Continuous-variable quantum key distribution with a "locally" generated local oscillator

Bing Qi,[1, 2, *] Pavel Lougovski,[1] Raphael Pooser,[1, 2] Warren Grice,[1]
Miljko Bobrek,[3] Charles Ci Wen Lim,[1] and Philip G. Evans[1]

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

(Dated: April 27, 2016)

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, 2]. Both discrete-variable (DV) QKD protocols based on single photon detection [1, 2] and continuous-variable (CV) QKD protocols based on coherent detection [3–6] have been demonstrated as viable solutions in practice.

One appealing feature of CV-QKD based on coherent detection 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 [7–9] or a free-space optical link [10].

However, there is a gap between CV-QKD theory and experiment. On one hand, existing security proofs of CV-QKD are based on the assumption that the LO is *trustable*. On the other hand, the above assumption cannot be justified in most practical implementations of CV-QKD, where both the quantum signal and the LO are generated from the same laser at the sender's end and propagate through an *insecure* quantum channel. This signal-LO co-propagating scheme has several limitations. First of all, it allows Eve to access both the quantum signal and the LO. Eve may launch sophisticated attacks by manipulating the LO, as demonstrated in recent studies [11–14]. Second, sending a strong LO through a lossy channel can significantly 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 [5, 6, 15]. With a 1 GHz pulse repetition rate and a channel loss of 20 dB, the required LO power at the input of the quantum channel would be 1.2 W (at 1550 nm). If optical fiber is used as the quantum channel, noise photons generated by the strong LO inside the optical fiber may significantly reduce QKD efficiency and multiplexing capacity. Third, the LO is typically 7 or 8 orders of magnitude brighter than the quantum signal, complicated multiplexing and 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 highly desirable to generate the LO "locally" using an independent laser source at the receiver's end. To prevent Eve from manipulating the LO, the LO laser should be isolated from outside both optically and electrically.

To close the above gap between theory and experiment, we proposed an *intradyne* CV-QKD scheme where the LO is generated from an *independent* laser source at the receiver's end [16] (see also a related work in [17]). This scheme not only removes the security issues related to an *untrusted* LO, but also greatly simplifies QKD implementation. In Section II, we summarize the main idea of the proposed scheme. In Section III, we summarize the results of proof-of-principle experiments. Section IV is a brief conclusion.

II. THEORETICAL ANALYSIS

In the Gaussian-modulated coherent state (GMCS) protocol [5], Alice draws two random numbers X_A and P_A from a set of Gaussian random numbers (with a mean of zero and a variance of $V_A N_0$), prepares a coherent state $|X_A + iP_A\rangle$ accordingly, and sends it to Bob. Here $N_0 = 1/4$ denotes the shot-noise variance. At Bob's end, he can perform either optical homodyne detection to measure a randomly chosen quadrature [5] or optical heterodyne detection to measure both X and P [18]. In the above discussion, we have implicitly assumed that Alice and Bob share a phase reference, so Bob can perform the required quadrature measurement. If the LO is generated from an independent laser source, how can Alice and Bob establish a phase reference?

Without loss of generality, for each transmission, we can choose the phase of the signal laser as the phase reference ($\phi_S = 0$). When Bob performs conjugated homodyne detection, the phase ϕ of his LO laser can be

* qib1@ornl.gov

treated as a random variable. Bob's measurement results (X_B, P_B) are given by (after scaling with the channel transmittance)

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

where N_X and N_P are assumed to be i.i.d. Gaussian noises with zero mean.

If Alice and Bob can determine ϕ after Bob has performed his measurement, one of them (for example, Bob) can use this post-measurement phase information to correct his data by performing the following rotation

$$\begin{aligned} X_B^{'} &= X_B cos\phi - P_B sin\phi \\ P_B^{'} &= X_B sin\phi + P_B cos\phi \end{aligned} \quad (2)$$

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

$$\begin{aligned} X_B^{'} &= X_A + N_X^{'} \\ P_B^{'} &= P_A + N_P^{'} \end{aligned} \quad (3)$$

where the noise terms in the rotated data are given by

$$\begin{aligned} N_X^{'} &= N_X cos\phi - N_P sin\phi \\ N_P^{'} &= N_X sin\phi + N_P cos\phi \end{aligned} \quad (4)$$

Given N_X and N_P are i.i.d. Gaussian noises, it is easy to see that $N_X^{'}$ and $N_P^{'}$ are also independent Gaussian noises with the same variance as N_X and N_P. This suggests that the above *quadrature remapping* process will not introduce additional noise if the phase ϕ can be determined precisely.

Next, we will present a scheme which allows Alice and Bob to determine ϕ under realistic scenarios using the *same* detector for quantum signal detection. The basic idea is as follows. For each quantum transmission, Alice sends out both a quantum signal and a relatively strong phase reference pulse generated from the same laser. The quantum signal carries Alice's random numbers, as in the case of standard CV-QKD. The reference pulse, on the other hand, is not modulated. These two pulses propagate through the same quantum channel to the measurement device, where Bob performs conjugate homodyne detection on both of them using LOs generated from the *same* LO laser. The measurement results from the phase reference pulse (X_R, P_R) can be used to determine ϕ using $\phi = -tan^{-1}\frac{P_R}{X_R}$. By using a relatively strong reference pulse, Bob can acquire an accurate estimation of ϕ and use this phase information to implement the above quadrature remapping scheme.

Note that the phase reference pulses are not directly used in the coherent detection of the quantum signals, as they are only used to provide (classical) phase information. In fact, in our scheme Eve can never access the LO itself. Eve can certainly interfere with the phase recovery process by manipulating the phase reference pulses when they propagate through the quantum channel. This could result in an increased phase noise and the secure key rate will be reduced. This is one type of denial-of-service attack, which can be performed on any QKD protocol. From Eve's point of view, whatever can be achieved by manipulating the reference pulses can also be achieved by manipulating the quantum signals directly. In a fact, it can be shown that the existing security proofs of CV-QKD based on heterodyne detection [19] (built upon the assumption that Eve can only access the quantum signals) can be applied in our scheme directly [16].

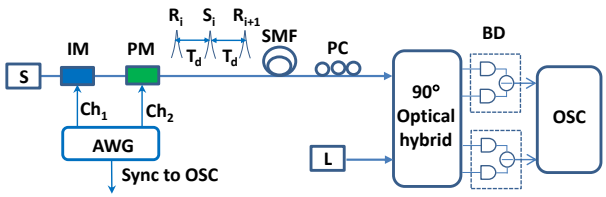

FIG. 1: Experimental setup. S-signal laser; L-LO laser; IM-optical intensity modulator; PM-optical phase modulator; AWG-arbitrary waveform generator; SMF-25km single mode fiber spool; PC- polarization controller; BD-balanced photodetector; OSC-oscilloscope.

III. PROOF OF PRINCIPLE DEMONSTRATION

We conduct a proof-of-principle experiment using the setup as 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 with no optical or electrical connections between them. The central frequency difference between the two lasers can stay within 10 MHz without requiring any feedback controls. A LiNbO3 waveguide intensity modulator (EOSpace) is used to generate 8 ns laser pulses at a repetition rate of 50 MHz. Since half of the laser pulses are used as phase references, the equivalent data transmission rate in our experiment is 25 MHz. A LiNbO3 waveguide phase modulator (EOSpace) is used to modulate the phase of the signal pulses.

Both the signal pulses and the reference pulses propagate through a spool of 25km single mode fiber before arriving at the measurement device. A commercial 90^o 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^o optical hybrid is a passive device featuring a compact design. No temperature control is required to stabilize its internal interferometers. The outputs of the two balanced photodetectors are sampled by a broadband oscilloscope at 1 GHz sampling rate. For simplicity, the LO laser is operated at the cw mode. A waveform generator with a bandwidth of 120 MHz pro-

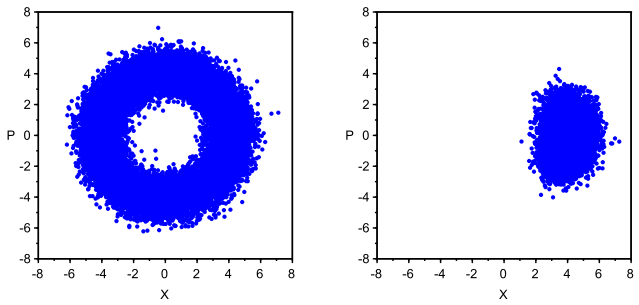

FIG. 2: The measured quadrature values in phase space. Left–before quadrature remapping; Right–after quadrature remapping (no phase information is encoded in this experiment).

vides the modulation signals to both the intensity and the phase modulator, and a synchronization signal to the oscilloscope.

To evaluate the effectiveness of the phase recovery scheme, we conduct an experiment by using the phase reference recovered from the reference pulses to remap quadrature values measured with weak quantum signals. The average photon number of each reference pulse at the receiver's end is about 1000, while that of each signal pulse is 66. Fig.2 shows the quadrature values (X, P) of the signal pulses in phase-space (sample size is 24000). The figure on the left shows the raw measurement results, where the phase randomly distributed in $[0, 2\pi)$ as expected. The figure on the right shows the results after performing quadrature remapping. The phase noise σ_ϕ in the above experiment has determined to be (0.034 ± 0.01), which is low enough to allow secure key distribution.

IV. DISCUSSION

A long outstanding problem in CV QKD based on coherent detection is how to generate the LO "locally". Conventionally, 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.

We solve the above problem by proposing and demonstrating an intradyne CV-QKD scheme where the LO is generated from an *independent* laser source at the receiver's end. This scheme not only removes the security issues related to an *untrusted* LO, but also greatly simplifies the CV-QKD design by getting rid of the cumbersome unbalanced fiber interferometers and the associated phase stabilization system. Proof of principle experiments based on commercial off-the-shelf components show that the noise due to the proposed scheme is tolerable in CV-QKD.

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 ORNL laboratory directed research and development (LDRD) program.

[1] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175-179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[4] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[5] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, Nature **421**, 238 (2003).
[6] P. Jouguet, S. Kunz-Jacques, A. Leverrier, Ph. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[7] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, New J. Phys. **12**, 103042 (2010).
[8] P. Jouguet, S. Kunz-Jacques, R. Kumar, H. Qin, R. Gabet, E. Diamanti, and R. Alléaume, Annual Conference on Quantum Cryptography (QCRYPT) (2013).
[9] R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015).
[10] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).
[11] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **87**, 052309 (2013).
[12] 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).
[13] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[14] 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).
[15] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).
[16] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).
[17] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041009 (2015).
[18] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[19] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).