photonics

MDPI

Article

Phase Compensation for Continuous Variable Quantum Key Distribution Based on Convolutional Neural Network

Zhuangzhuang Xing †, Xingqiao Li †, Xinchao Ruan, Yong Luo and Hang Zhang *

School of Automation, Central South University, Changsha 410083, China; xingzz1996@163.com (Z.X.); XingqiaoLi@csu.edu.cn (X.L.); rxc1126@csu.edu.cn (X.R.); luoxiaoyong1997@gmail.com (Y.L.)

* Correspondence: zhang22@csu.edu.cn

† These authors contributed equally to this work.

Abstract: Phase drift extremely limits the secure key rate and secure transmission distance, which is non-negligible in local oscillation continuous variable quantum key distribution (LLO CV-QKD). In order to eliminate the impact caused by phase drift, we analyze the phase noise of the system and propose a phase compensation method based on convolutional neural network (CNN). Moreover, the compensation is performed on the signal according to the estimated value of phase drift before coherent detection. In numerical simulation, we compare the performance of phase compensation methods based on CNN and Kalman filter (KF), and the results show that CNN-based phase compensation has higher accuracy and stability.

Keywords: phase compensation; phase drift; local local oscillation continuous variable quantum key distribution; convolution neural network

check for updates

Citation: Xing, Z.; Li, X.; Ruan, X.; Luo, Y.; Zhang, H. Phase Compensation for Continuous Variable Quantum Key Distribution Based on Convolutional Neural Network. *Photonics* **2022**, *9*, 463. https://doi.org/10.3390/photonics9070463

Received: 30 May 2022
Accepted: 28 June 2022
Published: 30 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Quantum key distribution (QKD) can establish a common secure key between two authenticated users over a public channel, and its unconditional security is guaranteed by the fundamental laws of quantum mechanics [1]. Continuous-variable quantum key distribution (CV-QKD) loads the key information on the quadrature of the optical field, which has the technical advantages of high key rate [2,3], convenient source preparation [4], high detection efficiency [5], and easy compatibility with existing fiber optic communication networks [6], and has attracted wide interest in the field of quantum information.

For Gaussian-modulated coherent state CV-QKD system, signal light and local oscillator (LO) light are generated by the transmitter and sent to the receiver through the same fiber channel. However, this experimental scheme has two problems in the actual system. In the actual optical fiber channel, the power of the optical pulse decreases with the transmission distance, so it is difficult to meet the detection requirements of coherent state in long-distance QKD. Additionally, eavesdropper can attack CV-QKD by controlling LO, such as the reported calibration attack [7], saturation attack [8,9], local oscillator jitter attack [10,11], which poses a threat to the security of communication systems. A feasible method is that the signal light and LO light in the system are generated by two independent lasers [12,13], and thus the security loopholes caused by LO transmission in public channel can be avoided. The subsequent problem is the phase drift caused by the frequency offset and phase jitter of the separated lasers [14].

P. Huang established a noise model of the CV-QKD system in 2015, and proposed a cross-correlation method [15] to compensate the phase of system. However, it is not applicable in LLO CV-QKD for the frequency offset between separated lasers, which causes the system phase drift quickly. To eliminate the impact of the fluctuation of LO's power on system stability, W. Liu proposed a support vector regression method [16] in 2018, aiming at compensating the LO's power through feedback control, and the power was finally controlled within a stable range. This is the first time that machine learning algorithms

have been applied to the CV-QKD system. In 2019, Y. Su proposed a phase compensation method based on Kalman filter (KF) [17], and the simulation showed that it effectively reduced the impact of phase noise on the system, which was then verified by experiments in 2021 [18].

The application of machine learning in CV-QKD is still in the preliminary stage, mainly focusing on the compensation of the non-ideal characteristics of the device [11,19,20] and the identification of attacks [21–23] in the CV-QKD system. Most studies only involve the traditional machine learning algorithm, and its effectiveness has been verified. In this paper, a compensation method based on convolutional neural network is proposed to compensate the phase drift in actual LLO CV-QKD system. Simulation results show that the CNN-based compensation method is more accurate and stable than KF-based. With the decrease of signal-to-noise ratio (SNR) in system, the performance of the KF-based method drops significantly while the CNN-based method can still maintain a relatively ideal performance.

2. Materials and Methods

2.1. Description of LLO CV-QKD

For the classical CV-QKD system, signal light and LO light are generated by the laser at the transmitter and transmitted to the receiver through time multiplexing and polarization multiplexing. In this process, attackers can obtain the secret key information by controlling LO, which threatens the security of system. By contrast, LLO CV-QKD is a more secure experimental scheme. The transmitter and receiver are equipped with separated lasers with the same central frequency. LO light is no longer transmitted through the fiber, which avoids the loopholes caused by its transmission in public channel.

Figure 1 shows the scheme of the LLO CV-QKD system based on pilot polarization multiplexing [24,25]. At the transmitter, Alice first transforms the continuous-wave light generated by laser into the optical pulse sequence with a time period of T_s. And then the optical pulse sequence is divided into signal pulse and reference pulse by BS. For signal light, Alice loads the Gaussian random number pairs (X_A, P_A) on the amplitude and phase of the signal pulse through AM and PM. After electro-optic modulation, the amplitude and phase of signal pulse are modulated to $\sqrt{X_A^2 + P_A^2}$ and $\arctan(P_A/X_A)$, respectively. Subsequently, the power attenuation of the signal pulse is carried out by OA to obtain the coherent state sequence $|X_A + iP_A\rangle$. Another optical pulse signal output by BS will be used as a reference pulse to provide phase information at the receiver. The reference pulse first delays $T_s/2$ to ensure that it is separated from the signal pulse in time, and then the reference pulse sequence with fixed amplitude is obtained through AM. Generally, the power of the reference pulse is larger than two orders of magnitude of the signal pulse, which avoids photon leakage while ensuring the SNR of the reference pulse. Then, PBC combines the signal pulse with the reference pulse and sends it to the receiver through the quantum channel.

At the receiver, Bob first demultiplexes the received optical pulse signal through PBS. The laser at the receiver will generate LO pulse sequence with a same time period of T_s, which is then divided into LO_1 and LO_2 by BS. LO_1 is first delayed by $T_s/2$ to ensure that it is aligned with the reference pulse in time. Then, the heterodyne detection of LO_1 and reference pulse is carried out after passing through the 90° mixer to obtain the measured values X_R and P_R, which is the quadrature component of reference pulse. The phase drift between LO and reference pulse is estimated based on this, and then the phase compensation of LO_2 can be performed with estimated value of phase drift. After compensation, LO_2 is used to measure the quadrature component of signal optical pulse with homodyne detection.

After that, Alice and Bob announce the partial raw key data over the public channel to estimate the key parameters of CV-QKD system, including excess noise, channel transmittance and modulation variance, and then evaluate the secure state of the system according to the estimated parameters. Follow-up processing occurs when the secure key rate exceeds the threshold, otherwise all key data will be discarded and the next round of

key distribution will be performed. In subsequent processing, Alice and Bob extract the final security secret key through the Reverse Negotiation and the Privacy Amplification to distribute the secret key between authorized users.

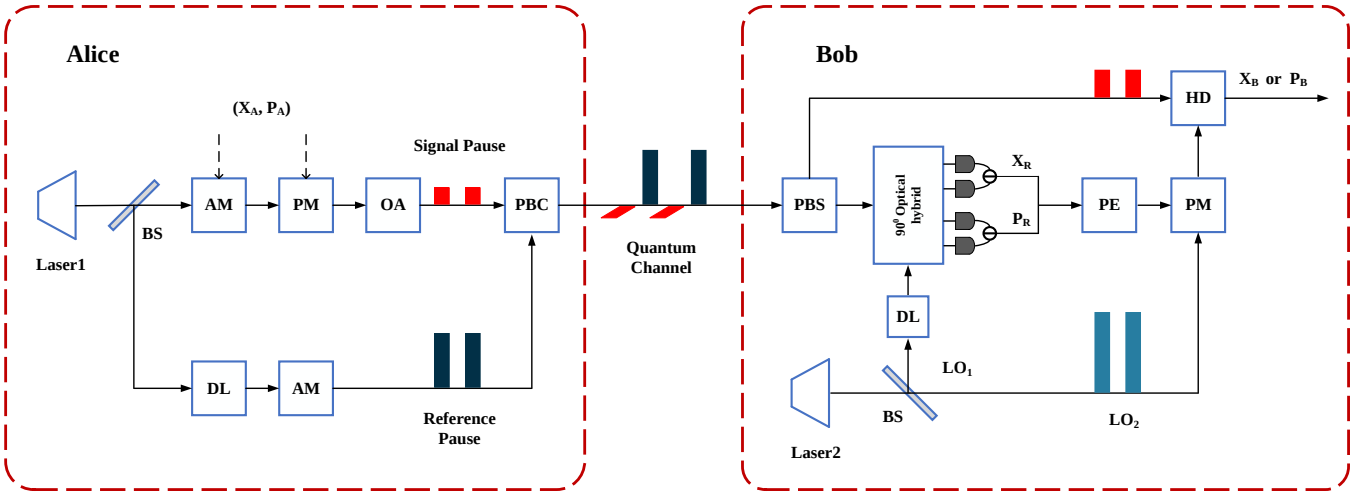


Figure 1. Illustration of LLO CV-QKD system based on pilot polarization multiplexing. BS—Beam Splitter; AM—Amplitude Modulator; PM—Phase Modulator; DL—Delay Line; OA—Optical Attenuator; PBC—Polarization Beam Combiner; PBS—Polarized Beam Splitter; LO—Local Oscillator; HD—Homodyne Detector; PE—Phase Estimation.

2.2. Analysis of Phase Noise

For LLO CV-QKD system, signal pulses and reference pulses have the same initial phase φ_0^A because they are generated by the same laser. Then the amplitude and phase of signal pulse are modulated to load the key information, assuming that the corresponding modulation phase in the pulse sequence is φ_{mod}. At the same time, in order to meet the requirements of time multiplexing, reference pulse is delayed $T_s/2$ at the transmitter and the corresponding phase delay is denoted as φ_{delay}^A. At the receiver, LO_1 and LO_2 also have the same initial phase φ_0^B. In order to extract the phase reference information of the reference pulse, it is necessary to use LO_1 to perform coherent detection of the reference pulse, so as to obtain the measured values of the quadrature component X_R and P_R. Therefore, the pulse sequence of LO_1 must also be delayed $T_s/2$ to align with the reference pulse sequence, and the corresponding phase delay is φ_{delay}^B. Therefore, the relative phase difference between the reference pulse and LO_1 is:

$$\Delta\varphi_1 = \varphi_0^A - \varphi_0^B + (\varphi_{\text{delay}}^B - \varphi_{\text{delay}}^A) \tag{1}$$

The relative phase difference between signal pulse and LO_2 is:

$$\Delta\varphi_2 = \varphi_0^A - \varphi_0^B \tag{2}$$

Ideally, the reference pulse and LO_1 are delayed by $T_s/2$ in time, and the corresponding phase delay φ_{delay}^B are equal to φ_{delay}^A. In experiment, the delay time error of the reference pulse and LO_1 can be controlled in a small range by adjusting the length of delay line at the transmitter and receiver. Therefore, it can be considered that the relative phase difference $\Delta\varphi_1$ is equal to the relative phase difference $\Delta\varphi_2$ between the signal pulse and LO_2. Under this condition, the relative phase difference $\Delta\varphi_1$ can be estimated with measured value of quadrature component of the reference pulse, and the phase compensation of LO_2 can be performed before the detection of signal pulse.

For CV-QKD experimental system, the phase of optical pulse will change with time for the non-ideal characteristics of device, which is called the phase drift. In LLO CV-QKD system, how to effectively compensate the drift is the key factor to system performance.

Since LO and signal light are generated by separated lasers, although the central frequencies of the laser at transmitter and receiver are the same, considering the frequency offset and phase jitter of the laser under actual conditions, there will be phase drift between signal light and LO light, which is called fast drift [17] ($\geq$100 ms). Moreover, the signal light and the LO transmission path have a fixed asymmetric structure, which is very sensitive to the instability of the system and can also cause phase drift, known as slow drift [26] (<100 ms). In pilot polarization multiplexing system, the relative phase difference between signal pulse and LO_2 is:

$$\Delta\varphi_2^{'} = \varphi_{fast} + \varphi_{slow} \tag{3}$$

In order to compensate the phase drift of the signal pulse, it is necessary to detect the homologous reference pulse to extract phase reference information. However, the preparation, transmission and detection of the reference pulse are affected by the system noise, including the excess noise introduced by the eavesdropper and the electrical noise of the detector. Therefore, the measurement value of the relative phase difference between the reference pulse and LO_1 is:

$$\Delta\varphi_1^{'} = \varphi_{fast} + \varphi_{slow} + \varphi_{noise} \tag{4}$$

where φ_{noise} is the phase noise of the actual system.

Due to the impact of phase noise, there is a deviation between the compensated phase drift value and real value of LO_2, which will affect the detection of the quadrature component of coherent state. The phase noise of actual CV-QKD system is denoted as $\Delta\theta$, which is shown in Figure 2. The non-ideal phase compensation process is equivalent to adding a phase shift operation $U(\Delta\theta) = \exp\left(i\Delta\theta a^{\dagger}a\right)$ to the coherent state. The measurement value of coherent state quadrature component obtained by homodyne difference detection at the receiver is [27]:

$$\begin{pmatrix} X_{\mathrm{B}}' \\ P_{\mathrm{B}}' \end{pmatrix} = \sqrt{\eta T}\left[\begin{pmatrix} \cos\Delta\theta & \sin\Delta\theta \\ -\sin\Delta\theta & \cos\Delta\theta \end{pmatrix}\begin{pmatrix} X_{\mathrm{A}} \\ P_{\mathrm{A}} \end{pmatrix} + \begin{pmatrix} X_{\mathrm{N}} \\ P_{\mathrm{N}} \end{pmatrix}\right] + \begin{pmatrix} X_{\mathrm{el}} \\ P_{\mathrm{el}} \end{pmatrix} \tag{5}$$

where η is the detection efficiency of the detector; T is the transmittance of the fiber channel; X_{N} and P_{N} are additive noise components caused by the excess noise of the system; X_{el} and P_{el} are the noise components introduced by the electrical noise of the detector. The two noise components obey the Gaussian distribution with the variance of ε_0 and v_{el}, respectively. In parameter estimation, we need to calculate the covariance $\mathrm{Cov}\left(X_{\mathrm{A}}, X_{\mathrm{B}}'\right)$ of the quadrature component sequences of Alice and Bob, where the quadrature component X is taken as an example.

$$\begin{aligned} \mathrm{Cov}\left(X_{\mathrm{A}}, X_{\mathrm{B}}'\right) &= E\left(X_{\mathrm{A}} \cdot X_{B}'\right) \\ &= E\left\{\left[\sqrt{\eta T}(\cos(\Delta\theta)X_{\mathrm{A}} + \sin(\Delta\theta)P_{\mathrm{A}}) + N\right] \cdot X_{\mathrm{A}}\right\} \\ &= \sqrt{\eta T}E[\cos(\Delta\theta)]V_{\mathrm{A}} \end{aligned} \tag{6}$$

where V_{A} is the modulation variance of Alice; N is the noise component introduced by excess noise and electrical noise. Since N is an independent noise component, there is $E(N \cdot X_{\mathrm{A}}) = 0$. Additionally, the two regular components of the coherent state are independent of each other, so $E(X_{\mathrm{A}} \cdot P_{\mathrm{A}}) = 0$.

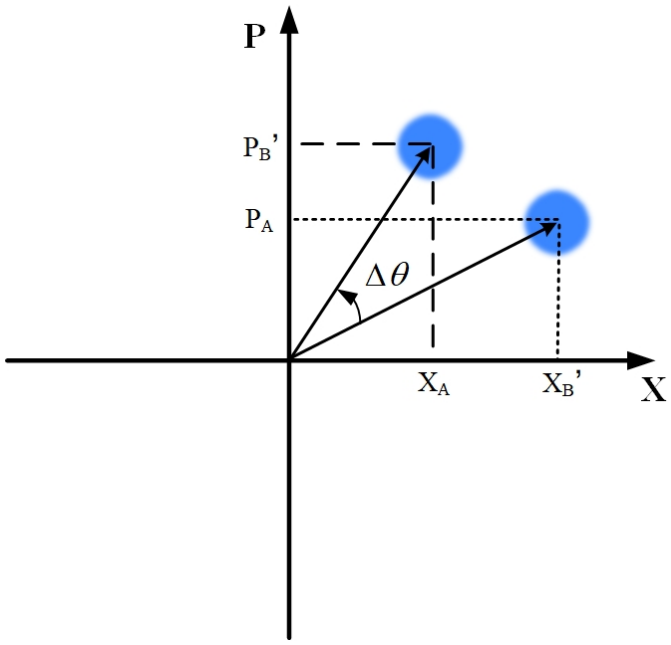


Figure 2. Diagram of influence of phase noise on quadrature component.

The estimated transmittance of optical fiber channel is given as:

$$\begin{aligned} \hat{t} &= \frac{\mathrm{Cov}(X_{\mathrm{A}}, X'_{\mathrm{B}})}{\mathrm{Var}(X_{\mathrm{A}})} \\ T' &= \hat{t}^2/\eta = \kappa T \end{aligned} \tag{7}$$

where $\kappa = E[\cos(\Delta\theta)]^2$. According to the reference [28], when $\Delta\theta$ is less than 5°, $\kappa \approx (1 - \frac{1}{2}V_{noise})^2$, where V_{noise} is the variance of phase noise. The estimated value of excess noise is calculated according to the estimated value of channel transmittance T'.

$$\begin{aligned} \hat{\sigma}^2 &= E\left[\left(X'_{\mathrm{B}} - \hat{t}X_{\mathrm{A}}\right)^2\right] \\ &= \eta T[(1-\kappa)V_A + \varepsilon_0] + 1 + v_{\mathrm{el}} \\ \varepsilon' &= (\hat{\sigma}^2 - 1 - v_{\mathrm{el}})/\hat{t}^2 \\ &= [\varepsilon_0 + (1-\kappa)V_A]/\kappa \end{aligned} \tag{8}$$

According to above equation, the excess noise caused by the non-ideal phase compensation process is $\varepsilon_{\mathrm{phase}} = (\frac{1}{\kappa} - 1)(V_A + \varepsilon_0)$. Considering that $\kappa < 1$, if phase noise $\Delta\theta \to 90°$, the excess noise $\varepsilon_{\mathrm{phase}} \to \infty$, and the excess noise of system already exceeds the secure threshold.

For the presence of phase noise, the covariance matrix of coherent states shared by Alice and Bob becomes:

$$\gamma(\Delta\theta) = \begin{bmatrix} V\mathrm{I} & \sqrt{T'(V^2-1)}\sigma_Z \\ \sqrt{T'(V^2-1)}\sigma_Z & T'\left(V + \frac{1-T'}{T'} + \varepsilon'\right)\mathrm{I} \end{bmatrix} \tag{9}$$

where $V = V_A + 1$, I is a second order unit matrix, $\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$; T' and ε' are the transmittance and excess noise under consideration of the phase noise in system.

Figure 3 shows the secure key rate of CV-QKD system under different phase noise levels. Parameters of system are from the experiment in reference [15]. The impact of phase noise on channel transmission and excess noise of system can be measured by parameter κ. The smaller κ value indicates the greater phase noise. $\kappa = 1$ indicates that the phase

difference between the signal light pulse and LO_2 is perfectly compensated. When the phase noise is zero, the secure key rate at 15 km is 0.082 bit/pulse. Additionally, when the phase noise is 4°, it decreases to 0.019 bit/pulse. The results show that the phase noise can significantly affect the secure key rate and transmission distance of the system.

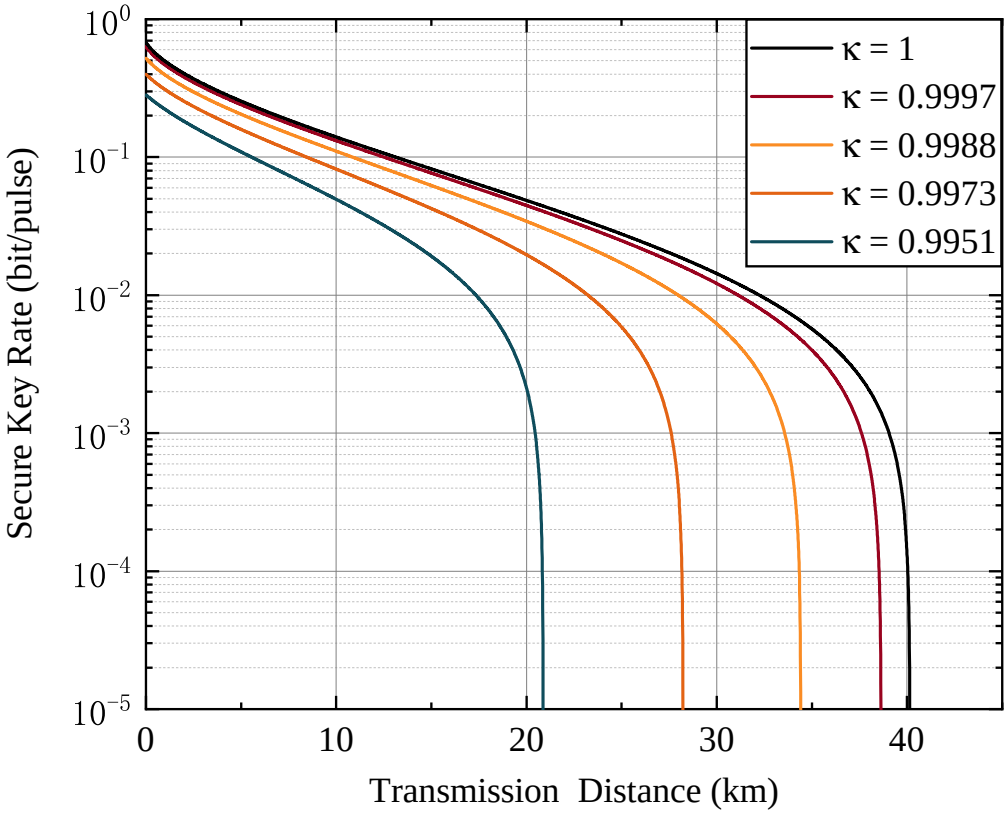


Figure 3. Secure key rate of CV-QKD system with different phase noise.

2.3. Phase Compensation Based on CNN

For LLO CV-QKD system, there is a deviation between the compensated phase drift value and the real value of LO_2 caused by phase noise, which affect the detection of the quadrature component of coherent state and the extraction of final key. There are few phase compensation methods for LLO CV-QKD nowadays, and the performance of most methods are not ideal. In initial LLO CV-QKD experiment [29], averaged phase measurement values of continuous N reference pulses are used as phase drift estimation of signal pulses. Later, some researchers proposed some phase estimation methods based on Bayesian estimation and KF [17,30,31]. The phase drift of LLO CV-QKD system is modeled as a stationary random process in traditional phase compensation methods, but actual noise cannnot be strictly described by mathematical model. Machine learning does not based on this assumption, but the data itself, which provides a new approach.

2.3.1. CNN Model

In recent years, deep learning, as one of the most rapidly developed and widely used sub-fields in machine learning, shows the data processing ability that human beings cannot reach. Deep learning can use multi-layer neural network to extract the features of input data by different layers, and realize the learning of mapping relationship between input and output data. As a typical neural network model, CNN is widely used in various tasks such as image processing [32–34], pattern recognition [35,36] and language processing [37–39].

Generally, there is an input layer, convolutional layer, pooling layer and full-connection layer in CNN.

Before the convolution operation of input data, the data is usually standardized by the input layer, which is beneficial to improve the convergence speed and final performance of training in CNN.

In the convolution layer, the convolution kernel will perform a convolution operation on the output of the upper layer, and finally the activation function will perform nonlinear activation of the output feature vectors. The output of each convolution layer is the convolution of multiple input feature vectors, which is mathematically described as [40]:

$$y_i^{l+1}(j) = \boldsymbol{K}_i^l * \boldsymbol{X}^l(j) + b_i^l \tag{10}$$

where $\boldsymbol{K}_i^l$ is weight matrix of the i-th convolution kernel of the l-th convolution layer; b_i^l is the bias vector of convolution kernel; $\boldsymbol{X}^l(j)$ is the j-th convolution field of the l-th convolution layer; the symbol $*$ represents dot product for convolution kernels and convolution fields.

After convolution, the activation function performs nonlinear operation on the output data of each convolution kernel. The nonlinear activation function is beneficial to increase the nonlinearity of the neural network model, which increases the robustness of the neural network, so as to establish a complex nonlinear mapping relationship between input data and output data. ReLU(x) = max{x, 0} is a classical activation function. When the input data is greater than 0, the derivative of the activation function is constant to 1, which is beneficial to overcome the gradient dispersion problem in the reverse propagation process. It can be expressed as:

$$a_i^{l+1}(j) = f\left(y_i^{l+1}(j)\right) = \max\left\{0, y_i^{l+1}(j)\right\} \tag{11}$$

where $y_i^{l+1}(j)$ is the output of convolution kernel; $a_i^{l+1}(j)$ is the nonlinear activation value of $y_i^{l+1}(j)$.

The pooling layer is designed to prevent the overfitting of model and reduce the amount of computation in forward propagation. The pooling layer will downsample the feature vector output from convolution layer to further extract the main information and reduce the vector dimension. In practical applications, maximum pooling, average pooling and overlapping pooling are three commonly used pooling layers. Considering the data characteristics in phase drift, the average pooling is used to downsample the feature vector, and the average value in the sensing domain is used as the output. The average pooling process can be described as:

$$P_i^{l+1}(j) = \frac{1}{W} \sum_{t=(j-1)W}^{jW} q_i^l(t) \tag{12}$$

where $q_i^l(t)$ is the value of the t-th component in the i-th feature vector of the l-th layer, $t \in [(j-1)W+1, jW]$, and W is width of the pooling layer sensing field.

The feature vector output by the last pooling layer will be expanded to a one-dimensional vector by the flatten layer, and then the predicted value of phase drift will be output by the full-connection layer. The full-connection layer can aggregate the local information of the input data extracted by the convolution layer and the pooling layer, and then output the final information.

2.3.2. Phase Compensation

For LLO CV-QKD system, the compensation of phase contains two steps. First, a phase estimation algorithm is used to estimate the value of phase drift between LO_1 and reference pulse, and then the estimated value of the phase drift is used to recover the phase of LO_2. The LO_2 after recovery will be used to measure the quadrature component of the signal optical pulse. The proposed CNN-based phase compensation method will directly

process the measured value of the quadrature component of the reference pulse to output the estimated value of the phase drift, as shown in Figure 4.

The CNN model proposed in this paper consists of an input layer, two convolution layers, two mean pooling layers and two full-connection layers. Convolution layer C1 includes 128 convolution kernels for extracting local information from input data, the size of which is 5×2. Then, the feature vector output by convolution layer C1 is down-sampled through mean pooling layer P1, and the information in the feature vector is further refined. The convolution layer C2 includes 128 convolution kernels, and the convolution kernel size is 3×2, which is then connected to the pooling layer P2. The feature vector output by the pooling layer P2 will be extended to one-dimensional vector by the flatten layer, and then the two full-connection layers aggregate the main local information extracted by the convolution layer to output the final phase drift estimation. The number of neurons in the full-connection layers are 64 and 1, respectively.

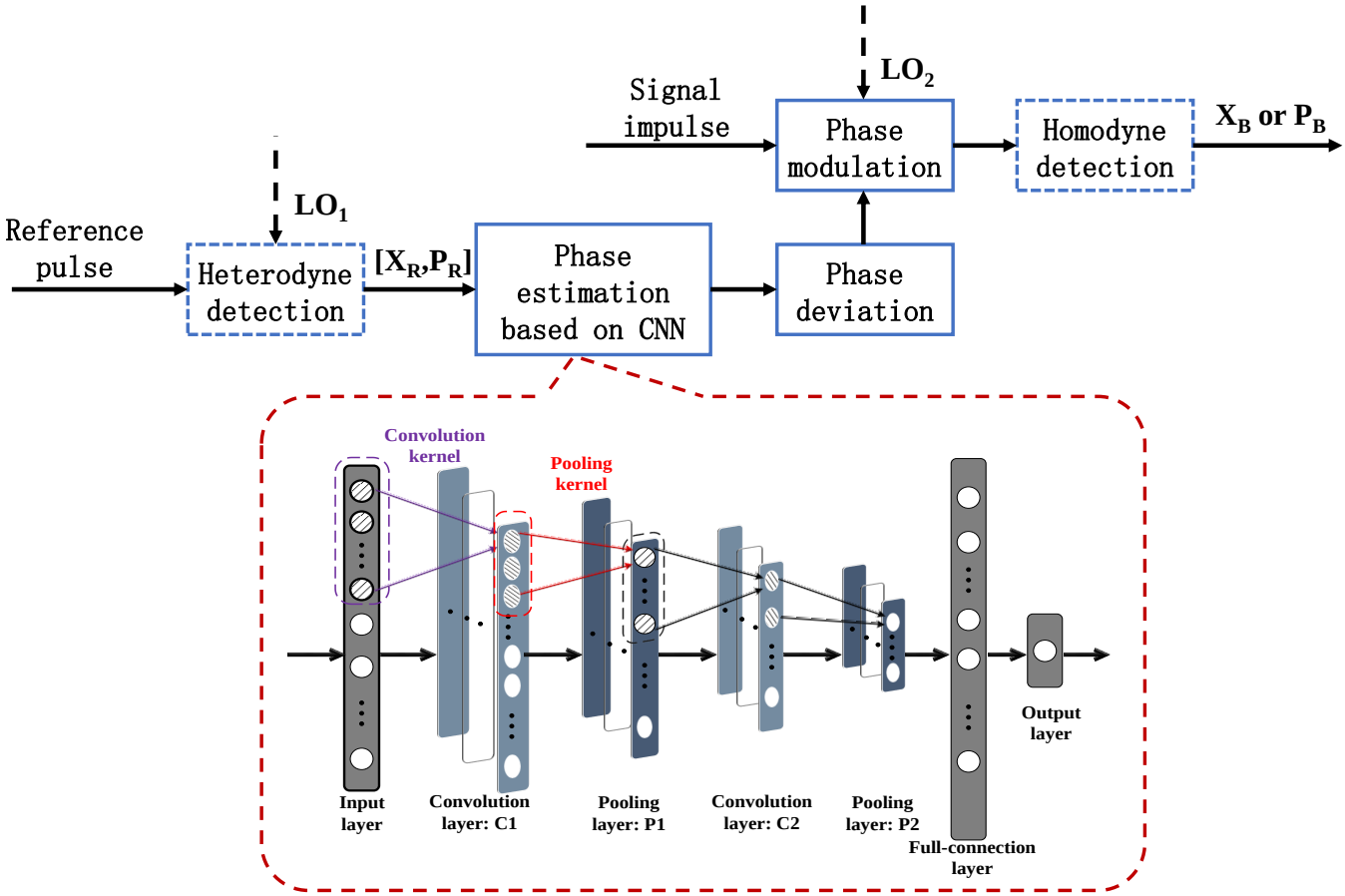


Figure 4. Phase compensation based on CNN.

The mean square error (*MSE*) loss function is used to evaluate the performance of training, which is defined as:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(\theta_i - \hat{\theta}_i)^2 \tag{13}$$

where N is the value of batch size, which is set to 600 in simulation. The above training is performed a total of 1000 epochs. The initial learning rate is set to 0.01, which decrease to one tenth of the original after 500 epochs. Figure 5 shows the change of the loss function value in training process of CNN-based phase compensation method. The loss of the training set and the verification set decreases rapidly, and tends to be stable after 500 epochs.

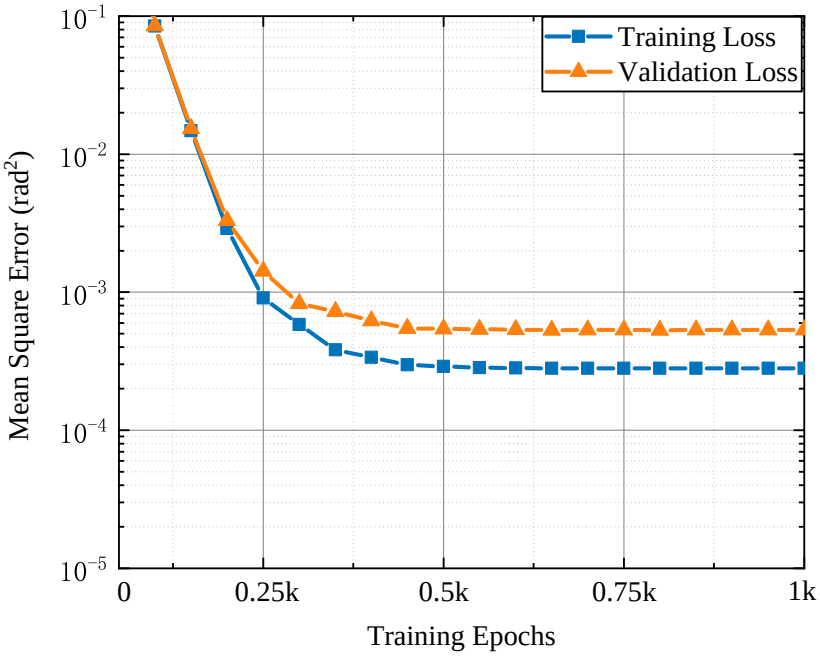


Figure 5. Loss in training of phase compensation based on CNN.

3. Results and Analysis

For LLO CV-QKD system, the compensation of phase drift consists of phase estimation and phase recovery, and the accuracy of phase estimation is the key factor to performance of compensation. According to this, we compare the results of phase estimation based on KF and CNN. The accuracy of phase estimation of KF-based method and CNN-based method are shown in Figure 6. The black scatter, measurement value of phase drift in reference pulse, uniformly distribute near the ideal phase drift curve.

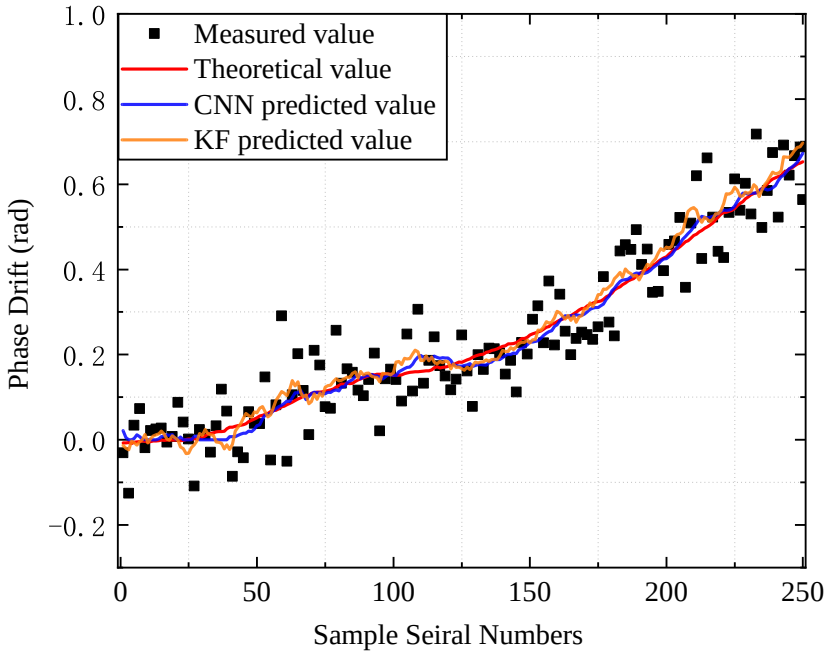


Figure 6. The prediction of phase drift based on KF and CNN.

It can be seen that the phase drift of LLO CV-QKD is a stationary random process, and the relative phase difference between LO light and signal light gradually increase with time. The excess noise caused by phase drift will exceed the safety threshold of CV-QKD

system in a period of time without effective phase compensation, and then Alice and Bob cannot extract the safe key. It can be concluded that both the phase estimation method based on KF and CNN can track the phase drift of the system, but the phase drift curve predicted by CNN is closer to the ideal phase drift curve, and the phase drift curve predicted by KF has large fluctuations in some time periods, resulting in greater phase noise than the phase estimation method based on CNN.

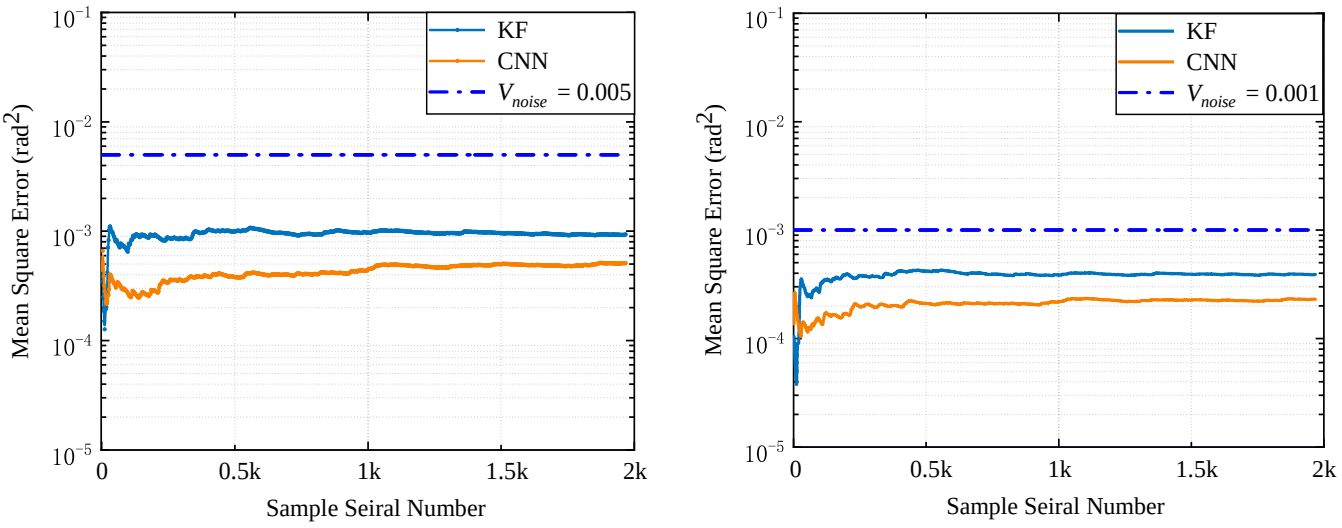
In order to compare the performance of the two methods under different *SNR*, simulation experiments are carried out under different phase noise levels. The *SNR* of LLO CV-QKD system reference pulse is defined as:

$$\sigma_v^2 = \frac{\chi_{tol} + 1}{E_R^2} \tag{14}$$

$$SNR = \frac{V_A}{\chi_{tol} + 1} = \frac{V_A}{\sigma_v^2 E_R^2} \tag{15}$$

where σ_v^2 is the variance of phase noise in the system; $E_{\mathrm{R}} = |\alpha_{\mathrm{R}}|$ is the amplitude of the reference pulse; χ_{tol} is the total noise of system, including channel noise χ_{tol} and detector noise χ_h. $\chi_{tol} = \chi_{line} + \chi_h / T$. And $\chi_{\mathrm{line}} = 1/T - 1 + \varepsilon_0$ is additive noise introduced by quantum channels and $\chi_h = [(1-\eta) + v_{el}]/\eta$ is the noise introduced by the detector.

The variance of noise σ_v^2 is 0.005 and 0.001, respectively, as shown in Figure 7a,b, and the MSE of KF-based and CNN-based phase compensation approaches is approximately stable after 150 reference pulses. In Figure 7a, the MSE of the CNN-based phase compensation method converges to 2.3×10^{-4} and the phase noise is reduced by 77%, while the MSE of the KF-based method converges to 3.894×10^{-4} and the phase noise is reduced by 61%. It can be seen from the comparison of the results that the accuracy of the CNN-based phase compensation method is better than that of the KF-based method under different SNR. Moreover, as the SNR of the system decreases, the performance of the KF-based method decreases significantly, and the CNN-based phase compensation method can still obtain ideal performance. In Figure 7b, The MSE of CNN-based method finally converges to 5.1×10^{-4}, and the phase noise is reduced by 89.8%, while the MSE of the method based on KF finally converges to 9.22×10^{-4}, and the phase noise is reduced by 81%.



(**a**) (**b**)

Figure 7. The performance of phase compensation based on KF and CNN under different variance of phase noise.

4. Conclusions

In this paper, a CNN-based method is proposed to compensate the phase drift in LLO CV-QKD system. We first analyze the phase noise in the system. According to the phase noise model, when the phase difference between the LO light and the signal light exceeds the threshold, the system will no longer generate the security key. In simulation, the phase compensation based on CNN is compared with that based on Kalman filter (KF). The results of the simulation show that the CNN-based phase compensation method has higher accuracy and stability. When the variance of phase noise is 0.001, the CNN-based phase compensation method can reduce the phase noise by 77%. When the phase noise variance is 0.005, the phase compensation method based on CNN can reduce the phase noise by 89.8%.

The analysis is based on Gaussian modulation CV-QKD protocol in this paper, and it is assumed that the coherent state sequence is transmitted in the optical fiber channel. However, in the current research on CV-QKD system, many works focus on discrete modulation CV-QKD protocols, such as four-state protocol [41,42] and eight-state protocol [43,44]. In addition, a large number of studies focus on the performance of CV-QKD in free space or underwater channels. For atmospheric and underwater channels, the communication environment is more complex and changeable, resulting in more serious nonlinear distortion effect and phase drift. More work is needed to apply the proposed machine learning based method in different environments and modulation modes.

Author Contributions: Conceptualization, Z.X., Y.L. and X.R.; methodology, Z.X., X.L. and Y.L.; software, Y.L. and X.L.; validation, Z.X., Y.L.; formal analysis, Z.X., Y.L., X.L. and X.R.; investigation, H.Z.; resources, H.Z.; data curation, Z.X. and X.L.; writing—original draft preparation, Z.X. and X.L.; writing—review and editing, Z.X., X.L. and H.Z.; visualization, Z.X. and Y.L.; supervision, X.R. and H.Z.; project administration, X.R. and H.Z.; funding acquisition, H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Natural Science Foundation of Hunan Province (Grant No. 2021JJ30878) and the Key Project of Research and Development Plan of Hunan Province (Grant No. 2020GK4063). We acknowledge the support from the Optoelectronic Information Center of Central South University and Hunan Railway Engineering Machinery Electro-hydraulic Control Engineering Technology Research Center.

Institutional Review Board Statement: "Not applicable" for studies not involving humans or animals.

Informed Consent Statement: "Not applicable" for studies not involving humans or animals.

Data Availability Statement: All data can be obtained from the authors under reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
2. Huang, D.; Lin, D.; Wang, C.; Liu, W.; Fang, S.; Peng, J.; Huang, P.; Zeng, G. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **2015**, *23*, 17511–17519. [CrossRef] [PubMed]
3. Wang, T.; Huang, P.; Zhou, Y.; Liu, W.; Ma, H.; Wang, S.; Zeng, G. High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express* **2018**, *26*, 2794–2806. [CrossRef] [PubMed]
4. Guo, Y.; Lv, G.; Zeng, G. Balancing continuous-variable quantum key distribution with source-tunable linear optics cloning machine. *Quantum Inf. Process.* **2015**, *14*, 4323–4338. [CrossRef]
5. Li, J.; Guo, Y.; Wang, X.; Xie, C.; Zhang, L.; Huang, D. Discrete-modulated continuous-variable quantum key distribution with a machine-learning-based detector. *Opt. Eng.* **2018**, *57*, 066109. [CrossRef]
6. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
7. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
8. Xu, S.; Li, Y.; Mao, Y.; Guo, Y. Counteracting a Saturation Attack in Continuous-Variable Quantum Key Distribution Using an Adjustable Optical Filter Embedded in Homodyne Detector. *Entropy* **2022**, *24*, 383. [CrossRef]

9. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef]
10. Ma, G.L. Decomposition of the jet fragmentation function in high-energy heavy-ion collisions. *Phys. Rev. C* **2013**, *88*, 021902. [CrossRef]
11. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef]
12. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **2015**, *5*, 041009. [CrossRef]
13. Soh, D.B.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **2015**, *5*, 041010. [CrossRef]
14. Juodawlkis, P.W.; Twichell, J.C.; Wasserman, J.L.; Betts, G.E.; Williamson, R.C. Measurement of mode-locked laser timing jitter by use of phase-encoded optical sampling. *Opt. Lett.* **2001**, *26*, 289–291. [CrossRef]
15. Huang, P.; Lin, D.K.; Huang, D.; Zeng, G.H. Security of continuous-variable quantum key distribution with imperfect phase compensation. *Int. J. Theor. Phys.* **2015**, *54*, 2613–2622. [CrossRef]
16. Liu, W.; Huang, P.; Peng, J.; Fan, J.; Zeng, G. Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 022316. [CrossRef]
17. Su, Y.; Guo, Y.; Huang, D. Kalman filter-based phase estimation of continuous-variable quantum key distribution without sending local oscillator. *Phys. Rev. A* **2019**, *383*, 2394–2399. [CrossRef]
18. Chin, H.M.; Jain, N.; Zibar, D. Machine learning aided carrier recovery in continuous-variable quantum key distribution. *Npj Quantum Inf.* **2021**, *7*, 20. [CrossRef]
19. Zhang, H.; Luo, Y.; Zhang, L.; Ruan, X.; Huang, D. Neural Network-Powered Nonlinear Compensation Framework for High-Speed Continuous Variable Quantum Key Distribution. *IEEE Photonics J.* **2022**, *14*, 1–8. [CrossRef]
20. Cavaliere, F.; Prati, E.; Poti, L.; Muhammad, I.; Catuogno, T. Secure quantum communication technologies and systems: From labs to markets. *Quantum Rep.* **2020**, *2*, 80–106. [CrossRef]
21. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Guo, Y.; Huang, D. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083073. [CrossRef]
22. He, Z.; Wang, Y.; Huang, D. Wavelength attack recognition based on machine learning optical spectrum analysis for the practical continuous-variable quantum key distribution system. *JOSA B* **2020**, *37*, 1689–1697. [CrossRef]
23. Mao, Y.; Wang, Y.; Huang, W.; Qin, H.; Huang, D.; Guo, Y. Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution. *Phys. Rev. A* **2020**, *101*, 062320. [CrossRef]
24. Wang, T.; Huang, P.; Zhou, Y.; Liu, W.; Zeng, G. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. *Phys. Rev. A* **2018**, *97*, 012310. [CrossRef]
25. Wang, H.; Pi, Y.; Huang, W.; Li, Y.; Shao, Y.; Yang, J.; Liu, J.; Zhang, C.; Zhang, Y.; Xu, B. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Opt. Express* **2020**, *28*, 32882–32893. [CrossRef]
26. VanWiggeren, G.D.; Roy, R. Transmission of linearly polarized light through a single-mode fiber with random fluctuations of birefringence. *Appl. Opt.* **1999**, *38*, 3888–3892. [CrossRef]
27. Biao, H.; Tiantian, M.; Yongmei, H.; Zhenming, P. Least Square Algorithm for Phase Estimation in Continuous-Variable Quantum Key Distribution. *Laser Optoelectron. Prog.* **2021**, *58*, 1127001.
28. Biao, H.; Yongmei, H.; Zhenming, P. Attack and Detectionon Reference-Pulse Phase of Continuous-Variable Quantum-Key Distribution. *Acta Opt. Sin.* **2019**, *39*, 327–333.
29. Huang, D.; Huang, P.; Lin, D.; Wang, C.; Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695–3698. [CrossRef]
30. Zhao, W.; Shi, R.; Huang, D. Practical security analysis of reference pulses for continuous-variable quantum key distribution. *Sci. Rep.* **2019**, *9*, 18155. [CrossRef]
31. Huang, B.; Huang, Y.; Peng, Z. Tracking reference phase with a Kalman filter in continuous-variable quantum key distribution. *Opt. Express* **2020**, *28*, 28727–28739. [CrossRef]
32. Liu, F.; Lin, G.; Shen, C. CRF learning with CNN features for image segmentation. *Pattern Recognit.* **2015**, *48*, 2983–2992. [CrossRef]
33. Han, F.; Yao, J.; Zhu, H.; Wang, C. Underwater image processing and object detection based on deep CNN method. *J. Sens.* **2020**, *2020*, 6707328 [CrossRef]
34. Huang, L.; He, M.; Tan, C.; Jiang, D.; Li, G.; Yu, H. Jointly network image processing: Multi-task image semantic segmentation of indoor scene based on CNN. *IET Image Process.* **2020**, *14*, 3689–3697. [CrossRef]
35. Wu, H.; Huang, Q.; Wang, D.; Gao, L. A CNN-SVM combined model for pattern recognition of knee motion using mechanomyography signals. *J. Electromyogr. Kinesiol.* **2018**, *42*, 136–142. [CrossRef]
36. Kwon, M.C.; Park, G.; Choi, S. Smartwatch user interface implementation using CNN-based gesture pattern recognition. *Sensors* **2018**, *18*, 2997. [CrossRef]
37. Yin, W.; Kann, K.; Yu, M.; Schütze, H. Comparative study of CNN and RNN for natural language processing. *arXiv* **2017**, arXiv:1702.01923.
38. Li, H. Deep learning for natural language processing: Advantages and challenges. *Natl. Sci. Rev.* **2017**, *5*, 24–26. [CrossRef]

39. Alzubaidi, L.; Zhang, J.; Humaidi, A.J.; Al-Dujaili, A.; Duan, Y.; Al-Shamma, O.; Santamaría, J.; Fadhel, M.A.; Al-Amidie, M.; Farhan, L. Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *J. Big Data* **2021**, *8*, 1–74. [CrossRef]
40. Wang, X.; Mao, D.; Li, X. Bearing fault diagnosis based on vibro-acoustic data fusion and 1D-CNN network. *Measurement* **2021**, *173*, 108518. [CrossRef]
41. Qu, Z.; Djordjevic, I.B.; Neifeld, M.A. RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection. *Opt. Lett.* **2016**, *41*, 5507–5510. [CrossRef]
42. Xu, B.; Tang, C.; Chen, H.; Zhang, W.; Zhu, F. Improving the maximum transmission distance of four-state continuous-variable quantum key distribution by using a noiseless linear amplifier. *Phys. Rev. A* **2013**, *87*, 062311. [CrossRef]
43. Djordjevic, I.B. Optimized-eight-state CV-QKD protocol outperforming Gaussian modulation based protocols. *IEEE Photonics J.* **2019**, *11*, 1–10. [CrossRef]
44. Qu, Z.; Djordjevic, I.B. Four-dimensionally multiplexed eight-state continuous-variable quantum key distribution over turbulent channels. *IEEE Photonics J.* **2017**, *9*, 1–8. [CrossRef]