f$ is the central frequency of the laser.
Δθ(t) can be treated as Gaussian noise with a mean of zero and a variance of

\[ \langle (\Delta \theta(t))^2 \rangle = \frac{2T}{\tau_c}. \]  

Here \( \tau_c \) is the coherence time of the laser, which is related to its linewidth \( \Delta f \) by \( \tau_c \approx \frac{1}{\pi \Delta f} \).

Suppose the linewidths of the signal laser and the LO laser are \( \Delta f_1 \) and \( \Delta f_2 \), respectively; the time delay between the signal pulse and the phase reference pulse is \( T_d \). Using eqs. 3 and 4, the phase noise contributed by the two lasers is given by

\[ \sigma_{\phi,L} \approx 2\pi T_d (\Delta f_1 + \Delta f_2). \]  

From eq. 5, the phase measurement precision can be improved by reducing either the laser linewidths or the time delay between the signal pulse and the phase reference pulse.

### III. EXPERIMENTAL SETUP AND RESULTS

We demonstrate the pilot-aided feedforward data recovery scheme using commercial off-the-shelf devices. The experimental setup is shown in Fig.1. 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 free-running mode and the central frequency difference between the two lasers can stay within 10 MHz without 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 will be used as phase references, the equivalent data transmission rate in our experiment is 25 MHz. A LiNbO3 waveguide phase modulator (EOSpace) is used to encode binary phase information on the signal pulses.

Both the signal pulses and reference pulses propagate through a spool of 25 km single mode fiber before arriving at the measurement device. At the receiver’s end, the average photon number is about \( 10^5 \) per pulse, which is significantly lower than that of the LO used in GMCS QKD. A commercial 90-degree 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-degree optical hybrid is a passive device featuring a compact design. No temperature control is required to stabilize its internal interferometers. The output of the balanced photodetectors are sampled by a broadband oscilloscope at 1 GHz sampling rate. For simplicity, the LO laser is operated in the cw mode. A waveform generator with a bandwidth of 120 MHz provides the modulation signals to both the intensity and the phase modulator, and a synchronization signal to the oscilloscope.

Note, a signal pulse \( S_i \) and the corresponding reference pulse \( R_i \) (see Fig.1) are measured at different times with a time delay of \( T_d \). If the central frequency difference of the two lasers \( (f_1 - f_2) \) is a constant over a long time period, we can simply correct the phase measurement result of \( R_i \) by adding a constant phase shift of \( 2\pi(f_1 - f_2)T_d \). In practice, however, both lasers present frequency drift over time. In our experiment, we use a simple scheme to estimate the phase difference \( \phi_{S,i} \) at the time when the signal pulse is measured. 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

\[ \overline{\phi}_{S,i} = \frac{\phi_{R,i} + \phi_{R,i+1}}{2} = \phi_{R,i} + 2\pi \overline{f}_d T_d \]  

where

\[ \overline{f}_d = \frac{\phi_{R,i+1} - \phi_{R,i}}{4\pi T_d} \]  

is the estimated frequency difference of the two lasers. One assumption made in the above equations is the frequency difference of the two lasers is stable within the time interval between two adjacent reference pulses (40 ns in our experiment), so the phase difference grows linearly with time.

To evaluate the effectiveness of the above LO 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 phase shift of 1.65. In total, 25000 signal pulses are transmitted. The experimental results are summarized in Fig.2. As shown in Fig.2(a) and (b), before phase correction, the measured phases are randomly distributed within \([0, 2\pi]\), regardless the encoded information. After phase correction, the measurement results for bit 0 and bit 1 are clearly separated. The residual phase noise variances (after phase correction) have been determined to be 0.040 (for bit 0) and 0.039 (for bit 1) respectively. As shown in the Appendix, phase noise at this level is tolerable in the GMCS QKD protocol.

One major cause of the observed phase noise is the laser phase noise associated with its linewidth. First of
all, due to the laser phase noise, the difference of the central frequencies of the two lasers cannot be determined precisely. Using Eqs. (5) and (7), the uncertainty of \( f_d \) is given by \( \Delta f_1 + \Delta f_2 \), which is translated into a phase noise of \( \pi T_d (\Delta f_1 + \Delta f_2) \) in the measurement system. Second, as discussed in the previous section, even with a precisely determined \( f_d \), there is still a noise variance of \( 2\pi T_d (\Delta f_1 + \Delta f_2) \) due to the finite linewidths of the two lasers. In total, the two lasers contribute a noise variance of \( 3\pi T_d (\Delta f_1 + \Delta f_2) \) in the above scheme. Using \( \Delta f_1 = 62 \text{ KHz}, \Delta f_2 = 70 \text{ KHz} \) (provided by the vendor), and \( T_d = 20 \text{ ns} \), the noise variance contributed by the two lasers is estimated to be 0.024. The difference between the experimentally observed and the theoretically estimated noise variances could come from the measurement system.

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 which 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. A proof of principle experiment based on commercial off-the-shelf components shows that the noise due to the proposed scheme is tolerable in CV-QKD. To further reduce the noise, laser sources with smaller linewidth can be applied.

Since a phase reference pulse is still required in our scheme, one may ask whether our scheme is really different from the conventional approach. The answer is twofold. First, the phase reference pulse is only used to provide the (classical) phase information, it is not directly used in the detection of the quantum signal. In fact, in our scheme Eve can never access the LO itself. Eve can certainly interfere with the phase estimation process by manipulating the phase reference pulse when it propagates through the quantum channel. This could result in 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 protocol. From Eve’s point of view, whatever can be achieved by manipulating the reference pulse can also be achieved by manipulating the quantum signal directly. So, sending the reference pulses through the quantum channel will not give Eve any additional advantages, thus the standard security proof of CV-QKD (built upon the assumption that Eve can only access the quantum signal) can be applied in our scheme. Second, the reference pulse used in our experiment (\( 10^5 \) photons per pulse) is much weaker than the LO itself (typically \( 10^8 \) photons per pulse). As a result, other problems associated with sending the strong LO through the channel, such as the reduction of QKD efficiency and the multiplexing capacity, are not present in our scheme.

To conduct a complete CV-QKD experiment with the current setup, broadband shot-noise limited homodyne detectors are required. Detectors with the desired performances have been implemented by several groups [29–31]. We expect our scheme will significantly improve the performance of CV-QKD. This technology also open the door for other quantum communication protocols, such as the measurement-device-independent (MDI) CV-QKD protocol.

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: 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 [32].

The secure key rate under the optimal collective attack,
in the case of reverse reconciliation, is given by
\[ R = f I_{AB} - \chi_{BE} \]  (A.1)
where \( I_{AB} \) is the Shannon mutual information shared between Alice and Bob; \( f \) is the efficiency of the reconciliation algorithm; \( \chi_{BE} \) is the Holevo bound of the information between Eve and Bob.

The mutual information between Alice and Bob is given by
\[ I_{AB} = \log_2 V + \chi_{\text{tot}} \]  (A.2)

The Holevo bound of the information between Eve and Bob is given by
\[ \chi_{BE} = \frac{1}{2} \sum_{i=1}^{2} G \left( \frac{\lambda_i - 1}{2} \right) - \sum_{i=3}^{5} G \left( \frac{\lambda_i - 1}{2} \right) \]  (A.3)
where \( G(x) = \left( x + 1 \right) \log_2 (x + 1) - x \log_2 x \)
\[ \lambda_{1,2} = \frac{1}{2} \left[ A \pm \sqrt{A^2 - 4B} \right] \]  (A.4)
where
\[ A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2 \]  (A.5)
\[ B = T^2(V\chi_{\text{line}} + 1)^2 \]  (A.6)
\[ \lambda_{3,4} = \frac{1}{2} \left[ C \pm \sqrt{C^2 - 4D} \right] \]  (A.7)
where
\[ C = \frac{1}{(T(V + \chi_{\text{tot}}))^2} \left[ A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}} \left( V\sqrt{B} + T(V + \chi_{\text{line}}) + 2T(V^2 - 1) \right) \right] \]  (A.8)
\[ D = \left( \frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})} \right)^2 \]  (A.9)
\[ \lambda_5 = 1 \]  (A.10)

System parameters in the above equations are defined as follows.

(a) \( V = V_A + 1 \), where \( V_A \) is Alice’s modulation variance.

(b) The total noise referred to the channel input \( \chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T} \), 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 \( T = 10^{-\frac{\alpha}{10} L} \), where \( L \) is the fiber length.

(c) The total channel-added noise referred to the channel input \( \chi_{\text{line}} = \frac{1}{T} - 1 + \varepsilon \), where \( \varepsilon \) is the excess noise outside of Bob’s system. We assume that \( \varepsilon \) is mainly due to imperfection of the LO phase recovery scheme
\[ \varepsilon = V_A\sigma_\varphi \]  (A.11)
where \( \sigma_\varphi \) is the noise variance associated with the LO phase recovery scheme.

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

We conduct numerical simulation using realistic parameters as summarized below: \( \alpha = 0.2 \text{ dB/km} \), \( \nu_{\text{el}} = 0.1 \), \( \sigma_\varphi = 0.04 \), \( \eta = 0.5 \), \( f = 0.95 \), and \( V_A = 1 \). Fig.3 shows the simulation result in the asymptotic case (ignoring the finite data size effect). The simulation result shows that the proposed LO phase recovery scheme can be applied to achieve efficient QKD.

[1] C. H. Bennett and G. Brassard, in Proceedings of International Conference on Computers, Systems, and Signal Processing, Bangalore, India, (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, *Nature Photonics* **8**, 595 (2014).
[6] D. Mayers, *J. ACM* **48**, 351 (2001).
[7] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
[8] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
[9] T. C. Ralph, *Phys. Rev. A* **61**, 010303(R) (2000).
[10] M. Hillery, *Phys. Rev. A* **61**, 022309 (2000).
[11] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, *Nature* **421**, 238 (2003).
[12] P. Jouguet, S. Kunz-Jacques, A. Leverrier, Ph. Grangier, and E. Diamanti, *Nat. Photonics* **7**, 378 (2013).
[13] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, *New J. Phys.* **12**, 103042 (2010).
[14] P. Jouguet, S. Kunz-Jacques, R. Kumar, H. Qin, R. Gaebet, E. Diamanti, and R. Allaume, in *Proc. 3rd Ann. Conf. Quantum Cryptography* (2013)
[15] R. Kumar, H. Qin, and R. Allaume, in *CLEO: 2014, OSA Technical Digest (online)* (Optical Society of America, 2014), paper FM4A.1.
[16] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, *Phys. Rev. A* **76**, 052323 (2007).
[17] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, *Phys. Rev. A* **87**, 052309 (2013).
[18] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **87**, 062329 (2013).
[19] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, *Phys. Rev. A* **87**, 062313 (2013).
[20] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, *Phys. Rev. A* **89**, 032304 (2014).
[21] E. Ip and J. M. Kahn, *J. Lightw. Technol.* **25**, 2675 (2007).
[22] H. Park, M. Lu, E. Bloch, T. Reed, Z. Griffith, L. Johansson, L. Coldren, and M. Rodwell, *Opt. Exp.* **20**, B197 (2012).
[23] M. J. Fice, A. Chiuchiarelli, E. Ciaramella, and A. J. Seeds, *J. Lightw. Technol.* **29**, 1152 (2011).
[24] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, and S. L. Braunstein, *arXiv:1312.4104v1*.
[25] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, *Phys. Rev. A* **89**, 052301 (2014).
[26] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
[27] B. Qi, Oak Ridge National Lab Invention Disclosure 201303218, DOE S-124,824 (2013).
[28] A. Yariv and P. Yeh, *Photons: optical electronics in modern communications* (sixth edition). Oxford University Press (2007).
[29] R. Okubo, M. Hirano, Y. Zhang, and T. Hirano, *Opt. Lett.* **33**, 1458 (2008).
[30] 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).
[31] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. H. Huntington, and A. I. Lvovsky, *Optics Communications* **285**, 5259 (2012).
[32] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and Ph. Grangier, *J. Phys. B* **42**, 114014 (2009).