



# Article Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution over Seawater Channel

Xinchao Ruan<sup>1</sup>, Hang Zhang<sup>1</sup>, Wei Zhao<sup>2</sup>, Xiaoxue Wang<sup>2</sup>, Xuan Li<sup>1,3</sup> and Ying Guo<sup>1,\*</sup>

- <sup>1</sup> School of Automation, Central South University, Changsha 410083, China; rxc1126@csu.edu.cn (X.R.); zhang22@csu.edu.cn (H.Z.); starrysky712@163.com (X.L.)
- <sup>2</sup> School of Computer Science and Engineering, Central South University, Changsha 410083, China; xunyicaozf@163.com (W.Z.); 174611021@csu.edu.cn (X.W.)
- <sup>3</sup> School of Economics and Management, Jingzhou Institute of Technology, Jingzhou 434020, China
- \* Correspondence: yingguo@csu.edu.cn; Tel.: +86-0731-8887-9336

Received: 16 October 2019; Accepted: 14 November 2019; Published: 18 November 2019



Abstract: We investigate the optical absorption and scattering properties of four different kinds of seawater as the quantum channel. The models of discrete-modulated continuous-variable quantum key distribution (CV-QKD) in free-space seawater channel are briefly described, and the performance of the four-state protocol and the eight-state protocol in asymptotic and finite-size cases is analyzed in detail. Simulation results illustrate that the more complex is the seawater composition, the worse is the performance of the protocol. For different types of seawater channels, we can improve the performance of the protocol by selecting different optimal modulation variances and controlling the extra noise on the channel. Besides, we can find that the performance of the eight-state protocol and there is little difference between homodyne detection and heterodyne detection. Although the secret key rate of the protocol that we propose is still relatively low and the maximum transmission distance is only a few hundred meters, the research on CV-QKD over the seawater channel is of great significance, which provides a new idea for the construction of global secure communication network.

Keywords: discrete modulation; seawater channel; continuous-variable quantum key distribution

# 1. Introduction

Continuous-variable quantum key distribution (CV-QKD) is one of the most promising technologies in the field of cryptography [1–3], which can avoid the risk of being eavesdropped to some extent, thus laying a theoretical and experimental foundation for the establishment of secure quantum information network. Most CV-QKD protocols typically utilize the Gaussian modulation scheme to distribute a shared secret string to the two distant users, but their secure transmission distance is limited, mainly because the reconciliation efficiency is quite low when the transmission distance is long [4,5]. To improve the performance of the protocol, discrete-modulated CV-QKD protocols were proposed. Thus far, CV-QKD protocols have been demonstrated in both fibers [6–8] and free-space air [9–11]. However, underwater CV-QKD has only recently become of interest to researchers. This is mainly because the oceans cover 70% of the Earth, and the completion of the undeveloped quantum communication under the seawater is an indispensable part for the establishment of a global secure communication network.

As an alternative to Gaussian modulation, discrete modulation scheme has attracted much attention in recent years. This is mainly because it not only allows us to simplify significantly both the modulation scheme and the key extraction task, but also makes it possible to distill secret keys

over much longer distance [12]. In Gaussian modulation, the secret information loaded onto the optical field is discrete data whose amplitude obeys the Gaussian distribution, and the information carrying amount is large, but the subsequent data are not easy to process. In the discrete modulation, the discrete 0 and 1 signals are directly modulated to the two orthogonal components of the optical field, and the information carrying capacity is slightly smaller, but it is easy to realize. When the channel attenuation is very large, the signal-to-noise ratio (SNR) is very low. In this case, if Gaussian modulation is adopted, the bit error rate will be very high, which brings great difficulties to error correction. However, if discrete modulation is adopted, the bit error rate can be reduced to a very low level. In this way, combining with low-density parity-check (LDPC) codes in classical communication, highly efficient error correction can be achieved. All of these indicate that discrete modulation is more suitable for long-distance transmission than its Gaussian counterpart.

Similar to quantum communication in free atmosphere [13–15], underwater secure communication is an indispensable part of the global secure communication network. In view of the complex composition and special optical properties of seawater, it is not easy to analyze the attenuation in the seawater channels and information errors in communication when developing underwater quantum communication. The absorption of light by seawater results in the loss of energy of the signal light reaching the receiver, thus affecting the final key generation. The scattering of light by seawater changes the polarization of photons, which in turn increases the error of information. The feasibility of quantum communication under seawater has been investigated theoretically [16,17] and demonstrated experimentally [18,19], but these studies are based on discrete variables. In recent years, with continuous variable quantum key distribution gradually becoming a research hotspot in the field of quantum communication, it has also been applied to the research model based on the seawater channel [20,21]. In this paper, we propose the discrete-modulated underwater CV-QKD protocol to improve the performance of the previous corresponding protocols that are based on Gaussian modulation. We investigate the optical property of the seawater channel and make an assumption for the security analysis of the protocol. Besides, the security of both the four-state protocol and the eight-state protocol in asymptotic and finite-size scenarios is analyzed.

This paper is organized as follows. In Section 2, we first briefly introduce the optical transmission characteristics of four different types of seawater, which are mainly reflected in the absorption and scattering of light by seawater, and then analyze the resulting changes in the intensity distribution of signal light during propagation. In Section 3, three kinds of underwater CV-QKD models with different link structures are presented, and the prepare-and-measure (PM) scheme and entanglement-based (EB) scheme of the discrete-modulated underwater CV-QKD with direct link structure are described in detail. In Section 4, the security of the protocol in asymptotic case and the finite-size scenario is analyzed. We conclude the paper in Section 5.

#### 2. Optical Transmission Characteristics of Seawater

Quantum key distribution can be realized by utilizing the "optical transmission window" of seawater to the blue and green light. However, it is difficult to make a detailed analysis of its transmission characteristics because of the complex composition of seawater and the influence of many factors such as environment and region. Here, we mainly take the influence of optical absorption and scattering on the performance of the CV-QKD system into account.

Absorption leads to the loss of light intensity, and scattering causes the deflection of light from its original direction [22], which is similar to beam-wander in the atmosphere [10]. Due to the existence of these two factors, the energy of the signal light that can be received by the receiver is continuously decaying. The absorption coefficient *a* and the scattering coefficient *b* are both functions of the optical wavelength  $\lambda$  and the chlorophyll concentration *C*, and they satisfy the following equation [20–23]

$$a(\lambda) = [a_w(\lambda) + 0.06a_c(\lambda)C^{0.65}][1 + 0.2e^{-0.014(\lambda - 440)}],$$
  

$$b(\lambda) = 0.3\frac{550}{\lambda}C^{0.62},$$
  

$$c(\lambda) = a(\lambda) + b(\lambda),$$
  
(1)

where  $a_w(\lambda)$  is the absorption coefficient of pure water,  $a_c(\lambda)$  is a nondimensional, statistically derived chlorophyll-specific absorption coefficient, and  $c(\lambda)$  is the total attenuation coefficient.

Without loss of generality, we mainly analyze four typical types of seawater, namely pure sea water, clear ocean water, coastal ocean water, and turbid harbor water, and the complexity of these four types of seawater increases gradually. The relationship between the attenuation coefficients of the four different types of seawater and the wavelength of the signal light is shown in Figure 1. As expected, the absorption and scattering coefficients of the four types of seawater to the signal light gradually increase with the complexity of seawater. It can also be seen in the figure that the scattering coefficient *b* decreases obviously as the wavelength increases, and this trend becomes more obvious with the increase of the complexity of the seawater. In addition, the scattering coefficient of turbid harbor water is much higher than the three other types water. By contrast, the light absorption coefficients of the four types of seawater on blue-green light with a wavelength of 450–550 nm, we select the light with a wavelength of 520 nm to study the influence of seawater on the secure transmission distance of the secure the simulation shown in Figure 1, and the values of each attenuation coefficients are listed in Table 1 [21,22,24].

 Table 1. Attenuation coefficients of four types of seawater at 520 nm wavelength.

Water Types	$a ({ m m}^{-1})$	$b ({ m m}^{-1})$	$c ({ m m}^{-1})$
Pure sea water	0.0405	0.0025	0.043
Clear ocean water	0.114	0.037	0.151
Coastal ocean water	0.179	0.219	0.398
Turbid harbor water	0.366	1.824	2.190

Without loss of generality, light with a wavelength of 1310 or 1550 nm is usually used as the signal light in standard single-mode fiber communication, and the corresponding attenuation coefficients are 0.34 and 0.21 dB/km, respectively [25,26]. In comparison, the attenuation coefficients of the optical signal propagating in the water channel are much larger than that in the fiber channel. As a result, the secure transmission distance of the secret key in a CV-QKD system mediated by a seawater channel is reduced by several orders of magnitude. In the case of such short distance communication, we can assume that the seawater channel is a linear attenuation model [20]. Similar to the optical fiber communication, transmittance of the seawater channel can be calculated by  $T_{sea} = e^{-cL}$ , where *c* represents the total attenuation coefficient and L is the transmission distance. Based on this assumption, taking the four-state protocol under the pure sea water channel as an example, we depict the light intensity distribution diagrams of the signal light at different transmission distances, as shown in Figure 2. Figure 2a represents the three-dimensional view of the light intensity distribution of the initial signal light at the sender, and Figure 2d is the corresponding plane view. Figure 2b,c illustrates the intensity distribution of the signal light at the receiver after transmitting through 8 and 20 m pure sea water, respectively, while Figure 2e,f presents their corresponding plane views. The three-dimensional views can describe the intensity variation of the signal light more vividly, while the plan views can show the divergence of the beam more intuitively. As can be seen in the figure, the energy of the beam is mainly distributed in the central focus position, and the farther it goes, the lower is its intensity. With the increase of the propagation distance, the intensity of signal light becomes weaker and the beam spot becomes larger at the reception plane. These are the obvious effects of the

absorption and scattering on the transmission of the signal light. There is no doubt that the longer is the transmission distance, the greater is the impact, and the worse is the performance of the quantum communication system.



**Figure 1.** (Color online.) The attenuation coefficients of the four different types of seawater as functions of wavelength of the signal light. The blue dashed line, the green dashed line, and the red solid line represent the change curves of the absorption coefficient  $a(\lambda)$ , the scattering coefficient  $b(\lambda)$ , and the total attenuation coefficient  $c(\lambda)$ , respectively.





**Figure 2.** (Color online.) Light intensity distribution at different transmission distances of the four-state protocol over a pure sea water channel: (**a**–**c**) the three-dimensional views of the intensity distribution of the signal light at the position of initial, 8 m, and 20 m of the seawater channel, respectively; and (**d**–**f**) are their corresponding plane views.

## 3. Description of the Discrete-Modulated Underwater CV-QKD

There are three main types of communication links in the end-to-end underwater continuous variable quantum key distribution system, namely the direct link, the feedback link and the reflection link, which are depicted in Figure 3. Direct link is the most common link structure in which signal light is transmitted from one side and received by the other. In this link structure, it is necessary to ensure accurate orientation between the sender and the receiver, so that the receiver can detect the light beam propagating along the direction of the transmitter. Feedback link can be viewed as a plug-and-play configuration [27,28], in which the signal light emitted by the sender is incident on a mirror, such as a Faraday mirror, and the receiver modulates the received signal light. The quantum information is then loaded onto the reflected light and fed back to the sender via the reverse channel. It should be noted here that the backscattering of the signal light on the forward channel may interfere with the reflected optical signal on the reverse channel, which may result in an increase in the bit error rate (BER) and a decrease in the SNR [29]. In addition, since the optical signal will pass through the seawater channel twice, the received signal will undergo extra attenuation. Reflective link utilizes the reflection of the sea surface to transmit information in case the signal light cannot travel in a straight line [30]. In this configuration, the transmitter projects the beam at an incident angle greater than the critical angle to the sea surface, causing it to experience total reflection. The receiver should keep the direction facing the sea surface roughly parallel to the reflected light to ensure proper reception of the signal. This structure is susceptible to the fluctuation of the sea surface.



(c) Reflection link

Figure 3. Three link models of end-to-end underwater CV-QKD system.

In this paper, we only consider the direct link structure of the end-to-end underwater continuous variable quantum key distribution for simplicity. In the previous investigation, the Gaussian modulated CV-QKD over the seawater channel has been investigated [20,21]. Although the transmission distance of the secret key is much shorter than that in optical fiber, the research still provides a new idea for us to study the underwater quantum communication and opens a new way for establishing a global quantum communication network. In what follows, the researchers should find ways to further promote the system so as to improve the performance of the system and finally realize practical application.

Studies have shown that discrete modulation is more suitable for long-distance communication than Gaussian modulation because of the relatively large key generation rate even at a lower SNR [12,31]. Up to now, different types of discretely modulated CV-QKD schemes have been investigated, including the four-state protocol, eight-state protocol, sixteen-state protocol, and so on. Here, we consider introducing this modulation scheme into the underwater CV-QKD system. The PM scheme can be described as follows:

- **Step 1** Alice firstly choose a random number *k* from the set  $\{0, 1, ..., N\}$  with equal probability to modulate the weak coherent light to prepare coherent states  $|\alpha_k\rangle = |\alpha e^{i(2k+1)\pi/N}\rangle$ , where  $\alpha$  is a positive number related to the modulation variance  $V_A$  and satisfies  $V_A = 2\alpha^2$ , and then sends them to the seawater channel.
- **Step 2** Due to the absorption and scattering of seawater, the quantum signal transmitted in the seawater channel will be attenuated. According to the above analysis, the transmittance of seawater channel to quantum signal is  $T_{sea}$  in the case of short distance. On the premise of assuming that the additional noise introduced by the seawater channel is  $\varepsilon$ , which mainly contributes to the variation of surrounding environmental factors, the noise added from the seawater channel referred to the channel input can be expressed as  $\chi_{ch} = 1/T_{sea} + \varepsilon 1$ .
- **Step 3** At Bob's side, the imperfect detector with efficiency  $\eta$  and electric noise  $v_{el}$  is used to measure the received coherent states. The noise introduced by the detector referred to Bob's input can be denoted as  $\chi_h$  in shot-noise units and it satisfies

$$\chi_{hom} = \left[ (1 - \eta) + v_{el} \right] / \eta \tag{2}$$

for homodyne detection, and

$$\chi_{het} = [(2 - \eta) + 2v_{el}]/\eta$$
(3)

for hetrodyne detection. The total noise referred to the channel input can be expressed as  $\chi_{tot} = \chi_{ch} + \chi_h / T_{sea}$ .

The EB version of the protocol is shown in Figure 4 and it can be described as follows:

**Step 1** Alice prepares two-mode entangled states  $|\Phi_N\rangle$  with variance of  $V = 1 + V_A$ , which can be defined as

$$|\Phi_N\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |\psi_k\rangle |\alpha_k\rangle, \tag{4}$$

where the states

$$|\psi_k\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} e^{i(2k+1)m\pi/N} |\phi_m\rangle$$
(5)

are orthogonal non-Gaussian states. The state  $|\phi_m\rangle$  is written as follows:

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} \frac{\alpha^{Nn+k}}{\sqrt{(Nn+k)!}} |Nn+k\rangle, \tag{6}$$

where

$$\lambda_{k} = e^{-\alpha^{2}} \sum_{n=0}^{\infty} \frac{(\alpha^{2})^{Nn+k}}{(Nn+k)!},$$
(7)

and  $|Nn + k\rangle$  denotes the Fock state with Nn + k photons. Subsequently, she performs the projective measurements  $|\psi_k\rangle\langle\psi_k|$  (k = 0, 1, ..., N - 1) on the half of the states (mode A) to get the variables  $X_A$  and  $P_A$ , thus preparing the coherent state  $\alpha_k$  when her measurement gives the result k. The other half of the states (mode  $B_0$ ) is then sent to Bob through the seawater channel. The quantum state attenuated by the seawater channel can be represented by the mode  $B_1$ .

- **Step 2** At Bob's side, the electronic noise introduced by the imperfect detector causes the received quantum state to be transformed before measurement, and the transformed quantum state can be represented by the mode *B*. Bob decides to measure one quadrature with homodyne detector or two quadratures with heterodyne detector to get the variable  $X_B$  ( $P_B$ ) or both  $X_B$  and  $P_B$  of the mode *B*, and then decodes the information by the sign of his measurement results. The electronic noise  $v_{el}$  can be modeled by an EPR state of variance  $V_d$ . For homodyne detection, we have  $V_{dhom} = \eta \chi_{hom}/(1 \eta)$ , and for heterodyne detection,  $V_{dhet} = (\eta \chi_{het} 1)/(1 \eta)$ .
- **Step 3** Bob sends the absolute value results to Alice through a classical channel, and they perform the post-processing procedures, including reverse reconciliation, privacy amplification and so on to share the final secret key.



**Figure 4.** The entanglement-based scheme of the discrete-modulated underwater CV-QKD. Alice randomly prepares one of the *N* states and sends it to Bob through the untrusted seawater channel. Bob detects the received model to derive a sequence of bits shared with Alice by using a homodyne detector or a heterodyne detector. The seawater channel is assumed to be a linear channel.

# 4. Security Analysis and Numerical Simulation

We mainly analyzed the security of the discrete-modulated underwater CV-QKD protocol under collective attack in asymptotic case and finite-size regime. The performance of the underwater communication systems based on the four-state protocol and the eight-state protocol were analyzed by numerical simulation, and the parameters were optimized to improve the system performance.

#### 4.1. Asymptotic Security Analysis

With a reverse reconciliation efficiency  $\beta$ , the secret key rate of the protocol is [12,32,33]

$$K \ge \beta I(A:B) - S_N(E:B), \tag{8}$$

where I(A : B) is the Shannon mutual information between Alice and Bob, and it can be calculated as

$$I(A:B) = \frac{1}{2} log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}},$$
(9)

for the homodyne detection case, and

$$I(A:B) = log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}},$$
(10)

for the heterodyne detection case. Besides,  $S_N(E : B)$  is the Holevo bound of the mutual information between Eve and Bob, and there is

$$S_N(E:B) = S(E) - S(E|B).$$
 (11)

Therefore, the key to calculate the secret key rate is how to calculate S(E) and S(E|B).

After Bob applies homodyne or heterodyne measurement, Eve purifies the whole system so that S(E) can be replaced by  $S(AB_1)$ , namely

$$S(E) = S(AB_1) = \sum_{i=1}^{2} G(\lambda_i),$$
 (12)

where

$$G(\lambda_i) = \frac{\lambda_i + 1}{2} \log \frac{\lambda_i + 1}{2} - \frac{\lambda_i - 1}{2} \log \frac{\lambda_i - 1}{2},$$
(13)

and  $\lambda_i$  (*i* = 1, 2) is the symplectic eigenvalues of the covariance matrix  $\gamma_{AB_1}$ . The conditional entropy S(E|B) satisfies

$$S(E|B) = S(\rho_{AFG}^B) = \sum_{i=3}^{5} G(\lambda_i),$$
 (14)

where  $\lambda_i (i = 3, 4, 5)$  is the symplectic eigenvalues of the conditional covariance matrix  $\gamma^B_{AFG}$ . The specific calculation process of the symplectic eigenvalues is shown in Appendix A.

Based on the above discussion, we can analyze the performance of the four-state and eight-state underwater CV-QKD protocols with homodyne detection and heterodyne detection for the four typical seawater types. For the underwater CV-QKD protocol, its performance is mainly affected by three parameters, namely channel transmissivity  $T_{sea}$ , excess noise  $\varepsilon$ , and Alice's modulated variance  $V_A$  [34]. Therefore, we can analyze the performance of the protocol from these three aspects.

Figures 5 and 6, respectively, show the relationship between secret key rate and distance for the underwater four-state and eight-state protocols in different types of seawater. Here, homodyne detection and heterodyne detection are considered. It is obvious that the secret key rate and the transmission distance decrease sharply with the increase of complexity of seawater; especially when the turbid harbor water is used as the quantum channel, the secure transmission distance of the key is less than 3 m. This result is what we expect. The main reason is that the complexity of seawater increases the attenuation of light, thus reducing the transmittance of signal light in the seawater channel. This indicates that channel transmittance has a great influence on the performance of the system. In addition, by comparing the performance of the protocol in the homodyne and heterodyne detection conditions, we can find that there is little difference between them, which is associated with the relatively small modulation variance. Compared with Figures 5 and 6, we can also find that the four-state protocol is obviously outperformed by the eight-state protocol. Under the eight-state protocol, the secure transmission distance of the key in the pure seawater increases most obviously, and its added value is about 30 m. At the same time, the secret key rate of the eight-state protocol also increases at the same transmission distance.



**Figure 5.** (Color online.) Secret key rate of the four-state protocol for realistic reconciliation efficiency of 90% and a quantum efficiency of Bob's detection equal to 0.6 with thermal noise  $v_{el} = 0.01$ .  $V_A = 0.6$ ,  $\varepsilon = 0.01$  (in shot-noise unit).



**Figure 6.** (Color online.) Secret key rate of the eight-state protocol for realistic reconciliation efficiency of 90% and a quantum efficiency of Bob's detection equal to 0.6 with thermal noise  $v_{el} = 0.01$ .  $V_A = 0.6$ ,  $\varepsilon = 0.01$  (in shot-noise unit).

Figures 7 and 8 show the maximum tolerable excess noise as a function of the transmission distance for four-state and eight-state protocols, respectively. The numerical simulation results indicate that the tolerable excess noise and the maximum transmission distance decrease with the increase of the complexity of the seawater. The sensitivity of the pure sea water, clear ocean water, coastal ocean water, and turbid harbor water channels to the excess noise increases gradually, which is mainly reflected in the steepness of the curve in the figures. Besides, the tolerable excess noise in the case of homodyne detection is more than that in the case of heterodyne. By comparing Figures 7 and 8, it can be found that the tolerance to the noise of the eight-state protocol surpasses that of the four-state protocol, and the maximum transmission distance of the former is much larger than that of the latter. In addition, we can know that the four different seawater channels are all sensitive to excess noise; especially the turbid harbor water, coastal ocean water, and clear ocean water have very low tolerance to the additional noise, resulting in a short secure transmission distance for the quantum key.



**Figure 7.** (Color online.) The maximum tolerable excess noise at each distance for four-state protocol.  $\beta = 0.9$ ,  $V_A = 0.6$ ,  $\eta = 0.6$ ,  $v_{el} = 0.01$ .



**Figure 8.** (Color online.) The maximum tolerable excess noise at each distance for eight-state protocol.  $\beta = 0.9$ ,  $V_A = 0.6$ ,  $\eta = 0.6$ ,  $v_{el} = 0.01$ .

To facilitate the complete analysis of the influence of modulation variance on the performance of the protocols with four different channels, we take the extra noise value of 0.005 to provide a relatively wide range of transmission distance values for the analysis under the conditions of four different channels. Since the four kinds of seawater channels have different transmittances, the corresponding optimal modulation variances are naturally different. Hence, we need to study the effect of modulation variance on the performance of the four systems with different channels, so that we can find the optimal variance of each system to improve its performance.

Figures 9 and 10 separately show the relationship between modulation variance and secret key rate of the four-state and the eight-state protocols when the four kinds of typical seawater are used as transmission channels. Combined with the transmission characteristics of the four types of seawater, we selected different transmission distances to study the influence of modulation variance on secret key rate with homodyne detection and heterodyne detection. It should be noted that when the variance  $V_A$  of the discrete modulation is small, the lower bound of the secret key rate is close to the secret key rate of the case in which Alice uses Gaussian modulation with variance  $V_A$  [35,36]. The results of the simulation show that the maximum modulation variance and the optimal modulation variance decrease with the increase of the complexity of seawater and the transmission distance of the quantum signals. The maximum modulation variance in the case of homodyne detection is slightly larger than

that of heterodyne detection, and the difference between them decreases with the increase of the complexity of seawater and the transmission distance. When the modulation variance is relatively large, the secret key rate in the case of homodyne detection is larger than that in the case of heterodyne detection, and the difference of the secret key rate between them gradually decreases as the modulation variance decreases, which explains why the performance of the protocol in the two different detection cases in Figures 5 and 6 is not much different. By comparing Figures 9 and 10, we can also find that the modulation variance range of the eight-state protocol is much wider than that of the four-state protocol, and the optimal modulation variance and maximum secret key rate of the eight-state protocol are both larger than that of the four-state protocol under the same conditions.

Through the comparative analysis above, we can conclude that the lower is the complexity of the seawater channel, the better is the performance of the CV-QKD system. Besides, the performance of the eight-state protocol is much better than that of the four-state protocol, and homodyne detection is slightly better than heterodyne detection.



**Figure 9.** (Color online.) The compressed variation trend of  $V_A$  optimal interval of the four-state protocol as the transmission distance extends.  $\beta = 0.9$ ,  $\varepsilon = 0.005$ ,  $\eta = 0.6$ ,  $v_{el} = 0.01$ .



**Figure 10.** (Color online.) The compressed variation trend of  $V_A$  optimal interval of the eight-state protocol as the transmission distance extends.  $\beta = 0.9$ ,  $\varepsilon = 0.005$ ,  $\eta = 0.6$ ,  $v_{el} = 0.01$ .

#### 4.2. Finite-Size Analysis

The above asymptotic security analysis is based on the assumption that the number of exchanged signals between Alice and Bob approaches infinity. However, this is not the case in reality: some signals between them are needed for parameter estimation to ensure the accuracy of CV-QKD. Here, we consider a more realistic security analysis, namely the finite-size analysis, where the number of exchanged signals is confined to a finite value [34,37]. Different from the fact that the modulated variance  $V_A$  can be optimized to improve the performance of the protocol, the values of transmittance  $T_{sea}$  and excess noise  $\varepsilon$  need to be estimated. In this part, we mainly analyze the finite-size effects on the parameter estimation procedure and the calculation of the secret key rate, which are based on the assumption that Gaussian collective attacks are optimal.

The secret key rate of the discrete-modulated underwater CV-QKD protocol against collective attack in the finite-size case can be written as [38–41]

$$K^{f} = \frac{n}{N} (\beta I(A:B) - S_{N}^{\epsilon_{PE}}(E:B) - \Delta(n)),$$
(15)

where  $\frac{n}{N}$  is the ratio of the number of photons used to establish the secret key to the total exchanged signals between Alice and Bob.  $\beta$  is the reconciliation efficiency and I(A : B) is the mutual information of Alice and Bob.  $S_N^{\epsilon_{PE}}(E : B)$  is the maximum of the Holevo information compatible with the statistics except with probability  $\epsilon_{PE}$  and  $\epsilon_{PE}$  is the failure probability of the parameter estimation process.  $\Delta(n)$  is a function corresponding to the privacy amplification, which can be approximately expressed by

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\widetilde{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{PA}),\tag{16}$$

where  $\tilde{\epsilon}$  is the smoothing parameter with an optimal value of  $10^{-10}$  in the private amplification processes, and  $\epsilon_{PA}$  is the failure probability of privacy amplification. Comparing Equation (15) with Equation (8), we can find that the coefficient  $\frac{n}{N}$  is added, which is mainly because only *n* of the *N* total exchanged data are used to generate the key. Considering the effect of finite-size on parameter estimation accuracy, the estimation of the conditional entropy in Equation (15) needs to take the failure probability of the channel parameter estimation into account. Thus, the conditional entropy  $S_N(E : B)$ in Equation (8) is replaced by  $S_N^{\epsilon_{PE}}(E : B)$ . In addition, in the post-processing stage of data, the failure probability of privacy amplification should also be considered, so the function  $\Delta(n)$  related to the privacy amplification is also added in the Equation (18).

As can be seen from the above analysis, the sampling estimation may fluctuate in the parameter evaluation process, which will make the evaluation of the secret key rate inaccurate. To ensure the security of the protocol, it is necessary to do the worst estimation to the parameters to minimize the secret key rate. In other words, we need to calculate the maximum value of the Holevo information  $S_N^{\epsilon_{PE}}(E:B)$  between Eve and Bob in the case of statistical fluctuation in the parameter estimation. In a practical discrete-modulated underwater CV-QKD system, Alice and Bob select m = N - n data samples to evaluate the variables  $T_{sea}$  and  $\varepsilon$ , which satisfy the following model

$$y = tx + z, \tag{17}$$

where  $t = \sqrt{T_{sea}}$  and z satisfies a centered Gaussian distribution with variance  $\sigma^2 = T_{sea}\varepsilon + 1$ . We can find a specific covariance matrix  $\gamma_{AB_1}^{\epsilon_{PE}}$  that can successfully minimize the secret key rate by selecting appropriate parameters. The matrix is compatible with the exchanged data except with failure probability of parameter estimation  $\epsilon_{PE}$  and has the following form

$$\gamma_{AB_1}^{\epsilon_{PE}} = \begin{bmatrix} (V_A + 1)I & t_{min}Z_N\sigma_z \\ t_{min}Z_N\sigma_z & (t_{min}V_A + \sigma_{max}^2)I \end{bmatrix},$$
(18)

where  $t_{min}$  is the minimum value of t and  $\sigma_{max}^2$  is the maximum value of  $\sigma^2$ .

Maximum-likelihood estimators  $\hat{t}$  and  $\hat{\sigma}^2$  are known for the normal linear mode [39,41]:

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2}, \hat{\sigma}^2 = \frac{1}{m} \sum_{i=1}^{m} (y_i - \hat{t} x_i)^2,$$
(19)

and they obey the following distribution:

$$\hat{t} \sim N(t, \frac{\sigma^2}{\sum_{i=1}^m x_i^2}), \frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1),$$
 (20)

where *t* and  $\sigma^2$  are the authentic values of the parameters. Therefore, we can obtain the worst-case value of the parameters *t* and  $\sigma^2$  to maximize the value of the Holevo information between Eve and Alice with the statistics except with probability  $\epsilon_{PE}$ , namely

$$t_{min} \approx \sqrt{T_{sea}} - z_{\epsilon_{PE}/2} \sqrt{\frac{T_{sea}\varepsilon + 1}{mV_A}},$$

$$\sigma_{max}^2 \approx T_{sea}\varepsilon + 1 + z_{\epsilon_{PE}/2} \frac{(T_{sea}\varepsilon + 1)\sqrt{2}}{\sqrt{m}},$$
(21)

where  $z_{\epsilon_{PE}/2}$  is the probability density value corresponding to the upper fractile of the normal distribution and it satisfies  $1 - erf(z_{\epsilon_{PE}/2}/\sqrt{2})/2 = \epsilon_{PE}/2$ . erf(x) is the error function which satisfies  $erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ .

Similar to the asymptotic case, the mutual information I(A : B) and the Holevo information  $S_{N}^{\epsilon_{PE}}(E:B)$  can be calculated by replacing the parameters *T* and  $\varepsilon$  with  $t_{min}$  and  $\sigma_{max}^{2}$ , respectively. Other basic parameter settings are shown in Table 2, and all the variances and noises are in shot noise unit. According to the above asymptotic safety analysis, there is little difference between homodyne detection and heterodyne detection in the discrete-modulated underwater CV-QKD system, so here we only consider homodyne detection in the finite-size scenario. We plot the functional relationship for the four-state and eight-state protocols between the secret key rate and the transmission distance under the four types seawater in finite-size scenario, and compare them with that in the asymptotic case, which are shown in Figures 11 and 12, respectively. The orange solid line, green solid line, purple solid line, blue solid line, and the red dash line in the subgraphs correspond to the block lengths of 10<sup>8</sup>, 10<sup>10</sup>, 10<sup>12</sup>, and 10<sup>14</sup>, and the asymptotic curves, respectively. We can know from the figures that the performance of the discrete-modulated CV-QKD protocols under four types of seawater in the finite-size scenario have the same trend, and their performance is not as good as those obtained in the asymptotic case. Although the transmission distance and secret key rate gradually increase with the increase of N, and the transmission distance is very close to the maximum transmission distance in the asymptotic case when  $N = 10^{14}$ , the secret key rate is always lower than the value in the asymptotic case, because a part of the exchanged signals between Alice and Bob are used for parameter estimation. When comparing the sub-figures in Figures 11 and 12, it can be found that, with the decrease of complexity of the seawater, the performance of the protocol is more influenced by the variation of N, which is mainly reflected in the reduction range of transmission distance. By comparing Figures 11 and 12, we can also find that the performance of eight-state protocol is also better than that of four-state protocol in the finite-size scenario, which is the same as that in the asymptotic case.

Table 2. Parameters setting of the system in the finite-size scenario.



Figure 11. Cont.



**Figure 11.** (Color online.) The finite-size and the asymptotic secret key rate of the four-state underwater CV-QKD protocol. From left to right in every sub-figure, curves of different colors correspond, respectively, to block lengths of 10<sup>8</sup>, 10<sup>10</sup>, 10<sup>12</sup>, and 10<sup>14</sup>, and the asymptotic curves.



**Figure 12.** (Color online.) The finite-size and the asymptotic secret key rate of the eight-state underwater CV-QKD protocol. From left to right in every sub-figure, curves of different colors correspond, respectively, to block lengths of 10<sup>8</sup>, 10<sup>10</sup>, 10<sup>12</sup>, and 10<sup>14</sup>, and the asymptotic curves.

#### 5. Discussion and Conclusions

In this work, we focus on the discrete-modulated CV-QKD protocol with different types of seawater channel. The optical propagation characteristics of the seawater channel and the performance of the four-state protocol and the eight-state protocol under the four different types of seawater are analyzed. Simulation results show that the performance of the system decreases with the increase of the complexity of seawater, and the performance of the eight-state protocol is better than that of the four-state protocol. Comparing the performance of the system in the asymptotic scenario and in the finite-size case, we can find that the performance of the former is better than that of the latter, and, with the increase of the amount of information used for key extraction in the latter, its performance is gradually closer to that of the former. Although the current theoretical maximum secure transmission distance of the CV-QKD protocol under seawater is only a few hundred meters away, it is enough to communicate securely with submarines and sensor network nodes in the hundreds of meters of water. Moreover, with the development of quantum communication technology, it is likely to play an important role in offshore underwater rescue, shallow sea exploration, diving communication and other aspects.

However, it should be noted here that the security analysis in this paper is based on the assumption that the seawater channel is linear. However, in reality, it is a nonlinear channel, and the factors that need to be considered are much more than just the absorption and scattering mentioned in this paper. Factors such as sea surface wind speed, temperature, and seawater sloshing will also affect the performance of the system. On the other hand, the new development on the security proof of the discrete-modulated CV-QKD proposed by Shouvik Ghorai et al. [42] waives the channel linearity assumptions. This provides a new idea for establishing the full security of continuous-variable protocols under seawater. All of these require researchers to do further investigation, and there is still a long way to go before establishing an underwater quantum communication network.

Author Contributions: Conceptualization, Y.G. and X.R.; writing—original draft, X.R. and H.Z.; writing—review and editing, W.Z. and X.W.; and validation, X.L.

**Funding:** This work was supported by the National Natural Science Foundation of China (Grant Nos. 61871407 and 61801522).

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

## Appendix A. The Calculation of the Symplectic Eigenvalues

The covariance matrix  $\gamma_{AB_1}$  depends on Alice and the seawater channel, and it has the following form

$$\gamma_{AB_1} = \begin{bmatrix} \gamma_A & \sigma_{AB_1} \\ \sigma_{AB_1} & \gamma_{B_1} \end{bmatrix} = \begin{bmatrix} VI & \sqrt{T_{sea}} Z_N \sigma_z \\ \sqrt{T_{sea}} Z_N \sigma_z & T_{sea} (V + \chi_{ch})I \end{bmatrix},$$
(A1)

where I = diag(1,1),  $\sigma_z = diag(1,-1)$ ,  $Z_N = 2\alpha^2 \sum_{k=0}^{N-1} \sqrt{\frac{\lambda_{k-1}^3}{\lambda_k}}$ . Therefore, we can calculate the corresponding symplectic eigenvalues

$$\lambda_{1,2} = \sqrt{\frac{1}{2}(A \pm \sqrt{A^2 - 4B})},\tag{A2}$$

with

$$A = det(\gamma_{AB_1}),$$
  

$$B = det\gamma_A + det\gamma_{B_1} + 2det(\sigma_{AB_1}).$$
(A3)

The quantum state  $\rho_{B_1}$  arriving at Bob's side introduces an electric noise  $v_{el}$  when it was detected by an imperfect detector. This trusted detection noise can be purified by introducing an additional EPR source with a variance of  $V_d$  as well as two modes  $F_0$  and G [43], which can be seen in Figure 4. The corresponding covariance matrix of this EPR state can be noted as

$$\gamma_{F_0G} = \begin{bmatrix} V_d I & \sqrt{V_d^2 - 1}\sigma_z \\ \sqrt{V_d^2 - 1}\sigma_z & V_d I \end{bmatrix}.$$
 (A4)

Subsequently, one of two modes of the EPR state is coupled to the signal. Then, the whole system can be represented by the quantum state  $\rho_{ABFG}$ , and its corresponding covariance matrix can be derived from [32]

$$\gamma_{ABFG} = \Gamma^{I}_{BS}(\gamma_{AB_{1}} \oplus \gamma_{F_{0}G})\Gamma_{BS},\tag{A5}$$

where

$$\Gamma_{BS} = I \oplus \begin{bmatrix} \sqrt{\eta}I & \sqrt{1-\eta}I\\ -\sqrt{1-\eta}I & \sqrt{\eta}I \end{bmatrix} \oplus I.$$
(A6)

The conditional covariance matrix  $\gamma^B_{AFG}$  can be derived from

$$\gamma^B_{AFG} = \gamma_{AFG} - \sigma^T_{AFGB} H \sigma_{AFGB}, \tag{A7}$$

where  $H = H_{hom} = (X^T \gamma_B X)^{MP}$  for homodyne detection and  $H = H_{het} = (\gamma_B + I)^{-1}$  for heterodyne detection. X = diag(1,0) when the homodyne detector detects the amplitude quadrature, and X = diag(0,1) when it detects the phase quadrature. *MP* denotes the pseudoinverse of the matrix. The matrices  $\gamma_{AFG}$ ,  $\sigma_{AFGB}$  and  $\gamma_B$  are the submatrices of the covariance matrix  $\gamma_{AFGB}$ , which can be obtained by rearranging the rows and columns of the matrix  $\gamma_{ABFG}$ .

By computing the symplectic eigenvalues of the matrix  $\gamma^B_{AFG}$ , we can get

$$\lambda_{3,4} = \sqrt{\frac{1}{2}(C \pm \sqrt{C^2 - 4D})}, \lambda_5 = 1,$$
 (A8)

where, for the homodyne case,

$$C_{hom} = \frac{\chi_{hom}B + T_{sea}(V + \chi_{ch}) + V\sqrt{A}}{T_{sea}(V + \chi_{thom})},$$

$$D_{hom} = \sqrt{A} \frac{\sqrt{A}\chi_{hom} + V}{T_{sea}(V + \chi_{thom})},$$
(A9)

and, for the heterodyne case,

$$C_{het} = \frac{B\chi_{het}^{2} + 2\chi_{het}[V\sqrt{A} + T_{sea}(V + \chi_{ch})] + A + 1 + 2T_{sea}(Z_{N})^{2}}{T_{sea}^{2}(V + \chi_{thet})^{2}},$$

$$D_{het} = (\frac{V + \sqrt{A}\chi_{het}}{T_{sea}(V + \chi_{thet})})^{2}.$$
(A10)

## References

- Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* 2002, *88*, 057902. [CrossRef]
- 2. 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*, 621–669. [CrossRef]
- 3. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* 2005, 77, 513–577. [CrossRef]
- 4. Yang, J.; Xu, B.J.; Peng, X.; Guo, H. Four-state continuous-variable quantum key distribution with long secure distance. *Phys. Rev. A* 2012, *85*, 052302. [CrossRef]

- 5. Diamanti, E.; Lo, H.K.; Qi, B.; Yuan, Z.L. Practical challenges in quantum key distribution. *NPJ Quantum Inform.* **2016**, *2*, 16025. [CrossRef]
- 6. Lodewyck, J.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Phys. Rev. A* **2005**, *72*, 050303. [CrossRef]
- 7. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [CrossRef]
- 8. Huang, D.; Huang, P.; Lin, D.K.; Zeng, G.H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [CrossRef]
- 9. Qu, Z.; Djordjevic, I.B. High-speed free-space optical continuous-variable quantum key distribution enabled by three-dimensional multiplexing. *Opt. Express* **2017**, *25*, 7919–7928. [CrossRef]
- 10. Usenko, V.C.; Peuntinger, C.; Heim, B.; Gunthner, K.; Derkach, I.; Elser, D.; Marquardt, C.; Filip, R.; Leuchs, G. Stabilization of transmittance fluctuations caused by beam wandering in continuous-variable quantum communication over free-space atmospheric channels. *Opt. Express* **2018**, *26*, 31106–31115. [CrossRef]
- Hosseinidehaj, N.; Babar, Z.; Malaney, R.; Ng, S.X.; Hanzo, L. Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook. *IEEE Commun. Surv. Tutor.* 2019, 21, 881–919. [CrossRef]
- 12. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [CrossRef] [PubMed]
- 13. Miao, E.L.; Han, Z.F.; Gong, S.S.; Zhang, T.; Diao, D.S.; Guo, G.C. Background noise of satellite-to-ground quantum key distribution. *New J. Phys.* **2005**, *7*, 215.
- 14. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-ground quantum key distribution. *Nature* **2017**, *549*, 43–47. [CrossRef] [PubMed]
- Zhao, W.; Liao, Q.; Huang, D.; Guo, Y. Performance analysis of the satellite-to-ground continuous-variable quantum key distribution with orthogonal frequency division multiplexed modulation. *Quantum Inf. Process.* 2017, 18, 39. [CrossRef]
- 16. Shi, P.; Zhao, S.C.; Gu, Y.J.; Li, W.D. Channel analysis for single photon underwater free space quantum key distribution. *J. Opt. Soc. Am. A Opt. Image Sci. Vis.* **2015**, *32*, 349–356. [CrossRef]
- 17. Hill, A.D.; Christensen, B.; Kwiat, P.G. Advanced techniques for free-space optical quantum cryptography over water. *SPIE* **2016**, *9739*, 973911.
- 18. Ji, L.; Gao, J.; Yang, A.L.; Feng, Z.; Lin, X.F.; Li, Z.G.; Jin, X.M. Towards quantum communications in free-space seawater. *Opt. Express* 2017, *25*, 19795–19806. [CrossRef]
- 19. Li, D.D.; Shen, Q.; Chen, W.; Li, Y.; Han, X.; Yang, K.X.; Xu, Y.; Lin, J.; Wang, C.Z.; Yong, H.L.; et al. Proof-of-principle demonstration of quantum key distribution with seawater channel: Towards space-to-underwater quantum communication. *Opt. Commun.* **2019**, 452, 220–226. [CrossRef]
- Guo, Y.; Xie, C.L.; Huang, P.; Li, J.W.; Zhang, L.; Huang, D.; Zeng, G.H. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* 2018, *97*, 052326. [CrossRef]
- 21. Xie, C.L.; Guo, Y.; Wang, Y.J.; Huang, D.; Zhang, L. Security simulation of continuous-variable quantum key distribution over air-to-water channel using Monte Carlo method. *Chin. Phys. Lett.* **2018**, *35*, 19–22. [CrossRef]
- 22. Kong, M.W.; Wang, J.L.; Chen, Y.F.; Ali, T.; Sarwar, R.; Qiu, Y.; Wang, S.L.; Han, J.; Xu, J. Security weaknesses of underwater wireless optical communication. *Opt. Express* **2017**, *25*, 21509–21518. [CrossRef] [PubMed]
- Xu, J.; Song, Y.H.; Yu, X.Y.; Lin, A.; Kong, M.W.; Han, J.; Deng, N. Underwater wireless transmission of high-speed QAM-OFDM signals using a compact red-light laser. *Opt. Express* 2016, 24, 8097–8109. [CrossRef] [PubMed]
- 24. Li, J.; Ma, Y.; Zhou, Q.Q.; Zhou, B.; Wang, H.Y. Monte Carlo study on pulse response of underwater optical channel. *Opt. Eng.* **2012**, *51*, 066001. [CrossRef]
- 25. Miya, T.; Terunuma, Y.; Hosaka, T.; Miyashita, T. Ultimate low-loss single-mode fiber at 1.55 um. *Electron. Lett.* **1979**, *15*, 106–108. [CrossRef]
- 26. Richardson, D.J. New optical fibres for high-capacity optical communications. *Philos. Trans.* **2016**, *374*, 20140441. [CrossRef]

- 27. Huang, D.; Huang, P.; Wang, T.; Li, H.S.; Zhou, Y.M.; Zeng, G.H. Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. *Phys. Rev. A* **2016**, *94*, 032305. [CrossRef]
- 28. Zhang, H.; Ruan, X.C.; Wu, X.D.; Zhang, L.; Guo, Y.; Huang, D. Plug-and-play unidimensional continuous-variable quantum key distribution. *Quantum Inf. Process.* **2019**, *18*, 128. [CrossRef]
- 29. Zeng, Z.Q.; Fu, S.; Zhang, H.H.; Dong, Y.H.; Cheng, J.L. A survey of underwater optical wireless communications. *IEEE. Commun. Surv. Tutor.* 2017, 19, 204–238. [CrossRef]
- Tarantino, S.; Cozzolino, D.; Rottwitt, K.; Bacco, D. Feasibility of quantum communications in aquatic scenario. In Proceedings of the 2018 IEEE Photonics Conference (IPC), Reston, VA, USA, 30 September–4 October 2018; pp. 1–2.
- Ma, H.X.; Huang, P.; Bai, D.Y.; Wang, T.; Wang, S.Y.; Bao, W.S.; Zeng, G.H. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. *Phys. Rev. A* 2019, 99, 022322. [CrossRef]
- 32. Becir, A.; El-Orany, F.A.A.; Wahiddin, M.R.B. Continuous-variable quantum key distribution protocols with eight-state discrete modulation. *Int. J. Quantum Inf.* **2012**, *10*, 1250004. [CrossRef]
- 33. Fang, J.; Lu, Y.; Huang, P.; He, G.Q.; Zeng, G.H. Discretely modulated continuous-variable quantum key distribution with a nondeterministic noiseless amplifier. *Int. J. Quantum Inf.* **2013**, *11*, 1350037. [CrossRef]
- 34. Guo, Y.; Li, R.J.; Liao, Q.; Zhou, J.; Huang, D. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier. *Phys. Lett. A* **2018**, *382*, 372–381. [CrossRef]
- 35. Shen, Y.; Zou, H.X.; Tian, L.; Chen, P.X.; Yuan, J.M. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *82*, 022317. [CrossRef]
- 36. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312. [CrossRef]
- 37. Ruppert, L.; Usenko, V.C.; Filip, R. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Phys. Rev. A* **2014**, *90*, 062310. [CrossRef]
- 38. Wang, X.Q.; Huang, C.H. Noise-enhanced CVQKD with untrusted source. *Mod. Phys. Lett. B* 2017, 31, 1750143. [CrossRef]
- 39. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* 2010, *81*, 062343. [CrossRef]
- 40. Zhang, X.Y.; Zhang, Y.C.; Zhao, Y.J.; Wang, X.Y.; Yu, S.; Guo, H. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042334. [CrossRef]
- 41. Wang, P.; Wang, X.Y.; Li, J.Q.; Li, Y.M. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Opt. Express* **2017**, *25*, 27995–28009. [CrossRef]
- 42. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **2019**, *9*, 021059. [CrossRef]
- 43. Usenko, V.C.; Filip, R. Trusted noise in continuous-variable quantum key distribution: a threat and a defense. *Entropy* **2016**, *18*, 20. [CrossRef]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).