entropy

MDPI

Article

Neural Network-Based Prediction for Secret Key Rate of Underwater Continuous-Variable Quantum Key Distribution through a Seawater Channel

Yun Mao [1,2], Yiwu Zhu [2], Hui Hu [2], Gaofeng Luo [1,*], Jinguang Wang [2], Yijun Wang [2] and Ying Guo [1,3,*]

[1] School of Information Engineering, Shaoyang University, Shaoyang 422000, China; maoyun3106@csu.edu.cn
[2] School of Automation, Central South University, Changsha 410083, China; zhuyw1@jiachengtech.com (Y.Z.); huh@jiachengtech.com (H.H.); wangjinguang@sdwm.edu.cn (J.W.); xxywyj@csu.edu.cn (Y.W.)
[3] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: gfluo@hnsyu.edu.cn (G.L.); guoying@bupt.edu.cn (Y.G.)

Abstract: Continuous-variable quantum key distribution (CVQKD) plays an important role in quantum communications, because of its compatible setup for optical implementation with low cost. For this paper, we considered a neural network approach to predicting the secret key rate of CVQKD with discrete modulation (DM) through an underwater channel. A long-short-term-memory-(LSTM)-based neural network (NN) model was employed, in order to demonstrate performance improvement when taking into account the secret key rate. The numerical simulations showed that the lower bound of the secret key rate could be achieved for a finite-size analysis, where the LSTM-based neural network (NN) was much better than that of the backward-propagation-(BP)-based neural network (NN). This approach helped to realize the fast derivation of the secret key rate of CVQKD through an underwater channel, indicating that it can be used for improving performance in practical quantum communications.

Keywords: continuous-variable; quantum key distribution; neural network; underwater channel

Citation: Mao, Y.; Zhu, Y.; Hu, H.; Luo, G.; Wang, J.; Wang, Y.; Guo, Y. Neural Network-Based Prediction for Secret Key Rate of Underwater Continuous-Variable Quantum Key Distribution through a Seawater Channel. *Entropy* **2023**, *25*, 937. https://doi.org/10.3390/e25060937

Academic Editor: Rosario Lo Franco

Received: 13 April 2023
Revised: 30 May 2023
Accepted: 8 June 2023
Published: 14 June 2023

1. Introduction

Information security has always been important. Current cryptosystems are dependent on mathematical puzzles without rigorous proofs, and with ever-increasing computing power, such cryptosystems are in danger of being violently broken. In this context, quantum communications have been suggested [1,2], which involve an important technical aspect called a quantum key distribution (QKD) [3–5]. Currently, security analysis of QKD protocols involves finding the low bound on the secret key rate: this task, which is usually complex and tedious, may apply to the specific protocols, whereas the achievable bound on the secret key rate is usually not compact enough. Recent results have demonstrated a reliable numerical method, in a finite dimensional environment, for deriving secret key rates [6,7], which depends on solving a convex optimization problem; however, when the Hilbert space in which the bipartite state is located becomes infinite-dimensional, this numerical method cannot be used efficiently.

QKD in discrete variables (DV) [8,9] can be reduced to finite dimensionality by using compressed mappings [10–12] or tagged state squarers [13]; however, for QKD in continuous variables (CV) [14–17], there is no accurate compression model to reduce the dimensionality. Therefore, we have to devote ourselves to finding an effective approach to achieving a compact bound of the secret key rate of the CVQKD system.

CVQKD has unique advantages, such as high-rate modulations with large capacity, which involve Gaussian modulation (GM) and discrete modulation (DM), for processing signals in optical communications. Compared to the GM scheme, the DM scheme has

received increasing attention, because of its low cost in experiments. Recent works have focused on asymptotic security proofs of DM-CVQKD with an arbitrary number of the modulated states [14–17]. The results introduced an assumption of photon number cutoff, in order to reduce the dimension of Hilbert space; therefore, it cannot be said that this approach is a completely strict security proof, and the photon number cutoff assumption cannot be justified. A dimensionality reduction algorithm, without using the photon number cutoff assumption, has been proposed recently [18], which approximates an infinite-dimensional optimization problem, by converting it to a convex optimization problem in a finite-dimensional subspace.

In recent decades, CVQKD has been designed for free-space (FS) communications [19]. Several kinds of CVQKD protocols have been suggested for FS channels, such as satellite-to-satellite links, satellite-to-ground links, air-to-water channels, and so on [20,21]. Unfortunately, the transmission coefficient fluctuates, due to the effects of turbulence in the FS channels, where coherent detection may be distorted, leading to the decreased performance of the quantum communication system. However, there have been a few studies on CVQKD through an underwater channel, where the transmission distance was decreased destructively due to the effect of the noise of the rapidly changing conditions in the seawater. In order to characterize a practical CVQKD through an underwater channel, it is necessary to counteract the effect of excess noise, for data post-processing. Machine learning (ML) has been applied in various fields [22–24]. An advantage of the ML-based method is that it consumes less time and resources, yet achieves remarkable results. In this paper, we realized a fast prediction of the secret key rate of the DM-CVQKD, by using an LSTM-based NN model [25], which was based on Bayes optimization for the data post-processing at the receiver. Moreover, prediction of the secret key rate could be achieved for the underwater channels.

The contribution of this work was to predicate the lower bound of the secret key rate, by using an NN model, which involved the LSTM-based NN and the BP-based NN, concerning the dimension-reduced algorithm. We demonstrated that the performance of the LSTM-based NN model was better than that of the BP-based NN model for CVQKD through an underwater channel. These models could speed up the derivation of the secret key rate, compared to the direct numerical method, from which we could obtain a reliable and compact bound of the secret key rate in infinite-dimensional Hilbert spaces.

This paper is organized as follows. In Section 2, we describe our DM-CVQKD through an underwater channel. In addition, we describe how our NN-based scheme for performance prediction of DM-CVQKD was designed. In Section 3, our security analysis with numerical simulation is shown. In Section 4, a summary of the work is provided.

2. DM-CVQKD through an Underwater Channel

2.1. Description of DM-CVQKD Protocol

The underwater CVQKD system is shown in Figure 1a. Usually, the CVQKD protocol can be described with a prepare-to-measure (PM) scheme, typically known as prepare and measure, where Alice prepares for the DM signals, and sends them to Bob, who performs the measurement operation, and then determines the final secret key by exchanging information over the public channel. In what follows, we detail the steps of CVQKD with the PM scheme:

1. Preparation: For each round, Alice randomly prepares for one of the four quantum states $\left\{ \left| \alpha e^{i(2k+1)\pi/4} \right\rangle : k \in \{1,2,3,4\} \right\}$ with equal probability, and sends it to Bob, where α is the amplitude of the quantum state;

2. Measurement: After receiving the signal state, Bob randomly selects a product value from $\{\hat{q}, \hat{p}\}$, to perform homodyne detection, in order to obtain the measurement result, where $\hat{q}$ corresponds to the real part of the quantum state, and $\hat{p}$ corresponds to the imaginary part of the quantum state;

3. Publication and parameter estimation: Alice and Bob exchange information through an authenticated public channel. Bob publishes his chosen summation values for each

round through the public channel, and then both parties choose a part of the rounds for parameter estimation, which part of the rounds Alice discloses the quantum states she sends, and Bob discloses the measurements. Based on the public information, both parties can derive the secret key rate under reverse reconciliation (RR). If a secret key rate is not available, both parties terminate the agreement; otherwise, they proceed to the next step;

4. Reverse reconciliation: After the previous steps, the communicating parties use the undisclosed rounds to extract the original key. The specific practice is that both communicating parties follow the same rule for key mapping, and Alice extracts the key according to Bob's public summation value, which we call reverse reconciliation;

5. Error correction and privacy amplification: in the transmission process of quantum states, the presence of excess noise ξ in the quantum channel makes it inevitable that there are inconsistencies in the interrelated original keys obtained by the two communicating parties. The error correction process is the use of error correction codes by both parties to correct the incomplete agreement bare code, so as to obtain a set of identical binary bits of data. The two communicating parties then have an identical set of binary bits. Unfortunately, Eve, the eavesdropper, may eavesdrop on a set of data sequences that will contain some information about the key; therefore, Alice and Bob choose the appropriate method for private amplification, to generate the final key.

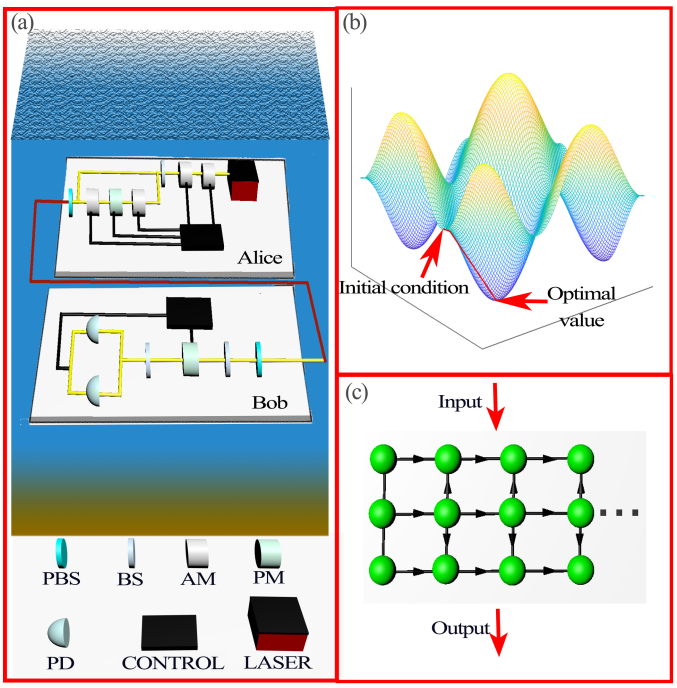

Figure 1. Scenario diagram of DM-CVQKD through an underwater channel: (**a**) Underwater environment. PBS: Polarization Beam Splitter, BS: Beam Splitter, AM: Amplitude Modulator, PM: Phase Modulator, PD: Photo Diode; (**b**) Bayesian optimization; (**c**) The trained neural network.

2.2. *An NN Model for Data Post-Processing*

Neural networks are capable of approximating a bounded continuous mapping in a given region [26]. The network model obtained through data training can learn the mapping relationship between input and output, leading to the achievable secret key rate quickly without going through a time-consuming optimization process. The more data that needs to be predicted, the higher the speedup effect is.

Without loss of generality, we suggest an LSTM-based NN model that has an input layer, an output layer, and multiple hidden layers. In addition, this model comes with a Bayes optimization module, as shown in Figure 1b [27,28], which automatically optimizes the hyperparameters based on the training effect, so that we do not need to manually adjust the hyperparameters to show the training effect on the performance of the system.

The LSTM-based NN can solve the gradient explosion or disappearance problem of simple recurrent neural networks [20], and it can update the network model when the received data are added. The main idea of the LSTM is the use of a cell (Figure 1c), which represents the state of a memory unit $\tilde{c}$, as shown in Figure 2.

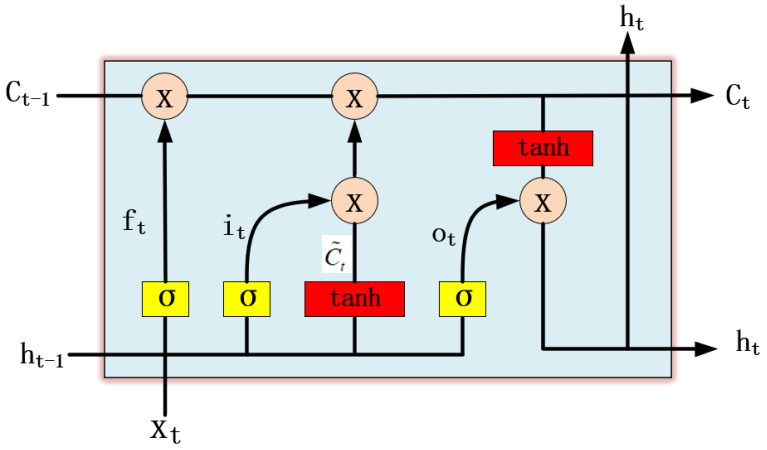

Figure 2. The internal structure of a cell of the LSTM-based NN. The internal state C_{t-1} of the previous moment, the external state h_{t-1}, and the network input x_t of the current moment are used as the input of the cell, and the current internal state C_t and external state h_t are obtained as the output of the cell by gate operations, i.e., forget gate, input gate, and output gate, respectively.

The data for our training model came from the simulation program of the downscaling algorithm. The distance range [0, 6 m] was varied by a step size of 0.5 m, the depth range [0, 100 m] by a step size of 20 m, the amplitude range [0.6, 0.7] by a step size of 0.02, and the over-noise range [0.001, 0.04] by a step size of 0.001. As the scheme was sensitive to over-noise, the sampling step size for over-noise was small. After sampling by the dimensionality reduction algorithm, we obtained the dataset. Performing the Bayes optimization, the prediction results could be achieved after training the network with the above dataset. When the prediction error was less than zero, i.e., when the predicted value was less than the true value, we considered the prediction result to be secure. The training results for the underwater channel are shown in Figure 3. When the error was less than or equal to 0, the predicted result was secure. The results show that most of the error values were concentrated in the interval $[-50\%, -10\%]$.

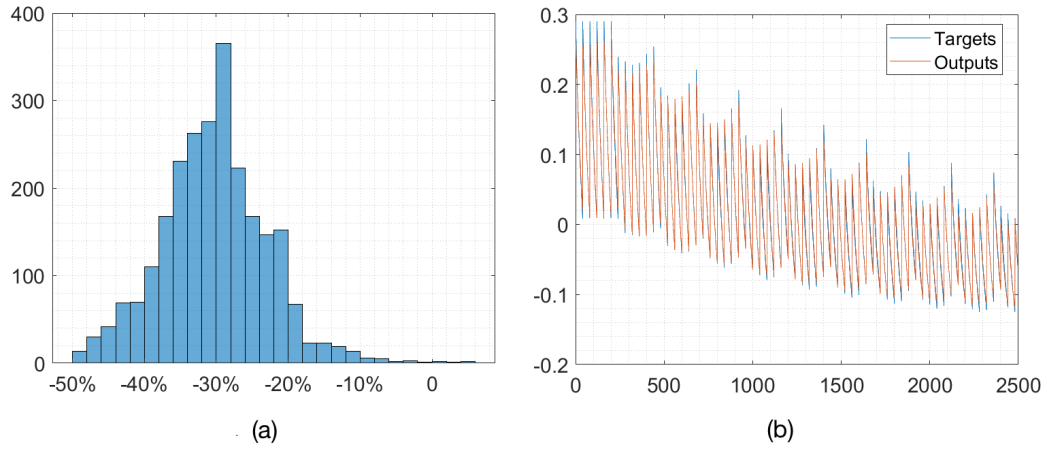

Figure 3. Training results of the LSTM-based NN: (**a**) Error histogram of prediction. The number of samples vs relative error of the train dataset; (**b**) The training set predicted and expected values. The red line is the predicted value, and the blue line is the expected value.

3. Security Analysis

3.1. Derivation of the Secret Key Rate

The well-known formula for deriving the asymptotic key rate is derived from the difference between the two information-theoretic quantities of private amplification (PA) and error correction (EC) [16,17]. The secret key rate K was derived as follows:

$$K = \left(\min_{\rho \in S} f(\rho) \right) - p_{pass} leak_{EC}, \tag{1}$$

where ρ was the density operator of the quantum states shared by Alice and Bob, S was the set of all ρ satisfying the condition known as the feasible set, p_{pass} was the screening probability of each round retained to generate the original key, and $leak_{EC}$ denoted the amount of information leaked in each round of the error correction step.

The first term in the key rate formulation was a convex optimization problem, with ρ as the independent variable. The calculation of the second term could be obtained directly from experimental data [21]. The density operator ρ was an unknown semi-positive definite matrix, but the asymptotic case ρ followed some constraints of the following form:

$$Tr(\Gamma_i \rho) = \gamma_i, \tag{2}$$

where Γ_i was the ergodic operator, and γ_i was the expected value of the corresponding ergodic operator. All ρ that satisfied the constraints were expressed as

$$f(\rho) = D(\mathcal{G}(\rho) || \mathcal{Z}(\mathcal{G}(\rho))), \tag{3}$$

where $D(\lambda_1 || \lambda_2) = Tr(\lambda_1 \log \lambda_1) - Tr(\lambda_1 \log \lambda_2)$ was a conditional entropy function, $\mathcal{G}$ was a completely positive mapping relation, and $\mathcal{Z}$ was a completely positive trace-preserving mapping relation. As both $\mathcal{G}$ and $\mathcal{Z}$ were linear mappings, and the conditional entropy function was convex, $f(\rho)$ was a convex function on the feasible set S. To extract the secret key rate required finding a ρ that satisfied the constraint, such that $f(\rho)$ was minimized. The solution to this optimization problem was divided into two steps. The first step found a density matrix ρ' that was close or equal to the optimal density matrix ρ^*, by an iterative algorithm, to obtain $f(\rho')$ as an upper bound on the key rate. The second step considered the dual problem of the minimization problem, and as the optimal value of the dual problem was less than or equal to the optimal value of the original problem, the optimal value of the dual problem was used as the lower bound of the secret key rate. The closer ρ' was to ρ^*, the closer these two bounds were, and when $\rho' = \rho^*$, the upper bound coincided with the lower bound.

Each photon received by Bob was different, and could be affected by Eve, so the received photon was in an infinite dimensional Hilbert space, which meant that ρ was infinite-dimensional. Numerical methods can only handle optimization problems where the variables are finite-dimensional, so we had to find a way to make ρ reduce to finite dimensionality. A photon number cutoff assumption was imposed, to achieve the dimensionality reduction of CVQKD, and the basis of Bob's infinite dimensional Hilbert space was a photon number state $\{|n\rangle : n \in N\}$, where N represented the natural number. This assumption assumed that the number of photons received by Bob was finite, and denoted as N_c. This assumption truncated the infinite-dimensional Hilbert space, and achieved the dimensionality reduction. The secret key rate obtained was reasonable when a large enough N_c was obtained. Improvement of the secret key rate was small when N_c was more than 20, as shown in Figure 4.

The imposed photon number cutoff assumption did not constitute a strict security proof; hence, we needed to find an exact security analysis method that eliminated the assumption. In the following, we specify this dimensionality reduction method.

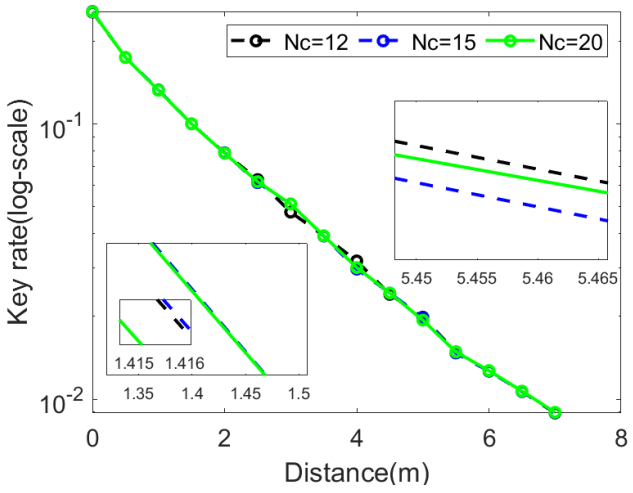

Figure 4. The secret key rate as a function of the transmission distance for the given photon cutoff numbers. The black dashed line is $N_c = 12$, the blue dashed line is $N_c = 15$, and the green line is $N_c = 20$. The key rate float is about 0.55% for N_c from 12 to 15, and 0.2% for N_c from 15 to 20. For the increased N_c, the secret key rate is not obviously improved, but the computation time increases significantly.

We used $\mathcal{H}_\infty$ to represent the infinite-dimensional Hilbert space in which ρ resided; $D(\mathcal{H}_\infty)$ to represent the normalized density operator on $\mathcal{H}_\infty$; $\tilde{D}(\mathcal{H}_\infty)$ to represent the set of semi-positive definite operators on $D(\mathcal{H}_\infty)$; S_∞ to represent the feasible set on $\tilde{D}(\mathcal{H}_\infty)$; and $\tilde{\rho}$ to represent the density operator on $\tilde{D}(\mathcal{H}_\infty)$. Then, the infinite-dimensional optimization problem could be formulated as

$$\min_{\tilde{\rho} \in \mathbf{S}_\infty} f(\tilde{\rho}). \tag{4}$$

We needed to find a density operator $\tilde{\rho}^\infty$, to achieve the optimal value, by projecting the infinite-dimensional space onto the finite-dimensional space, to obtain a reduced dimensional representation $\tilde{\rho}^N$ of $\tilde{\rho}^\infty$. With $\mathcal{H}_N$ representing the finite-dimensional Hilbert space on $\mathcal{H}_\infty$, the semi-positive definite density operator on $\mathcal{H}_N$ being denoted by $\tilde{D}(\mathcal{H}_N)$, and S_N denoting the feasible set on $\tilde{D}(\mathcal{H}_N)$, the following projection relations were satisfied:

$$\Pi \tilde{D}(\mathcal{H}_N) \Pi \subseteq \tilde{D}(\mathcal{H}_\infty), \quad \Pi S_\infty \Pi \subseteq S_N, \quad \Pi \tilde{\rho}^\infty \Pi \subseteq \tilde{\rho}^N, \tag{5}$$

and the finite-dimensional optimization problem was reformulated as

$$\min_{\tilde{\rho} \in \mathbf{S}_N} f(\tilde{\rho}), \tag{6}$$

where Π was a projection operator. Next, we needed to find $\tilde{\rho}^N$ that achieved the optimal value of $f(\tilde{\rho})$. As shown by [18], the infinite-dimensional optimization problem was related to the finite-dimensional optimization problem, in that

$$f\left(\tilde{\rho}^N\right) - \Delta(W) \leq f(\tilde{\rho}^\infty), \tag{7}$$

where $\Delta(W)$ was a non-negative correction term that was used to compensate for errors arising from the photon number cutoff assumption, and W represented the weight of the key rate bound outside the finite-dimensional subspace. The conditions also required that the projection of $f(\tilde{\rho})$ on S_∞ was nearly uniformly decreasing [18], satisfying $Tr(\tilde{\rho}^\infty) \leq W$. Therefore, we needed to determine four components in Equation (7): finite-dimensional

subspace $\mathcal{H}_N$; finite-dimensional feasible set S_N; weights W outside the subspace W; and correction term Δ.

By this stage, we had obtained all the components of the infinite-dimensional optimization problem; hence, the secret key rate under the infinite-dimensional space could be derived as

$$K_\infty = \left(\min_{\rho \in S_N} f(\tilde{\rho}) \right) - leak_{EC} - \Delta(W). \tag{8}$$

3.2. *Effects of Excess Noise*

In order to show the performance of the DM-CVQKD, we describe the characteristics of the underwater channel. Then, we show the effects of excess noise on the secret key rate.

In what follows, we demonstrate the transmission rate in the underwater channel. The calculation of the transmission rate of the underwater channel was complicated, involving water type and chlorophyll content, as shown in Appendix A. The attenuation rate was high in the underwater channel. We considered the Monte-Carlo model [19], where the communication light wavelength is 520 nm, and the water type is pure seawater. The transmission rate T of the underwater channel was related to the absorption coefficient a and the scattering coefficient b, depending on transmission distance and depth. Then, we had

$$T = e^{-cL}, \tag{9}$$

where c was a constant that involved the sum of a and b related to the depth.

Next, we considered the excess noise in the underwater channel. In Figures 5 and 6, we show the effects of excess noise ξ on the secret key rate. We took a step size of 0.005, and simulated in the interval $[0.005, 0.04]$ for excess noise. The result shows that the secret key rate decreased as the excess noise decreased gradually.

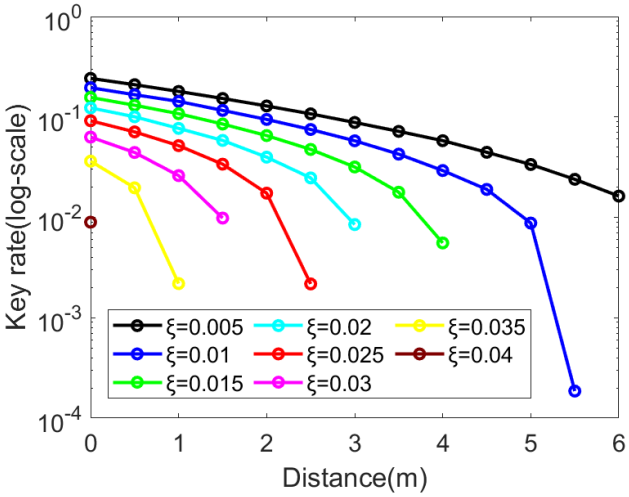

Figure 5. Effects of excess noise ξ on the secret key rate. The lines from top to bottom indicate the excess noise $\xi \in \{0.005, 0.01, 0.015, 0.02, 0.025, 0.03, 0.035, 0.04\}$. We set the amplitude $\alpha = 0.66$, post-selection parameter $\Delta = 0$, depth = 100 m, and reconciliation efficiency $\beta = 0.95$.

Moreover, the numerical simulations showed that the underwater DM-CVQKD system was sensitive to excess noise, and that the transmission distance decreased as the excess noise increased. When the excess noise reached 0.04, the maximum transmission distance in the underwater channel was less than 0.5 m.

3.3. Post-Selection

Alice and Bob were able to use post-selection for data reconciliation, filtering out unqualified data, so as to improve reconciliation efficiency and tolerance to excess noise, resulting in an increased secret key rate. When enabling the post-selection or not, we set the given post-selection parameter Δ to zero or greater than zero. As shown in Figure 6, we considered numerical simulations for types of excess noises.

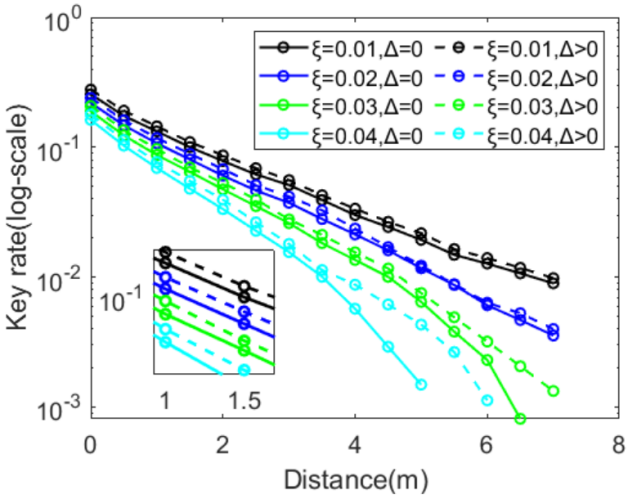

Figure 6. Effects of excess noise ξ on the secret key rate with the given post-selection. The solid line indicates $\Delta = 0$, and the dashed line indicates $\Delta > 0$.

We found that post-selection in CVQKD reduced the error rate, by discarding the results near zero: this was why, as the excess noise increased, erroneous results were more likely to occur around the zero point [21]. The numerical simulations showed that the post-selection operation improved the protocol key rate and the tolerance to noise. For the small excess noises, such as $\xi = 0.01$ and $\xi = 0.02$, the post-selection-involved improvement seemed small; when the excess noise reached $\xi = 0.03$, the post-selection was an obvious improvement on the secret key rate; therefore, the post-selection was necessary when the excess noise underwater became high.

3.4. Simulation Results

In Figure 7, we show the prediction of the secret key rate of the CVQKD system in an underwater channel. The parameter settings in numerical simulations are shown in Table 1.

Table 1. Parameter Setting.

Symbols	Value	Description
α	0.6–0.7	Amplitude
$\hat{q}$	–	Orthogonal amplitude components
$\hat{p}$	–	Orthogonal phase component
N_c	20	Photon cutoff number
ξ	0–0.04	Excess noise
Δ	0.01	Post-selection parameter
β	0.95	Reconciliation efficiency

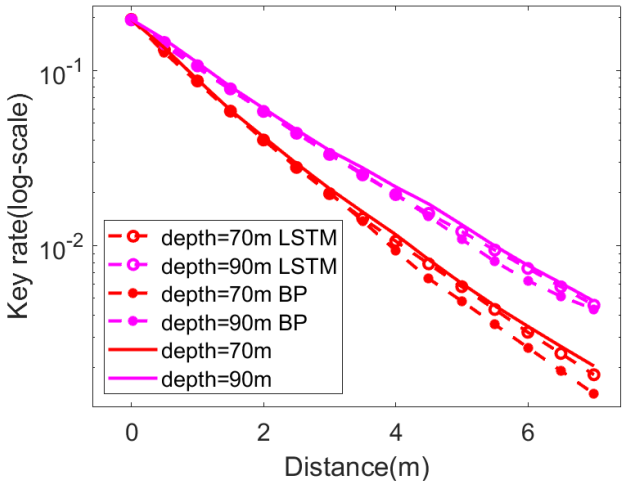

Figure 7. Prediction results of the NN-based CVQKD. Solid lines represent the initial value with photon cutoff method, the hollow dotted line represents LSTM-based NN, and the solid dotted line represents BP-based NN. The pink line represents a depth of 70 m, and the red line represents a depth of 90 m.

In order to demonstrate the advantage of the LSTM-based NN on performance improvement, we compared the prediction results of the LSTM-based NN and the BP-based NN to the traditional CVQKD, without involving the NN model. In the numerical simulations, we set excess noise $\xi = 0.01$, post-selection $\Delta = 0$, reconciliation efficiency $\beta = 0.95$, and modulation amplitude $\alpha = 0.66$, respectively. At the transmission distance of 0.5 m and 7 m, the prediction results of the BP-based NN and the LSTM-based NN improved by about 1.5% and 5.5%, respectively. According to the simulation results, both the BP-based NN and the LSTM-based NN showed performance improvement of the secret key rate, whereas the LSTM-based NN resulted in a higher secret key rate, compared to the BP-based NN.

4. Conclusions

We propose an NN approach to predicting the achievable secret key rate of the DM-CVQKD system through an underwater channel. The secret key rate of the CVQKD system can be improved when NN-based data post-processing is used for the receiver. In addition, the prediction performance of the LSTM-based NN model performs better than that of the BP-based NN model for the CVQKD. The numerical simulations show that the LSTM-based NN model can improve prediction accuracy compared to the BP-based NN model. Our approach paves the way for predicting the performance of the CVQKD system.

Author Contributions: Conceptualization, Y.M.; Writing—original draft preparation, Y.Z. and J.W.; Writing—review, G.L.; Writing—editing, Y.W. and Y.G.; Software, Y.Z., H.H. and G.L.; Investigation, Y.M. and Y.W.; Supervision, Y.G. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by the key research and development project in Hunan Province (Grant No. 2022GK2016), the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 22C0446), Key project of Scientific Research of Hunan Provincial Education Department (Grant No. 21A0470, 22A0669), and the Natural Science Foundation of Hunan Province (Grant No. 2023JJ50268, 2023JJ50269).

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request from the authors.

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

Appendix A. The Seawater Chlorophyll Model

Many factors—such as seawater density, turbulence, and bubble surface—have effects on light propagation in ocean quantum links.

Table A1. Variables of the ocean model.

	Meaning of the Variates	Parameter
$\mathrm{l}_{\mathrm{c}}^{0}$	Absorption coefficient of chlorophyll a at wavelength λ	0.009 m^2/mg
l_{w}	Loss of light propagation in pure water	0.0507 m^{-1}
$\mathrm{l}_{\mathrm{f}}^{0}$	Fulvic acid's absorption coefficient	35.959 m^2/mg
k_{f}	Fulvic acid's exponential coefficient	0.0189 nm^{-1}
λ	Wavelength	532 nm
l_{h}^{0}	Humic acid's absorption of coefficient	18.828 m^2/mg
k_{h}	Humic acid's exponential coefficient	0.01105 nm^{-1}
u_{b}	The surface's background chlorophyll content	0.0429 mg/m^3
s	Vertical gradient of concentration	-0.000103 mg/m^2
h	Total chlorophyll a above the background levels	11.87 mg
$d_{\max}$	Depth of the deep chlorophyll maximum	115.4 m
u_{chl}	Maximum chlorophyll concentration at the chlorophyll maximum layer	0.708 mg/m^3
m_{s}^{0}	Scattering coefficient of small particulate matter	$1.1513(400/\lambda)^{1.7}$
m_{l}^{0}	Scattering coefficient of large particulate matter	$0.3411(400/\lambda)^{0.3}$
m_w	Scattering coefficient of the pure water	$0.005826(400/\lambda)^{4.322}$
d	Depth of the ocean	

The deterministic losses caused by ocean extinction have an effect on transmittance:

$$T_{\mathrm{ext}} = e^{-zt}, \tag{A1}$$

where T_{ext} is extinction-induced transmittance, z denotes the transmission distance, and t is the seawater extinction coefficient, which is related to the wavelength λ, and is defined by

$$T = T_{\mathrm{abs}} + T_{\mathrm{sca}}. \tag{A2}$$

Here, t_{abs} is the ocean absorption factor, which has the form

$$T_{\mathrm{abs}} = \mathrm{l}_{\mathrm{c}}^{0}[\mathrm{u}_{\mathrm{c}}(\mathrm{d})]^{0.602} + \mathrm{l}_{\mathrm{w}} + \mathrm{l}_{\mathrm{f}}^{0}\mathrm{u}_{\mathrm{f}}(\mathrm{d})\mathrm{e}^{-\mathrm{k}_{\mathrm{f}}\lambda} + \mathrm{l}_{\mathrm{h}}^{0}\mathrm{u}_{\mathrm{h}}(\mathrm{d})\mathrm{e}^{-\mathrm{k}_{\mathrm{h}}\lambda}. \tag{A3}$$

The notation u_c is the chlorophyll, and it is defined as

$$u_c(d) = u_b + ds + \frac{h\sqrt{2\pi}}{\varsigma}\exp\left(-\frac{(d-d_{\max})^2}{2\varsigma^2}\right). \tag{A4}$$

The standard deviation of the concentration of chlorophyll ς is given by

$$\& = \frac{\mathrm{h}}{\sqrt{2\pi(\mathrm{u}_{\mathrm{chl}} - \mathrm{u}_{\mathrm{b}} - \mathrm{d}_{\max}\mathrm{s})}}. \tag{A5}$$

The content of fulvic acid is defined as

$$\mathrm{u}_{\mathrm{f}}(\mathrm{d}) = 1.74098\mathrm{u}_{\mathrm{c}}(\mathrm{d})\mathrm{e}^{0.12327\mathrm{u}_{\mathrm{c}}(\mathrm{d})}. \tag{A6}$$

The concentration of humic acid has the following form:

$$\mathrm{u}_{\mathrm{h}}(\mathrm{d}) = 0.19334\mathrm{u}_{\mathrm{c}}(\mathrm{d})\mathrm{e}^{0.12343\mathrm{u}_{\mathrm{c}}(\mathrm{d})}. \tag{A7}$$

The parameter t_{sca} is the scattering factor, given by

$$t_{\mathrm{sca}} = m_{\mathrm{s}}^{0}\mathrm{u_s(d)} + m_{\mathrm{l}}^{0}\mathrm{u}_{l}(\mathrm{d}) + m_{\mathrm{w}}, \tag{A8}$$

where $\mathrm{u_s(d)}$ represents the small particles' concentration, given by

$$\mathrm{u_s(d)} = 0.01739\mathrm{u_c(d)e}^{0.11631\mathrm{u_c(d)}}, \tag{A9}$$

and $\mathrm{u}_{l}(d)$ represents the large particles' concentration, given by

$$\mathrm{u}_{l}(d) = 0.76284\mathrm{u}_{c}(d)e^{0.03092\mathrm{u}_{c}(d)}. \tag{A10}$$

The meaning and parameter of these variables are summarized in Table A1.

References

1. Bennett, C.H.; Brassard, G. Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
4. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
5. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Ping, K.L. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [CrossRef]
6. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev.* **2019**, *9*, 021059. [CrossRef]
7. Liao, Q.; Liu, H.; Gong, Y.; Wang, Z.; Peng, Q.; Guo, Y. Practical continuous-variable quantum secret sharing using plug-and-play dual-phase modulation. *Opt. Express* **2022**, *30*, 3876. [CrossRef]
8. Liao, Q.; Xiao, G.; Xu, C.G.; Xu, Y.; Guo, Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. *Phys. Rev.* **2020**, *A102*, 032604. [CrossRef]
9. Lo H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604 . [CrossRef]
10. Beaudry, N.J.; Moroder, T.; Luetkenhaus, N. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.* **2008**, *101*, 093601. [CrossRef]
11. Tsurumaru, T. Squash operator and symmetry. *Am. Phys.* **2010**, *81*, 012328. [CrossRef]
12. Gittsovich, O.; Beaudry, N.J.; Narasimhachar, V.; Alvarez, R.R.; Moroder, T.; Lütkenhaus, N. Squashing model for detectors and applications to quantum-key-distribution protocols. *Phys. Rev.* **2014**, *89*, 12325. [CrossRef]
13. Zhang, Y.; Coles, P.J.; Winick, A.; Lin, J.; Lutkenhaus, N. Security proof of practical quantum key distribution with detection-efficiency mismatch. *Phys. Rev.* **2009**, *9*, 131–165. [CrossRef]
14. Braunstein, S.L.; Pati, A.K. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577. [CrossRef]
15. Weedbrook, C.; Pirola, S.; Garcia-Patron, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [CrossRef]
16. 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]
17. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [CrossRef]
18. Upadhyaya, T.; Himbeeck, T.V.; Lin, J.; Lütkenhaus, N. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. *PRX Quantum* **2021**, *2*, 020325. [CrossRef]
19. Xu, D.L.; Yue, P.; Yi, X.; Liu, J.Y. Improvement of a monte-carlo-simulation-based turbulence-induced attenuation model for an fiber wireless optical communications channel. *J. Opt. Soc. Am. Opt. Image Sci. Vis.* **2022**, *39*, 1330–1342. [CrossRef]
20. Liu, Z.P.; Zhou, M.G.; Liu, W.B.; Li, C.L.; Gu, J.; Yin, H.L.; Chen, Z.B. Automated machine learning for secret key rate in discrete-modulated continuous-variable quantum key distribution. *Opt. Express* **2022**, *30*, 15024–15036. [CrossRef]
21. Liu, W.B.; Li, C.L.; Xie, Y.M.; Weng, C.X.; Chen, Z.B. Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise. *PRX Quantum* **2021**, *2*, 040334. [CrossRef]
22. Rath, A.; Van Bijnen, R.; Elben, A.; Zoller, P.; Vermersch, B. Importance Sampling of Randomized Measurements for Probing Entanglement. *Phys. Rev. Lett.* **2021**, *127*, 200503. [CrossRef] [PubMed]
23. Mu, Y.; Ren, C.L.; Ma, Y.C.; Xiao, Y.; Guo, G.C. Experimental simultaneous learning of multiple non-classical correlations. *Phys. Rev. Lett.* **2019**, *123*, 190401.
24. Ahmed, S.; Muoz, C.S.; Nori, F.; Kockum, A.F. Classification and reconstruction of optical quantum states with deep neural networks. *Phys. Rev. Res.* **2021**, *3*, 033278. [CrossRef]
25. Hochreiter, S.; Schmidhuber, J. Long short-term memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef]

26. Hornik, K.; Stinchcombe, M.; White, H. Multilayer feedforward networks are universal approxmations neural networks. *Neural Netw.* **1989**, *2*, 359–366. [CrossRef]
27. Martinez-Cantin, R. Bayesopt: A bayesian optimization library for nonlinear optimization, experimental design and bandits. *J. Mach. Res.* **2014**, *15*, 3735–3739.
28. Will-Cole, A.R.; Kusne, A.G.; Tonner, P.; Dong, C.; Liang, X.; Chen, H.; Sun, N.X. Application of bayesian optimization and regression analysis to ferromagnetic materials development. *IEEE Trans. Magn.* **2022**, *58*, 2800108. [CrossRef]