Journal of Applied Mathematics and Physics, 2019, 7, 2751-2759
https://www.scirp.org/journal/jamp
ISSN Online: 2327-4379
ISSN Print: 2327-4352

Practical Security of the Continuous-Variable Quantum Key Distribution with Locally-Generated Local Oscillators

Biao Huang[1,2,3,4,5*], Yongjun Zhu[5], Pu Tang[5], Yongmei Huang[1,2,3], Zhenming Peng[4]

[1]Key Laboratory of Optical Engineering, Chinese Academy of Sciences, Chengdu, China
[2]Institute of Optics and Electronics, Chinese Academy of Sciences, Chengdu, China
[3]University of Chinese Academy of Sciences, Beijing, China
[4]School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China
[5]Southwest Communication Institute, Chengdu, China
Email: *1002970532@qq.com

How to cite this paper: Huang, B., Zhu, Y.J., Tang, P., Huang, Y.M. and Peng, Z.M. (2019) Practical Security of the Continuous-Variable Quantum Key Distribution with Locally-Generated Local Oscillators. *Journal of Applied Mathematics and Physics*, **7**, 2751-2759.
https://doi.org/10.4236/jamp.2019.711188

Received: May 25, 2019
Accepted: November 10, 2019
Published: November 13, 2019

Abstract

Continuous-variable quantum key distribution (CVQKD) with the local local oscillator (LLO) is confronted with new security problems due to the reference pulses transmitted together with quantum signals over the insecure quantum channel. In this paper, we propose a method of phase attack on reference pulses of the LLO-CVQKD with time-multiplexing. Under this phase attack, the phase drifts of reference pulses are manipulated by eavesdroppers, and then the phase compensation error is increased. Consequently, the secret key rate is reduced due to the imperfect phase compensation for quantum signals. Based on the noise model of imperfect phase compensation, the practical security of LLO-CVQKD under phase attack is analyzed. The simulation results show that the practical security is reduced due to the phase attack, yet it is still tight when system parameters are estimated by training signals.

Keywords

Continuous-Variable Quantum Key Distribution, Local Oscillator, Reference Pulse, Practical Security, Phase Attack

1. Introduction

Continuous-variable quantum key distribution (CVQKD) allows two remote participants to establish a common key through an insecure quantum channel [1]. The CVQKD scheme using Gaussian-modulated coherent state (GMCS) is

the most favorable one due to its optimal transmission rate under the Gaussian noise channel and its excellent compatibility with the standard optical equipments [2]. So far, the GMCS scheme has been theoretically proven to be unconditionally secure against collective attacks and coherent attacks [3] [4]. Meanwhile, some experiments have demonstrated its availability over long distance [5] [6].

In the traditional GMCS-CVQKD experiments, the local oscillator (LO) needs to be transmitted from the sender Alice to the receiver Bob over the insecure quantum channel for the homodyne detection at Bob's side. However, the LO transmission brings secure issues quickly. The LO transmitted in the insecure quantum channel is most likely to be controlled and manipulated by eavesdroppers who may cause practical attacks on GMCS-CVQKD system, such as the LO fluctuation attack [7], the wavelength attack [8] and the saturation attack [9]. Although some solutions have been proposed to enhance the security of practical systems [10] [11] [12] [13], it is difficult to protect practical systems against all the potential loopholes caused by the LO transmission have been discovered.

Recently, in order to completely solve those loopholes caused by the LO transmission, several researchers adopt the local LO (LLO) scheme that the LO is generated locally at Bob's side, while the reference pulses are transmitted instead of the LO pulses to ensure the reliability of coherent detection [14] [15] [16]. The local LO is absolutely controlled by Bob so that the shot-noise-limited coherent detection becomes secure and the high-speed homodyne detection can be achieved. Moreover, the reference pulses provide phase information for Bob's coherent detection, so that the phase drift between Alice and Bob can be compensated exactly in real time. Besides, the reference pulses can be transmitted with quantum signals over the same quantum channel by time-multiplexing and polarization-multiplexing [17] [18], so that it is easy for practical systems to separate them.

However, while the issues caused by the LO transmission are eliminated in the LLO-CVQKD system, the reference pulses may open new loopholes at the same time. The role of reference pulses is to provide reliable phase information for phase compensation at Bob's side, but reference pulses are also confronted with the potential threats in the insecure quantum channel. If these reference pulses are manipulated by eavesdroppers, the phase information carried by them will become unreliable, and the phase compensation during Bob's coherent detection will become imperfect. As a result, the security of the practical LLO-CVQKD system will be reduced due to the imperfect phase compensation [19] [20].

In this paper, we present a type of phase attack on reference pulses in the LLO-CVQKD system with time-multiplexing. Under this phase attack, the phase noise of reference pulses can be easily manipulated by eavesdroppers, and then the phase compensation error is increased. The practical security of the LLO-CVQKD scheme under the phase attack is analyzed based on the noise model of imperfect phase compensation. The simulation results show that the practical security is reduced but it is still tight when the phase attack is present.

2. Theoretical Analysis

2.1. System Description

The practical LLO-CVQKD system using time-multiplexing is depicted in **Figure 1**. The sender Alice uses a commercial laser to generate a set of optical pulses, which are split by a beam splitter (BS) into the signal path and the reference path. In the signal path, the optical pulses are modulated by an amplitude modulator (AM) and a phase modulator (PM), and then the quantum signal pulses of Gaussian-modulated coherent states are generated, in which the quadratures X_A and P_A are two independent random variables with Gaussian distribution $N(0,V_A)$, where V_A denotes the modulation variance. In the reference path, the reference pulses with source phase information θ_S are delayed by a delay line and then they are multiplexed with the quantum signals in time-domain. Then, both the signal pulses and reference pulses are sent to the receiver Bob through a quantum channel with transmittance T and excess noise ε_c, where the total channel-added noise referred to the channel input is expressed in shot noise units as $\chi_{line} = 1/T - 1 + \varepsilon_c$.

At Bob's side, the received pulses are split into reference path and signal path by time-demultiplexing. In the reference path, the phase values of the reference pulses are measured by a heterodyne detector and they are used to modify the phase of LO generated locally at Bob's side. In the signal path, the quantum signals are detected by a homodyne detector with the local LO, where the phase drift is compensated, so that the quadrature X or quadrature P of a coherent state can be measured exactly according to Bob's random selection of measurement basis. For a practical homodyne detector of detection efficiency η and electronic noise variance v_{el}, the detection noise referred to Bob's input is expressed in shot noise units as $\chi_{hom} = (1+v_{el})/\eta - 1$. Thus, the total noise referred to the channel input can be expressed as $\chi_{tot} = \chi_{line} + \chi_{hom}/T$.

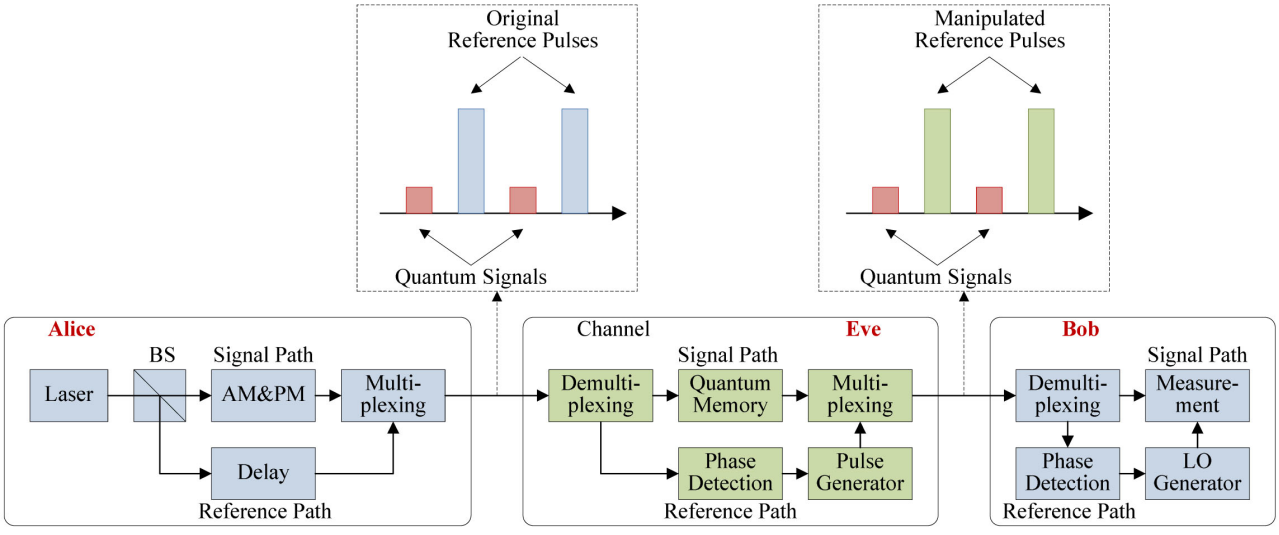

Figure 1. The phase attack on reference pulses of the LLO-CVQKD system with time-multiplexing (BS: beam splitter, LO: local oscillator).

2.2. Phase Attack

In the LLO-CVQKD system with time-multiplexing, the reference pulses are located uniformly among signal pulses, where the reference pulses and signal pulses are transmitted alternately one by one. This simple multiplexing pattern enables Bob to demultiplex the signal pulses and reference pulses precisely. While this multiplexing pattern is employed by Alice and Bob, it is reasonable to assume that the eavesdropper Eve also knows this pattern.

For the signal pulses and reference pulses transmitted into quantum channel, Eve can easily split these pluses into signal path and reference path according to the multiplexing pattern (see **Figure 1**). In the signal path, the signal pulses are stored by quantum memories for being resent later. In the reference path, the reference phase of Alice's reference pulse is measured by a phase detector, and then a forged reference pulse is produced where an additional phase noise is introduced. After being multiplexed, the signal pulses and the forged reference pulses are transmitted to Bob. At Bob's side, the phase drift of a quantum signal is estimated by the adjacent reference pulse, so that the phase compensation error can be written as:

$$\delta\theta = \theta_{drift} - \theta'_{drift} - \theta_{eve} \tag{1}$$

where θ_{drift} and θ'_{drift} are the phase drifts for a quantum signal and its following reference pulse, and θ_{eve} is the additional phase noise caused by Eve's phase attack. Assuming that the phase drifts of quantum signals can be can be compensated by reference pulses, namely $\theta_{drift} = \theta'_{drift}$, the additional phase noise is left and then it leads to the imperfect phase compensation. Furthermore, assuming that this phase noise is zero-mean and with variance V_E, the deviation of the actual phase compensation error can be given by

$$D[\delta\theta] = V_E \tag{2}$$

2.3. Security Analysis

The security analyses of the traditional GMCS-CVQKD scheme with the imperfect phase compensation have been analyzed in the existing researches [19] [20]. Here, we utilize the noise model of imperfect phase compensation for GMCS-CVQKD to analyze the practical security of LLO-CVQKD scheme.

For the LLO-CVQKD scheme with imperfect phase compensation, the Gaussian modulated coherent states are transmitted from Alice to Bob over a quantum channel with transmittance T and excess noise ε_c. At Bob's side, The phase compensation error $\delta\theta$ leads to a random phase rotation between the modulated coherent state (X_A, P_A) and the measured one (X_B, P_B). Therefore, the measurement results can be expressed as

$$X_B = \sqrt{T}(X_A \cos\delta\theta - P_A \sin\delta\theta) + W_X \tag{3}$$

$$P_B = \sqrt{T}(X_A \sin\delta\theta + P_A \cos\delta\theta) + W_P \tag{4}$$

where W_X and W_Y are Gaussian noises with variance $T\varepsilon_c$ for quadrature X

and P respectively. In the noise model of imperfect phase compensation, it is assumed that the phase compensation error $\delta\theta$ is zero-mean, so that the covariance matrix of the mixture state ρ_{AB} shared by Alice and Bob can be given by

$$\gamma_{AB} = \begin{pmatrix} V\mathbf{I}_2 & \sqrt{T_\kappa(V^2-1)}\sigma_z \\ \sqrt{T_\kappa(V^2-1)}\sigma_z & T_\kappa(V+\chi_{tot}^\kappa)\mathbf{I}_2 \end{pmatrix} \tag{5}$$

where $\mathbf{I}_2$ is a second-order identity matrix, $\sigma_z = \mathrm{diag}(1,-1)$ and $V = V_A + 1$. The parameter T_κ denotes the actual transmittance, and the parameter χ_{tot}^κ denotes the actual total noise referred to the channel input. On the one hand, due to the imperfect phase compensation, the actual transmittance can be expressed as

$$T_\kappa = \kappa T \tag{6}$$

where κ denotes the phase compensation accuracy which will be introduced in detail later. On the other hand, the actual total noise can be given by

$$\chi_{tot}^\kappa = \chi_{line}^\kappa + \chi_{hom}/T_\kappa \tag{7}$$

where $\chi_{line}^\kappa = 1/T_\kappa + \varepsilon_c^\kappa - 1$ is the actual total channel-added noise referred to the channel input, and ε_c^κ is the actual excess noise given by

$$\varepsilon_c^\kappa = [\varepsilon_c + (1-\kappa)(V-1)]/\kappa \tag{8}$$

For the CVQKD with imperfect phase compensation, the parameters T_κ and ε_c^κ are closely related to the phase compensation accuracy κ which can be expressed as

$$\kappa = (E[\cos\delta\theta])^2 \tag{9}$$

where $E[x]$ denotes the expectation of a random variable x. When the phase compensation error $\delta\theta$ is smaller than 5 degrees, the Taylor approximation $\cos x \approx 1 - x^2/2$ can be achieved, so that the phase compensation accuracy can be approximated as

$$\kappa' = (1 - \frac{1}{2}D[\delta\theta])^2 \tag{10}$$

where $D[\delta\theta]$ is the deviation of phase compensation error that has been introduced in Equation (2).

In the case of reverse reconciliation, the secret key rate of the CVQKD system under collective attack is calculated asymptotically as

$$K_R = \beta I_{AB} - \chi_{BE} \tag{11}$$

where β is the reconciliation efficiency, I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo bound that defines the maximum information available to Eve on Bob's secret information. For the homodyne detection employed by Bob, the Shannon mutual information is given by

$$I_{AB} = \frac{1}{2}\log_2\frac{V+\chi_{tot}^\kappa}{1+\chi_{tot}^\kappa} \tag{12}$$

The Holevo bound can be derived from the covariance matrix γ_{AB} shown in Equation (5) and then it is calculated as

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right) \tag{13}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and $\lambda_i (i = 1,2,...,5)$ are given by

$$\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}) \tag{14}$$

$$\lambda_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}) \tag{15}$$

$$\lambda_5 = 1 \tag{16}$$

with symbols defined as

$$A = V^2 + 2T_\kappa(1 - V^2) + T_\kappa^2(V + \chi_{line}^\kappa)^2 \tag{17}$$

$$B = T_\kappa^2(1 + V\chi_{line}^\kappa)^2 \tag{18}$$

$$C = \frac{A\chi_{hom} + V\sqrt{B} + T_\kappa(V + \chi_{line}^\kappa)}{T_\kappa(V + \chi_{line}^\kappa)} \tag{19}$$

$$D = \frac{V\sqrt{B} + B\chi_{hom}}{T_\kappa(V + \chi_{line}^\kappa)} \tag{20}$$

2.4. Parameters Estimation

For the practical LLO-CVQKD system, the actual transmittance T_κ and the actual excess noise ε_c^κ should be estimated by training signals which are randomly selected from the received quantum signals at Bob's side. It is supposed that Bob randomly selects M quantum signals for training, and then the quadrature measurements of them are denoted as $\{y_1, y_2, ..., y_M\}$. Also, the modulated quadratures of them, denoted as $\{x_1, x_2, ..., x_M\}$, are announced by Alice via a classical channel. According to the training signals, Alice and Bob would estimate the actual transmittance and the actual excess noise such as

$$\hat{T}_\kappa = \left(\frac{\sum_{i=1}^{M} x_i y_i}{\sum_{i=1}^{M} x_i^2}\right)^2 \tag{21}$$

and

$$\hat{\varepsilon}_c^\kappa = \frac{1}{M\hat{T}_\kappa}\sum_{i=1}^{M}(y_i - \sqrt{\hat{T}_\kappa}x_i)^2 \tag{22}$$

Statistically, the expectations of the estimated parameters are consistent with the theoretical ones as $E[\hat{T}_\kappa] = T_\kappa$ and $E[\hat{\varepsilon}_c^\kappa] = \varepsilon_c^\kappa$, so that the practical secret key rate for the LLO-CVQKD under collective attacks can also be calculated.

3. Simulation and Discussion

The secret key rates for the LLO-CVQKD under phase attack are shown in **Figure 2**. In the simulations, the parameters are fixed at $V_A = 18.9$, $v_{el} = 0.001$,

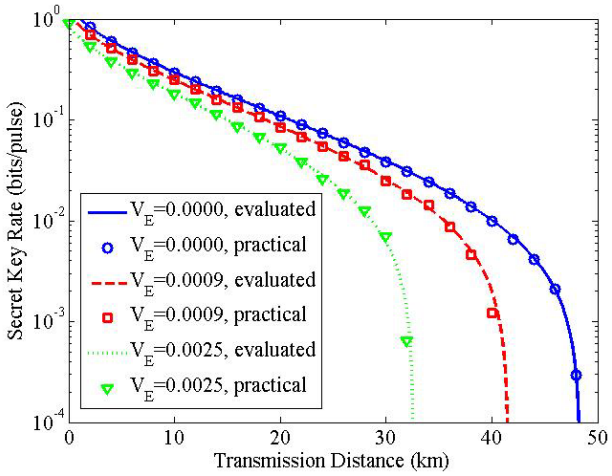

Figure 2. The secret key rates of the LLO-CVQKD system under phase attack. The phase noise variance is 0.0000, 0.0009 and 0.0025 respectively. The solid line, dash line and dotted line are the secret key rates evaluated in theory, while the circles, squares and triangles are the secret key rates estimated by 2000 training signals.

$\varepsilon_c = 0.01$ (in shot-noise units), $\beta = 0.926$ and $\eta = 0.59$, all of which are determined by the practical CVQKD experiment [19]. Besides, it is assumed that the phase noise caused by Eve's phase attack is normally distributed from $-\Phi$ to Φ degree, where Φ is given by 0, 3 and 5 degrees respectively, so that the corresponding noise variance V_E is 0.0000, 0.0009 and 0.0025 (rad^2), and then the phase compensation accuracy κ is evaluated as 1.0000, 0.9991 and 0.9975 respectively. With the noise model of imperfect phase compensation, the theoretical secret key rates of the LLO-CVQKD system under phase attack can be evaluated.

In order to confirm the validity of our security analysis, 2000 Gaussian-modulated coherent states are generated for training, all of which are added with a uniformly-distributed phase noise, and then the actual transmittance $\hat{T}_\kappa$ and the actual excess noise $\hat{\varepsilon}_c^\kappa$ are estimated by them. The practical secret key rates based on the estimated parameters are depicted by the circles, squares and triangles in **Figure 2**. By the comparison of the theoretical secret key rates and the practical ones, the security analysis of the LLO-CVQKD under phase attack is confirmed to be correct.

4. Conclusion

In this paper, we propose a method of phase attack on reference pulses of the LLO-CVQKD with time-multiplexing. The phases of reference pulses can be manipulated by eavesdroppers, and then the secret key rate is reduced because of the increased phase compensation error. The practical security of LLO-CVQKD under phase attack is analyzed based on the noise model of imperfect phase compensation. The simulation results show that the practical security is reduced due to Eve's phase attack, yet it is still tight when system parameters are estimated by training signals.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grants No. U1738204, 61571096 and 61775030) and the Foundation of Key Laboratory of Optical Engineering Chinese Academy of Sciences (Grant No. 2017LBC003). The authors thank Dr. Bingjie Xu and Dr. Heng Wang for discussion.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ralph, T.C. (2000) Continuous Variable Quantum Cryptography. *Physical Review A*, **61**, Article ID: 010303. https://doi.org/10.1103/PhysRevA.61.010303

[2] Grosshans, F., Assche, G.V., Wenger, J., Brouri, R., Cerf, N.J. and Grangier, P. (2003) Quantum Key Distribution Using Gaussian-Modulated Coherent States. *Nature*, **421**, 238-241. https://doi.org/10.1038/nature01289

[3] Leverrier, A., Grosshans, F. and, P. (2010) Finite-Size Analysis of a Continuous-Variable Quantum Key Distribution. *Physical Review A*, **81**, Article ID: 062343. https://doi.org/10.1103/PhysRevA.81.062343

[4] Leverrier, A., García-Patrón, R., Renner, R. and Cerf, N.J. (2013) Security of Continuous-Variable Quantum Key Distribution against General Attacks. *Physical Review Letters*, **110**, Article ID: 030502. https://doi.org/10.1103/PhysRevLett.110.030502

[5] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. and Diamanti, E. (2013) Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution. *Nature Photonics*, **7**, 378-381. https://doi.org/10.1038/nphoton.2013.63

[6] Huang, D., Huang, P., Lin, D.K. and Zeng, G.H. (2016) Long-Distance Continuous-Variable Quantum Key Distribution by Controlling Excess Noise. *Scientific Reports*, **6**, Article ID: 19201. https://doi.org/10.1038/srep19201

[7] Ma, X.C., Sun, S.H., Jiang, M.S. and Liang, L.M. (2013) Local Oscillator Fluctuation Opens a Loophole for Eve in Practical Continuous-Variable Quantum-Key-Distribution Systems. *Physical Review A*, **88**, Article ID: 022339. https://doi.org/10.1103/PhysRevA.88.022339

[8] Huang, J.Z., Weedbrook, C., Yin, Z.Q., Wang, S., Li, H.W., Chen, W., Guo, G.C. and Han, Z.F. (2013) Quantum Hacking of a Continuous-Variable Quantum-Key-Distribution System Using a Wavelength Attack. *Physical Review A*, **87**, Article ID: 062329. https://doi.org/10.1103/PhysRevA.87.062329

[9] Qin, H., Kumar, R. and Alléaume, R. (2016) Quantum Hacking: Saturation Attack on Practical Continuous-Variable Quantum Key Distribution. *Physical Review A*, **94**, Article ID: 012325. https://doi.org/10.1103/PhysRevA.94.012325

[10] Ma, X.C., Sun, S.H., Jiang, M.S., Gui, M., Zhou, Y.L. and Liang, L.M. (2014) Enhancement of the Security of a Practical Continuous-Variable Quantum-Key-Distribution System by Manipulating the Intensity of the Local Oscillator. *Physical Review A*, **89**, Article ID: 032310.

https://doi.org/10.1103/PhysRevA.89.032310

[11] Liu, W.Q., Peng, J.Y., Huang, P., Huang, D. and Zeng, G.H. (2017) Monitoring of Continuous-Variable Quantum Key Distribution System in Real Environment. *Optics Express*, **25**, 19429-19443. https://doi.org/10.1364/OE.25.019429

[12] Jouguet, P., Kunz-Jacques, S. and Diamanti, E. (2013) Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution. *Physical Review A*, **87**, Article ID: 062313. https://doi.org/10.1103/PhysRevA.87.062313

[13] Huang, P., Huang, J.Z., Wang, T., Li, H.S. and Huang, D. (2017) Robust Continuous-Variable Quantum Key Distribution against Practical Attacks. *Physical Review A*, **95**, Article ID: 052302. https://doi.org/10.1103/PhysRevA.95.052302

[14] Qi, B., Lougovski, P., Pooser, R., Grice, W. and Bobrek, M. (2015) Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Physical Review X*, **5**, Article ID: 041009. https://doi.org/10.1103/PhysRevX.5.041009

[15] Soh, D.B.S., Brif, C., Coles, P.J., Lütkenhaus, N., Camacho, R.M., Urayama, J. and Sarovar, M. (2015) Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. *Physical Review X*, **5**, Article ID: 041010. https://doi.org/10.1103/PhysRevX.5.041010

[16] Huang, D., Lin, D.K., Huang, P. and Zeng, G.H. (2015) High-Speed Continuous-Variable Quantum Key Distribution without Sending a Local Oscillator. *Optics Letters*, **40**, 3695-3698. https://doi.org/10.1364/OL.40.003695

[17] Wang, T., Huang, P., Zhou, Y.M., Liu, W.Q., Ma, H.X., Wang, S.Y. and Zeng, G.H. (2018) High Key Rate Continuous-Variable Quantum Key Distribution with a Real Local Oscillator. *Optics Express*, **26**, 2794-2806. https://doi.org/10.1364/OE.26.002794

[18] Wang, T., Huang, P., Zhou, Y.M., Liu, W.Q. and Zeng, G.H. (2018) Pilot-Multiplexed Continuous-Variable Quantum Key Distribution with a Real Local Oscillator. *Physical Review A*, **97**, Article ID: 012310. https://doi.org/10.1103/PhysRevA.97.012310

[19] Huang, P., Lin, D.K., Huang, D. and Zeng, G.H. (2015) Security of Continuous-Variable Quantum Key Distribution with Imperfect Phase Compensation. *International Journal of Theoretical Physics*, **54**, 2613-2622. https://doi.org/10.1007/s10773-014-2492-z

[20] Jouguet, P., Kunz-Jacques, S., Diamanti, E. and Leverrier, A. (2012) Analysis of Imperfection in Practical Continuous-Variable Quantum Key Distribution. *Physical Review A*, **86**, Article ID: 032309. https://doi.org/10.1103/PhysRevA.86.032309