electronics

MDPI

Article

Adjusting Optical Polarization with Machine Learning for Enhancing Practical Security of Continuous-Variable Quantum Key Distribution

Zicheng Zhou [1,2] and Ying Guo [2,3,*]

[1] School of Mathematics and Statistics, Qingdao University, Qingdao 266071, China
[2] School of Automation, Central South University, Changsha 410083, China
[3] School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: guoying@bupt.edu.cn

Abstract: An available trick to mitigate the interference of environmental noise in quantum communications is to modulate signals with time-polarization multiplexing. Conversely, due to effects of the atmospheric turbulence in free space, the polarization of signals fluctuates randomly, resulting in feasible information leakage when direct polarization demultiplexing is carried out at the receiver, drowning out the noise-contained signals. For enhancing the practical security of the continuous-variable quantum key distribution (CVQKD), we propose a machine learning (ML) approach for optimization of the dynamic polarization control (DPC) of signals transmitted through atmospheric turbulence. An optimal DPC scheme can be adaptively adjusted with ML algorithms, which is based on the received signals at the receiver for solving the loophole problem of information leakage since it provides an accurate response to the polarization changes regarding the anamorphic signals. The performance of the CVQKD system can be increased in terms of secret key rates and maximal transmission distance as well. Numerical simulation shows the positive effect of the ML-based DPC while taking into account the secret key rate of the CVQKD system. The ML-based DPC effectively reduces the feasibility of information leakage and hence results in an increased secret key rate of the practical CVQKD system.

Keywords: continuous-variable quantum key distribution; polarization control; machine learning

Citation: Zhou, Z.; Guo, Y. Adjusting Optical Polarization with Machine Learning for Enhancing Practical Security of Continuous-Variable Quantum Key Distribution. *Electronics* **2024**, *13*, 1410. https://doi.org/10.3390/electronics13081410

Academic Editor: Carlo Mastroianni

Received: 27 February 2024
Revised: 6 April 2024
Accepted: 7 April 2024
Published: 9 April 2024

1. Introduction

Quantum key distribution (QKD) is a kind of secure communication [1] that uses the principles of quantum mechanics to enable security for legitimate parties to exchange secret keys in quantum communications. Despite the challenges posed by optical extinction and the detrimental effects of atmospheric turbulence in free space, terrestrial free-space quantum key distribution (QKD) has garnered significant interest due to its inherent flexibility in establishing secure global communication links [2].

Traditional QKD schemes, which produce random secret keys for the two participants, Alice and Bob, can be composed of the discrete-variable (DV) QKD scheme [3,4] and the continuous-variable (CV) QKD scheme [5,6]. DVQKD encodes the secret key information of bits in polarization states of single photons, whereas CVQKD encodes the secret key information with the two related quadratures ($\hat{x}$ and $\hat{p}$) of optical fields, including either discretely modulated states (DM) or Gaussian modulation (GM) states. The initial QKD was called DVQKD since it makes full use of single photons for the signal source and the valuable single-photon detector for precise detection. For the counterpart CVQKD, it uses continuous light for the signal source and employs a homodyne detector or heterodyne detector for accurate detection. This method has the advantages of compatibility and usability, great strengths since they can be implemented with the available optical communication technology [6]. Since CVQKD was proposed in practical implementations, many schemes

have been proposed in the exploration of their theories and experimentation, such as smart detection of feasible eavesdroppers and different types of modulation of Gaussian states. The security of the corresponding CVQKD system has been proven regarding both the finite-size regime and asymptotic limit [7]. In addition, non-Markovianity has been used to enhance CVQKD system security [8,9]. Noisy propagation of Gaussian states has been demonstrated in optical media with finite bandwidth [10], which can potentially be used for performance improvement. However, there is little work on enhancement of practical security related to secret key generation at the receiver of a system.

In terms of the performance improvement of the CVQKD system, CVQKD can be performed by using quantum signals prepared with Gaussian modulations (GM) [11,12]. However, it is still hard to approach the low bound of quantum signal-to-noise ratios, which results in decreased reconciliation efficiency in practice [13,14]. Fortunately, the discretely modulated (DM) aspect of quantum signals has been suggested for CVQKD to break the low-bound limitations [15,16], and thus the security of the DM-CVQKD system with it has been theoretically proven in an asymptotic regime [17,18]. However, there are still loopholes in the practical CVQKD system that are vulnerable to attack. These loopholes can be used for weakening the security of the system by an eavesdropper who may perform potential attack strategies, such as a local oscillator (LO) attack [19,20], finite sampling bandwidth effects [21], wavelength attack [22,23], polarization attack [24], jitter in clock synchronization [25], and a blinding attack on the detector [26]. Consequently, there are several countermeasures determined to resist the aforementioned attack strategies. For example, measurement–device–measurement (MDI) CVQKD has been suggested in experiments for defending against potential attacks in detectors [27]. In addition, real-time shot-noise measurement detection [28] has been employed at the receiver to defend against LO-involved attacks. However, it is still vulnerable to practical security because of imperfectness of devices or appliances that contain potential loopholes concealed in the practical system.

For decades, continuous-variable quantum key distribution (CVQKD) has been rapidly developed and implemented due to its efficient source preparations and compatibility with current optical devices. For example, a pioneering demonstration of the feasibility of free-space CVQKD has been achieved using coherent polarization states under actual atmospheric circumstances. Building upon the advantages of coherent detection, such as resistance to background noise and high detection efficiency [29], the recent theoretical and experimental results have confirmed the practicality of all-day free-space quantum communications utilizing coherent detection. Some techniques have been proposed for promoting the experimental realization of free-space CVQKD, such as the Kramers–Kronig scheme [30] and discrete modulation scheme [31], where the effects of excess noise on the practical system were demonstrated to weaken the transmittance of quantum signals in atmospheric turbulence channels.

While implementing CVQKD in the free space channels in practice, the transmission coefficient usually fluctuates because of atmospheric turbulence effects. Phase modulation of coherent states plays an important role in performance improvement regarding the system [32]. In addition, probabilistic noiseless linear amplifiers can be employed both at the encoding stage [33] and at the decoding stage [34]. However, the coherent detection of the transmitted quantum signals at the receiver can be distorted by atmospheric turbulence, and the practical security of the CVQKD system will be weakened. Fortunately, dynamic polarization control (DPC) can be employed for mitigating the turbulence-induced wavefront aberrations of the received quantum states.

When considering the performance improvements of practical free-space CVQKD systems, DPC optimization turned out to be a perfect solution to the problem of deteriorated quantum signals through atmospheric turbulence channels [35]. However, the occurrence of fading in atmospheric turbulence channels can intensify the risk of a light leakage challenge [36], potentially leading to a decreased secret key rate of the free-space CVQKD system. The reason is that the polarization state of the weakened quantum signals is

deformed during propagation through the atmospheric turbulence channel. If polarization demultiplexing is not accurately estimated for data processing at the receiver, it may result in light leakage of the local oscillator into quantum signals. Consequently, effective and efficient DPC is required for the free-space CVQKD system. In this paper, we focus on an optimized DPC scheme based on machine learning algorithms [37], which can be used to redress the deteriorated quantum signals through atmospheric turbulence channels. Numerical simulations demonstrate the positive effect of the ML-based DPC on the practical security of the CVQKD system.

The organization of this paper is as follows. In Section 2, a DPC scheme is described for the receiver of the CVQKD system. In Section 3, we provide a theoretical derivation of the ML-based DPC to make an argument for the proposed scheme. In Section 4, the effects of the ML-based DPC on the free-space CVQKD system are illustrated with numerical simulations for security analysis. Section 5 draws the conclusions.

2. ML-based DPC Scheme

The polarization control scheme can be described as follows. As shown in Figure 1, the transmitted local oscillator and signals are received by a telescope, after passing through an atmospheric fading channel. They undergo an adjustment through a dynamic polarization controller (DPC) so that they can be successfully separated by the polarizing beam splitter (PBS). A portion of the light is split before and after PBS, measured via photoelectric detectors (PDs).

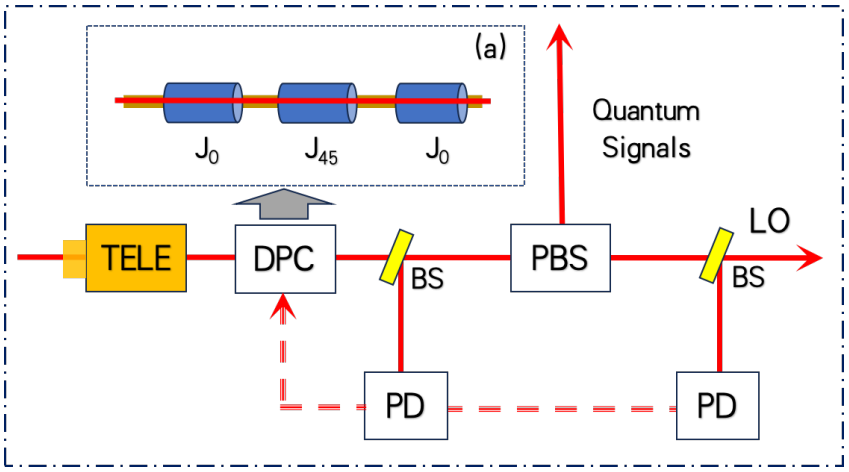

Figure 1. Schematic diagram of the dynamic polarization control scheme. (**a**) A cascade of 0-degree- and 45-degree-oriented fiber optic squeezers can be suitably adjusted to bring any input polarization state to a specified position regarding DPC. TELE, telescope; DPC, dynamic polarization controller; BS, beam splitter; PD, photodetector; PBS, polarizing beam splitter.

The ratio r_p of the light intensity of the input light fields of two PDs can be calculated as the feedback input signal to DPC, from which we have [36]

$$r_p = \frac{E_2^\dagger E_2}{E_1^\dagger E_1} = \frac{R_2 T_{\mathrm{PBS}}(1-R_1)}{R_1}\frac{I_{e2}}{I_{e1}}, \tag{1}$$

where E_1 and E_2 are input light fields described as

$$E_1 = \sqrt{R_1 T} e^{i\Delta\delta} J_{\mathrm{DPC}} E, \quad E_2 = \sqrt{R_2 T_{\mathrm{PBS}}(1-R_1)T} e^{i\Delta\delta} J_{\mathrm{PBS}} J_{\mathrm{DPC}} E. \tag{2}$$

Parameter E is is the Jones vector form of light emitted by Alice, T is the channel transmittance, $\Delta\delta$ is the channel-induced phase drift, T_{PBS} is the transmittance of the polarization BS, R_1 and R_2 are the reflectivity of the first and the second BS, and J_{PBS} and J_{DPC} are the Jones matrices of DPC and PBS, respectively.

Subsequently, we have the light intensities $I_{e1} = J_{\mathrm{DPC}}E$ and $I_{e2} = J_{\mathrm{PBS}}J_{\mathrm{DPC}}E$, respectively. We find that the effect of fluctuations in channel transmittance on light intensity is eliminated by the division operation $r_e = I_{e2}/I_{e1}$, and then we will focus on how to adjust DPC to maximize the parameter r_e.

DPC involves a cascade of fiber optic squeezers, as shown in Figure 1a. Different points on the Poincaré sphere represent the corresponding polarization states, and a cascade of fiber optic squeezers can be suitably adjusted to bring any input polarization state to a specified position. Taking 0-degree- and 45-degree-oriented fiber optic squeezers as an example, the Jones matrix of the DPC can be expressed as

$$J_{\mathrm{DPC}} = J_0(\gamma_3) \times J_{45}(\gamma_2) \times J_0(\gamma_1), \tag{3}$$

where γ_j, $\forall j \in \{1, 2, 3\}$ is the phase generated by the j-th fiber squeezer, $J_0(\gamma_j)$ and $J_{45}(\gamma_j)$ are matrices described as

$$J_0(\gamma_j) = \begin{pmatrix} e^{i\gamma_j/2} & 0 \\ 0 & e^{-i\gamma_j/2} \end{pmatrix}, \quad J_{45}(\gamma_j) = \begin{pmatrix} \cos(\gamma_j/2) & i\sin(\gamma_j/2) \\ i\sin(\gamma_j/2) & \cos(\gamma_j/2) \end{pmatrix}. \tag{4}$$

The Jones matrix of the PBS is provided by

$$J_{\mathrm{PBS}} = \begin{pmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix}, \tag{5}$$

where θ is the deflected angle of the optical axis.

When three fiber squeezers are cascaded in an optical fiber system, there exists a challenge to simultaneously adjust their parameters due to the mutual interactions between them. Since each squeezer introduces changes to the path length of the light propagating through the fiber, it results in phase delays that make it difficult for synchronous control. In what follows, we suggest a workflow of the dynamic polarization control system.

Step 1: Power up DPC and turn all fiber optic squeezers to half of the maximum voltage to allow for the direction adjustment of polarization states.

Step 2: Based on the derived ratio r_e as inputs to DPC, a machine learning algorithm is used to find the maximum value of r_p. Instead of adjusting all three fiber squeezers at the same time, we optimize the parameter r_p by independently regulating each fiber squeezer, whereas the voltages of the other squeezers are made constant during the process.

Step 3: When the optimal voltage value for the first DPC is achieved, the voltage on the first DPC will be provided to that voltage, and then repeat Step 2 until the optimal voltage value for each of the three DPCs is obtained.

This approach takes into account the fact that, when three fiber squeezers are cascaded in an optical fiber system, each one causes changes to the path length of the propagating light, resulting in phase delays that make it difficult for synchronous control.

3. Description of the CVQKD System

In the CVQKD system with Gaussian modulation, the transmitter Alice generates a series of Gaussian states $|\alpha_A\rangle$ involving amplitude I_A and phase θ [1]. In the phase space, the state $|\alpha_A\rangle$ can be described as

$$|\alpha_A\rangle = ae^{i\theta} = x_A + ip_A, \tag{6}$$

where $x_A = a\cos\theta$ and $p_A = a\sin\theta$ are both independent quadrature variables, with the variance denoted by V_A and a mean of zero. The variance V_A of quadratures variables x_A or p_A can be derived from $V_A = 2\langle n\rangle$, which is the average number of photons detected in the quantum signals. We have the relationship between the intensity I_A and the amplitude a, which can be described as $I_A \propto a^2$. When generating the quantum signals in an experiment, the parameters x_A and p_A demand constant change and adjustment to the suitable values, performed by Alice using the amplitude and phase modulators. After the transmitted

quantum signals arrive at the receiver, we assume that x_B and p_B are quadrature variables of the quantum signals. Therefore, we have the achieved Gaussian-modulated coherent state $|\alpha_B\rangle = x_B + ip_B$.

Apart from that, due to the influence of atmospheric turbulence in free space and the light leakage from the optical devices, the intensity of the quantum signals usually deviates from the initial value. Fortunately, effects of optical attenuation on the quantum signals can be avoided while performing real-time shot-noise measurement in practical CVQKD system. To carry out the shot-noise measurement, Bob first splits a part of the received quantum signals, which is put into a balanced homodyne detector. Subsequently, the interference between the separated quantum signals and the vacuum mode is used for evaluating the scattered noise in free space. Therefore, it is feasible to evaluate the variance of the received quantum signals through calibrating the relationship between the variance of scattered noise and the intensity of the quantum signals while we monitor the intensity of the quantum signals in real time. In what follows, we will focus on effect of the leakage of the Gaussian-modulated coherent state from the imperfect DPC on the performance of the CVQKD system.

Before performing the optimized DPC with the machine learning (ML) algorithms to achieve the maximum value of r_e, we demonstrate characteristics of quantum signals in what follows.

For any light beam, its Jones vector can be expressed as [36]

$$I = I_x e^{i(kz-\omega t+\phi_x)}\vec{x} + I_y e^{i\left(kz-\omega t+\phi_y\right)}\vec{y}, \tag{7}$$

where vectors $\vec{x}$ and $\vec{y}$ represent the unit vectors in the x-direction and y-direction of the coordinate axes, I_x and I_y represent the amplitudes, and ϕ_x and ϕ_y represent the initial phases, respectively. Therefore, I, which depends on two orthogonal components, determines its polarization state. It can be represented by

$$I = \begin{bmatrix} I_x e^{i(kz-\omega t+\phi_x)} \\ I_y e^{i\left(kz-\omega t+\phi_y\right)} \end{bmatrix}, \tag{8}$$

which can be simplified as $I = (I_x, I_y e^{i\delta})^T$ with $\delta = \phi_y - \phi_x$, omitting its common phase factor and using δ to denote the phase difference of I_x with respect to I_y. The known Stokes coefficients are a complete set of coefficients used to describe the polarization state of quantum signals provided by

$$S_0 = I_x^2 + I_y^2, \quad S_1 = I_x^2 - I_y^2, \quad S_2 = 2I_x I_y \cos\delta, \quad S_3 = 2I_x I_y \sin\delta. \tag{9}$$

4. Security Analysis

4.1. Derivation of the Secret Key Rate

The effect of the ML-based DPC on CVQKD can be assessed through the derived secret key rate. Alice and Bob can distill the secret key using the traditional parameters, such as variance V_A, transmittance of quantum channel T, reconciliation efficiency β, excess noise ε, detector efficiency η, and detector noise v_{el}. These parameters can be used for derivation of the maximum information available to the eavesdropper. Here, we employ reverse reconciliation as it has been shown to offer an advantage in the security analysis of CVQKD systems. We consider the finite-size effect of secret key rate K provided by [1,13]

$$K = \frac{n}{N}[\beta I_{AB} - S_{EB} - \Delta(n)], \tag{10}$$

where $n = N - m$ represents the number of received pulses that can be used for calculation of the secret key. In addition, the notation I_{AB} represents the mutual information between Alice and Bob, which is compatible with the statistics and can be calculated as follows

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A + \chi_{tot} + 1}{\chi_{tot} + 1}, \tag{11}$$

where $\chi_{tot} = \chi_{line} + \chi_{hom}/T$ represents channel's total noise with parameters $\chi_{line} = 1/T - 1 - \varepsilon$ and $\chi_{hom} = (1 + \nu_{el} - \eta)/T$. The notation S_{EB} denotes the maximum value of the Holevo information between Bob and Eve, which is determined by the covariance matrix provided by

$$\Gamma = \begin{bmatrix} u \cdot diag(1,1) & s \cdot diag(1,-1) \\ s \cdot diag(1,-1) & v \cdot diag(1,1) \end{bmatrix}, \tag{12}$$

where $u = V_A + 1$, $v = T_{min}(V_A + \epsilon_{max}) + 1$, and $s = \sqrt{T_{min}\left(V_A^2 + 2V_A\right)}$. Here, T_{min} represents the lower bound of T and ε_{max} represents the upper bound of ε. If the value of $m = N/2$ is large enough, then the resulting parameters T_{min} and ϵ_{max} can be expressed as

$$T_{\min} = \frac{(t + \Delta t)^2}{\eta}, \quad \epsilon_{\max} = \frac{\hat{\sigma}^2 + \Delta\sigma^2 - N_0(1 + \nu_{el})}{N_0 t^2}, \tag{13}$$

with the notations provided by

$$t = \sqrt{\eta T}, \quad \sigma^2 = \eta T\xi + \nu_{el} + 1, \quad \Delta t = Z_{\varepsilon_{PE}/2}\sigma/\sqrt{mV_A}, \quad \Delta\sigma^2 = Z_{\varepsilon_{PE}/2}\sigma^2\sqrt{2/m}. \tag{14}$$

Then, S_{EB} can be derived as follows,

$$S_{EB} = \sum_{i=1}^{2} G\left(\frac{\gamma_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\gamma_i - 1}{2}\right), \tag{15}$$

where $G(t) = (t+1)\log_2(t+1) - t\log_2 t$. The parameters $\gamma_{1,2}$ are the symplectic values that can be calculated as

$$\gamma_{1,2}^2 = \frac{1}{2}\left(U \pm \sqrt{U^2 - 4V}\right), \tag{16}$$

with the notations

$$U = u^2 + v^2 - 2s^2, \quad V = uv - s^2. \tag{17}$$

The parameters $\gamma_{3,4}$ are the symplectic values and can be written as

$$\gamma_{3,4}^2 = \frac{1}{2}\left(M \pm \sqrt{M^2 - 4F}\right), \tag{18}$$

with the notations

$$M = \frac{v + uV + U}{v + 1}, \quad F = \frac{V(u + V)}{v + 1}. \tag{19}$$

In addition, parameter $\Delta(n)$ is related to the security of privacy amplification. In the practical CVQKD system, it can be approximately derived as

$$\Delta(n) = \sqrt{-(\log_2\bar{\varepsilon} + 2\log_2\varepsilon_{PA})/n}, \tag{20}$$

where $\bar{\varepsilon}$ and ε_{PA} represent the smoothing parameter and the failure probability of privacy amplification, respectively. Typically, the above-mentioned parameters are assumed with the same value as $\bar{\varepsilon}$ since the value of ϵ_{PA} predominantly relies on the number n of the received quantum signals.

4.2. Numerical Simulations

The overnoise caused by the optical leakage of the actual principal vibrations of DPC can be defined as

$$\xi_{leak} = \frac{2n_0 T}{R_{\mathrm{AM}} R_{\mathrm{PI}}}, \tag{21}$$

where the average number of photons in the local oscillator (LO) is denoted by n_0, while the extinction ratio of amplitude modulator (AM) is represented by R_{AM}. In addition, let I and I_{leak} be the intensities of the signal light and the leaked light, respectively, and then we can define the gain g of the ML-based DPC. The output intensity of DPC can be denoted as I'. The detection efficiency increases as the optical intensity rises, and thus we have $T' = gT$. The additional noise decreases with the increase in optical intensity, from which we have $\varepsilon' = \varepsilon/g$. Consequently, there are two scenarios occurring in the practical CVQKD system. On the one hand, it involves DPC without the ML-based optimization, resulting in the secret key rate $K = (T, \varepsilon, v_{el})$, but, on the other, when the ML-based DPC is employed in CVQKD, we achieve the secret key rate $K_{leak} = (T', \varepsilon', v'_{el})$, where ξ_{leak} is included for derivation of v'_{el}. In numerical simulations, we consider the whale optimization algorithm (WOA) as an example to illustrate effect of the ML-based DPC under the leakage lights. The parameters are set as follows, $V_A = 4$, $n_0 = 4 \times 10^8$, $R_{\mathrm{AM}} = 63$ dB, $\eta = 0.5$, $v_{el} = 0.01$, $\beta = 95\%$, $\epsilon = 10^{-10}$, $N = 7 \times 10^9$, and $g = 1.5$, respectively.

Figure 2 shows the secret key rate with light leakage (denoted as K_{leak}) and the secret key rate without light leakage (denoted as K). To illustrate the performance of the CVQKD system, we compare with secret key rates K_{leak} and K. When the ML-based DPC fails to detect the imperfections that result in photon leakage, it may overestimate the actual secure key rate, compromising the practical security. The region below is achieved from the derived secret key rate K_{leak} when taking into account the photon leakage. When the secret key rate falls within this region, it is trustworthy, even in the presence of the information leakage of the imperfect DPC. As for the region above K, the security of the derived secret key rate of the system is not ensured. Additionally, the region between K_{leak} and K corresponds to the information leakage caused by the effects of the imperfect DPC on the system. When the secret key rate falls within this intersecting region, with the light leakage undetected, the leaked light results in a potential security loophole, which can be potentially employed by Eve to perform the attack strategy to steal the secret key. This loophole causes an overestimation of the secret key rate, leading to vulnerability to the practical security of the CVQKD system. The reason is that an eavesdropper may perform an intercept-resend attack strategy on the imperfect DPC, from which the secret key can be pilfered without being detected. Fortunately, the legal participants can trace back the information leakage with the ML-based DPC scheme, which can be used for defeating the leakage attack in CVQKD. Moreover, it can be observed that the ML-based DPC can raise the secret key rate of the CVQKD system, although the leakage can weaken its security. Consequently, we find an advantage of the ML-based DPC embedded in the CVQKD system.

In a practical CVQKD system, Eve can perform a DPC-involved attack. As shown in Figure 3, we demonstrate the secret key rate of the practical CVQKD system with or without the ML-involved DPC. It is obvious that the evaluated secret key rate k_e is overestimated in the absence of the protection of the ML-based DPC, which is compared with the secret key rate K_o of the system with the ML-based DPC. Numerical simulations show that, if the system has the ability to detect DPC-involved attacks, the practical secret key rate K_p will be made smaller than that of the secret key rate K_o with the ML-based DPC. Therefore, the DPC-involved attack will make the estimated secret key rate untrustworthy, whereas the estimated secret key rate can be increased with the ML-based DPC. In addition, in the absence of the ML-based DPC protection, the increase in output light intensity will give birth to the leakage of key information. The more output light intensity caused by the DPC-involved attack means the larger the difference between the evaluated security key rate and the actual value. Namely, the difference between the estimated secret key rate without

protection of DPC and the actual secret key rate under the same conditions shows that Eve can open a security loophole to distill the secret key from the practical CVQKD system.

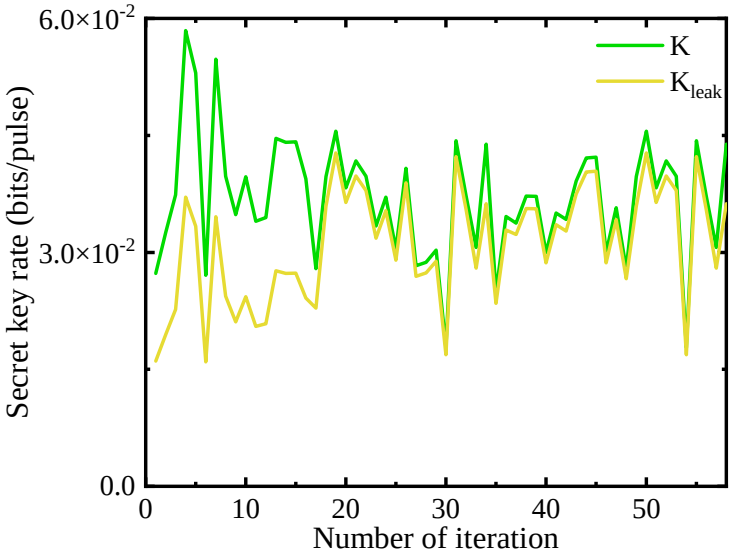

Figure 2. Secret key rate of the DPC-based CVQKD system using the whale optimization algorithm with light leakage.

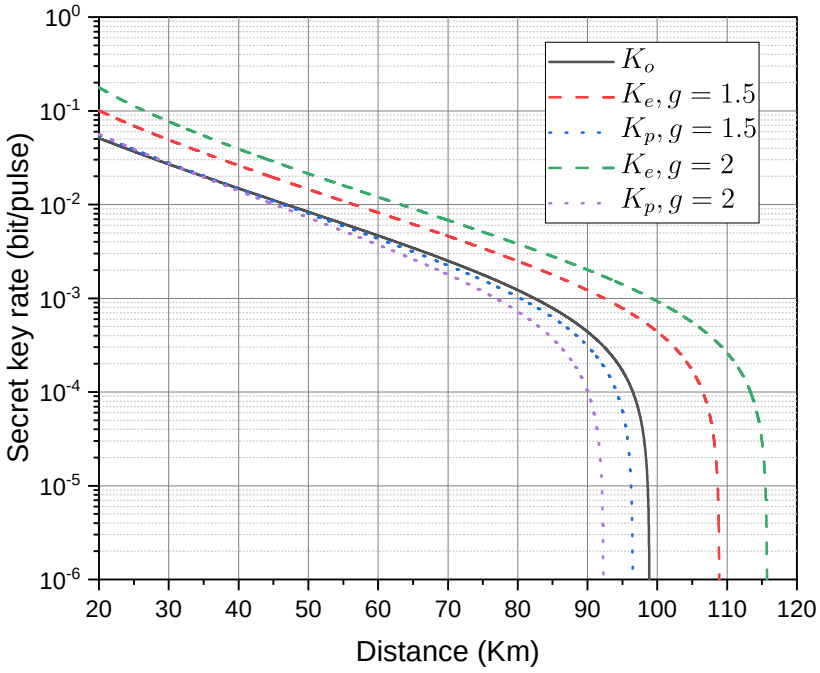

Figure 3. Secret key rate as a function of the transmission distance from Alice to Bob. The solid line represents the secret key rate without the ML-based DPC. The dashed curves represent the evaluated secret key rate K_e with the ML-based DPC. The dotted curves show the actual secret key rate K_p due to the optical leakage.

5. Conclusions

We suggested an ML-based DPC for optimizing the practical CVQKD system over fading channels with randomly fluctuating transmittance. The ML-based DPC can be improved in terms of its ability to handle the polarization deteriorations of the transmitted quantum signals in fading channels. An ML-involved optimization algorithm was used to deliver a precise response to the abnormal transformation of polarization states. Numerical

simulations confirmed the robustness and adaptability of the ML-based DPC while demonstrating its ability to quickly converge to the optimal configuration of quantum signals even under dynamic conditions. The proposed scheme demonstrated effectiveness in suppressing light leakage and preserving the integrity of deteriorated quantum signals, leading to increased reliability of practical CVQKD systems. We focused on revealing the oblivious imperfectness of DPC, which compromises the theoretical security of the CVQKD system. We note that assessment of DPC-involved light leakage allowed us to precisely evaluate the channel parameters, enabling the practical security enhancement of the CVQKD system. Actually, machine learning has been used for the design and implementation of quantum communications [38,39]. However, there are few studies regarding ML-involved DPC in a practical CVQKD system. As for the practical security of the system in terms of the ML-based DPC, we will consider its effects on the CVQKD system in our future work.

Author Contributions: Writing—original draft preparation, Z.Z.; writing—review and editing, Y.G. All authors have read and agreed 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 nos. 21A0470 and 22A0669), and the Natural Science Foundation of Hunan Province (grant nos. 2023JJ50268 and 2023JJ50269).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

References

1. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–699. [CrossRef]
2. Pirandola, S.; Andersen, U.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, 74, 145. [CrossRef]
4. Scarani, V.; Renner, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **2008**, *100*, 200501. [CrossRef]
5. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
6. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef]
7. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-variable quantum key distribution with gaussian modulation–the theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011. [CrossRef]
8. Vasile, R.; Olivares, S.; Paris, M.A.; Maniscalco, S. Continuous-variable quantum key distribution in non-Markovian channel. *Phys. Rev. A* **2011**, *83*, 042321. [CrossRef]
9. Teklu, B. Continuous-variable entanglement dynamics in Lorentzian environment. *Phys. Lett. A* **2022**, *432*, 128022. [CrossRef]
10. Teklu, B.; Bina, M.; Paris, M.A. Noisy propagation of Gaussian states in optical media with finite bandwidth. *Sci. Rep.* **2022**, *12*, 11646. [CrossRef]
11. Gottesman, D.; Preskill, J. Secure quantum key distribution using squeezed states. *Phys. Lett. A* **2001**, *63*, 022309. [CrossRef]
12. Usenko, V.C.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Lett. A* **2015**, *92*, 062337. [CrossRef]
13. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402. [CrossRef]
14. Becir, A.; El-Orany, F.A.A.; Wahiddin, M.R.B. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier. *Int. J. Quantum Inf.* **2010**, *10*, 12500041.
15. Guo, Y.; Liao, Q.; Huang, D.; Zeng, G. Quantum relay schemes for continuous-variable quantum key distribution. *Phys. Lett. A* **2017**, *95*, 042326. [CrossRef]

16. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2008**, *102*, 180504. [CrossRef] [PubMed]
17. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Lett. A* **2013**, *88*, 022339. [CrossRef]
18. Liao, Q.; Xiao, G.; Xu, C.G.; Xu, Y.; Guo, Y. Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source. *Phys. Lett. A* **2020**, *102*, 032604. [CrossRef]
19. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Lett. A* **2013**, *87*, 062313. [CrossRef]
20. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Lett. A* **2013**, *87*, 062329. [CrossRef]
21. Wang, C.; Huang, P.; Huang, D.; Lin, D.; Zeng, G. Practical security of continuous-variable quantum key distribution with finite sampling bandwidth effects. *Phys. Lett. A* **2016**, *93*, 022315. [CrossRef]
22. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Lett. A* **2013**, *87*, 052309. [CrossRef]
23. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Lett. A* **2016**, *94*, 012325. [CrossRef]
24. Zhao, Y.; Zhang, Y.; Huang, Y.; Xu, B.; Yu, S.; Guo, H. Polarization attack on continuous-variable quantum key distribution. *J. Phys. B* **2018**, *52*, 015501 [CrossRef]
25. Xie, C.; Guo, Y.; Liao, Q.; Zhao, W.; Huang, D.; Zhang, L.; Zeng, G. Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization. *Phys. Lett. A* **2018**, *382*, 811–817. [CrossRef]
26. Qin, H.; Kumar, R.; Makarov, V.; Alléaume, R. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Phys. Lett. A* **2018**, *98*, 012312. [CrossRef]
27. Li, Z.; Zhang, Y.C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Lett. A* **2014**, *89*, 052301. [CrossRef]
28. Kunz-Jacques, S.; Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Lett. A* **2015**, *91*, 022307. [CrossRef]
29. Wang, S.Y.; Huang, P.; Wang, T.; Zeng, G.H. Feasibility of All-Day Quantum Communication with Coherent Detection. *Phys. Lett. App.* **2019**, *12*, 024041. [CrossRef]
30. Zhen, Q.; Djordjevic, I.B. High-Speed Free-Space Optical Continuous Variable-Quantum Key Distribution Based on Kramers–Kronig Scheme. *IEEE Photonics J.* **2018**, *10*, 7600807.
31. Zhen, Q.; Djordjevic, I.B. Approaching Gb/s Secret Key Rates in a Free-Space Optical CV-QKD System Affected by Atmospheric Turbulence. In Proceedings of the 2017 European Conference on Optical Communication (ECOC), Gothenburg, Sweden, 17–21 September 2017. [CrossRef]
32. Teklu, B.; Genoni, M.G.; Olivares, S.; Paris, M.A. Phase estimation in the presence of phase diffusion: The qubit case. *Phys. Scr.* **2010**, *2010*, 140. [CrossRef]
33. Adnane, H.; Teklu, B.; Paris, M.A. Quantum phase communication channels assisted by non-deterministic noiseless amplifiers. *J. Opt. Soc. Am. B* **2019**, *36*, 2938–2945. [CrossRef]
34. Rosati, M.; Mari, A.; Giovannetti, V. Coherent-state discrimination via nonheralded probabilistic amplification. *Phys. Lett. A* **2016**, *93*, 062315. [CrossRef]
35. Karinou, F.; Comandar, L.; Brunner, H.H.; Hillerkuss, D.; Peev, M. Experimental evaluation of the impairments on a QKD system in a 20-channel WDM co-existence scheme. In Proceedings of the 2017 IEEE Photonics Society Summer Topical Meeting Series (SUM), San Juan, PR, USA, 10–12 July 2017.
36. Wang, S.Y.; Huang, P.; Wang, T.; Zeng, G.H. Dynamic polarization control for free-space continuous-variable quantum key distribution. *Opt. Lett.* **2020**, *45*, 5921–5924. [CrossRef] [PubMed]
37. Elhani, D.; Megherbi, A.C.; Zitouni, A.; Dornaika, F.; Sbaa, S.; Taleb-Ahmed, A. Optimizing convolutional neural networks architecture using a modified particle swarm optimization for image classification. *Expert Syst. Appl.* **2023**, *229*, 120411. [CrossRef]
38. Wallnöfer J.; Melnikov, A.A.; Dür W.; Briegel Hans, J. Machine Learning for Long-Distance Quantum Communication. *PRX Quantum* **2020**, *1*, 010301.
39. Melnikov, A.A.; Sekatski, P.; Sangouard, N. Setting Up Experimental Bell Tests with Reinforcement Learning. *Phys. Rev. Lett.* **2020**, *125*, 160401. [CrossRef]