Automatic phase compensation of a continuous-variable quantum-key-distribution system via deep learning

Zhe-Kun Zhang,[1] Wei-Qi Liu,[1,*] Jin Qi,[1] Chen He,[1] and Peng Huang[2,†]

[1]*School of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, People's Republic of China*

[2]*Center for Quantum Sensing and Information Processing, State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China*

(Received 5 December 2022; accepted 14 June 2023; published 30 June 2023)

In a practical continuous-variable quantum-key-distribution (CVQKD) system, it is vital to accurately evaluate and then compensate for the phase drifts of the signals, so that the involved system can achieve better performance and stability. In this paper, based on the long short-term memory network (LSTM) model, an automatic phase compensation approach of the CVQKD system is proposed. The LSTM model is first trained to predict the phase drift value of the quantum signal relative to the local oscillator over time. Then, the predicted phase drift value can be used by Alice to reconstruct her data. Finally, Alice and Bob can obtain the raw key, so that the CVQKD system can achieve enhancements in terms of performance and stability. The experimental results indicate that the proposed LSTM-based automatic phase compensation algorithm can accurately predict the phase drift value and perform phase compensation instead of real-time phase drift measurement, which improves the performance of the CVQKD system without requiring any additional quantum resources and extra experimental hardware.

DOI: 10.1103/PhysRevA.107.062614

I. INTRODUCTION

The quantum key distribution (QKD) enables two distant partners (Alice and Bob) to exchange a cryptographic key by transmitting nonorthogonal quantum states in the presence of an eavesdropper [1,2]. After receiving the quantum state, Alice and Bob perform postprocessing to generate the final key. Generally, two implementation methods of the discrete-variable quantum key distribution [3,4] and the continuous-variable quantum key distribution [5,6] are employed to distribute the secret key. Recently, both theoretical [7–16]and experimental [17–27] studies on continuous-variable quantum-key-distribution (CVQKD) systems have been extensively investigated. Among them, the well-known protocol of the CVQKD system, i.e., the Gaussian-modulated coherent state (GMCS) protocol, has been successfully demonstrated in both laboratory [28,29] and field tests [30,31]. For practical application of the GMCS protocol purpose, it is urgently necessary to adopt strategies to enhance the performance and stability of the GMCS protocol [32–37].

In order to make the practical GMCS QKD system operate stably for a long time, it must be resistant to the fluctuation of signal, birefringence, and phase drift caused by environmental variations in optical fiber. For the impact of signal fluctuations on the system, a support vector regression model is proposed to predict the intensity of the local signal and perform the feedback control [38]. For the case of the phase drift of the fiber CVQKD system, the general method is to use a strong reference signal sent by Alice, which carries a well-known phase. Bob performs heterodyne or homodyne detection of the reference signal, and then he can determine the deviation from the reference phase. The measured drift is used to readjust the phase of the quantum signal accordingly [39,40]. However, a strong reference signal will increase the complexity of the CVQKD system. Especially, under low signal-to-noise ratio (SNR) situations, the attempt to compensate for the phase drift with stronger optical signals compared with the quantum signals would compromise the practical security of the CVQKD system [39]. In addition, the main challenge in a CVQKD system with a real local oscillator is that Bob must compensate efficiently for the phase drift between two different lasers in order to perform CVQKD with a tolerable noise level [41–44].

In this paper, we propose a method utilizing a long short-term memory (LSTM) model to compensate for the phase drift in CVQKD systems due to that LSTM can well solve the long-term dependency problem of the general recurrent neural network in predicting time series. Particularly, the LSTM model is first trained to predict the evolution of phase drifts over time in a CVQKD system, and then the predicted phase values are used to compensate for the phase drift so that the secret key can be obtained by Alice and Bob. The experimental results show that the proposed LSTM model has high prediction and compensation accuracy, which significantly optimizes the performance of the CVQKD system and further makes the secret key rate greatly improved. More importantly, this method no longer requires real-time phase calculation, so the system overhead is reduced and, even at low SNR, phase compensation can be performed simply and efficiently.

The structure of this paper is as follows. In Sec. II, we investigate an LSTM model to compensate the phase drift.

*vickylwq1991@nwu.edu.cn

†huang.peng@sjtu.edu.cn

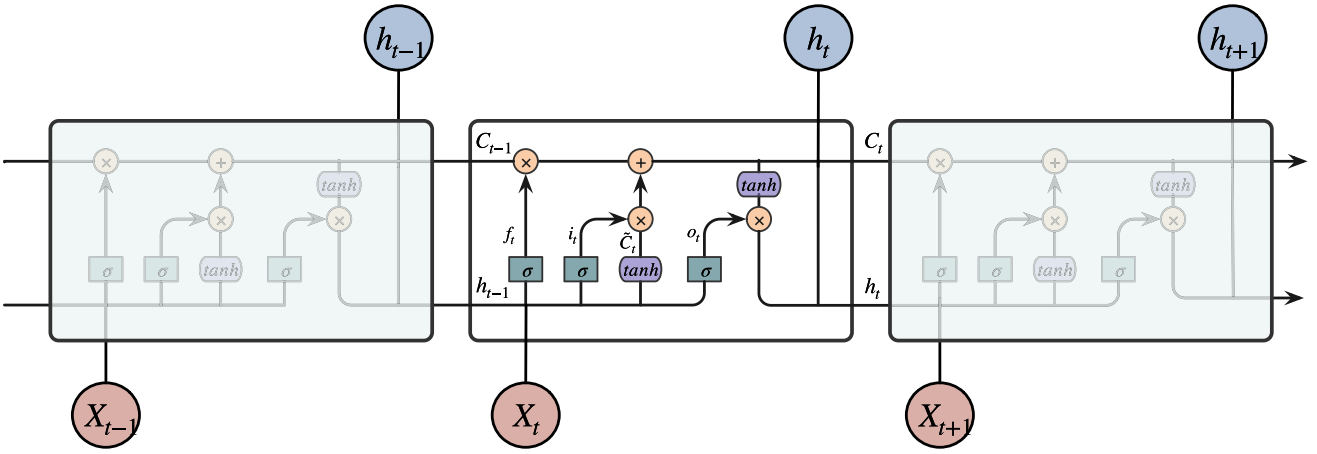


FIG. 1. Schematic diagram of the internal structure of an LSTM block

In Sec. III, we detail the source of the data and leverage a machine-learning algorithm to estimate the phase drift in CVQKD systems, further using these predictions for phase compensation. Then, the performance optimization of the LSTM-based phase compensation method for the involved CVQKD system is analyzed in Sec. IV. Finally, conclusions are drawn in Sec. V.

II. LEARNING FOR AUTOMATIC PHASE COMPENSATION IN THE CVQKD SYSTEM

To implement automatic phase compensation, we first need to train the LSTM model to predict the phase drift of the CVQKD system. The internal structure of an LSTM block is shown in Fig. 1. The cell state is responsible for conveying relevant information in the sequence chain. To be specific, the particular information is added to or removed from the cell state by different gates, i.e., the forget gate, the input gate, and the output gate. Gates are different neural networks that include sigmoid and tanh activation functions, where sigmoid takes values between 0 and 1 and helps with updating or forgetting data. As a result, the LSTM network enables one to combine the information from the previous LSTM block and the current input together to generate a newly predicted value [45–47]. Hereinafter, the updating mechanism of the cell state is briefly described.

The forget gate is responsible for selectively retaining or discarding the type of information from the previous cell state. It reads the previous output h_{t-1}, and the current input x_t goes through the synapses with certain weights W_f and biases b_f and then does a nonlinear mapping of the sigmoid activation function. The output value f_t of the forget gate can be calculated by

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f), \tag{1}$$

where σ denotes the sigmoid activation function. Afterwards, the input gate determines how much new data should be taken into the current cell state. The calculation of the input gate can be expressed by

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i). \tag{2}$$

Meanwhile, the new candidate values $\tilde{C}_t$ can be obtained by employing the hyperbolic tangent (tanh) activation function, which can be calculated by

$$\tilde{C}_t = \tanh(W_C[h_{t-1}, x_t] + b_C). \tag{3}$$

Then, with the values of the input gate and the cell candidate $\tilde{C}_t$, the previous cell state C_{t-1} can be updated to the current cell state C_t by linearly combining the input gate and the forget gate. This process can be formulated by

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t, \tag{4}$$

where $\odot$ denotes the Hadamard product. The final step is to decide the output values h_t, which can be complemented by the forget gate. The cell state C_t is passed to the tanh activation function and multiplied by the output of the sigmoid, and then the information that the current hidden state h_t should carry is obtained. This process is given by

$$\begin{aligned} o_t &= \sigma(W_o[h_{t-1}, x_t] + b_o), \\ h_t &= o_t \odot \tanh(C_t). \end{aligned} \tag{5}$$

After the model finishes training, we need to evaluate the accuracy of the algorithm in predicting future data. Here, we use the mean square error (MSE) as a performance metric of the model, which is defined as

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(Y_i - Y_i')^2, \tag{6}$$

where N is the number of samples, Y_i is the measured real value, and Y_i' represents the value, which is predicted by using the LSTM model.

III. INTEGRATING THE LSTM MODEL FOR PHASE COMPENSATION IN THE CVQKD SYSTEM

The proposed LSTM model can be used to predict the phase drift of the GMCS CVQKD system by learning from the historic data.

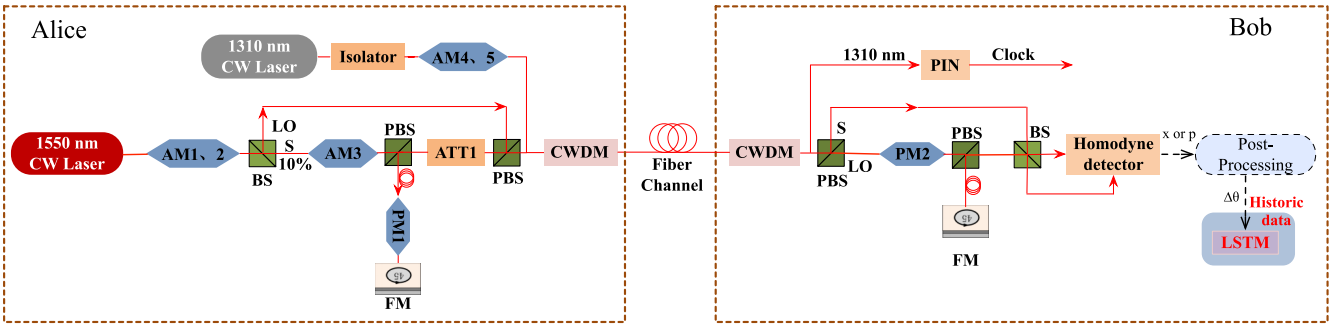


FIG. 2. The experimental setup for obtaining the training data. AM is the amplitude modulator, BS is the beam splitter, PBS is the polarization beam splitter, PM is the phase modulator, ATT is the adjustable attenuator, and CWDM means the coarse wavelength division multiplexing.

A. Preparation of historic data

In order to make the LSTM model capable of phase prediction, we first need to obtain the training data of the evolution of the phase drift. The experimental setup of the GMCS QKD system used for collecting the training data is presented in Fig. 2. At Alice's side, the continuous-wave (CW) laser with the center wavelength of 1550 nm is transformed into a pulse by using the amplitude modulators (AM). The pulse is then divided into two parts, the local oscillator (LO) and the signal (Sig) through the beam splitter (BS). In the signal path, the signal pulse passes through the Faraday mirror, the original polarization state of the pulse is rotated by 90°, and the signal pulse finally returns to the polarization beam splitter (PBS). By using the time-multiplexing and polarization-multiplexing techniques, the quantum signal will be sent to Bob through a fiber link together with a LO signal. At Bob's side, in order to develop the Mach-Zehnder interference structure, the signal pulse needs to go through the short arm and the LO pulse needs to go through the long arm. Finally, we use a shot-noise-limited homodyne detector to detect the LO pulse and the signal pulse. In addition, we use a coherent laser with a center wavelength of 1310 nm as the clock synchronization signal, and the clock synchronization signal is integrated through a coarse wavelength division multiplexer (CWDM).

Now we describe the process of collecting training data for the LSTM model to predict the evolution of the phase drift. As shown in Fig. 2, we first let the system run for a while to get some phase drift angle values as the historic data. To be specific, Alice sends the signal pulse carrying information and the LO pulse, which are transmitted through the quantum channel to Bob. Then Bob uses a homodyne detector to measure the quadrature component x or p of the received data and estimate the phase drift by the postprocessing module. We collected 1500 values of the phase drift, which are divided into the training set, the verification set, and the testing set with the lengths of 1191, 15, and 298, respectively.

B. Using the LSTM model to predict the phase drift of the system

After the LSTM is learned, we can use it to predict the phase drift value at the current and future time. Based on the aforementioned discussions, we use the collected data to train the LSTM network to obtain a predictive model. Experimentally, we design an LSTM network, which consists of three LSTM layers and four full-connection layers. The number of hidden neurons in the LSTM layers is 100, and the input size and the output size are both 1. After the optimization procedure, we choose the initial learning rate as 0.01, the batch size is set to 64, and the above training is iterated 1000 epochs in total. To illustrate the performance of our proposed LSTM model, the variation of training loss and validation loss during the training process is shown in Fig. 3. As shown, the losses in the training and validation sets drop rapidly and eventually stabilize at very low levels, which means that the constructed model has been well trained.

Moreover, in order to further clarify the prediction performance of the proposed LSTM model, we respectively draw the variations of phase estimation results in different cases, as shown in Figs. 4(a)–4(d). Figures 4(a) and 4(b) are the prediction results using the training set and the testing set when the frame length of the system in order to obtain values of the phase drift is 2000 points. Figures 4(c) and 4(d) are the results using the training set and the testing set when the frame length is 3000 points (after 4 h of operation). The results show that the predicted data via the predictive model are similar to the practical measured values. Moreover, when measuring per 2000 points, we calculated that the prediction MSE of the

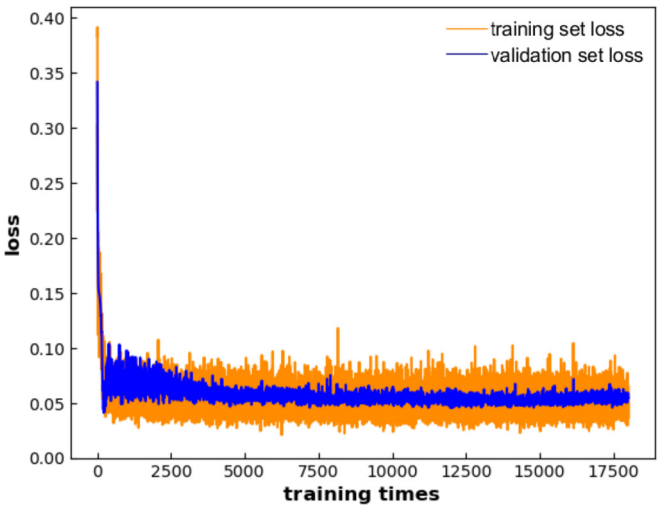
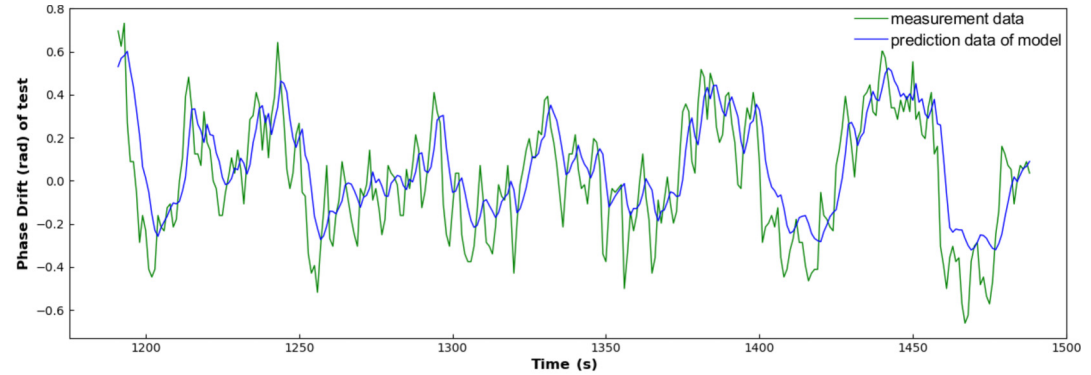
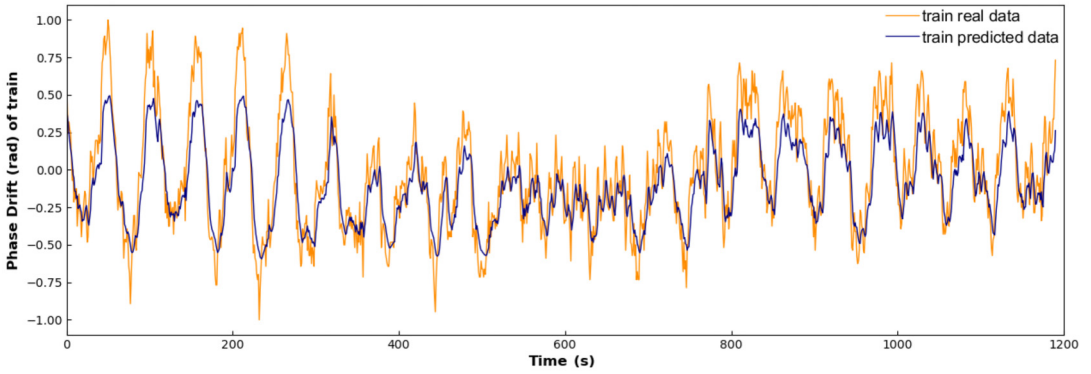


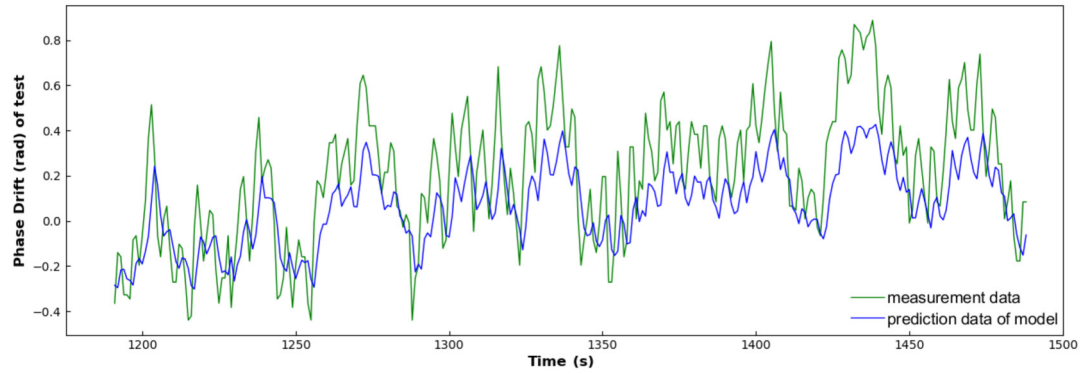
FIG. 3. Loss function value during the training of the LSTM.



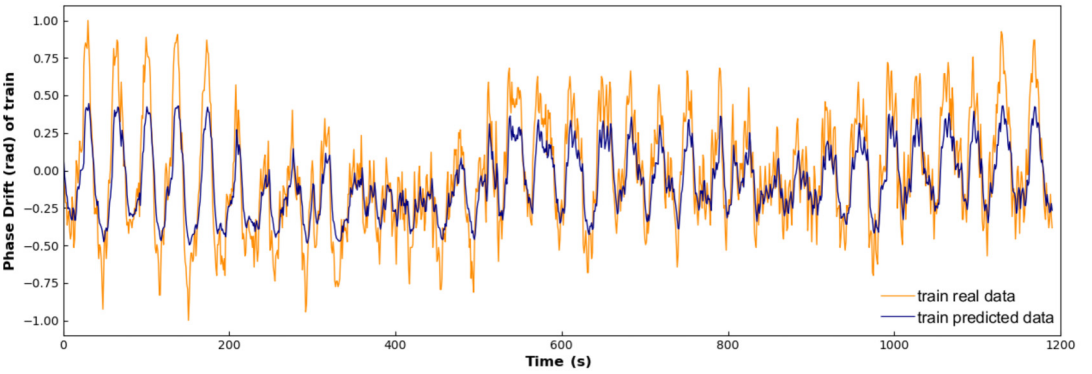
(a)



(b)



(c)



(d)

FIG. 4. The variations of prediction results of the phase drift. Panel (a) shows the performance of the LSTM model with the testing set when the phase value is measured in a 2000-point frame length, and panel (b) shows the performance of the LSTM model with the training set at the same measurement length. Panel (c) shows the performance of the LSTM model with the testing set when the phase value is measured in a 3000-point frame length, and panel (d) shows the performance of the LSTM model with the training set at the same measurement length.

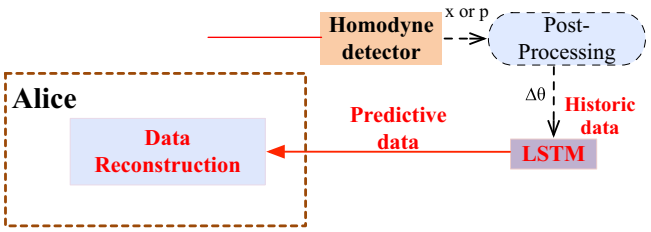


FIG. 5. Schematic setup of the phase compensation module.

training data is 2.91×10^{-5}, and the MSE of the testing data is 1.06×10^{-4}. As for measuring per 3000 points, the prediction MSE of the training data is 3.96×10^{-5}, and the MSE of the testing data is 1.26×10^{-4}.

It should be noted that, with the changes of environment, the proposed model will be updated to better predict the next time period with an off-line updating mechanism, and the latest monitoring data will be input into the training set to update the neural network model. Particularly, when drastic changes occur in the environment, resulting in a large average error of the data of the previous and the later time steps, we will update the training data set with the newly measured phase value, retrain, and predict.

C. Learning to compensate the phase drift

In the previous subsections, we have applied the LSTM model for phase prediction. Here, we further use the predicted values for the compensation of the CVQKD system, thereby ensuring the stable operation of the involved CVQKD system and optimizing the system performance. This process is simple and can decrease the system overhead. Figure 5 shows the schematic setup of the automatic phase compensation module. The process consists of the following two steps: First, Bob obtains the predicted values of the phase drifts in the CVQKD system via the LSTM model, and then he sends such predicted values to Alice, which can be used by Alice to reconstruct her data. This approach can guarantee the practical security of the involved system, but requires neither extra experimental hardware nor additional quantum resources. Moreover, it can avoid the problem that the increase of inaccuracy of phase compensation at low SNR can inevitably result in a higher level of the excess noise. The effect of the proposed approach on improving the performance of the CVQKD system is discussed in detail in the next section.

IV. THE PERFORMANCE OPTIMIZATION USING THE LSTM-BASED AUTOMATIC PHASE COMPENSATION

To evaluate the performance of the automatic phase compensation module in improving the performance of the CVQKD system, the secret key rate of the involved system needs to be analyzed.

The compensation accuracy is directly related to the estimation accuracy of the phase drift; therefore, the prediction accuracy of the model is very important. To demonstrate clearly the effect of the predictive model, it is vital to evaluate the excess noise $\varepsilon_{\text{phase}}$, induced by the phase drifts of the involved system. Assuming that the modulation variance is V_A, the phase noise due to the inaccuracy of the phase compensation can be given by

$$\varepsilon_{\text{phase}} = \left(\frac{1}{\kappa} - 1\right)(V_A + \varepsilon_0), \tag{7}$$

where ε_0 is the excess noise of the system, and $\kappa = (E[\cos \Delta\theta])^2$, with $\Delta\theta = \theta' - \theta$ (θ is the real value of the phase drift of the system and θ' represents the value of the phase drift given by the phase compensation algorithm).

When the phase noise $\Delta\theta$ is small, we obtain

$$\kappa = (E[1 - (\Delta\theta)^2/2])^2 = \left(1 - \frac{1}{2}V_p\right)^2, \tag{8}$$

where V_p is the variance of the remaining phase noise. The impact of the phase noise on the system can be measured by the parameter κ. When κ is smaller, it means that the phase noise is larger [40].

In the CVQKD system, the relationship between Alice and Bob is given by

$$y = tx + z, \tag{9}$$

where x and y are two correlated vectors $x = \{x_1, x_2, \ldots, x_N\}$ and $y = \{y_1, y_2, \ldots, y_N\}$, shared by Alice and Bob (N depicts the sum of the number of the received pulses). $t = \sqrt{\eta T}$ is related to the transmittance of the quantum channel, and z is the noise term whose variance $\sigma^2 = \eta T \varepsilon_0 + N_0 + V_{\text{el}}$ follows a central normal distribution. The involved N_0 is the variance of the shot noise, η represents the efficiency of the homodyne detector, T is the transmittance of the quantum channel, and V_{el} is the electronic noise of the detector. Moreover, when we evaluate the secret key rate of the CVQKD system, all parameters should be expressed in shot noise units.

In the case of considering the phase noise in the system, $T' = \kappa T$, $t' = \sqrt{\eta T'} = \sqrt{\eta \kappa T}$, and the total excess noise is ε, namely, $\varepsilon = \varepsilon_{\text{phase}} + \varepsilon_0$. Hence, the variance of the excess noise σ'^2 can be written as

$$\begin{aligned} \sigma'^2 &= \eta T' \varepsilon + N_0 + V_{\text{el}} \\ &= \eta T[(1 - \kappa)V_A + \varepsilon_0] + N_0 + V_{\text{el}}. \end{aligned} \tag{10}$$

Then, the information shared by Alice and Bob and the maximum amount of information available to the eavesdropper can be calculated. According to Refs. [48,49], the equation used to calculate the key rate between Alice and Bob is

$$K = \frac{n}{N}[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{11}$$

where $n = N - m$, n represents the data volume length used for generating the final key, m represents the data volume length used for the parameter estimation procedure, and $\beta \in (0, 1)$ is the efficiency of reverse reconciliation. I_{AB} is the Shannon mutual information between Alice and Bob. χ_{BE} represents the maximum amount of information that Eve can obtain, limited by the number of Holevos. In addition, $\Delta(n)$ is related to confidentiality enhancement, which is a linear function of n.

By calculating Bob's measured variance V_B and conditional variance $V_{B|A}$, we can obtain the mutual information I_{AB} as

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \tag{12}$$

Here, $V = V_A + 1$, the total noise referred to the channel input can be expressed as $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T'$, in which $\chi_{\text{line}} = (1/T') - 1 + \varepsilon$ and $\chi_h = [(1 + V_{\text{el}})/\eta] - 1$ represents a homodyne detection added noise referred to Bob's input.

The maximum information obtain by Eve from Bob, χ_{BE}, can be expressed as

$$\chi_{BE} = S(\rho_E) - \int dm_B p(m_B) S\left(\rho_E^{m_B}\right), \tag{13}$$

where m_B represents the measurement result of Bob, $p(m_B)$ represents the probability density of the measurement, $\rho_E^{m_B}$ represents the state of Eve under Bob's measurement conditions, and $S(\rho)$ is the von Neumann entropy of the quantum state ρ.

Since Bob's measurement can purify the system ρ_{AEFG} and Eve's eavesdropping can purify the system ρ_{AB_1}, for Gaussian-modulated coherent states, $S(\rho_{AFG}^{m_B})$ does not depend on Bob's measurement m_B, so χ_{BE} takes the form

$$\begin{aligned}\chi_{BE} &= S(\rho_{AB_1}) - S\left(\rho_{AFG}^{m_B}\right) \\ &= \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right),\end{aligned} \tag{14}$$

among which $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix γ_{AB_1} that characterize the quantum state ρ_{AB_1}. $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{AFG}^{m_B}$ that characterize the quantum state $\rho_{AFG}^{m_B}$.

By taking the finite-size effect into account [48,49], the covariance matrix ρ_{AB_1} of the Gaussian modulation protocol can be expressed in the following form:

$$\Gamma_{AB} = \begin{bmatrix} (V_A + 1)\text{II}_2 & \sqrt{T'_{\min}\left(V_A^2 + 2V_A\right)}\sigma_z \\ \sqrt{T'_{\min}\left(V_A^2 + 2V_A\right)}\sigma_z & [T'_{\min}(V_A + \varepsilon_{\max}) + 1]\text{II}_2 \end{bmatrix}, \tag{15}$$

where the matrices $\text{II}_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $\sigma_z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. $T'_{\min}$ is the minimum value of transmittance, and $\varepsilon_{\max}$ represents the maximum value of the excess noise. They can be calculated by

$$\begin{aligned} T'_{\min} &= (t'_{\min})^2, \\ \varepsilon_{\max} &= \frac{\sigma'^2_{\max} - 1}{T'}. \end{aligned} \tag{16}$$

When m is large enough, $t'_{\min}$ and $\sigma_{\max}$ can be approximately calculated by

$$\begin{aligned} t'_{\min} &\approx \sqrt{T'} - z_{\epsilon_{\text{PE}}/2}\sqrt{\frac{1 + T'\varepsilon}{mV_A}}, \\ sigma'_{\max} &\approx 1 + T'\varepsilon + z_{\epsilon_{\text{PE}}/2}\frac{(1 + T'\varepsilon)\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{17}$$

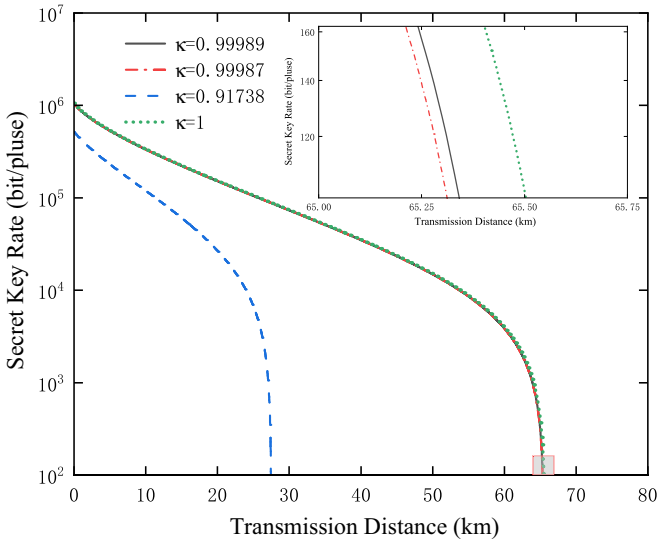


FIG. 6. Secret key rate of the CVQKD system in different cases. The curves from top to bottom represent the secret key rates in the perfect situation (dotted green line, $\kappa = 1$), in the situations with our proposed approach based on the LSTM model (solid gray line, $\kappa = 0.999\,89$ and dot-dashed red line, $\kappa = 0.999\,87$), and in the practical situation without compensation (dashed blue line, $\kappa = 0.917\,38$), respectively. The parameters are fixed in simulation to the values $V_A = 4$, $\eta = 0.95$, $\varepsilon = 0.02$ (in shot noise units) $\beta = 0.926$, and $V_{\text{el}} = 0.001$ (in shot noise units)

where $z_{\epsilon_{\text{PE}}/2}$ can be computed as

$$1 - \frac{1}{2}\,\text{erf}\left(\frac{z_{\epsilon_{\text{PE}}/2}}{\sqrt{2}}\right) = \frac{1}{2}\epsilon_{\text{PE}}, \tag{18}$$

and the error function $\text{erf}(\cdot)$ is defined by

$$\text{erf}(x) = 2\pi^{-1/2}\int_0^x e^{-t^2}dt. \tag{19}$$

Hence, symplectic eigenvalues λ_i are given by

$$\begin{aligned} \lambda_{1,2}^2 &= \tfrac{1}{2}[A \pm \sqrt{A^2 - 4B}], \\ \lambda_{3,4}^2 &= \tfrac{1}{2}[C \pm \sqrt{C^2 - 4D}], \\ \lambda_5 &= 1, \end{aligned} \tag{20}$$

with the following parameters:

$$\begin{aligned} A &= (V_A + 1)^2 - 2T'_{\min}\left(V_A^2 + 2V_A\right) + [T'_{\min}(V_A + \varepsilon_{\max}) + 1]^2, \\ B &= [(T'_{\min}\varepsilon_{\max} + 1)(V_A + 1) - T'_{\min}V_A]^2, \\ C &= \frac{A(1 - \eta + V_{\text{el}})/\eta + (V_A + 1)\sqrt{B} + T'_{\min}(V_A + \varepsilon_{\max}) + 1}{\eta T'_{\min}(V_A + \varepsilon_{\max}) + 1 + v_{\text{el}}}, \\ D &= \frac{\sqrt{B}[V_A + 1 + \sqrt{B}(1 - \eta + V_{\text{el}})/\eta]}{\eta T'_{\min}(V_A + \varepsilon_{\max}) + 1 + v_{\text{el}}}. \end{aligned} \tag{21}$$

To show how the proposed phase compensation procedure improves the performance of the CVQKD system, we compare the key rates under different conditions. The secret key rate K can be regarded as the function $K = K(V_A, T, \eta, V_{\text{el}}, N_0)$ and we obtain the relationship between

the secret key rate of the system and the transmission distance in Fig. 6. We plot the secret key rates under the perfect situation, i.e., $\kappa = 1$ and the cases with the proposed approach based on the LSTM model (when the phase values are measures at intervals of 2000 points and 3000 points), i.e., $\kappa = 0.999\,89$ and $\kappa = 0.999\,87$. To more clearly show the performance of the proposed method, we plot the secret key rate of the system without the phase compensation procedure as a comparison, i.e., $\kappa = 0.917\,38$. It can be observed that the two key rate curves with the proposed approach based on the LSTM model almost coincide with the curve of perfect compensation, but without the proposed method, the key rate deviates significantly and the security transmission distance that Alice and Bob actually share is reduced. The results illustrate that the proposed method performs well and can greatly improve the final key rate and the transmission distance. It is worth noting that, due to the use of prediction data for compensation, this approach not only breaks the limitation that real-time phase drift angle measurement cannot be performed at low SNR but also reduces the overhead of the involved system.

V. CONCLUSION

In this paper, considering that accurate evaluation and compensation of phase drifts have an important impact on the performance and stability of practical CVQKD systems, we propose an automatic phase compensation approach to reduce the phase drift and optimize the involved system. This algorithm relies on machine-learning techniques, training an LSTM model by learning from historical data, and predicting future phase angle values. These predicted values are eventually used to compensate for the phase drifts of the system, instead of real-time phase drift measurement. Our experimental results show that the proposed method accurately predicts the time evolution of phase drifts and has a great compensation effect, which can improve the performance of the CVQKD system effectively, while it requires neither additional quantum resources nor extra experimental hardware.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grant No. 62001383), the National Natural Science Foundation of China (Grant No. 61971276), the Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), the Key R&D Program of Guangdong Province (Grant No. 2020B030304002), and Scientific Research Plan Projects of Shaanxi Education Department (Natural Science Special Project No. 19JK0847).

W.-Q.L. and Z.-K.Z. contributed equally to this work.

[1] C. H. Bennet, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computing Systems and Signal Processing, Bangalore, Dec. 1984* (IEEE, New York, 1984), pp. 175–179.

[2] G. Zeng, *Quantum Private Communication* (Springer, Berlin, 2010).

[3] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[4] A. Warke, B. K. Behera, and P. K. Panigrahi, Experimental realization of three quantum key distribution protocols, Quantum Inf. Process. **19**, 407 (2020).

[5] S. L. Braunstein and P. van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[6] 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).

[7] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[8] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[9] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[10] N. J. Cerf, M. Levy, and G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

[11] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[12] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[13] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum Cryptography Without Switching, Phys. Rev. Lett. **93**, 170504 (2004).

[14] L. Kong, W. Liu, F. Jing, and C. He, Practical security analysis of continuous-variable quantum key distribution with an unbalanced heterodyne detector, Chin. Phys. B **31**, 070303 (2022).

[15] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052301 (2014).

[16] 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).

[17] 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 (2013).

[18] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin *et al.*, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[19] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, Phys. Rev. A **76**, 052323 (2007).

[20] 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).

[21] W. Liu, J. Peng, P. Huang, D. Huang, and G. Zeng, Monitoring of continuous-variable quantum key distribution system in real environment, Opt. Express **25**, 19429 (2017).

[22] L. Li, P. Huang, T. Wang, and G. Zeng, Practical security of a chip-based continuous-variable quantum-key-distribution system, Phys. Rev. A **103**, 032611 (2021).

[23] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[24] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).

[25] 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 **5**, 041009 (2015).

[26] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu *et al.*, Continuous-variable QKD over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[27] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, High-rate point-to-multipoint quantum key distribution using coherent states, arXiv:2302.02391.

[28] Y. Chi, B. Qi, W. Zhu, L. Qian, H. K. Lo, S. H. Youn, A. Lvovsky, and L. Tian, A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution, New J. Phys. **13**, 013003 (2011).

[29] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Continuous-variable quantum key distribution with 1 Mbps secure key rate, Opt. Express **23**, 17511 (2015).

[30] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, Field demonstration of a continuous-variable quantum key distribution network, Opt. Lett. **41**, 3511 (2016).

[31] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache *et al.*, Field test of classical symmetric encryption with continuous variables quantum key distribution, Opt. Express **20**, 14030 (2012).

[32] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, Y.-L. Zhou, and L.-M. Liang, Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator, Phys. Rev. A **89**, 032310 (2014).

[33] 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).

[34] 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).

[35] X. Wang, T. Wu, C. Dong, H. Zhu, Z. Zhu, and S. Zhao, Integrating deep learning to achieve phase compensation for free-space orbital-angular-momentum-encoded quantum key distribution under atmospheric turbulence, Photonics Res. **9**, B9 (2021).

[36] Z. Liu, M. Zhou, W. Liu, C. Li, J. Gu, H. Yin, and Z. Chen, Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution, Opt. Express **30**, 15024 (2022).

[37] H. Luo, L. Zhang, H. Qin, S. Sun, P. Huang, Y. Wang, Z. Wu, Y. Guo, and D. Huang, Beyond universal attack detection for continuous-variable quantum key distribution via deep learning, Phys. Rev. A **105**, 042411 (2022).

[38] W. Liu, P. Huang, J. Peng, J. Fan, and G. Zeng, Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution, Phys. Rev. A **97**, 022316 (2018).

[39] 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).

[40] P. Huang, D. Lin, D. Huang, and G. Zeng, Security of continuous-variable quantum key distribution with imperfect phase compensation, Int. J. Theor. Phys. **54**, 2613 (2015).

[41] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express **26**, 2794 (2018).

[42] T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator, Phys. Rev. A **97**, 012310 (2018).

[43] B. Huang, Y. Huang, and Z. Peng, Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack, Opt. Express **27**, 20621 (2019).

[44] K. A. Alaghbari, K. Rumyantsev, T. Eltaif, O. Elmabrok, and H.-S. Lim, Adaptive modulation for continuous-variable quantum key distribution with real local oscillators under phase attack, IEEE Photonics J. **13**, 7600107 (2021).

[45] S. Hochreiter and J. Schmidhuber, Long short-term memory, Neural Comput. **9**, 1735 (1997).

[46] J. T. Connor, R. D. Martin, and L. E. Atlas, Recurrent neural networks and robust time series prediction, IEEE Trans. Neural Networks **5**, 240 (1994).

[47] J.-Y. Liu, H.-J. Ding, C.-M. Zhang, S.-P. Xie, and Q. Wang, Practical Phase-Modulation Stabilization in Quantum Key Distribution via Machine Learning, Phys. Rev. Appl. **12**, 014059 (2019).

[48] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[49] C. Wang, P. Huang, D. Huang, D. Lin, and G. Zeng, Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects, Phys. Rev. A **93**, 022315 (2016).