entropy

MDPI

Article

Improving Underwater Continuous-Variable Measurement-Device-Independent Quantum Key Distribution via Zero-Photon Catalysis

Yuang Wang [1,†], Shanhua Zou [1,2,*,†], Yun Mao [1] and Ying Guo [1,2,3,*]

1 School of Automation, Central South University, Changsha 410083, China; wya1759991046@gmail.com (Y.W.); maocsu@sina.com (Y.M.)
2 School of Internet of Things Engineering, Wuxi Taihu University, Wuxi 214064, China
3 State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China
* Correspondence: 000037@wxu.edu.cn (S.Z.); yingguo@csu.edu.cn (Y.G.)
† These authors contributed equally to this work.

Received: 27 March 2020; Accepted: 16 May 2020; Published: 19 May 202

Abstract: Underwater quantum key distribution (QKD) is tough but important for modern underwater communications in an insecure environment. It can guarantee secure underwater communication between submarines and enhance safety for critical network nodes. To enhance the performance of continuous-variable quantum key distribution (CVQKD) underwater in terms of maximal transmission distance and secret key rate as well, we adopt measurement-device-independent (MDI) quantum key distribution with the zero-photon catalysis (ZPC) performed at the emitter of one side, which is the ZPC-based MDI-CVQKD. Numerical simulation shows that the ZPC-involved scheme, which is a Gaussian operation in essence, works better than the single photon subtraction (SPS)-involved scheme in the extreme asymmetric case. We find that the transmission of the ZPC-involved scheme is longer than that of the SPS-involved scheme. In addition, we consider the effects of temperature, salinity and solar elevation angle on the system performance in pure seawater. The maximal transmission distance decreases with the increase of temperature and the decrease of sunlight elevation angle, while it changes little over a broad range of salinity.

Keywords: continuous-variable quantum key distribution; measurement device independent; zero-photon catalysis; underwater channel

1. Introduction

Quantum key distribution (QKD) [1–3] is a key part of quantum communications. There are two categories of protocols, that is, the discrete-variable (DV) QKD protocol [4,5] and the continuous variable (CV) QKD protocol [6–8]. DVQKD, which was proposed in 1984 with the proposal of Bennett-Brassard 1984 (BB84) [9], codes on different states of a single photon to convey information. Currently, it has gotten fully developed and has been experimented in free space, optical fiber, and so forth. However, DVQKD can be easily interfered by various factors such as background noise light and noise from components. Besides, because single-photon source is quite hard to realize even nowadays, people use attenuating laser sources for substitution, which could exert bad effects on secret key rate. Fortunately, two decades after BB84 was proposed, CVQKD was born, which was based on the continuity of quantum eigenstate and modulates information on continuous variable of quantum such as phase and amplitude for communications. Compared with DVQKD, CVQKD can automatically filter background noise light with simple light source at the same time. Subsequently, CVQKD is compatible with contemporary optical communication system, which makes it a hot topic

in QKD realm quickly. Moreover, in terms of measurement devices, CVQKD relies on homodyne or heterodyne detectors, which are more efficient to achieve higher secret key rates than single-photon detectors. Of course, CVQKD is still imperfect. There exist disadvantages like short transmission distance, but these defects are being overcome by advancing technology.

Currently, there have been several CVQKD protocols in terms of system model, such as the point-to-point (PP) CVQKD and measurement-device-independent [10,11] (MDI) CVQKD [12]. PP-CVQKD, as literally interpreted, is conducted between two parties, Alice and Bob, directly. It is vulnerable to attacks aimed at detector imperfection. However, in MDI-CVQKD, Alice and Bob first prepare and transmit coherent states to the third party Charlie. Subsequently, Charlie interferes the received states to make Bell measurement and announces measurement results publicly. Finally, the secret key can be shared between Alice and Bob after post-processing. Compared with PP-CVQKD, MDI-CVQKD is born to solve the flaw of detector imperfection. It can resist side-channel attacks such as the local oscillator calibration attack [13], the wavelength attack [14], and the detector saturation attack [15].

At present, CVQKD is always conducted through free space and fiber channel, both of which are meaningful but challenging. Light transmission in air channel can be disturbed by natural environment like atmospheric turbulence [16–18], rain, fog, sunlight, and so forth. Fiber channel seems immune to external disturbance, but it is difficult to be wired up and could be easily destroyed. Underwater CVQKD may be more meaningful than air or fiber channel in a sense. Common QKD methods for two underwater vehicles nowadays are using periscopes and satellite link. However, these methods require underwater vehicles to rise to the sea surface. Fortunately, CVQKD can be feasibly implemented through underwater channel in practice, which provide a more convenient scheme for underwater vehicles to communicate safely. However, the realization of underwater CVQKD is more difficult considering attenuation caused by ocean current, molecular impact, microorganism, scattering, and so forth. These factors could exert adverse effects on entanglement between quantum, thus leading to short transmission distance. In what follows, we consider something different as the effects of temperature, salinity and sun elevation angle.

Recently, there have been several works for QKD underwater. For example, John proposed the underwater BB84 protocol using pairs of polarization entangled photons [19]. Bouchard suggested a high dimensional BB84 protocol with twisted photons in outdoor conditions [20]. After that Ruan proposed a method to estimate parameters to improve CVQKD performance [21]. However, the implementation of MDI-QKD underwater has been waiting for some researches to fill the gaps. Note that despite the absolute device security of MDI-QKD, its transmission distance is unsatisfactory, and thus it is difficult to be implemented in harsh environments like seawater. Fortunately, to lengthen the transmission distance, the non-Gaussian operations [22] like single photon subtraction (SPS) [23] and zero-photon catalysis (ZPC) [24] are the most commonly used means. One article has put forward a plan of operating single photon subtraction (SPS) in the fiber-based CVQKD [25]. In this paper, we dedicate to lengthen the transmission distance of underwater CVQKD via the Gaussian operations. Motivated by the characteristics of noiseless attenuation, we perform the zero-photon catalysis, which can keep the Gaussian behavior of photon to prolong the maximal transmission distance of the CVQKD system underwater with the achievable high secret key rate.

This paper is structured as follows. In Section 2, we propose the ZPC-based MDI-CVQKD for underwater secure communication. In Section 3, we show the performance improvement of the ZPC-based scheme by using numerical simulations. Finally, a conclusion is drawn in Section 4.

2. The ZPC-Based MDI-CVQKD Protocol

In this section, we suggest the ZPC-based MDI-CVQKD system through underwater channel. Due to the equivalence of prepare-and-measure (PM) scheme and entanglement-based (EB) scheme, we consider the EB ZPC-involved scheme to simplify the security proof of the underwater MDI-CVQKD system.

Figure 1 shows the schematic diagram of the EB ZPC-involved scheme. In this scheme, Alice in deep water aims to establish a secret channel with Bob in shallow water. Note that Alice and Bob may not locate in the same vertical area. For the convenience of demonstration, we suppose that Alice is vertically below Bob, and the transmission distance turns into depth. First, Alice and Bob prepare entanglement resource EPR1 and EPR2 with variances V_A and V_B, respectively. Then, they keep modes A_1 and B_1, and send other modes A_2 and B_2 to an untrusted party Charlie through water channel. To simplify equipment, we assume that the ZPC operation is conducted by David on Alice's side, which turns mode A_2 into mode $\widetilde{A_2}$. After that, Charlie receives modes $\widetilde{A_2}$ and B_2, and performs BSM (Bell state measurement)-based detection and announces measurement results P_{C_2} and X_{C_1} publicly through a classical channel. Ultimately, Bob modifies mode B_1 to mode $\widetilde{B_1}$ through operation $D(\alpha)$, where $D(\alpha)$ is a displacement operation. In this way, Alice and Bob obtain two mode A_1, $\widetilde{B_1}$ for heterodyne detection to get data (X_A, P_A) and (X_B, P_B), which can be used for estimation of channel parameter, coordinate information, and so forth. After series of post-processing, secret key will be achieved successfully.

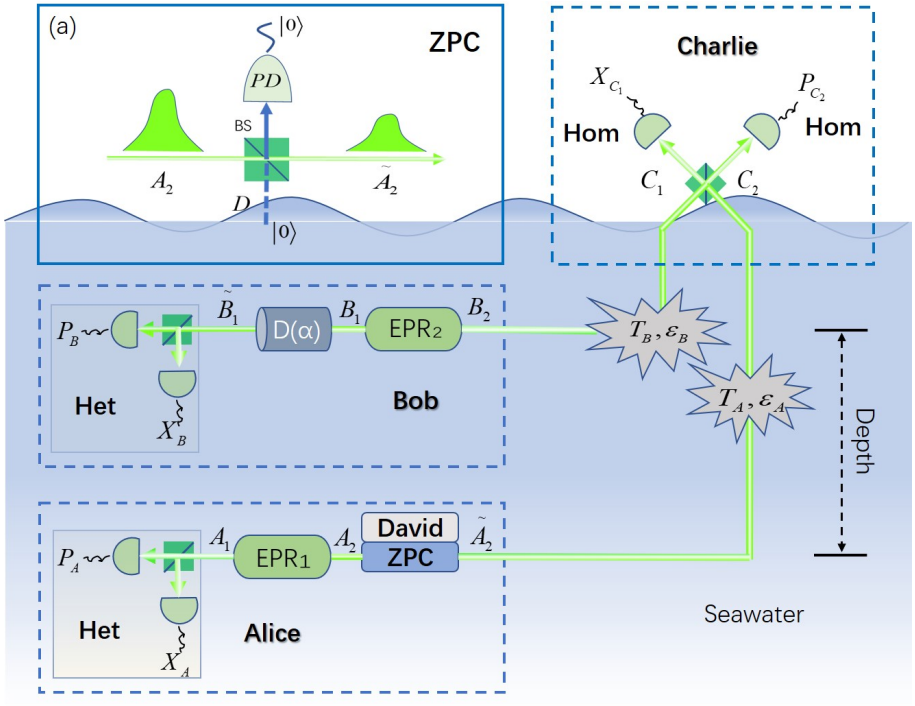


Figure 1. Schematic diagram of the zero-photon catalysis (ZPC) based measurement-device-independent-continuous-variable quantum key distribution (MDI-CVQKD) through underwater channel. Hom: homodyne detection, Het: heterodyne detection, PD: photon detector, BS: beam splitter.

As for the ZPC-involved data-processing shown in Figure 1 (a), vacuum state in auxiliary mode D is injected into an input port of beam splitter (BS) with transmittance T, which is detected at the corresponding output port of BS at the same time. That is exactly the ZPC operation. This process is usually represented by an equivalent operator given by

$$\hat{O_0} \equiv Tr[B(T)\prod_{\text{off}}^{\wedge}] = {}_D\langle 0|\, B(T)|0\rangle_D, \tag{1}$$

where $B(T)$ is the operator representing BS with transmittance T and can be described as

$$B(T) = \exp[\sqrt{T}-1)(a_2{}^{\dagger}a_2 + d^{\dagger}d) + (d^{\dagger}a_2 - da_2{}^{\dagger})\sqrt{1-T}], \tag{2}$$

and $\overset{\wedge}{\prod_{\text{off}}}$ is the projection operator in photon detector(PD), which here is an on/off detector. Now we consider how the ZPC operation makes effect. State EPR1 is essentially a two-mode squeezed vacuum state, which can be expressed as

$$\begin{aligned} |EPR_1\rangle_{A_1A_2} &= S_2(r)|0,0\rangle_{A_1A_2} \\ &= \sqrt{1-\lambda^2}\sum_{l=0}^{\infty}\lambda^l|l,l\rangle_{A_1A_2}, \end{aligned} \tag{3}$$

where $\lambda=\sqrt{(V_A-1)(V_A+1)}$. After conducting the ZPC operation, this state turns into $|\psi\rangle_{A_1\widetilde{A_2}}$, which can be described as

$$|\psi\rangle_{A_1\widetilde{A_2}} = \frac{\widehat{O}_0}{\sqrt{P_d}}|EPR_1\rangle_{A_1A_2}, \tag{4}$$

where $P_d = 2/(1+\mathrm{T}+(1-\mathrm{T})V_A)$, standing for the success probability of the ZPC operation. Subsequently, the covariance matrix of $|\psi\rangle_{A_1\widetilde{A_2}}$ can be calculated as

$$V_{A_1\widetilde{A_2}} = \begin{pmatrix} x\prod & z\sigma_z \\ z\sigma_z & y\prod \end{pmatrix}, \tag{5}$$

where $\sigma_z = \mathrm{diag}(1,-1)$, $x = y = (2V_A - RV_A + R)/(1+T+RV_A)$, and $z = 2\sqrt{T({V_A}^2-1)}/(1+T+RV_A)$. We note that the above-mentioned ZPC operation is actually a Gaussian operation in essence, which have an effect on the performance of the underwater CVQKD system.

3. Security Analysis

While demonstrating the effect of the ZPC-involved scheme on the underwater CVQKD system, we consider transmittance of seawater channel, which characterizes the transparency of seawater, thus affecting the ability of light transmission, which is shown in Appendix A. Subsequently, we show the performance improvement of the ZPC-based system.

3.1. Derivation of the Secret Key Rate

As shown in Figure 2, we have an equivalent point-to-point (PP) protocol of the underwater ZPC-based MDI-CVQKD. It should be noticed that the reasonableness of this equivalence has been proved [26]. Thus we use T_c and ε_{th} to represent the transmittance and excess noise of the PP CVQKD protocol given by

$$T_c = g^2 T_A/2, \tag{6}$$

and

$$\varepsilon_{th} = T_B/T_A(\varepsilon_B - 2) + \varepsilon_A + 2/T_A. \tag{7}$$

Taking into account the noise caused by Charlie's imperfect detection, the whole channel noise can be expressed as

$$\chi_{tot} = 1 - T_c/T_c + \varepsilon_{th} + 2\chi_{\mathrm{hom}}/T_A, \tag{8}$$

with $\chi_{\mathrm{hom}} = (\nu_{el}+1-\eta)/\eta$, where ν_{el} stands for electronic noise and η stands for quantum efficiency. The transmittance $T_{A(B)}$ of seawater channel can be expressed as

$$T_{A(B)} = e^{-\alpha(\lambda)D_{AC(BC)}}, \tag{9}$$

where $\alpha(\lambda)$ means attenuation coefficient shown in Appendix A.

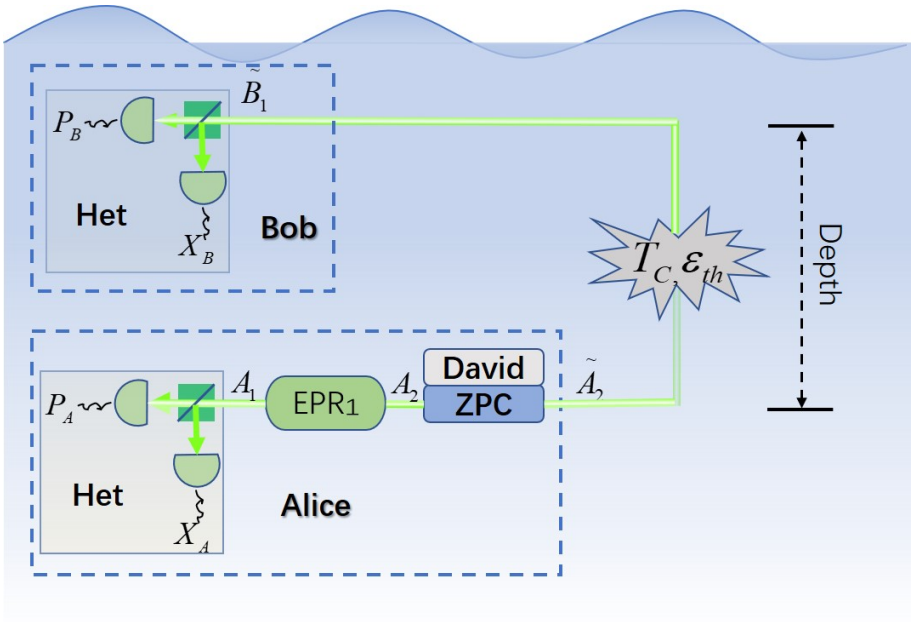


Figure 2. Schematic diagram of the ZPC-based point-to-point (PP) CVQKD system.

Different from non-Gaussian operation, after performing ZPC, the resulting state $|\psi\rangle_{A_1\widetilde{A_2}}$ is still a Gaussian state, thus it is reasonable to derive the secret key rate directly from the conventional Gaussian CVQKD given by

$$K{=}P_d\{(\beta I(A:B)) - \chi(B:E)\}, \tag{10}$$

where β means the reverse-reconciliation efficiency, $I(A:B)$ represents the mutual information between Alice and Bob, and $\chi(B:E)$ denotes the Holevo bound between Bob and Eve. Assuming $|\psi\rangle_{A_1\widetilde{B_1}}$ denotes the state when $|\psi\rangle_{A_1\widetilde{A_2}}$ passes through the channel in the equivalent PP CVQKD protocol, the covariance matrix of $|\psi\rangle_{A_1\widetilde{B_1}}$ can be described as

$$\begin{aligned} V_{A_1\widetilde{B_1}} &= \begin{pmatrix} X\prod & Z\sigma_z \\ Z\sigma_z & Y\prod \end{pmatrix} \\ &= \begin{pmatrix} x\prod & \sqrt{T_c}z\sigma_z \\ \sqrt{T_c}z\sigma_z & T_c(x+\chi_{tot})\prod \end{pmatrix}. \end{aligned} \tag{11}$$

Then, $I(A:B)$ can be calculated as

$$I(A:B){=}\log_2\frac{(X+1)(Y+1)}{(X+1)(Y+1)-Z^2}. \tag{12}$$

To calculate $\chi(B:E)$, we assume Eve is aware of David's existence and can purify the whole system $\rho_{A_1\widetilde{B_1}ED}$. Based on this, $\chi(B:E)$ can be described as

$$\begin{aligned} \chi(B:E) &{=}S(E) - S(E|B) \\ &= \sum_{i=1}^{2} G(\tfrac{\lambda_i-1}{2}) - G(\tfrac{\lambda_3-1}{2}), \end{aligned} \tag{13}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, representing the von Neumann entropy, and $\lambda^2_{1,2} = (\Delta \pm \sqrt{\Delta^2 - 4\omega^2})/2$ with $\omega = XY{-}Z^2$ and $\Delta = X^2{+}Y^2{-}2Z^2$.

3.2. Numerical Simulations

In the following, we show the performance improvement of the ZPC-based MDI-CVQKD in terms of the maximal transmission distance and the secret key rate as well, compared with the SPS-based MDI-CVQKD and the traditional MDI-CVQKD.

In numerical simulations of the secret key rate of the ZPC-based MDI-CVQKD, we set $D_{BC} = 0$, which is the asymmetric case that achieves the longest transmission distance. Moreover, we take into account $\varepsilon_A = \varepsilon_B = 0.01$, $\beta = 0.96$, $\eta = 1$, and $\nu_{el} = 0$. First of all, we consider the influence of the tunable variance V_A and V_B, where V_A and V_B are significant to system, as shown in Figure 3. For the simplicity, we set $V_A = V_B$. We find that the traditional scheme is sensitive to $V_A(V_B)$, whereas the SPS-based and ZPC-based schemes show the stable transmission depth even when $V_A(V_B)$ changes in a big range in Figure 3a. In addition, the secret key rate decreases fast with the increase of $V_A(V_B)$, as shown in Figure 3b. By contrast, the secret key rate of the other two schemes decrease slowly with the increase of $V_A(V_B)$. This result shows that the ZPC-based and SPS-based schemes have a more flexible application in the underwater CVQKD system.

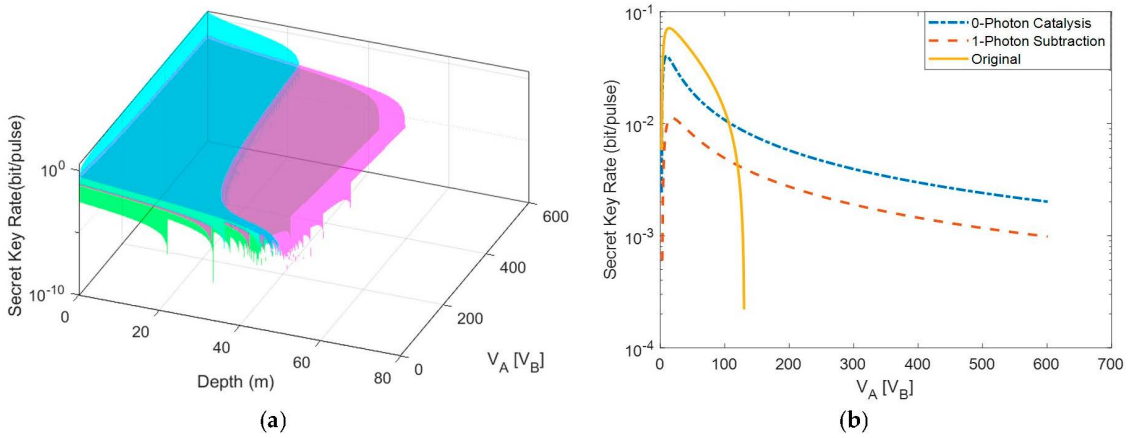
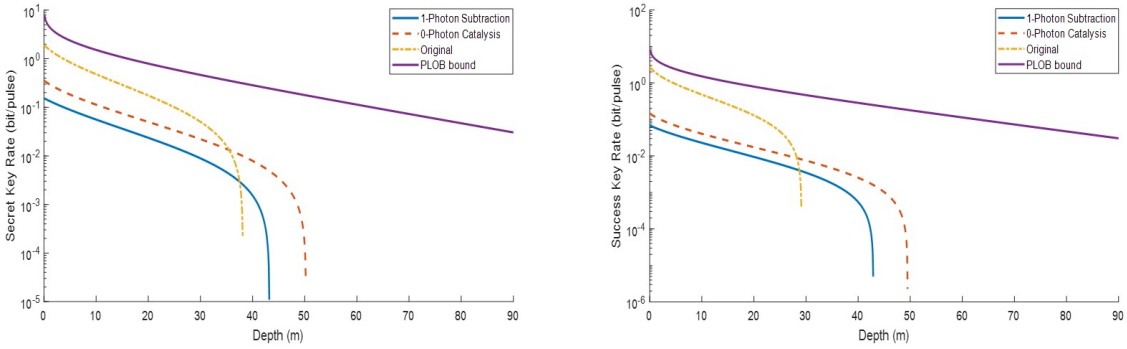


Figure 3. (**a**) The secret key rate as a function of V_A (V_B) for the traditional scheme (blue surface) and the ZPC-based (magenta surface) and the single photon subtraction (SPS)-based scheme (green surface). (**b**) A cross section of (a) where depth is set to 30 m for the traditional (yellow), the ZPC-based (blue), and the SPS-based (red).

Note that in practical system, the performance of CVQKD is related to the perfection of components. For example, the Faraday-mirror, which is used for adjusting the polarization angle of signal, is quite sensitive to the rotation angle. The rotation angle should be set as 45° accurately to make the polarization angles of signal and local oscillator orthogonal. However, in practice, the rotation angle could not be perfectly set, thus leading to the decrease of secret key rate, especially when transmittance T is small. Fortunately, increasing variance appropriately can provide us an efficient ploy to make up for the defects [27].

In Figure 4, we illustrate the performance of the related schemes in terms of the secret key rate and the maximal transmission depth under different variance. From Figure 4a, when variance V_A (V_B) is small, both underwater ZPC-based and SPS-based schemes show no obvious advantages in terms of depth compared with the condition on land. For the SPS-based scheme, it reaches the longest depth at about 43 m, which is close to that of the traditional scheme. For the ZPC-based scheme, it has the longest transmission distance of 50 m. This phenomenon may be caused by the small transmittance in the sea. Due to the small transmittance of seawater, the secret key rate of all three schemes comes to zero fast, thus giving fewer chances for the SPS-based scheme and ZPC-based scheme to show distance advantages. However, In Figure 4b, it shows a different result. When variance V_A (V_B) is increased, the longest distance of traditional scheme decreases to 30 m, while the performance of the SPS-based and ZPC-based schemes maintain stable. It seems that for the increased modulation

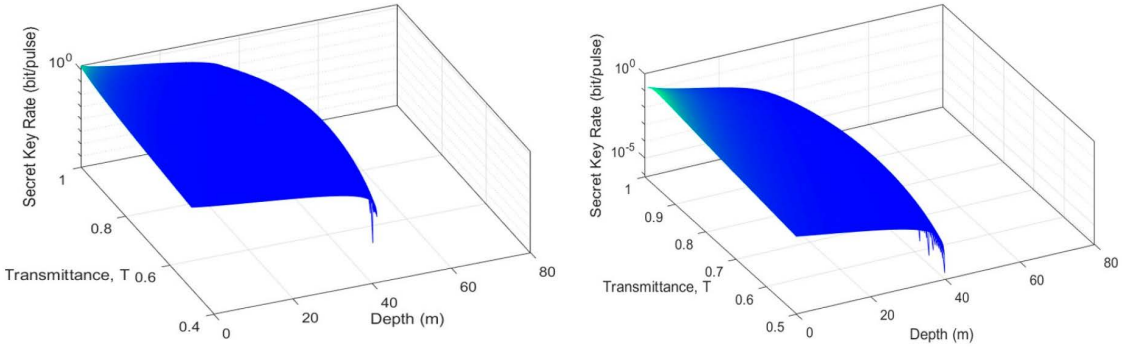
variance the SPS-based and ZPC-based schemes show better performance than the traditional protocol, of which the ZPC operation works better. Moreover, it also shows that for the high modulation variance, the ZPC-based scheme is the best among the three schemes discussed above.



(*a*) (*b*)

Figure 4. The secret key rate of the MDI-CVQKD system under pure seawater via the ZPC-based scheme, the SPS-based scheme, and the traditional scheme. T(SPS) = 0.9. The purple line represents PLOB [28] bound. (**a**). $V_A = V_B = 40$. (**b**). $V_A = V_B = 150$.

To show the advantages of the ZPC-based scheme over the SPS-based scheme, we plot the secret key rate as a function of transmittance (T) of beam splitter (BS) and depth. As shown in Figure 5, the ZPC-based scheme has apparent advantages in terms of both secret key rate and depth compared with the SPS-based scheme. Besides, from this figure, we can get the optimal transmittance (T) of both two schemes. We find that the optimal transmittance (T) is 0.75 for the ZPC-based scheme and 0.72 for the SPS-based scheme. This result proves that the ZPC operation does improve system performance and works better than the SPS operation.



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

Figure 5. The secret key rate of the MDI-CVQKD system under pure seawater for $V_A = V_B = 40$. (**a**) the ZPC-based scheme, (**b**) the SPS-based scheme.

Subsequently, we consider effects of factors of pure sea water on the ZPC-based MDI-CVQKD system. First of all, we consider the effects of temperature in Figure 6. It shows that the transmission depth changes by about 5 m when the temperature ranges from 0 °C to 40 °C. It seems that the colder the seawater means the better the performance. This characteristic is easily to be comprehended since colder seawater means weaker thermal movement of molecular, thus leading to weaker influence on the performance of the underwater CVQKD system. It should be noticed that this range of change is possible, considering differences in seasons, time in a day and geographical location.

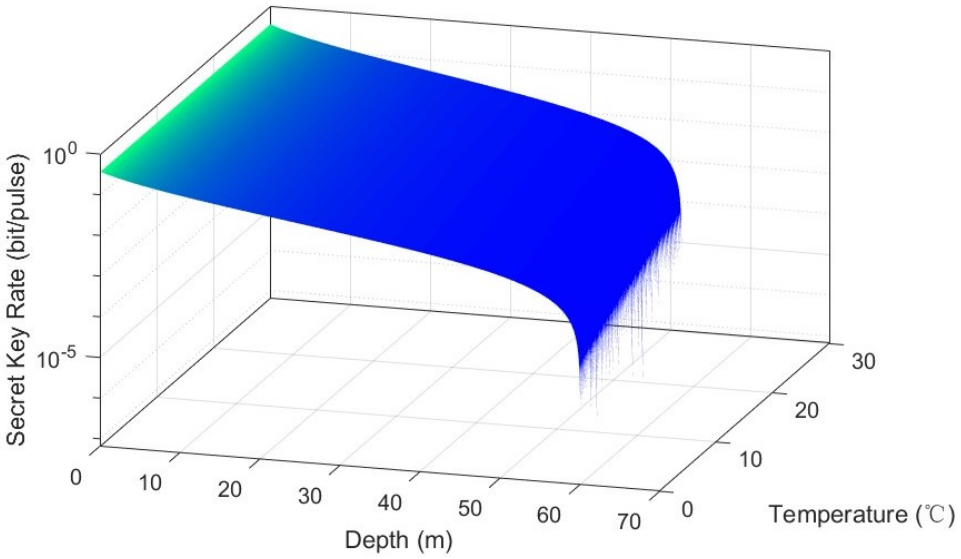


Figure 6. Relationship among secret key rate, transmission depth and temperature for $V_A = V_B = 40$.

Figure 7 shows the effects of sun elevation angle. Here we consider the influence that sunlight exerts on transmittance and omit the influence on the excess noise. The reason for this simplification is based on the assumption that the photon detector is ideal and not affected by background light. It is shown that depth lengthens by about 15 m when the sun elevation angle changes from 70° to 20°. Therefore, we could deduce that the underwater CVQKD system has the best performance around midday and has the worst performance at dusk. This result is quite different from the situation of CVQKD in free space, transmittance of which has little relationship to background light while background noise is influenced profoundly by background solar light.

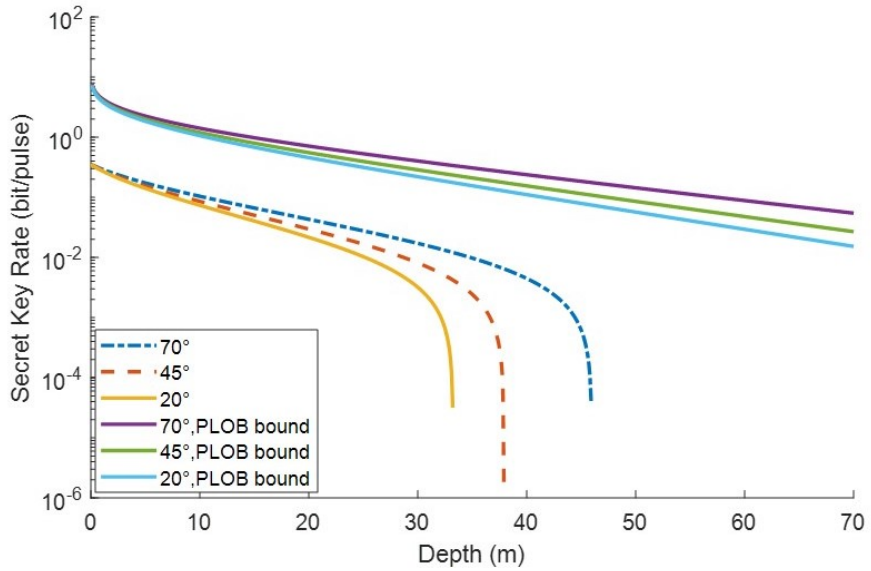


Figure 7. Secret key rate of the ZPC-based MDI-CVQKD in oligotrophic seawater under different sun elevation angle for $V_A = V_B = 40$. The upper three lines represent PLOB bound corresponding different sun elevation angle.

From simulation above, we can find that even if ZPC operation improves the performance of CV-MDI-QKD to some extent, our scheme is still constrained by transmission distance compared with conditions in fiber and open air, which is secure up to at least 100 km. However, its flexibility compared with fiber allows it to become the next generation of optical switch underwater. For example,

it can be used as a non-contact optical switch to establish secure net for underwater vehicles. Besides, it can be applied to optical communication system for autonomous underwater robots [29] and remote underwater robot operation [30]. Moreover, the development of underwater wireless optical communication (UWOC) provides another chance for our scheme. Recently, Sun verified the operation of UWOC at tens of gigabits per second or close to a hundred meters of distance [31]. With the help of our proposed scheme, UWOC will be safer and more credible.

4. Conclusions

We have proposed a ZPC-involved scheme for strengthening the security of the underwater MDI-CVQKD system in terms of the secret key rate and the maximal transmission depth. This scheme aims to establish a potential underwater MDI-CVQKD channel between two underwater parties. We consider the influence that the ZPC operation exerts on the MDI-CVQKD system and derive the secret key rate. To make it more persuasive, we compare the ZPC-involved scheme with the SPS-involved and traditional schemes as well. Numerical simulations show that the ZPC-involved scheme has better performance, prolonging the transmission depth by about 5 m. We find that the ZPC-involved scheme shows better performance obviously when the tunable modulation variance is set high. Besides, we consider the possible factors influencing our proposed method. It is found that temperature has a relatively considerable impact on transmission depth while salinity is not an important factor in terms of the maximal transmission depth and the secret key rate. In addition, sun elevation angle influences the system performance to some extent as well, which implies that the performance of the underwater CVQKD system may be changeable with different time.

Author Contributions: Conceptualization, writing–traditional draft preparation, Y.W. and Y.M.; software and validation, Y.M.; formal analysis, Y.W. and Y.M.; Data curation, S.Z.; supervision, Y.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (Grant No. 61871407).

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

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key Distribution
DVQKD	Discrete-variable Quantum key Distribution
CVQKD	Continuous-variable Quantum key Distribution
MDI	Measurement-device-independent
TMSV	Two-mode squeezed vacuum
SPS	Single-photon subtraction
ZPC	Zero-photon catalysis
EB	Entanglement-based
PM	Prepare- and-measure
Het	Heterodyne detection
Hom	Homodyne detection
BS	Beam splitter

Appendix A. A: Seawater Channel

Usually, transmittance is a function of distance (here means depth) D and attenuation coefficient $\alpha(\lambda)$. Since the transmission distance of light in seawater is short, seawater channel could be regarded as a linear attenuation model, which can be expressed as

$$T_{sea} = e^{-\alpha(\lambda)D}, \tag{A1}$$

where $\alpha(\lambda)$ is related to wavelength λ. In seawater, the blue-green light (450 nm < λ < 550 nm) has the smallest attenuation coefficient. For the performance improvement, we use 520 nm laser in numerical simulations. The attenuation coefficient $\alpha(\lambda)$ is affected by absorption and scattering [32,33]. Absorption, as it is literally comprehended, means irreversible energy loss of light caused by the interaction of photons and particles, which is a kind of electromagnetic action. However, scattering is a purely physical collision process happening between photons and particles, which just changes the direction of photon movement and does not cause energy degradation. Involving these two factors, the expression of $\alpha(\lambda)$ can be written as

$$\alpha(\lambda) = a(\lambda) + b(\lambda), \tag{A2}$$

where $a(\lambda)$ is absorption coefficient and $b(\lambda)$ is scattering coefficient. More specifically, the parameters $a(\lambda)$ and $b(\lambda)$ consist the effects of seawater and other particles given by [34]

$$a(\lambda) = a_w(\lambda) + a_{CDOM}(\lambda) + a_{phy}(\lambda) + a_{\text{det}}(\lambda), \tag{A3}$$

and

$$b(\lambda) = b_w(\lambda) + b_{phy}(\lambda) + b_{det}(\lambda), \tag{A4}$$

where w means pure sea water, $CDOM$ means colored dissolved organic matter, phy means plankton, and det means detritus. Consequently, it is impossible to calculate all impact factors. However, researchers have demonstrated some effects of factors such as chlorophyll, bubbles, and salt, providing us valuable experience. In fact, besides the above-mentioned factors, temperature and sunlight could have potential impacts on $\alpha(\lambda)$ as well. Therefore, we will further consider the mixing effects of temperature and salinity, and the effects of sun elevation angle in the following part of this section. Since the factors we consider have little effects on impurity not belonging to seawater, our security analysis is based on pure seawater.

Appendix A.1. Mixing Effects of Temperature and Salinity

In what follows, we consider the effect of temperature and salinity on the ZPC-based MDI-CVQKD in pure seawater environment. Then the attenuation coefficient α can be simplified to

$$\alpha = a_w + b_w, \tag{A5}$$

where a_w stands for absorption coefficient of seawater and b_w stands for scattering coefficient. Moreover, b_w contains two parts, the fluctuation of the density of pure water (b_{wd}) and the electro shrinkage effect of hydrated ions (b_{we}) given by

$$b_w = b_{we} + b_{wd}, \tag{A6}$$

where b_{we} and b_{wd} can be respectively expressed as

$$b_{we} = \frac{64\pi^5 NR^6(2+\delta)}{3\lambda^4(1+\delta)}\left(\frac{\varepsilon_{wa}-\varepsilon_{pw}}{\varepsilon_{wa}+2\varepsilon_{pw}}\right)^2, \tag{A7}$$

$$b_{wd} = \frac{8\pi^3}{\lambda^4}\left(\rho\frac{\partial n^2}{\partial\rho}\right)^2 k\tau\beta h(\delta), \tag{A8}$$

where λ is light wavelength, N is number of ions in unit volume, δ is solution depolarization, n is the refractive index of pure water, k is Boltzmann constant, β is isothermal compressibility, τ is absolute temperature, ρ is seawater density, R represents hydration radius [35], ε_{wa} and ε_{pw} represent the average dielectric constant of the hydrated ions and the average dielectric constant of pure

water respectively, and $h(\delta) = (2+\delta)/(7-7\delta)$. In addition, we take into account $\varepsilon_{pw} = {n_w}^2$, and $\varepsilon_{wa} = \varepsilon_{hw}(\mathrm{R}^3 - r^3)/r^3 + \varepsilon_i r^3/\mathrm{R}^3$, where r represents the effective radius of ions [36], ε_i is the Dielectric constant of ions, ε_{hw} denotes the Dielectric constant of water in the first hydrated layer. Both ε_i and ε_{hw} can be obtained from Clausius-Mossotti equation [37].

In Equation (12), it shows that the increase of N (number of ions in unit volume) will lead to the increase of b_{we}, whereas the increase of salinity will lead to the decrease of b_{wd}, as shown in Equation (13). Besides, the increase of temperature will cause the increase of b_{wd}. In reality, it is analyzed that b_{we} acts as the main factor affecting b_w because the increase of salinity also causes the increase of b_w, the trend of which is similar to that of b_{we}. However, b_we is quite small and is slightly influenced by salinity [38]. Therefore, we ignore the effect of b_w on the CVQKD system while deriving the secret key rate. Note that the scattering coefficient b_w is also negligible compared with the absorption coefficient a_w in terms of temperature [39].

Therefore, the change of total attenuation coefficient α with temperature and salinity mainly reflects the change of absorption coefficient a_w with temperature and salinity, and the change of attenuation coefficient and absorption coefficient is consistent. Note that the effect of temperature on absorption coefficient in seawater can be expressed as [40]

$$a_w(\lambda, T, S) = a_w(\lambda, T_0, 0) + \psi_S S + \psi_T (T - T_0), \tag{A9}$$

where T and T_0 mean real-time temperature and initial temperature respectively, S means salinity, ψ_S and ψ_T stand for linear salinity slope and temperature slope, respectively. From analysis all above, we obtain the expression of transmittance in pure seawater

$$T_{puresea} = e^{-[a_w(\lambda,T_0,0)+\psi_S S+\psi_T(T-T_0)]D}. \tag{A10}$$

To show the mixing effects of temperature and salinity visually, we simulate in the pure seawater environment, where attenuation coefficient α is around 0.04. Note that according to Reference [40], when λ = 520 nm, $\psi_S = -0.00002$ and ψ_T = 0.0002 for seawater respectively. In Figure A1, we find that temperature has a great influence on the attenuation coefficient α. Specifically, the attenuation coefficient α increases by 0.008 when temperature changes from 0 °C to 40 °C. However, salinity has little influence on the attenuation coefficient α. The range of 40 PSU brings no significant changes.

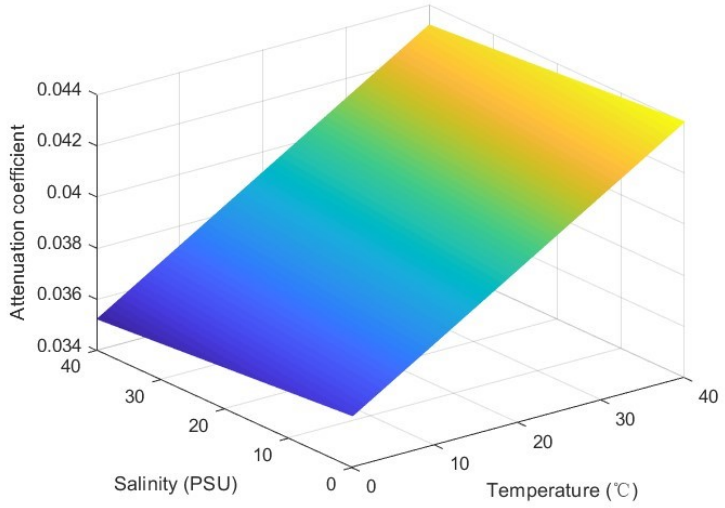


Figure A1. Effects of temperature and salinity on attenuation coefficient.

Appendix A.2. Effects of Sun Elevation Angle

Generally speaking, the intensity of sunlight, which is closely related to sun elevation angle, mainly influences transmittance of seawater and excess noise. In this section, we will have a deep insight into these two effects.

First, we study its influence on transmittance. It is generally admitted that the transparency and color of ocean water are determined by the optical properties of sea water, which are related to sunlight illumination. Thus, the optical properties changed by sunlight could have a certain impact on the underwater ZPC-based MDI-CVQKD system. To have a quantitative elaboration of the impact of sunlight or more specifically, the irradiance on the transmittance of seawater, we consider the effects of sun elevation angle on the performance of the CVQKD system.

Actually, the transmittance of seawater in different depth z relates with sun light through the following equation [41]

$$T_{sea}(z) = [E_d(z) + \mu_s F_s e^{-kz/\mu_s}]/(E_0 + \mu_s F_s), \tag{A11}$$

where $E_d(z)$ is downward irradiance, μ_s is the angle at which sun rays enter the water, and F_s is the irradiance from the sky just below the sea surface given by $F_s = qE_0$ with a parameter q related to characteristics of atmosphere and the air-water interface. In addition, E_0 is the irradiance of the sky diffuse light going into the water and $k = a + 2b_B$, where a is the absorption coefficient, and b_B is the backscattering coefficient. According to the Snellius law, μ_s and sun elevation angle have the following relationship

$$\mu_s = \sqrt{1 - \cos^2 h_s / {n_w}^2}, \tag{A12}$$

where h_s is the sun elevation angle, and n_w is the refraction coefficient of seawater (usually takes value 1.34). $E_d(z)$ can be calculated through irradiance attenuation coefficient, which takes different value in different depth z, given by

$$k_d(z) = -\frac{1}{E_d(z)} \times \frac{dE_d(z)}{dz}. \tag{A13}$$

Therefore, the relationship among $k_d(z)$, absorption coefficient a and scattering coefficient b can be expressed by [42]

$$k_d(z) = \frac{1}{\mu_0}[a^2 + G(\mu_0)ab]^{\frac{1}{2}}, \tag{A14}$$

where $G(\mu_0) = q_1\mu_0 - q_2$. q_1 and q_2 are related to the average value of $k_d(z)$, which in practice we often take the value of intermediate depth.

From the elaboration of $T(z)$, it is still not easy to get an accurate simulation of the transmittance $T(z)$. Fortunately, we can obtain data directly from the derived chart [41]. For example, the transmittance (520 nm light) of 10 m deep oligotrophic seawater is 62%, 56%, and 52% corresponding sun elevation angle of 70°, 45°, and 20°, respectively. Thus, it is possible to calculate the attenuation coefficient through the equation $\alpha = -\ln T/D$, which are 0.047, 0.057 and 0.065, correspondingly.

Then, we analyze its influence on excess noise. According to Reference [43], the solar background noise underwater is

$$P = L\Omega B\pi r^2, \tag{A15}$$

where $\Omega = \pi$ and L, B, r mean solar radiance, filter bandwidth determined by laser generating local oscillator (LO), radius of virtual telescope on sea surface to receive background light respectively. The parameter L can be calculated by

$$L = \frac{HRL_f e^{-cD}}{\pi}, \tag{A16}$$

where H is downwelling irradiance, $R = 1.25\%$, $L_f = 1$ are underwater reflectance of H and the factor of directional dependence of the underwater radiance. Finally, we derive the expression of excess noise underwater:

$$\varepsilon = \varepsilon_{\text{lim}} + \frac{\tau P}{h\nu}, \tag{A17}$$

where ε_{lim} means excess noise limit and is estimated as 0.01 (SNU), $\tau = 1$ ns is the reciprocal of frequency of homodyne detector at Bob's end, h is Planck's constant and ν is the frequency of noise photons, which is in the range of visible light. Note that H ranges from about 0.5 to 2 for clear day time. The according excess noise ranges from 0.01 to 0.012, which is so trivial that could be ignored.

References

1. Vazirani, U.; Vidick, T. Fully Device Independent Quantum Key Distribution. *Commun. ACM* **2019**, *62*, 133. [CrossRef] [CrossRef]
2. Eriksson, T.; Hirano, T.; Puttnam, B.; Rademacher, G.; Luís, R.; Fujiwara, M.; Namiki, R.; Awaji, Y.; Takeoka, M.; Wada, N.; et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2019**, *2*, 1301–1350. [CrossRef] [CrossRef]
3. Wang, Y.J.; Mao, Y.Y.; Huang, W.T.; Huang, D.; Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 25314–25329. [CrossRef] [CrossRef]
4. Gessner, M.; Pezzè, L.; Smerzi, A. Efficient entanglement criteria for discrete, continuous, and hybrid variables. *Phys. Rev. A* **2016**, *94*, 020101. [CrossRef] [CrossRef]
5. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. *arXiv* **2019**, *1906*, 01645. [CrossRef] [CrossRef]
6. Ye, W.; Zhong, H.; Liao, Q.; Huang, D.; Hu, L.Y.; Guo, Y. Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis. *Opt. Express* **2019**, *27*, 17186–17198. [CrossRef] [CrossRef] [PubMed]
7. Liao, Q.; Guo, Y.; Huang, D.; Huang, P.; Zeng, G. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection. *New J. Phys.* **2018**, *20*, 023015. [CrossRef] [CrossRef]
8. Zhao, W.; Guo, Y.; Zhang, L.; Huang, D. Coherent communications; Phase compensation; Phase estimation; Phase noise; Phase shift; Quantum key distribution. *Opt. Express* **2019**, *27*, 1838–1853. [CrossRef] [CrossRef] [PubMed]
9. Shor, P.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [CrossRef]
10. Braunstein, S.; Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef] [CrossRef]
11. Lo, H.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [CrossRef] [PubMed]
12. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.; Lloyd, S.; Gehring, T.; Jacobsen, C.; Andersen, U. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402. [CrossRef] [CrossRef]
13. Ma, X.; Sun, S.; Jiang, M.; Liang, L. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef] [CrossRef]
14. Huang, J.; Weedbrook, C.; Yin, Z.; Wang, S.; Li, H.; Chen, W.; Guo, G.; Han, Z. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef] [CrossRef]
15. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef] [CrossRef]
16. Paterson, C. Atmospheric Turbulence and Orbital Angular Momentum of Single Photons for Optical Communication. *Phys. Rev. Lett.* **2005**, *94*, 153901. [CrossRef] [CrossRef]
17. Berman, G.; Chumak, A. Photon distribution function for long-distance propagation of partially coherent beams through the turbulent atmosphere. *Phys. Rev. A* **2006**, *74*, 013805. [CrossRef] [CrossRef]
18. Semenov, A.; Töppel, F.; Vasylyev, D.; Gomonay, H.; Vogel, W. Homodyne detection for atmosphere channels. *Phys. Rev. A* **2012**, *85*, 013826. [CrossRef] [CrossRef]
19. Gariano, J.; Djordjevic, I. Theoretical study of a submarine to submarine quantum key distribution systems. *Opt. Express* **2019**, *27*, 3055–3064. [CrossRef] [CrossRef]

20. Bouchard, F.; Sit, A.; Hufnagel, F.; Abbas, A.; Zhang, Y.; Heshami, K.; Fickler, R.; Marquardt, C.; Leuchs, G.; Boyd, R.; et al. Underwater Quantum Key Distribution in Outdoor Conditions with Twisted Photons. *arXiv* **2018**, *1801*, 10299. [CrossRef]
21. Ruan, X.; Zhang, H.; Zhao, W.; Wang, X.; Li, X.; Guo, Y. Discrete-Modulated Continuous-Variable Quantum Key Distribution over Seawater Channel. *Appl. Sci.* **2019**, *9*, 4956. [CrossRef] [CrossRef]
22. Kitagawa, A.; Takeoka, M.; Sasaki, M.; Chefles, A. Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states. *Phys. Rev. A* **2006**, *73*, 042310. [CrossRef] [CrossRef]
23. Guo, Y.; Liao, Q.; Wang, Y.; Huang, D.; Huang, P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [CrossRef] [CrossRef]
24. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [CrossRef] [CrossRef]
25. Peng, Q.; Chen, G.; Li, X.; Liao, Q.; Guo, Y. Performance Improvement of Underwater Continuous-Variable Quantum Key Distribution via Photon Subtraction. *Entropy* **2019**, *21*, 1011. [CrossRef] [CrossRef]
26. Bennett, C.; Brassard, G.; Mermin, N. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef] [CrossRef]
27. Yang, R.H.; He, G.Q. The Influence of Faraday Mirror's Imperfection in Continuous Variable Quantum Key Distribution System. *Acta Photonica Sinica* **2015**, *44*, 2.
28. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef] [CrossRef]
29. Tian, B.; Zhang, F.; Tan, X. Design and development of an LED-based optical communication system for autonomous underwater robots. In Proceedings of the 2013 IEEE/ASME International Conference on Advanced Intelligent Mechatronics, Wollongong, Australia, 9–12 July 2013; pp. 1558–1563.
30. Doniec, M.;Detweiler, C.; Vasilescu, I.; Rus, D. Using optical communication for remote underwater robot operation. In Proceedings of the 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems, Taipei, Taiwan, 18–22 October 2010; pp. 4017–4022.
31. Sun, X.; Kang, C.; Kong, M.; Alkhazragi, O.; Guo, Y.; Ouhssain, M.; Weng, Y.; Jones, B.; Ng, T.; Ooi, B. A Review on Practical Considerations and Solutions in Underwater Wireless Optical Communication. *OSA* **2020**, *38*, 421–431. [CrossRef] [CrossRef]
32. Wiscombe, W. Improved Mie scattering algorithms. *Appl. Opt.* **1980**, *19*, 1505–1509. [CrossRef] [CrossRef]
33. Lock, J.; Gérard, G. Generalized Lorenz–Mie theory and applications. *J QUANT SPECTROSC RA* **2009**, *110*, 800–807. [CrossRef] [CrossRef]
34. Zeng, Z.; Fu, S.; Zhang, H.; Dong, Y.; Cheng, J. A Survey of Underwater Optical Wireless Communications. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 204–238. [CrossRef]
35. Danielewicz-Ferchmin, I. Phase Diagram of Hydration Shells in Ionic Solutions. *J. Phys. Chem.* **1995**, *99*, 5658–5665. [CrossRef] [CrossRef]
36. Shvab, I. Sadus, R. Structure and polarization properties of water: Molecular dynamics with a nonadditive intermolecular potential. *Phys. Rev. E* **2012**, *85*, 051509. [CrossRef] [CrossRef] [PubMed]
37. Coker, H. Empirical free-ion polarizabilities of the alkali metal, alkaline earth metal, and halide ions. *J. Phys. Chem.* **1976**, *80*, 2078–2084. [CrossRef] [CrossRef]
38. Farinato, R.; Rowell, R. New values of the light scattering depolarization and anisotropy of water. *J. Chem. Phys.* **1976**, *65*, 593. [CrossRef]
39. Duntley, S. Light in the Sea∗. *J. Opt. Soc. Am.* **1963**, *53*, 214–233. [CrossRef] [CrossRef]
40. Pegau, W.; Gray, D.; Zaneveld, J. Absorption and attenuation of visible and near-infrared light in water: dependence on temperature and salinity. *OSA* **1997**, *36*, 6035–6046. [CrossRef] [CrossRef]
41. Haltrin, V. Apparent optical properties of the sea illuminated by sun and sky: case of the optically deep sea. *Appl. Opt.* **1998**, *37*, 8336–8340. [CrossRef] [CrossRef]

42. Zaneveld, J.; Barnard, Z.; Boss, E. Theoretical derivation of the depth average of remotely sensed optical parameters. *Opt. Express* **2005**, *13*, 9052–9061. [CrossRef] [CrossRef]
43. Guo, Y.; Xie, C.; Huang, P.; Li, J.; Zhang, L.; Huang, D.; Zeng, G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [CrossRef]