Research Article | Vol. 26, No. 3 | 5 Feb 2018 | OPTICS EXPRESS 2794
Optics EXPRESS

High key rate continuous-variable quantum key distribution with a real local oscillator

TAO WANG,[1] PENG HUANG,[1,4] YINGMING ZHOU,[1] WEIQI LIU,[2] HONGXIN MA,[3] SHIYU WANG,[1] AND GUIHUA ZENG[1,2,5]

[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China*
[2]*College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China*
[3]*Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China*
[4]*huang.peng@sjtu.edu.cn*
[5]*ghzeng@sjtu.edu.cn*

Abstract: Continuous-variable quantum key distribution (CVQKD) with a real local oscillator (LO) has been extensively studied recently due to its security and simplicity. In this paper, we propose a novel implementation of a high-key-rate CVQKD with a real LO. Particularly, with the help of the simultaneously generated reference pulse, the phase drift of the signal is tracked in real time and then compensated. By utilizing the time and polarization multiplexing techniques to isolate the reference pulse and controlling the intensity of it, not only the contamination from it is suppressed, but also a high accuracy of the phase compensation can be guaranteed. Besides, we employ homodyne detection on the signal to ensure the high quantum efficiency and heterodyne detection on the reference pulse to acquire the complete phase information of it. In order to suppress the excess noise, a theoretical noise model for our scheme is established. According to this model, the impact of the modulation variance and the intensity of the reference pulse are both analysed theoretically and then optimized according to the experimental data. By measuring the excess noise in the 25km optical fiber transmission system, a 3.14Mbps key rate in the asymptotic regime proves to be achievable. This work verifies the feasibility of the high-key-rate CVQKD with a real LO within the metropolitan area.

OCIS codes: (270.5585) Quantum information and processing; (270.5568) Quantum cryptography; (270.5565) Quantum communications.

References and links

1. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621 (2012).
2. F. Grosshans, and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
3. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238 (2003).
4. F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation–The Theory of Practical Implementations," arXiv:1703.09278v2 [quant-ph] (2017).
5. J. Lodewyck, M. Bloch, R. García-Patrón, and S. Fossier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
6. S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography," Phys. Rev. Lett. **101**, 200504 (2008).
7. A. Leverrier, and P. Grangier, "Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **81**, 062314 (2010).
8. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
9. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **109**, 100502 (2012).

#314970 https://doi.org/10.1364/OE.26.002794
Journal © 2018 Received 5 Dec 2017; revised 13 Jan 2018; accepted 17 Jan 2018; published 25 Jan 2018

Optics EXPRESS

10. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
11. A. Leverrier, "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction," Phys. Rev. Lett. **118**, 200501 (2017).
12. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378-381 (2013).
13. 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).
14. C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel," Sci. Rep. **5**, 14607 (2015).
15. D. Huang, D. Lin, C. Wang, W. Liu, and G. Zeng, "Continuous-variable quantum key distribution with 1 Mbps secure key rate," Opt. Express **23**, 17511 (2015).
16. X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems," Phys. Rev. A **88**, 022339 (2013).
17. 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).
18. D. Huang, D. K. Lin, P. Huang, and G. H. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," Opt. Lett. **40**, 3695 (2015).
19. 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).
20. 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 **40**, 041009 (2015).
21. A. Marie, and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," Phys. Rev. A **95**, 012316 (2017).
22. R. Corvaja, "Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection," Phys. Rev. A **95**, 022315 (2017).
23. Z. Qu, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," Opt. Lett. **41**, 5507 (2016).
24. Z. Qu, and I. B. Djordjevic, "High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing," Opt. Express **25**, 7919 (2017).
25. 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).
26. B. Schrenk, and H. Hübel, "Pilot-Assisted Local Oscillator Synchronisation for CV-QKD," Qcrypt 2016 (Poster).
27. F. Laudenbach, B. Schrenk, C. Pacher, R. Lieger, E. Querasser, G. Humer, M. Hentschel, H. Hübel, C. H. F. Fung, A. Poppe, and M. Peev, "Pilot-Disciplined CV-QKD with True Local Oscillator," Qcrypt 2017 (Contributed Talk).
28. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**, 050303 (2005).
29. R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. H. Huntington, and A. I. Lvovsky,"Versatile wideband balanced detector for quantum optical homodyne tomography," Optics Communications **285**, 5259–5267 (2012).
30. H. Qin, A. Q. Huang, and V. Makarov, "Short pulse attack on continuous-variable quantum key distribution system," Qcrypt 2017 (Poster).
31. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77**, 042325 (2008).
32. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
33. B. Qi, and C. C. W. Lim, "Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator," arXiv: 1708.08742v1 [quant-ph] (2017).
34. W. Liu, X. Wang, N. Wang, S. Du, and Y. Li, "Imperfect state preparation in continuous-variable quantum key distribution," Phys. Rev. A **96**, 042312 (2017).

1. Introduction

Continuous variable quantum key distribution (CVQKD) provides a secure way allowing two remote participants, the sender Alice and the receiver Bob, to establish a secret key through an insecure quantum channel [1]. CVQKD using coherent states and homodyne detection is a promising protocol due to its compatibility with existing telecom equipment and high detection efficiency [2–4]. In theory, the Gaussian-modulated coherent-state (GMCS) protocol has been proven secure both in the asymptotic regime [5–7] and in the non-asymptotic regime [8–11]. In the actual implementation, such protocol has been achieved both in long distance [12, 13] and at high speed [14, 15]. Therefore, it becomes an appealing competitor for future secure quantum

Optics EXPRESS

communication.

In a practical GMCS CVQKD system, in order to implement the high-efficiency homodyne detection at Bob's side, the local oscillator (LO) needs to be transmitted from Alice to Bob, acting as a fixed phase reference for the signal detection and a filter for the wavelength division multiplexing environment. However, the transmission of the LO brings about some issues. Firstly, scattered photons from the intense LO may contaminate the signal [18], which requires a complicated hardware to separate these two components [19]. Besides, the LO is attenuated after transmission, thus the shot-noise-limited detection may not be achieved [20]. More seriously, the LO may be controlled and modified by Eve, the eavesdropper, during transmission, which may cause practical attacks, such as the LO fluctuation attack [16] and the calibration attack [17]. In order to solve these problems, referring to the classical coherent optical communication, CVQKD with a local LO is proposed and experimentally demonstrated [18–27]. Meanwhile, with the help of the phase reference, the phase drift due to the non-synchronization of two remote lasers can be recovered, so that the phase noise is reduced to ensure the key distributed properly.

In this paper, we propose a novel implementation of a fiber-based GMCS CVQKD with a local LO. By means of the simultaneously generated reference pulse, the phase drift of the quantum signal is tracked in real time and then compensated, thus the phase noise is suppressed and expected to reach the magnitude of $10^{-3}\ rad^2$. By utilizing the multiplexing techniques and meanwhile controlling the intensity of the reference pulse, not only the photons scattered from it are reduced but also a high accuracy of the phase compensation is guaranteed. Besides, a homodyne measurement, which measures one of the quadratures (X or P), is performed on the signal pulse to ensure the high quantum efficiency, and meanwhile a heterodyne measurement, which measures both quadrature values (X and P), is performed on the reference pulse to obtain the complete phase information of it. In order to suppress the excess noise, the theoretical noise model, especially the phase noise model for our scheme, is first established. Under such model, one can find that the choice of the modulation variance will be affected by the phase noise, thus we propose a method calibrating the phase noise and therefore achieve the modulation variance optimization. Besides, the excess noise will be influenced by the intensity of the reference pulse and therefore the relationship between them is experimentally measured, providing the optimal range of its intensity. Moreover, a high ratio of the shot noise and the electronic noise can be achieved by locally generated LO, which is helpful for improving the key rate. By testing the excess noise existing in our optical system based on commercial devices, it is confirmed that the secure key rate of 3.14Mbps in the asymptotic regime can be achieved over 25km standard telecom fiber, promoting the development of the high-key-rate CVQKD with a real LO.

The paper is organized as follows. In Section 2, the set-up of our experiment as well as the method of the data processing is introduced. The noise model for our scheme is established and then the crucial parameters are determined in Section 3. In Section 4, the excess noise is measured and the corresponding key rate is calculated, verifying the feasibility of the high key rate through experiments. The paper is concluded in Section 5.

2. Scheme description

2.1. Experimental set-up

We perform an experiment based on the GMCS CVQKD protocol with a local LO. The experimental setup is depicted in Fig. 1. At Alice's side, a commercial frequency-stabilized CW laser at 1542.3814 nm with a linewidth of about 150 kHz (Wavelength Reference Clarity-NLL-1542-HP) is employed as the laser source. One Lithium Niobate electro-optic amplitude modulator (EOSpace) is used to generate a pulse train with 2ns pulse width and at a repetition rate of 50MHz. Then, a 50 : 50 beamsplitter (BS) is used to split into the signal path and the reference path. In the signal path, an amplitude modulator and a phase modulator are adopted to achieve the Gaussian modulation, followed by a variable optical attenuator (VOA) to adjust to the

Optics EXPRESS

required modulation variance V_A. In the reference path, the reference pulse is delayed by a delay line so that it can be in the middle of the signal pulses in the time domain, greatly isolating it from the signal. A second VOA is used to adjust the intensity of the reference pulse. Next, these two pulses are converged by a polarizing beam collector (PBC) and then transmitted through a 25km SMF-28 fiber spool with a typical attenuation coefficient of 0.2dB/km to the receiver. At Bob's side, by adjusting the polarization controller (PC), these two pulses are separated accurately through the polarizing beamsplitter (PBS). Meanwhile, a LO is generated from another frequency-stabilized CW laser at 1542.3814 nm with a linewidth of about 150 kHz (Wavelength Reference Clarity-NLL-1542-HP) and then divided into two parts by a fiber coupler (FC) with a splitting ratio of 99 : 1. Such arrangement of the splitting ratio has two benefits: Firstly, in order to meet the requirements of the shot-noise-limited detection, a great LO power is demanded for the detection on the quantum signals, which can make the shot noise greater than the electronic noise, and also increase the key rate. Secondly, as for the reference pulse's detection, it does not need to meet the shot-noise-limited detection. Besides, a relatively small LO power can reduce the detection's shot noise, thereby enhancing the signal to noise ratio of the phase detection. Next, the large one is modulated by a phase modulator to randomly choose the measurement basis (X or P) and then interfered with the signal pulse through a BS. Two VOAs with the same length are employed to adjust the balance of the intensity, followed by a 350 MHz balanced detector (BD1, Thorlabs PDB130C) to achieve the signal detection. On the other hand, the small portion of the LO along with the reference pulse is sent to a commercial 90 degree optical hybrid (LYNIA), followed by two 350 MHz balanced detectors (BD2 and BD3, Thorlabs PDB130C) to detect both X-quadrature and P-quadrature of the reference pulse. Note, the frequency offset between the transmitter and the LO is measured by interfering with these two lasers. Through the oscilloscope, the intermediate frequency can be observed, which is around 20 MHz, implying that the frequency offset between the transmitter laser and LO is 20 MHz. This offset is far less than the detector's bandwidth, so this intermediate frequency can be detected. All the modulation signals as well as the synchronization signal are generated by an Arbitrary Waveform Generator (Tektronix AWG7122C). It is worth noting that the delay line at the signal path is used to compensate both the delay of the reference due to the time-multiplexing design and the delay of the large LO due to the inherent device length of the phase modulator, so that the reference pulse and the signal can be precisely aligned and then interfered with the same optical wavefront of the LO.

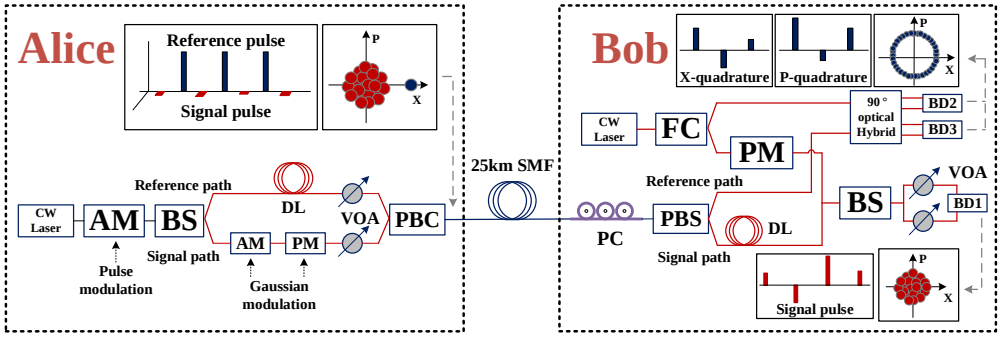

Fig. 1. **Set-up of our experiment.** CW laser: continuous-wave laser; AM: amplitude modulator; PM: phase modulator; BS: beamsplitter; DL: delay line; VOA: variable optical attenuator; PBC: polarizing beam collector; SMF: single mode fiber; PC: polarization controller; PBS: polarizing beamsplitter; FC: fiber coupler; BD: balanced detector.

Optics EXPRESS

2.2. Signal acquisition and data processing

After the signal detection, an oscilloscope with 5 GS/s sample rate is used to oversample the analog outputs from three balanced detectors. In Fig. 2(a) one can see the acquisition process for the signal pulse and the reference pulse. Since the repetition rate of the key distribution is 50 MHz, a peak or valley value of one pulse will be collected in each 100 sampling points. In the channel 1 (CH1), the peak values of the signal pulses A_i are screened out and constitute Bob's measurements of the signal $\mathbf{y} = \{y_1, y_2, y_3, \ldots, y_N\}$, where N is the total pulse number in one data block and chosen as 10^6 in our experiment. Besides, the raw data modulated on each quadratures by Alice are represented as $\mathbf{X^S} = \{X_1^S, X_2^S, X_3^S, \ldots, X_N^S\}$ and $\mathbf{P^S} = \{P_1^S, P_2^S, P_3^S, \ldots, P_N^S\}$. Meanwhile, in the channel 2 and 3 (CH2, CH3), the peak values of the reference pulses B_i and C_i are screened out as Bob's measurements of the reference and represented as the reference vectors $\mathbf{X^R} = \{X_1^R, X_2^R, X_3^R, \ldots, X_N^R\}$ and $\mathbf{P^R} = \{P_1^R, P_2^R, P_3^R, \ldots, P_N^R\}$ respectively. Note, in the CH1, the pulses D_i formed by the interference of the large LO and the leaked photons from the reference pulse may also be observed, where the leaked photons are induced by the polarization crosstalk due to the imperfection of the actual devices. The tail of these pulses may contaminate the signal pulse, thus the intensity of them should be limited to reduce such disturbance. After the data acquisition, the phase compensation of the whole block is processed, which is shown in Fig. 2(b). In our scheme, each signal pulse is accompanied by a reference pulse tracking the phase drift of itself. Therefore, one can use the reference vectors to calculate each phase drift θ_i^f as

$$\theta_i^f = \arctan\left(\frac{P_i^R}{X_i^R}\right). \tag{1}$$

Considering that Bob has only a single quadrature component due to the homodyne detection, this angle value is then transmitted to Alice through the authenticated classical channel to execute the phase compensation. That is, the raw data modulated by Alice $\mathbf{X^S}$ and $\mathbf{P^S}$ are rotated according to the corresponding θ_i^f:

$$\begin{pmatrix} X_i^{S'} \\ P_i^{S'} \end{pmatrix} = \begin{pmatrix} \cos\theta_i^f & \sin\theta_i^f \\ -\sin\theta_i^f & \cos\theta_i^f \end{pmatrix} \begin{pmatrix} X_i^S \\ P_i^S \end{pmatrix}, \tag{2}$$

where $X_i^{S'}$ and $P_i^{S'}$ constitute the first corrected vectors $\mathbf{X^{S'}}$ and $\mathbf{P^{S'}}$. The security of this process is analyzed and guaranteed [19, 20]. In brief, there is a standard assumption in CVQKD that Eve can have full knowledge of the phase reference, so the reference pulses will not give Eve any additional information and therefore sending phase-reference pulses through the quantum channel will not cause any security problem [20]. However, since the asymmetrical Mach-Zehnder interferometer (AMZI) is employed in both sides, the fluctuation of the different path will cause an unexpected phase drift θ^s [13,21]. θ^s drifts with time slowly and therefore one can compensate it by dynamic phase estimation in one block [19]. A high-precision phase compensation method in the conventional CVQKD is proposed in [13], which utilizes the cross-correlation of two sets of data to calculate the phase drift. Based on this, we propose a method of finding θ^s by traversing all angle values and then estimating it according to the cross-correlation values. That is, Bob first announces a subset $\mathbf{y'}$ which is randomly selected from the vector $\mathbf{y}$. Meanwhile, Alice takes out the corresponding subsets $\mathbf{x^0}$ and $\mathbf{p^0}$ from the first corrected vectors $\mathbf{X^{S'}}$ and $\mathbf{P^{S'}}$. Then, Alice constructs two rotated vectors $\mathbf{x}^\varphi$ and $\mathbf{p}^\varphi$ with an angle φ according to the rotation formula:

$$\begin{pmatrix} \mathbf{x}^\varphi \\ \mathbf{p}^\varphi \end{pmatrix} = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} \mathbf{x^0} \\ \mathbf{p^0} \end{pmatrix}. \tag{3}$$

Next, the measurement bases in $\mathbf{y'}$ are announced by Bob and then Alice picks out the corresponding data from $\mathbf{x}^\varphi$ and $\mathbf{p}^\varphi$ to constitute a single rotated vector $\mathbf{s}^\varphi$. Finally the cross-correlation between Alice's and Bob's data is calculated as

Optics EXPRESS

$$Cov(\mathbf{y}', \mathbf{s}^{\varphi}) = \sum_{i=1}^{m} y_i' s_i^{\varphi}, \tag{4}$$

where m is the number of the selected data pairs and chosen as 10^4 in our experiment. According to Eqs. (3) and (4), one can traverse all angle values φ in $[0, 2\pi)$ to calculate the corresponding cross-correlation. The maximal value of them is picked out and the corresponding φ is regarded as θ^s. Then, Alice executes her second phase rotation with θ^s:

$$\begin{pmatrix} \mathbf{X}^{\mathbf{S}''} \\ \mathbf{P}^{\mathbf{S}''} \end{pmatrix} = \begin{pmatrix} \cos\theta^s & \sin\theta^s \\ -\sin\theta^s & \cos\theta^s \end{pmatrix} \begin{pmatrix} \mathbf{X}^{\mathbf{S}'} \\ \mathbf{P}^{\mathbf{S}'} \end{pmatrix}, \tag{5}$$

where vectors $\mathbf{X}^{\mathbf{S}''}$ and $\mathbf{P}^{\mathbf{S}''}$ constitute the final data of Alice. Note, since those data used for estimating θ^s will eventually be discarded, the security of this process is also guaranteed. After these two compensations, Alice's and Bob's measurement bases are almost aligned. However, because of the noise in the actual situation, the estimated rotation angle may still deviate from the real phase drift, resulting in a remaining phase bias $\Delta\theta^r$, which is marked in Fig. 2(b) and will be discussed detailly in Section 3. Next, the chosen bases in the whole block are published and therefore $N - m$ couples of correlated data $\{(x_i, y_i)|i = 1, 2, \ldots, N - m\}$ are shared by Alice and Bob. Then, the parameter estimation is carried out to estimate the transmission efficiency T as well as the excess noise ε [4]. If the excess noise is low enough to guarantee the security, the corresponding secure key rate is calculated. Finally, these correlated data are processed into the information reconciliation and then the privacy amplification to generate the secure key.

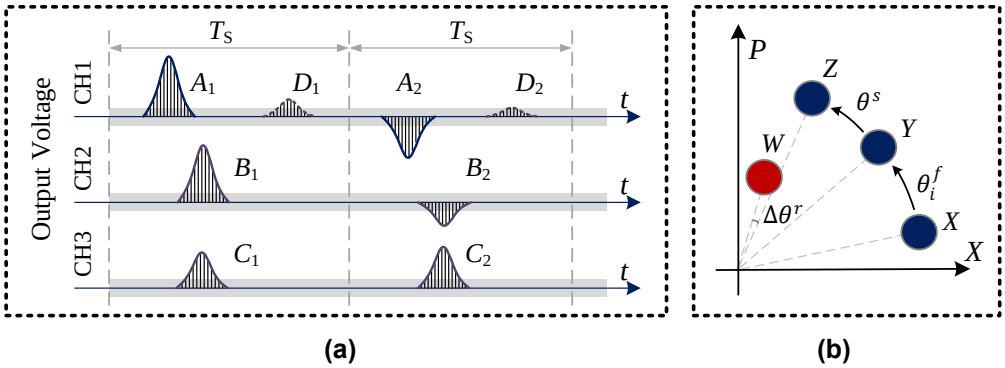

Fig. 2. (a) **Acquisition process for the signal pulses and the reference pulses.** The sample rate in each channel is 5 GS/s. Pulses A_i represent the interference results of the signal. Pulses B_i and pulses C_i represent the interference results of the reference pulse. Pulses D_i represent the interference results of the large LO and the leaked photons from the reference pulse. T_s represents the symbol time, which is 20 ns in our experiment. (b) **Phase compensation process for the signal.** Circle X represents Alice's raw data in the phase space. Circle Y represents the data after the first rotation with the angle θ_i^f. Circle Z represents the data after the second rotation with the angle θ^s. Circle W represents Bob's detection data.

3. Parameter optimization

3.1. Excess noise model

In CVQKD, controlling excess noise is a very important process, which determines the performance of the system [13, 28]. In the local-LO schemes, the noise model is different from the

conventional one. Since two different lasers are employed, the non-synchronization of them will result in a very fast phase drift. Although such drift is compensated through the phase reference, the phase bias $\Delta\theta^r$ still remains, undesirably leading to an additional noise associated with the modulation variance V_A [19–21]. It is worth noting that although this phase noise originates from QKD devices, we still consider the most pessimistic situation that it might be controlled by Eve. Therefore, the excess noise in the local-LO schemes can be modeled as

$$\varepsilon = V_A\sigma_r + \varepsilon_{rest}, \tag{6}$$

where σ_r represents the variance of the remaining phase bias $\Delta\theta^r$ following the Gaussian distribution, and ε_{rest} represents the noise that is independent with V_A, such as the reference-overlap noise, the LO fluctuation noise, and so on. The first term is a generalization of the phase noise expression for the case of small phase noise [19–21]. As for our scheme, since the phase reference and the signal as well as the corresponding LOs are simultaneously generated, which is similar to the LLO-delayline scheme [21], therefore the remaining phase noise should have come only from the phase reference's measurement errors theoretically. However, in practice, although the delay line is employed to adjust the optical path, it is still difficult to achieve the accurate alignment with the same wavefront of the LO. Different wavefronts used for measuring the signal pulse and the reference pulse are just like the LLO-sequential scheme at a very short time interval [18–20], leading to an additional phase noise σ_{misal} due to the misalignment. Specifically, in [21], the phase noise of the LLO-sequential scheme is given, that is,

$$\sigma_{misal} = var(\theta_{i+1}|\theta_i) = 2\pi(\Delta v_A + \Delta v_B)\Delta t, \tag{7}$$

where Δv_A and Δv_B is the linewidth of two lasers, and Δt is the time interval. This equation gives the accuracy requirements of the alignment in our scheme. For example, considering that the linewidth of both lasers is around 150 kHz, if σ_{misal} is expected to be less than 10^{-2} rad^2 or 10^{-3} rad^2, one can roughly infer that Δt needs to be controlled in 5.30 ns and 0.53 ns correspondingly. Besides, considering that the phase information of the reference is acquired at Bob's side, the corresponding measurement noise should also be expressed by Bob's output parameters. Therefore, the remaining phase noise can be expressed as

$$\sigma_r = \frac{N_{ch} + N_{shot} + N_{ele}}{I_{ref}} + \sigma_{misal}, \tag{8}$$

where N_{ch}, N_{shot} and N_{ele} represent the channel noise during the reference pulse's transmission, the shot noise and the electronic noise during its detection respectively (in mV^2), and I_{ref} represents the intensity of it (in mV^2). Finally, one can plug Eq. (8) into Eq. (6) yielding

$$\varepsilon = V_A \times (\frac{N_{total}}{I_{ref}} + \sigma_{misal}) + \varepsilon_{rest}, \tag{9}$$

where $N_{total} = N_{ch} + N_{shot} + N_{ele}$, and such equation totally represents the noise model for our scheme.

Optics EXPRESS

3.2. Modulation variance

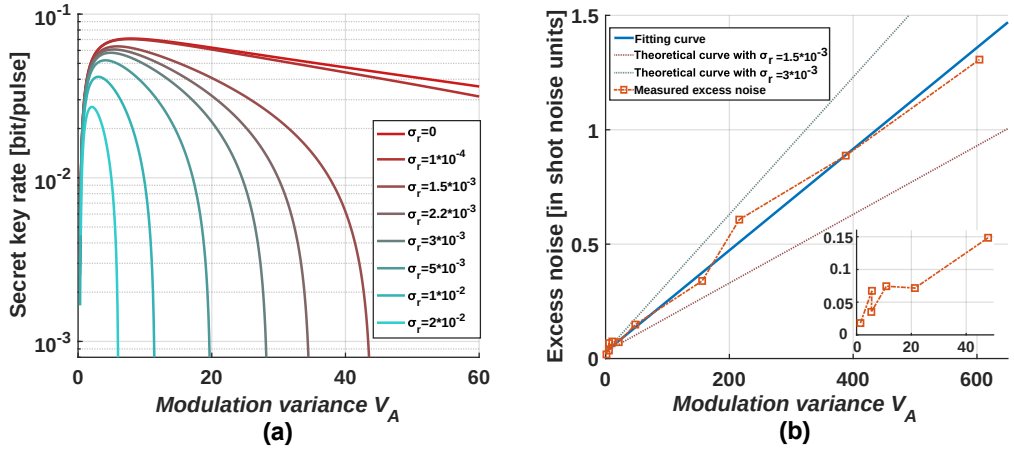

Fig. 3. (a) **Secret key rate as a function of V_A with different phase noise.** The phase noise is selected as $\sigma_r = 0, 10^{-4}, 1.5\times10^{-3}, 2.2\times10^{-3}, 3\times10^{-3}, 5\times10^{-3}, 10^{-2}, 2\times10^{-2}$ (in rad^2) respectively. Other parameters are set as: the transmission distance $L = 25$ km, the attenuation coefficient $\alpha = 0.2$ dB/km, the quantum efficiency $\eta = 0.58$, the rest noise $\varepsilon_{rest} = 0.03$, which corresponds to the intercept in Fig. 3(b), the electronic noise $v_{el} = 0.1$, and the reconciliation efficiency $\beta = 95\%$. (b) **Measured excess noise with different modulation variance.** The red squares represent the measured excess noise with a block size of 10^6, and the blue curve represents the fitting curve based on the measured data, whose slope and intercept are 2.2×10^{-3} and 0.03 respectively. Two dotted lines represent the theoretical curves with $\sigma_r = 1.5\times10^{-3}\ rad^2$ and $\sigma_r = 3\times10^{-3}\ rad^2$ respectively. The inset shows the result in the range of V_A from 0 to 50.

In the conventional CVQKD, the modulation variance V_A will influence the secure key rate. In the local-LO schemes, since the phase noise is a dominant noise, the selection of V_A also greatly affects the excess noise, which further affects the key rate and the transmission distance. Therefore, under the noise model of Eq. (6), we first simulate the key rate as a function of the modulation variance V_A with different phase noise σ_r. In Fig. 3(a), the key rate is calculated under the assumption of the collective attacks in the asymptotic regime [5]. It is clear that the value of V_A does affect the secret key rate. More importantly, the optional range as well as the optimal value of V_A will decrease with the increasing σ_r: When σ_r is $10^{-4}\ rad^2$, the maximum V_A can be larger than 60 and the optimal value is around 8, but when σ_r is $10^{-2}\ rad^2$, V_A should be less than 12 to achieve 25km key distribution, and the optimal V_A is around 3. Therefore, in order to choose the suitable modulation variance, one must first clarify the value of the phase noise σ_r, which plays an important role in the local-LO schemes.

Here we introduce a method for roughly measuring the phase noise, that is, by utilizing the linear relationship in Eq. (6) to calibrate σ_r. Specifically, one can first block the reference pulse through the VOA in the reference path at Alice's side and only send the quantum signals. Meanwhile, the electrical signals from the output of the heterodyne detector at Bob's side are collected, the variance of which is calculated as N_{total}. Then, the reference pulses are sent, and the corresponding electrical signals from the heterodyne detector are recorded as I_{ref}. In the case of maintaining the reference pulse's intensity, one can select several values of the modulation variance by adjusting the VOA and then measure the corresponding excess noise. Results are depicted in Fig. 3(b), which verifies that ε does increase with V_A. Next, we fit the curve with

Optics EXPRESS

these measured data. According to Eq. (6), the excess noise is increased mainly due to the phase noise when V_A increases, so the slope of this fitting curve is the phase noise σ_r, and the intercept represents the rest noise ε_{rest} which is independent with V_A. Therefore, due to $\sigma_r = 2.2 \times 10^{-3}$ rad^2, the optimal V_A can be determined as 5.5 according to Fig. 3(a), and a 6.08×10^{-2} bit/pulse key rate can be achieved. Furthermore, since the term $\frac{N_{total}}{I_{ref}}$ is calibrated as 1.0×10^{-3} in advance, $\sigma_{misal} = 1.2 \times 10^{-3}$ rad^2 can be solved through Eq. (8). Such phase noise is inherent in the established optical structure but fortunately small enough to meet CVQKD requirements. Note, in Fig. 3(b), the deviation between the measured noise and the fitting curve exists, which may be derived from the statistical errors due to the finite block size and the fluctuation of the employed LO, and it may further cause the phase noise measurement inaccurate. Considering these deviations, we also plot two theoretical curves with $\sigma_r = 1.5 \times 10^{-3}$ rad^2 and $\sigma_r = 3 \times 10^{-3}$ rad^2, the region between which contains all the measured data. Therefore, according to the corresponding curves in Fig. 3(a), it can be inferred that the optimal modulation variance is between 5 and 6.

3.3. Intensity of the reference pulse

In addition to the modulation variance, the intensity of the reference pulse in our scheme is also an important parameter. In the local-LO schemes, the phase reference is expected to be introduced without interfering with the quantum signal and meanwhile ensure a high accuracy of the phase compensation. Since CVQKD is sensitive with the disturbance, the time-multiplexing and polarization-multiplexing techniques are adopted to isolate the reference pulse. Even so, the interference still exists due to the polarization crosstalk, which is labeled as the reference-overlap noise. In order to suppress such interference, the intensity of the reference should be limited, but too small intensity will lead to a large phase noise and further a large excess noise according to Eq. (9). Here, we experimentally verify the relationship between the excess noise and the reference's intensity, providing the optimal parameter range of it. Specifically, we first calibrate the reference pulse's noise N_{total}. Next, we slowly adjust the intensity of the reference pulse by VOA and meanwhile record the value of I_{ref} at Bob's output. Then, the quantum signal is sent and the corresponding excess noise ε is estimated through the collected data. The experimental results are shown in Fig. 4(a). The red squares represent the measured excess noise and the blue curve represents the theoretical relationship according to Eq. (9). One can note that the measured data indeed verifies the relationship between the intensity of the reference pulse and the excess noise. However, when $\frac{I_{ref}}{N_{total}} > 10^3$, the excess noise apparently increases. This increment originates from the overlap of the reference pulse, which can also be observed on the oscilloscope. In the noise model, the reference-overlap noise will enhance ε_{rest}, but the theoretical curve is drawn with a constant ε_{rest}, so there is a deviation between the measured data and the theoretical curve. The gray line shows the upper bound of the excess noise with a 25km transmission distance, implying that the range of $\frac{I_{ref}}{N_{total}}$ should be controlled in $[5 \times 10^1, 3 \times 10^3]$. As for the optimal intensity range, the measured data implies that $\frac{I_{ref}}{N_{total}}$ is expected to be in $[4 \times 10^2, 8 \times 10^2]$.

Optics EXPRESS

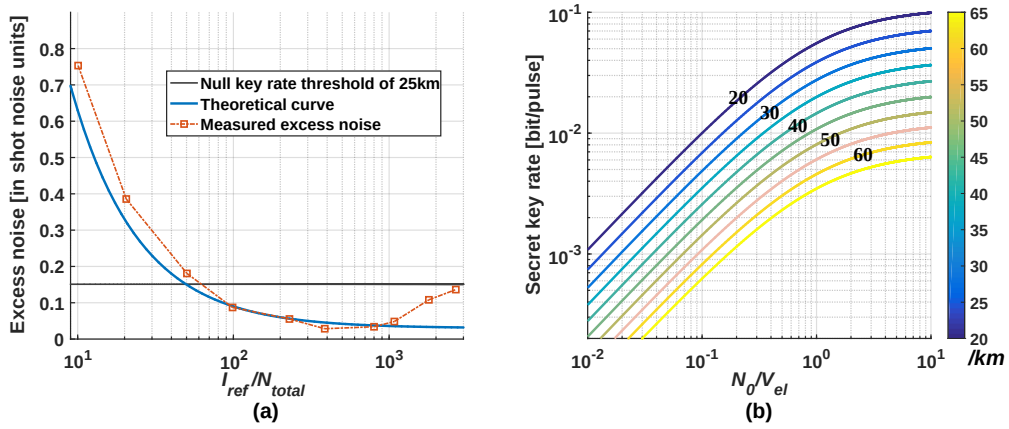

Fig. 4. (a) **Measured excess noise with different intensity of the reference pulse.** The red squares represent the measured excess noise with a block size of 10^6, and the blue curve represents the theoretical relationship between the excess noise and the ratio of I_{ref} and N_{total}. The theoretical curve is drawn according to Eq. (9) with the parameters set as $\varepsilon_{rest} = 0.03$, $V_A = 6$ and $\sigma_{misal} = 1.2 \times 10^{-3}\ rad^2$. (b) **Secret key rate as a function of N_0/V_{el} under different distance.** From top to bottom, the distance increases by 5 km from 20 km to 65 km. Other parameters are set as: the modulation variance $V_A = 6$, the attenuation coefficient $\alpha = 0.2$ dB/km, the quantum efficiency $\eta = 0.58$, the excess noise $\varepsilon = 0.03$, and the reconciliation efficiency $\beta = 95\%$.

3.4. *High ratio of the shot noise and the electronic noise*

As we all know, in CVQKD, the shot-noise-limited detection is a crucial condition to ensure the secure key generated, especially in the long distance transmission [12, 13]. For this reason, the bandwidth of the homodyne detector is always limited to suppress the electronic noise, but this operation will also limit the repetition rate of the key distribution and further reduce the total secure key rate. Considering the linear relationship between the shot noise and the intensity of LO, the shot noise will be improved by increasing the LO intensity, which can be achieved with a local LO. In particular, since the LO does not need to be transmitted through the channel, no attenuation occurs. More importantly, because the LO is no longer required for time division multiplexing, it does not need to be converted into a pulse form, so the attenuation during the pulse generation can also be avoided. In Fig. 4(b), the effect of the shot noise enhancement on the key rate at different distances is shown. One can note that the key rate will increase with N_0/V_{el} which refers to the detection of the signal. For example, within a 25 km transmission distance, if the ratio can be raised from 1 to 10, the key rate will be improved from 4×10^{-2} bit/pulse to 7×10^{-2} bit/pulse. In our experiment, a 350 MHz balanced detector and a 10 dbm continuous-wave LO are employed. Through the 200 MHz low-pass filter attached on the oscilloscope, the ratio can reach 10, that is, the electronic noise $v_{el} = 0.1$ in shot noise units. However, the bandwidth will reduce the homodyne output efficiency significantly if it is smaller than the inverse temporal width of the signal temporal mode [29], which may further lead to the short pulse attack [30]. Therefore, the quantum efficiency η is recalibrated and result shows $\eta = 0.58$ can be reached.

4. System performance

Based on the above discussion about parameter settings, the modulation variance V_A and the reference pulse's intensity $\frac{I_{ref}}{N_{total}}$ have been set as 6 and 6×10^2 respectively according to the optimal parameter range. Combined with the pre-calibrated parameters $\varepsilon_{rest} = 0.03$ and

$\sigma_{misal} = 1.2\times10^{-3}\ rad^2$, one can roughly estimate the overall excess noise ε is 0.0472 according to Eq. (9). However, such inference is not sufficient as a basis for evaluating the key rate. So after the above parameters are determined, the actual excess noise is measured in our optical system. In Fig. 5(a), each red square represents the excess noise we estimate by a data block of 10^6 and their average is 0.0408 represented by the blue line. One can note that this value is lower than our inference, which can be explained by the overestimation of ε_{rest}. These measured noise are essentially derived from the residual phase noise, the modulation noise and the quantization noise, and the fluctuation of these noise mainly comes from the fluctuation of the employed LO and the statistical noise due to the finite samples for the parameter estimation. Based on the measured noise, combined with the calibrated quantum efficiency $\eta = 0.58$, the achievable reconciliation efficiency $\beta = 95\%$ [31, 32], and the repetition rate $f_{rep} = 50$ MHz, the key rate can be evaluated. The final secure key rate definition based on the assumption of the collective attacks in the asymptotic regime is given as [5]

$$R = f_{rep} \times (\beta I_{AB} - \chi_{BE}), \tag{10}$$

where $\beta \in (0, 1)$ is the efficiency of reverse reconciliation, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo bound. Specifically, I_{AB} can be identified as

$$I_{AB} = \frac{1}{2}\log_2\frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{11}$$

where $V = V_A + 1$, and χ_{tot} representing the total noise referred to the channel input can be calculated as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T$, in which $\chi_{\text{line}} = 1/T - 1 + \varepsilon$, and $\chi_{\text{hom}} = [(1-\eta) + v_{el}]/\eta$. Besides, χ_{BE} is identified as follows

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{12}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. λ_i are symplectic eigenvalues derived from the covariance matrices and can be expressed as

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right), \\ \lambda_{3,4}^2 &= \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right), \\ \lambda_5 &= 1, \end{aligned} \tag{13}$$

where

$$\begin{aligned} A &= V^2(1-2T) + 2T + T^2(V + \chi_{\text{line}})^2, \\ B &= T^2(V\chi_{\text{line}} + 1)^2, \\ C &= \frac{V\sqrt{B} + T(V + \chi_{\text{line}}) + A\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}, \\ D &= \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}. \end{aligned} \tag{14}$$

According to the above calculation formula, the secure key rate is eventually evaluated. In Fig. 5(b), a key rate of 3.14 Mbps that can be achieved in our 25km optical fiber transmission system is marked with the red square. The realization of such a high key rate with a real LO is mainly due to the fact that the phase noise σ_r has been suppressed to the magnitude of $10^{-3}\ rad^2$, which is also achieved in [33]. Besides, the excess noise thresholds for different key rates are plotted

Optics EXPRESS

with dash lines in Fig. 5(a), and the solid curves with the same color in Fig. 5(b) represent the corresponding key rate. One can note that in order to reach a higher key rate such as 4 Mbps with the same parameters, the excess noise needs to be further suppressed to 0.0173, which has higher requirements for controlling excess noise and the stability of the system. Considering the fluctuation of LO, the real-time shot-noise measurement can be further introduced to calibrate the shot noise in real time, thus the effect of the fluctuation can be mitigated [12, 34]. Furthermore, taking into account the size of the data block, we analyze the key rate under the finite-size effect. In Fig. 5(b), following the calculations in [8], we draw the key rate curves with different data block N, of which 90% is used to extract the key and 10% is used to evaluate the parameters. It can be seen that there is no key generation at 25km when the size of block is 10^6, but the key rates of 2.18 Mbps and 2.74 Mbps can be achieved by raising the block size to 10^8 and 10^{10}. Therefore, for further improvement, three-channel synchronous analog-digital converters (ADCs) with large storage capacity are expected to be employed to obtain larger data blocks, thereby mitigating the influence of the finite-size effect and realizing the secure key rate in the non-asymptotic regime.

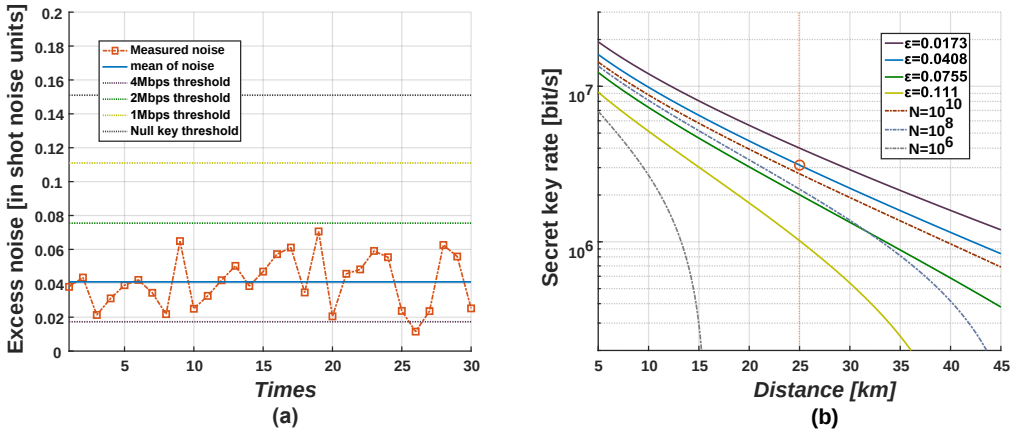

Fig. 5. (a) **Measured excess noise.** The red squares represent the measured excess noise and each of them is measured with a block size of 10^6, while the blue line represents the average value of them. Other dash lines represent the threshold of 4 Mbps, 2 Mbps, 1 Mbps and null key respectively. (b) **Secret key rate as a function of distance.** From top to bottom, the solid curves represent the achievable key rate with different excess noise, which is 0.0173, 0.0408, 0.0755 and 0.111, and corresponds to the key rate 4 Mbps, 3.14 Mbps, 2 Mbps, and 1 Mbps within a 25km distance. The red circle represents that 3.14 Mbps can be achieved by our scheme. Besides, the dash-dot curves represent the achievable key rate considering the finite-size effect with $N = 10^{10}$, $N = 10^8$ and $N = 10^6$ respectively, where 90% of the data is used to distill the key, and 10% of the data is used to parameter estimation. Other parameters are set as: the modulation variance $V_A = 6$, the quantum efficiency $\eta = 0.58$, the electronic noise $v_{el} = 0.1$, and the reconciliation efficiency $\beta = 95\%$.

5. Conclusion

In conclusion, we propose a novel implementation of CVQKD with a real LO and experimentally verify the feasibility of it. On the scheme design, with the simultaneously generated phase reference and subsequent phase compensation method, the phase drift of the quantum signal is real-time tracked and then compensated. By exploiting the multiplexing techniques and controlling the intensity of the reference pulse, the interference from it can be reduced as much as possible. Besides, we employ the homodyne detection on the signal to ensure the high quantum efficiency and the heterodyne detection on the reference pulse to acquire the complete phase

Optics EXPRESS

information of it. On the parameter settings, we first establish the noise model of this scheme. According to this model, the impacts of the modulation variance and the intensity of the reference pulse are both analysed theoretically and then optimized according to the experimental data. Finally, the excess noise is measured in such implementation with a 25 km standard optical fiber, which proves the key rate of 3.14 Mbps in the asymptotic regime could be achieved. This work verifies the feasibility of the high-key-rate CVQKD with a real LO, promoting the integration with the classic communication and the large-scale implementation.

Funding

National Natural Science Foundation of China (Grants No. 61332019, 61671287, 61631014); National Key Research and Development program (Grant No. 2016YFA0302600).