Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution

Weiqi Liu,[1] Peng Huang,[2] Jinye Peng,[1] Jianping Fan,[3] and Guihua Zeng[1,2,*]

[1]*College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China*

[2]*Center of Quantum Sensing and Information Processing (QSIP), State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China*

[3]*Department of Computer Science, University of North Carolina-Charlotte, Charlotte, North Carolina 28223, USA*

(Received 2 July 2017; published 12 February 2018)

For supporting practical quantum key distribution (QKD), it is critical to stabilize the physical parameters of signals, e.g., the intensity, phase, and polarization of the laser signals, so that such QKD systems can achieve better performance and practical security. In this paper, an approach is developed by integrating a support vector regression (SVR) model to optimize the performance and practical security of the QKD system. First, a SVR model is learned to precisely predict the time-along evolutions of the physical parameters of signals. Second, such predicted time-along evolutions are employed as feedback to control the QKD system for achieving the optimal performance and practical security. Finally, our proposed approach is exemplified by using the intensity evolution of laser light and a local oscillator pulse in the Gaussian modulated coherent state QKD system. Our experimental results have demonstrated three significant benefits of our SVR-based approach: (1) it can allow the QKD system to achieve optimal performance and practical security, (2) it does not require any additional resources and any real-time monitoring module to support automatic prediction of the time-along evolutions of the physical parameters of signals, and (3) it is applicable to any measurable physical parameter of signals in the practical QKD system.

DOI: 10.1103/PhysRevA.97.022316

I. INTRODUCTION

The quantum key distribution enables the sender, called Alice, and the receiver, called Bob, to exchange a cryptographic key (i.e., a secret key), in the presence of an eavesdropper, called Eve [1,2]. Its security is guaranteed by quantum mechanics laws, e.g., Heisenberg's uncertainty principle and the quantum no-cloning theorem. Significant progress has led to the availability of secure quantum communication in real-world conditions. Currently, two implementation methods, i.e., the discrete-variable quantum key distribution and the continuous-variable quantum key distribution (CVQKD), are often referenced. Here we focus on the CVQKD scheme which usually encodes the information on the position and momentum quadratures of quantum states [3–8]. It is worth noting that our proposed approach also fits the discrete-variable quantum key distribution.

In the past decades, CVQKD schemes have made great achievements both theoretical [5–8] and experimental [9–14]. One of the most notable achievements is that the Gaussian modulated coherent state (GMCS) scheme [3–5] has been proven theoretically to be secure against collective and coherent attacks [15–19]. In addition, the practical security associated with imperfections of the GMCS CVQKD system has also been investigated [20–32]. Recently, to improve the performance and security of the system, many schemes have proposed [33–35]. Moreover, field tests based on the GMCS scheme in telecommunication optical networks have been successfully implemented by several groups [36–38].

It has been shown that the instability of physical parameters of signals, e.g., the intensity, phase, and polarization of the laser signals, has significant influence on the performance and practical security of the involved GMCS CVQKD system, which is needed to run continually and stably for a long time [20–22]. Many factors may cause the instability, such as the fluctuation of signal transmitting in the channel, the variation of environment temperatures, the fiber birefringence effects, and the disturbances of eavesdropping. To maintain the stability of the practical CVQKD system, a real-time monitoring module is often deployed in the involved system to control the physical parameters of signals, e.g., the laser intensity. In such scenarios, the additional module depends on the precision of the measurement devices. In addition, the involved CVQKD system needs to be monitored in real time, which may significantly increase the complexity of the system. Especially, the deployed monitoring module may induce practical security loopholes due to its imperfections [39].

In this paper, we propose an approach that makes use of support vector regression (SVR) [40,41], which is one of the most popular machine learning tools and itself can handle small disturbances of the environment. In our proposed approach, a SVR model is first learned to predict the time-along evolutions of the physical parameters of the signals, and such predictive time-along evolutions are then employed as the feedback to control the involved system and optimize its performance and

*ghzeng@sjtu.edu.cn

practical security. Considering the importance of stabilizing the local oscillator (LO) light in the CVQKD system [20–26], we have exemplified our proposed approach by predicting the time-along intensity evolutions of the laser light and the LO pulse. Our experimental results have demonstrated that our SVR model can provide good predictions of the time-along evolutions of the intensity and optimize the performance and practical security of the CVQKD system. In addition, tuning the intensity of each LO pulse to a desired value, all known attacks that are based on the LO pulse may be defeated and the practical security of the CVQKD system can be guaranteed effectively.

The paper is organized as follows. In Sec. II, a general prediction algorithm is presented for estimating physical parameters of the signal in the involved CVQKD system. To exemplify our proposed algorithm, the algorithm is used to estimate the time-along intensity evolutions of the laser light and LO pulse, and such predicted values are further employed to optimize the stability of the LO pulse in Sec. III. Then, we analyze the performance and practical security of the involved CVQKD system with the feedback module in Sec. IV. Finally, we conclude this paper in Sec. V.

II. LEARNING FOR AUTOMATIC PARAMETER PREDICTION IN THE CVQKD SYSTEM

To automatically predict the instantaneous values for the physical parameters of the signal in the CVQKD system, we need to learn a SVR model to find a function f that returns the best fit of a given signal serials $F_{\mathbf{t}}\,|_{\mathbf{t}=1}^{L}$ for a given time period $t \in [1,L]$, where $F_{\mathbf{t}}$ is the instantaneous value for the physical parameters of the signal at the time t. The SVR model can be represented as $F(\mathbf{t}) = w_0 + \sum_t w F_t$ [42–44]. To find the best fit, we minimize the sum of squared errors as

$$\min\left\{\sum_{t=1}^{L}[F_{\mathbf{t}} - F(\mathbf{t})]^2\right\}.$$

After the SVR model is learned by achieving the best fitting with the given signal serials $F_{\mathbf{t}}\,|_{\mathbf{t}=1}^{L}$ in the given time period $t \in [1,L]$, it can further be used to predict the instantaneous values for the physical parameters of the signal accurately in a certain time period (time window) in the future until such SVR model fails. When such a SVR model fails, we can collect more recent signals to update the SVR model, so that it can achieve accurate predictions of the instantaneous values for the physical parameters of the signals in another time window. In other words, when the CVQKD system starts running in the practical environment, we first collect the signal serials used to train the SVR model, then the SVR model is trained for every other time window. Thus such a SVR model can be used to estimate the instantaneous values for the physical parameters of the signal, and such predicted values can be further employed to optimize the stability of the involved CVQKD system.

The mapping function $F(\mathbf{t}) = w_0 + \sum_t w F_t$ could be linear or even nonlinear [45,46]. As illustrated in Fig. 1, the instantaneous values for the physical parameters of the signal, which are predicted by our SVR model are used as the feedback instead of using the values of the physical parameters that are captured directly from the involved CVQKD system. In

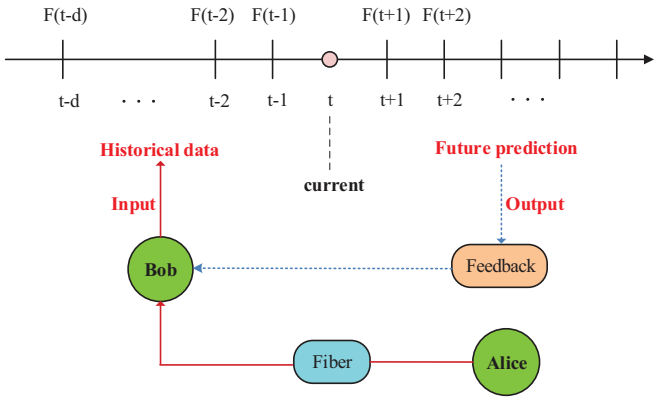

FIG. 1. Basic idea of SVR to solve the physical parameters prediction problem. Assume the current time is t. The red solid line represents the procedure for obtaining the data for machine learning, and the blue dotted line represents the procedure for the feedback.

general, three categories of data for the instantaneous values of the physical parameters of the signal are related to the SVR model: (1) historical data in a previous time period $t \in [1,L]$ that have been used to learn the SVR model, (2) current data for the time t that are captured or generated by the involved CVQKD system, and (3) predictive data that are predicted by the SVR model [47]. Thus the underlying machine learning algorithm trains the SVR model by using the historical data $\{F(t-1), F(t-2), \ldots, F(t-d)\}$, and such SVR model is further used to predict the future values of $\{F(t+1), F(t+2), \ldots, F(t+d)\}$. Actually, the main idea of the parameter prediction is based on the fact that devices possess the deterministic and partially fluctuated properties. The predictive results can be obtained by reconstructing the deterministic part and predicting the probable fluctuated behaviors.

Consider a set of training data (signal serials) $F_{\mathbf{t}}\,|_{\mathbf{t}=1}^{L}$ in the given time period $t \in [1,L]$, when the mapping is nonlinear, the SVR estimating function takes the form

$$F(\mathbf{t}) = [\mathbf{w} \cdot \Phi(\mathbf{t})] + b, \tag{1}$$

where Φ is a function used to project the training data onto a higher dimensional space, $\mathbf{w}$ is the weight vector, and $b \in R^n$ is the bias. Our goal is to find the function that has the optimal parameters $\mathbf{w}$ and b, and at the same time is as fat as possible in the feature space. We denote the fatness as a tube and the tube width is denoted as 2ϵ. Then the optimal regression function is determined by

$$\min \frac{1}{2}\|\mathbf{w}\|^2 + C\sum_i(\xi_i + \xi_i^*), \quad C > 0, \tag{2}$$

subject to

$$\begin{aligned} &F_i - [\mathbf{w} \cdot \Phi(\mathbf{t})] - b \leqslant \epsilon + \xi_i, \\ &[\mathbf{w} \cdot \Phi(\mathbf{t})] + b - F_i \leqslant \epsilon + \xi_i^*, \\ &\xi_i, \xi_i^* \geqslant 0, \quad i = 1, \ldots, l, \quad \epsilon > 0. \end{aligned} \tag{3}$$

Here, C is a regularization parameter, which represents the trade-off between the regularization and the tube violation, ξ_i and ξ_i^* are the upper and lower constraints on the outputs, and

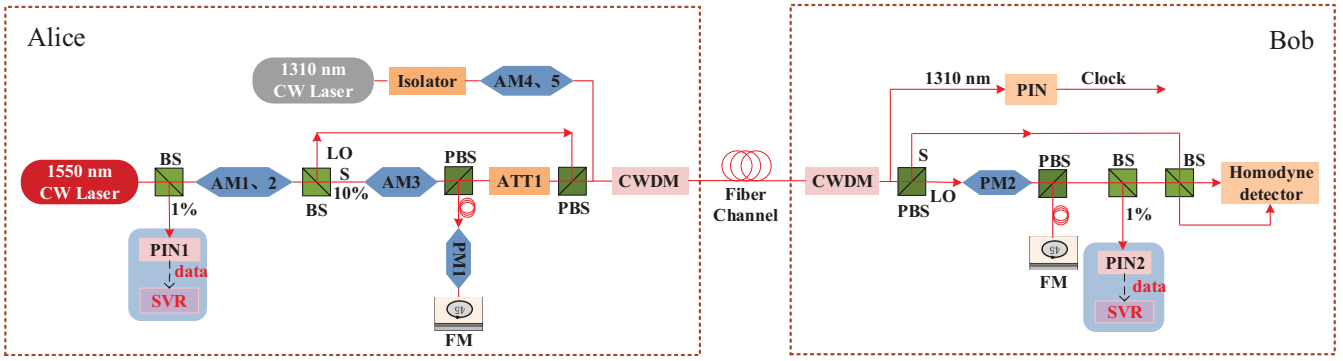

FIG. 2. Experimental setup for obtaining the training data. AM, amplitude modulator; PM, phase modulator; BS, beam splitter; PBS, polarization beam splitter; ATT, adjustable attenuator; CWDM, coarse wavelength division multiplexer.

$\mathbf{w}$ can be written as

$$\mathbf{w} = \sum_i (\alpha_i - \alpha_i^*)\Phi(\mathbf{t}_i). \tag{4}$$

By substituting Eq. (4) into Eq. (1), the equation can be rewritten as

$$\begin{aligned} F(\mathbf{t}) &= \sum_i (\alpha_i - \alpha_i^*)[\Phi(\mathbf{t}_i)\cdot\Phi(\mathbf{t})] + b \\ &= \sum_i (\alpha_i - \alpha_i^*)k(\mathbf{t}_i,\mathbf{t}) + b, \end{aligned} \tag{5}$$

where α_i is the Lagrange multiplier, and k is a kernel function which enables the dot product to be performed in the feature space. Now there are the following three basic kernels: the linear kernel, polynomial kernel, and radial basis function (RBF) kernel. Each kernel has its own advantages and disadvantages. In general, the RBF kernel is a reasonable first choice [40,47,48]. This kernel can handle the case when the relation is nonlinear. The second reason is the number of hyperparameters which influence the performance of model selection. The polynomial kernel has more hyperparameters than the RBF kernel and it is difficult to calculate the results when the degree of polynomial is high. Finally, the RBF kernel has fewer numerical difficulties. Thus we choose the commonly outstanding RBF as the kernel function for the physical parameter regression of the CVQKD system,

$$k(\mathbf{t}_i,\mathbf{t}) = \exp\{-\gamma|\mathbf{t} - \mathbf{t}_i|^2\}, \tag{6}$$

where γ represents the scale parameter of the RBF kernel and the selection of it determines the performance of the model. In order to evaluate the algorithm accuracy and perform a correct estimation of the future physical parameters, we routinely collect some historical data as the test data. Based on the test data, we calculate the mean-squared error (MSE) as performance indices of the algorithm

$$\mathrm{MSE} = \frac{1}{a}\sum_{i=1}^{a}(Y_i^* - Y_i)^2, \tag{7}$$

where a is the amount of the test data, Y_i^* is a vector of a predictions when using the SVR model, and Y_i is the vector of observed values of the test data.

III. INTEGRATING MACHINE LEARNING FOR SIGNAL OPTIMIZATION IN THE CVQKD SYSTEM

By learning from historic data, our proposed SVR model can be used for physical parameter prediction and signal optimization in the GMCS CVQKD system. In this section, we exemplify such a general approach with the intensity evolutions of the laser light and LO pulse. In the parameter prediction and signal optimization procedure, the package LIBSVM, which is currently one of the most widely used SVM libraries, is employed.

A. Historic data preparation

To learn the SVR model for physical parameter prediction, we first need to obtain the training data of the intensity evolutions of the laser light and the LO pulse. The training data are collected from the CVQKD system developed in Shanghai Jiao Tong University [14]. This system is based on the GMCS scheme and can stably work. Figure 2 presents the schematic setup of the system, which includes the data acquisition module in the blue boxes and the data are usually updated every 2 s. In detail, at Alice's side, a 1550-nm wavelength continuous-wave laser generates a narrow linewidth light, which is transformed into a pulse by using the amplitude modulators. This pulse is then split into a weak signal path and a strong local oscillator path with a beam splitter. In the signal path, the key information is encoded in the quadratures of amplitude and phase of the coherent optical pulses according to a centered Gaussian distribution. Moreover, the signal pulse is delayed with respect to the LO pulse by inserting a delay line, and the Faraday mirror imposes a 90° rotation on the signal pulse's original polarization state. By using the polarization-multiplexing and time-multiplexing techniques, the quantum signal together with the LO signal are sent to Bob through a fiber link. Simultaneously, a coarse wavelength division multiplexer is used to integrate the quantum signals for classical communication, which includes a 1310-nm wavelength clock synchronization signal. At Bob's side, the LO and signal are demultiplexed and measured in a shot-noise-limited homodyne detector.

We now describe how to collect the training data for the SVR model to predict the intensity evolutions of the laser light and LO pulse. As shown in Fig. 2, the laser pulse is split with a BS and a small part is collected as the training data for the machine learning. We collect data from the first 5 days as the

training set and use the data from the last 2 days as the testing set. Simultaneously, a BS placed at the LO path aims to obtain the training data of the SVR model for predicting the intensity evolution of the LO pulse. In the experiment, we collect data from the first 2 days as the training set and use the data from the last day as the testing set. After these operations we own two signal serials in the given time periods, which will be employed as training data for learning the SVR models for the intensity evolutions of the laser light and the LO pulse, respectively.

We emphasize here that our main aim is to predict the intensity evolution of the LO pulse so that one may optimize the CVQKD signal. For better learning the SVR model and guaranteeing the practical security of the involved CVQKD system, the intensity distribution of the laser light is considered as a reference. Generally, if the intensity distribution of the LO pulse does not match the the intensity distribution of the laser signal, the learned SVR model for the intensity evolution of the LO pulse maybe fails. In this situation, one needs to collect more recent LO signal data to achieve a more fitting SVR model.

B. Using SVR model to predict intensity evolutions of laser light and LO pulse

After the SVR model is learned, it can be used to predict the physical parameter at the current time t, i.e., the intensity $I(t+d)$ at the future time $t+d$ with the knowledge of the historic values $I(t-d), I(t-d+1), \ldots, I(t)$ for the time $t-d, t-d+1, \ldots, t$, respectively. As discussed previously, we perform the SVR experiments with the collected training data, to obtain the predictive estimation model. Experimentally, after the optimization procedure of the kernel function, we finally chose the RBF as the kernel function to reach the optimal intensity prediction, by making use of the well-known LIBSVM library with $C = 1000$ and $\gamma = 0.1$. The result also indicates that the RBF kernel can be the first choice once again.

First, we have trained the predictive model of the laser signal intensity in the CVQKD system. To demonstrate clearly the effects of the predictive model, the RBF model for the intensity prediction of laser with any 5000 training data, is shown in Fig. 3. Obviously, the regression curve matches the intensity distribution of the laser very well. Meanwhile, according to Eq. (7), we calculate the MSE for the laser intensity prediction as $\mathrm{MSE}_1 = 1.1425 \times 10^{-7}$ with all the collected training data. This indicates that we have obtained an optimal RBF model for the intensity prediction of laser light. Then, in a similar way, we learned the predictive intensity model of the LO pulse. In Fig. 4, we represent the RBF model for the intensity evolution prediction of the LO pulse with any 500 training data. In addition, the MSE for the LO intensity prediction is obtained as $\mathrm{MSE}_2 = 4.2162 \times 10^{-7}$ with all the collected training data, which means that the obtained predictive model can work well.

C. Learning to optimize the intensity parameters

Feedback controls can be employed to guarantee the stable operation of the involved CVQKD system, so that the fluctuations of optical pulse signals in the CVQKD system can be degraded. Here, we concentrate on the stability of the intensity evolution of the LO pulse in the CVQKD system. In

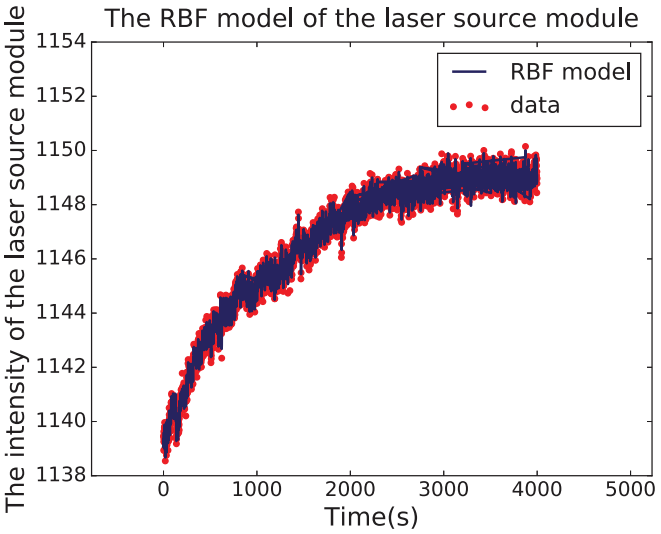

FIG. 3. RBF model for the intensity prediction of laser with several training data points.

the previous sections, we integrated the SVR model for the intensity prediction. Here we leverage the learned SVR model to stabilize the LO intensity to a required constant value with the predicted intensity values as feedback, which will decrease the system overhead meanwhile. Figure 5 demonstrates the schematic setup of the feedback module. The process can be divided into two steps as follows. First, Bob obtains the predictive intensity of LO via the SVR model for the LO pulse, and then he amplifies or attenuates the LO intensity based on the predictive values. To simplify the implementation, for example, here we use an adjustable attenuator (ATT) to stabilize the LO to a required constant value.

To demonstrate the effects of the feedback in improving the stability of the CVQKD system, we plot the LO intensity of the system in Fig. 6. From top to the bottom, the curves represent the LO intensity without the feedback procedure, the

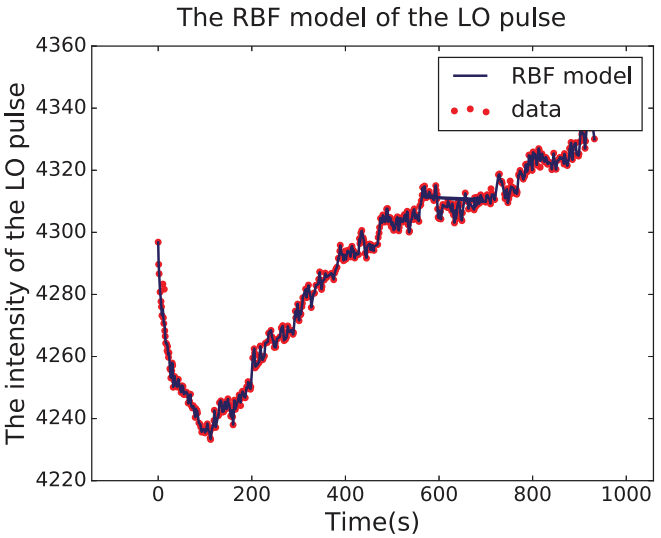

FIG. 4. RBF model for the intensity prediction of LO pulse with several training data points.

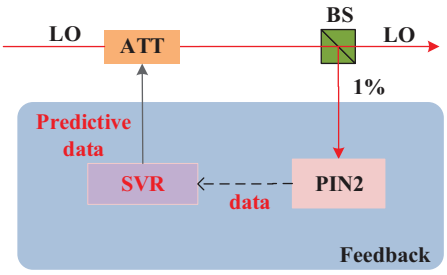

FIG. 5. Experimental setup of the feedback control module.

experimental results of the LO intensity with feedback, and the theoretical initial value of the LO intensity, respectively. Clearly, there is a little difference between the theoretical and experimental values. This results from the accuracy of the SVR algorithm, the precision of the attenuator used for the feedback, and the relative intensity noise (RIN) of the laser, which will be discussed in detail in the next section.

IV. INTEGRATING SVR MODEL TO ACHIEVE PERFORMANCE OPTIMIZATION AND PRACTICAL SECURITY

A. Performance optimization of CVQKD

To demonstrate the performance of the feedback module in improving the performance of the CVQKD system, we need to analyze the secret key rate of the involved system. In a CVQKD system, after the quantum transmission, Alice and Bob share two correlated vectors $x = \{x_1, x_2, \ldots, x_N\}$ and $y = \{y_1, y_2, \ldots, y_N\}$, where N is the total number of received pulses. The involved quantum channel of the system is a normal linear model with the following relation between Alice and Bob, i.e.,

$$y = tx + z, \tag{8}$$

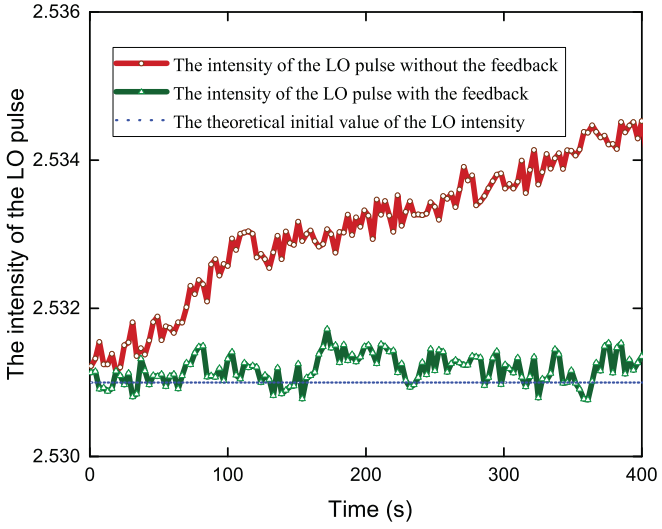

FIG. 6. LO intensity of the CVQKD system with and without the feedback controls.The LO intensity without the feedback shows the predictive values. That with the feedback shows the measuring values.

where $t = \sqrt{\eta T} \in R^n$, which relates to the transmittance of the quantum channel in the following sections, and z is the noise term following a centered normal distribution with variance $\sigma^2 = N_0 + \eta T\varepsilon + V_{\mathrm{el}}$. The involved N_0 is the variance of the shot noise, which is proportional to the intensity of the local oscillator. The parameter η denotes the efficiency of the homodyne detector, T is the transmittance of the quantum channel, ε is the excess noise, and V_{el} is the detector's electronic noise.

In the evaluation of the secret key rate of the CVQKD system, all parameters should be expressed in shot noise units. Obviously, it is important to exactly evaluate the N_0 due to the fluctuations of LO. A common method is to scale Bob's measurements with the instantaneous intensity value of each pulse of LO. However, it makes Bob's measuring complicated. In the above scheme, we propose an alternative countermeasure to stabilize the LO intensity to a desired constant value via machine learning. However, due to the accuracy of the algorithm, the precision of the device used for the feedback and the relative intensity noise of the laser, fluctuations of LO pulses may still exist. If Alice and Bob are aware of pulse fluctuations, they use the instantaneous values to estimate the parameters, namely,

$$I'_{\mathrm{LO}} = \chi I_{\mathrm{LO}}, \tag{9}$$

where I_{LO} is the LO intensity, which is connected with the shot noise of system, the parameter χ represents the remaining fluctuation of the LO pulses and the prime symbol indicates the fluctuation parameters in the forthcoming part. In detail, we denote the precision of the machine learning algorithm in shot noise units and define the accuracy of the device used for the feedback as χ_ε. Therefore,

$$\chi = \chi_{\mathrm{RIN}} + \chi_\varepsilon + \frac{N_0 - \mathrm{MSE}}{N_0}, \tag{10}$$

where χ_{RIN} is the relative intensity noise of the laser, which is usually 10^{-16} Hz and thus can be neglected in general. Expressed in the instantaneous shot noise units, the parameters used in the evaluation of the secret key rate become

$$\begin{aligned} V'_A &= V_A, \quad \varepsilon' = \frac{1}{\chi^2}\varepsilon + \frac{1}{\eta T}\left(\frac{1}{\chi^2} - 1\right), \\ V'_{\mathrm{el}} &= V_{\mathrm{el}}, \quad T' = T, \quad N'_{\mathrm{LO}} = \chi^2 N_{\mathrm{LO}}. \end{aligned} \tag{11}$$

Given these parameters, Alice and Bob can calculate the information they shared, as well as the maximal bound on the information available to the eavesdropper. According to Refs. [30,49], the secret key rate K with n received pulses used for the key establishment is expressed as

$$K = \frac{n}{N}[\beta I_{AB} - S_{BE}^{\epsilon_{\mathrm{PE}}} - \Delta(n)], \tag{12}$$

where $n = N - m$, and $\beta \in (0,1)$ is the efficiency of reverse reconciliation. $S_{BE}^{\epsilon_{\mathrm{PE}}}$ represents the maximal value of the Holevo information with finite-size effect, i.e., Alice and Bob select m values from the total number of the received pulses N to perform the parameter estimation procedure, where ϵ_{PE} is the probability that the true values of the parameters are not inside the confidence region. $S_{BE}^{\epsilon_{\mathrm{PE}}}$ can be determined by the following

covariance matrix between Alice and Bob:

$$\Gamma_{AB}=\begin{bmatrix} (V_A+1)\cdot\mathbb{1}_2 & \sqrt{T_{\min}\left(V_A^2+2V_A\right)}\cdot\sigma_z \\ \sqrt{T_{\min}\left(V_A^2+2V_A\right)}\cdot\sigma_z & [T_{\min}(V_A+\varepsilon_{\max})+1]\cdot\mathbb{1}_2 \end{bmatrix}, \tag{13}$$

where the matrices $\mathbb{1}_2=\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$, and $\sigma_z=\left[\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right]$. $T_{\min}$ and $\varepsilon_{\max}$ represent the lower bound of T and the upper bound of ε, respectively. They are defined as

$$\begin{aligned} T_{\min} &= (t_{\min})^2, \\ \varepsilon_{\max} &= \frac{\sigma_{\max}^2-1}{T}. \end{aligned} \tag{14}$$

Moreover, when m is large enough, we could compute $t_{\min}$ and $\sigma_{\max}^2$ as

$$\begin{aligned} t_{\min} &\approx \sqrt{T}-z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\varepsilon}{mV_A}}, \\ \sigma_{\max} &\approx 1+T\varepsilon+z_{\epsilon_{\mathrm{PE}}/2}\frac{(1+T\varepsilon)\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{15}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ follows

$$1-\frac{1}{2}\mathrm{erf}\left(\frac{z_{\epsilon_{\mathrm{PE}}/2}}{\sqrt{2}}\right)=\frac{1}{2}\epsilon_{\mathrm{PE}}, \tag{16}$$

and erf(.) is the error function defined as

$$\mathrm{erf}(x)=2\pi^{-1/2}\int_0^x e^{-t^2}\,dt. \tag{17}$$

Therefore, $S_{BE}^{\epsilon_{\mathrm{PE}}}$ is calculated as follows

$$S_{BE}^{\epsilon_{\mathrm{PE}}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right), \tag{18}$$

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

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}(A\pm\sqrt{A^2-4B}), \\ \lambda_{3,4}^2 &= \frac{1}{2}(C\pm\sqrt{C^2-4D}), \\ \lambda_5 &= 1, \end{aligned} \tag{19}$$

where

$$\begin{aligned} A &= (V_A+1)^2-2T_{\min}\left(V_A^2+2V_A\right)+[T_{\min}(V_A+\varepsilon_{\max})+1]^2, \\ B &= [(T_{\min}\varepsilon_{\max}+1)(V_A+1)-T_{\min}V_A]^2, \\ C &= \frac{A(1-\eta+V_{\mathrm{el}})/\eta+(V_A+1)\sqrt{B}+T_{\min}(V_A+\varepsilon_{\max})+1}{\eta T_{\min}(V_A+\varepsilon_{\max})+1+\upsilon_{\mathrm{el}}}, \\ D &= \frac{\sqrt{B}[V_A+1+\sqrt{B}(1-\eta+V_{\mathrm{el}})/\eta]}{\eta T_{\min}(V_A+\varepsilon_{\max})+1+\upsilon_{\mathrm{el}}}. \end{aligned} \tag{20}$$

In Eq. (12), I_{AB} represents the Shannon mutual information between Alice and Bob, which can be derived from Bob's measured variance V_B and the conditional variance $V_{B|A}$ as

$$I_{AB}=\frac{1}{2}\log_2\frac{V_B}{V_{B|A}}=\frac{1}{2}\log_2\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}. \tag{21}$$

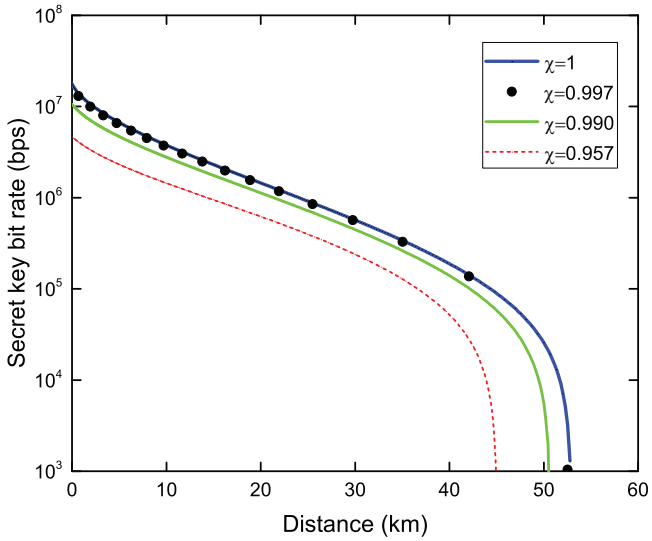

FIG. 7. Secret key rate vs transmission distance for reverse reconciliation scheme. From top to bottom, curves represent the secret key rates in the perfect situation with perfect feedback devices (solid line, $\chi=1$), the practical situation with perfect feedback devices supported by the learned SVR model (dotted line, $\chi=0.997$), the practical situation with practical feedback devices supported by the learned SVR model (green solid line, $\chi=0.990$), and in the practical situation with previous countermeasure (red dashed line, $\chi=0.957$), respectively. The fiber loss is 0.2 dB/km and the other parameters for the simulation are $f_{\mathrm{rep}}=25$ MHz, $V_A=20$, $\eta=0.6$, $\beta=0.939$, $\varepsilon=0.01$, and $V_{\mathrm{el}}=0.05$, respectively.

Here, the total noise referred to the channel input can be expressed as $\chi_{\mathrm{tot}}=\chi_{\mathrm{line}}+\chi_h/T$, in which $\chi_{\mathrm{line}}=1/T-1+\varepsilon$, and $\chi_h=[(1-\eta)+V_{\mathrm{el}}]/\eta$, which represents a homodyne detection-added noise referred to Bob's input. In addition, $\Delta(n)$ is a linear function of n in Eq. (12), which is related to the security of the privacy amplification [49].

Based on Eqs. (19) and (20), one may evaluate the secret key bit rate with finite-size effect against collective attacks. For a practical CVQKD system, the secret key bit rate is given by

$$R=f_{\mathrm{rep}}K, \tag{22}$$

where f_{rep} is the frequency of the CVQKD system. Let m be the typical value $m=N/2=10^9$, and the secret key rate K can be regarded as a function $K=K(V_A,T,\varepsilon,V_{\mathrm{el}},N_0)$. If the system fluctuates with time, these parameters will be changed to $V_A',T',\varepsilon',V_{\mathrm{el}}',N_0'$ respectively, namely, $K'=K(V_A',T',\varepsilon',V_{\mathrm{el}}',N_0')$.

To demonstrate the optimization performance of our proposed approach based on the SVR model for stabilizing the CVQKD system, we compare the secret key rates under different circumstances. Without loss of generality, we consider the situation of the employed devices for feedback being perfect, i.e., $\chi_\varepsilon=0$. In this case, Eq. (10) becomes $\chi=1-\mathrm{MSE}/N_0$. In our proposed approach based on the SVR model, $\mathrm{MSE}=4.2162\times10^{-7}$, thus we have $\chi=0.997$. The relationship between the secret key rate of the system and the transmission distance under the SVR model is shown in Fig. 7. For comparison, we also plot the secret key rates under the perfect situation, i.e., $\chi=1$, and the situation with

imperfect feedback devices with our proposed approach based on the SVR model, e.g., $\chi = 0.990$. Obviously, two curves for the secret key rates almost coincide at the condition of perfect feedback devices. Even if the feedback devices are not perfect, the output secret key rate is very close to the perfect situation. This means that our proposed approach can stabilize well the CVQKD system and the secret key rate can be optimized.

However, without our proposed approach based on the SVR model, the deviations for the secret key rate are obvious. To demonstrate this result, we consider the previous countermeasure for controlling the fluctuations of LO pulse, i.e., Bob measures the shot noise in real time. In this case, we have $\chi = 0.957$ which is obtained based on the experiment results from the employed CVQKD system in Fig. 2. The secret key rate against collective attacks is also plotted in Fig. 7. Clearly, both the truly secret key rate Alice and Bob actually shared and the secure distance decrease. Accordingly, in our approach, since Bob can tune the LO intensity to a required constant value, the SNR of the homodyne detector can be changed to a desired value at the same time, which will improve the tolerance of the channel excess noise in a practical CVQKD system [50].

B. Practical security of CVQKD system against LO attacks

In a practical GMCS CVQKD system, shot noise can be evaluated based on the measured LO pulse intensity, which is generally assumed to be constant. Unfortunately, the LO pulse intensity always fluctuates during the key distribution process. This will inevitably give Eve advantages in exploiting the fluctuations. In detail, Eve can simulate the fluctuations of the LO pulse intensity to hide many kinds of attacks, then the excess noise introduced by her will be reduced arbitrarily by reducing the intensity of the LO pulse. Consequently, Alice and Bob would underestimate Eve's information. Actually, Refs. [20–23] have pointed out that the instability of the LO pulse intensity will leave loopholes for Eve and could jeopardize severely the practical security of the involved CVQKD system.

To resist the practical attacks induced by the instability of LO pulse intensity, the previous countermeasures often monitor the LO intensity and meanwhile Bob's measurements should be scaled with the instantaneous intensity value of each LO pulse. Such ways have drawbacks as discussed in the Sec. I. In this paper, we propose an alternative countermeasure, which may degrade the fluctuation and stabilize the LO intensity via machine learning algorithms. The proposed scheme is as follows. Bob obtains the predictive values of the LO pulse intensity via machine learning, and then he amplifies or attenuates the LO intensity to a desired value according to the predictive values obtained through the learned SVR model. As described in the above sections, we can reach very accurate predictions of the LO pulse intensity and then optimize the performance of the involved CVQKD system. Consequently, almost any practical attacks due to the LO pulse instability can be resisted. This result has been confirmed by the experiment described in Sec. IV. Therefore, our proposed approach based on a SVR model may provide a perfect solution in this scenario.

V. CONCLUSIONS

In this work, considering that the instability has significant influences on the performance and practical security of CVQKD system, we proposed an approach to optimize the involved system. Implementing this approach requires neither additional quantum resources nor extra experimental hardware. Instead we rely on software-based machine learning techniques, which extract optimal performance from information that would have already been collected during the implementations of CVQKD system. The proposed approach is exemplified by making use of the intensity evolutions of laser light and local oscillator pulses in the CVQKD system. Our experimental results show that the proposed approach performs well and the secret key rate of the CVQKD system can be optimized by tuning the intensity of the LO pulse with feedback which is obtained via machine learning. Especially, all known practical attacks associated with the LO instability will be defeated and the practical security of the system can be perfectly guaranteed.

ACKNOWLEDGMENTS

This work was performed in QSIP of Shanghai Jiao Tong University during the visit of W.Q.L. Support was recieved from the National Natural Science Foundation of China (Grants No. 61332019, No. 61471239, No. 61671287, No. 61631014); Northwest University Doctorate Dissertation of Excellence Funds (YYB17022); and the National Key Research and Development Program (Grant No. 2016YFA0302600).

W.L. and P.H. contributed equally to this work.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.

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

[3] 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).

[4] 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).

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

[6] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, No-Switching Quantum Key Distribution using Broadband Modulated Coherent Light, Phys. Rev. Lett. **95**, 180503 (2005).

[7] L. Gong, H. Song, C. He, Y. Liu, and N. Zhou, A continuous variable quantum deterministic key distribution based on two-mode squeezed states, Phys. Scr. **89**, 035101 (2014).

[8] H. Song, L. Gong, Y. He, and N. Zhou, Continuous-variable quantum deterministic key distribution protocol based

on quantum teleportation, Acta Phys. Sin. **61**, 154206 (2012).

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

[10] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photon. **7**, 378 (2013).

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

[12] 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).

[13] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[14] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel, Sci. Rep. **5**, 14607 (2015).

[15] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[16] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

[17] R. Renner and J. I. Cirac., De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[18] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks, Phys. Rev. Lett. **109**, 100502 (2012).

[19] A. Leverrier, Security of Continuous-Variable Quantum Key Distribution via a Gaussian De Finetti Reduction, Phys. Rev. Lett. **118**, 200501 (2017).

[20] 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).

[21] 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).

[22] 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).

[23] J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking on quantum key distribution using homodyne detection, Phys. Rev. A **89**, 032304 (2014).

[24] J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, Phys. Rev. A **87**, 062329 (2013).

[25] X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol, Phys. Rev. A **87**, 052309 (2013).

[26] S. Kunz-Jacques and P. Jouguet, Robust shot-noise measurement for continuous-variable quantum key distribution, Phys. Rev. A **91**, 022307 (2015).

[27] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[28] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Risk analysis of Trojan-Horse attacks on practical quantum key distribution systems, IEEE J. Sel. Top. Quantum Electron. **21**, 3 (2015).

[29] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. **16**, 123030 (2014).

[30] 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).

[31] H. Qin, R. Kumar, and R. Alléaume, Saturation attack on continuous-variable quantum key distribution system, Proc. SPIE **8899**, 88990N (2013).

[32] 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).

[33] Y. Guo, Q. Liao, D. Huang, and G. Zeng, Quantum relay schemes for continuous-variable quantum key distribution, Phys. Rev. A **95**, 042326 (2017).

[34] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction, Phys. Rev. A **95**, 032304 (2017).

[35] Y. Guo, C. Xie, Q. Liao, W. Zhao, G. Zeng, and D. Huang, Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel, Phys. Rev. A **96**, 022320 (2017).

[36] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, Field test of a continuous-variable quantum key distribution prototype, New J. Phys. **11**, 045023 (2009).

[37] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Field test of classical symmetric encryption with continuous variables quantum key distribution, Opt. Express **20**, 14031 (2012).

[38] 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).

[39] T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, The practical security of real-time shot-noise measurement in continuous-variable quantum key distribution, Quant. Info. Proc. **17**, 11 (2018).

[40] S. Mavadia, V. Frey, S. D. Jarrah Sastrawan, and M. J. Biercuk, Prediction and real-time compensation of qubit decoherence via machine learning, Nat. Commun. **8**, 14106 (2017).

[41] C. Chang and C. Lin, LIBSVM: A library for support vector machines, ACM Trans. Intell. Syst. Technol. **2**, 27 (2011).

[42] C. H. Wu, J. M. Ho, and D. T. Lee, Travel-time prediction with support vector regression, IEEE Trans. Intell. Transp. Syst. **5**, 276 (2004).

[43] H. Yang, L. Chan, and I. King, Support vector machine regression for volatile stock market prediction, in *International Conference on Intelligent Data Engineering and Automated Learning* (Springer, Berlin, 2002), p. 391.

[44] D. C. Sansom, T. Downs, and T. K. Saha, Evaluation of support vector machine based forecasting tool in electricity price forecasting for Australian national electricity market participants, J. Electr. Electron. Eng. Aust. **22**, 227 (2003).

[45] D. Basak, S. Pal, and D. C. Patranabis, Support vector regression, Neural Info. Process. Lett. Rev. **11**, 203 (2007).

[46] C. Chang and C. Lin, Training *v*-support vector regression: Theory and algorithms, Neural Comput. **14**, 1959 (2002).

[47] R. Chrobok, O. Kaumann, J. Wahle, and M. Schreckenberg, Travel-time prediction with support vector regression, in Proceedings of the 9th International Federation of Automatic Control Symposium on Control in Transportation Systems, 2000, p. 250 (unpublished).

[48] C. W. Hsu, C. C. Chang, and C. J. Lin, A practical guide to support vector classification, Technical Report, Department of Computer Science and Information Engineering, National Taiwan University, 2003 (unpublished).

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

[50] J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, Electronic noise in optical homodyne tomography, Phys. Rev. A **75**, 035802 (2007).