entropy

MDPI

Article

Underwater Wavelength Attack on Discrete Modulated Continuous-Variable Quantum Key Distribution

Kangyi Feng [1], Yijun Wang [1], Yin Li [1], Yuang Wang [1,*], Zhiyue Zuo [1,*] and Ying Guo [1,2]

[1] School of Automation, Central South University, Changsha 410083, China
[2] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: caeserwang@mail.ustc.edu.cn (Y.W.); zuo.zhiyue.csu@gmail.com (Z.Z.)

Abstract: The wavelength attack utilizes the dependence of beam splitters (BSs) on wavelength to cause legitimate users Alice and Bob to underestimate their excess noise so that Eve can steal more secret keys without being detected. Recently, the wavelength attack on Gaussian-modulated continuous-variable quantum key distribution (CV-QKD) has been researched in both fiber and atmospheric channels. However, the wavelength attack may also pose a threat to the case of ocean turbulent channels, which are vital for the secure communication of both ocean sensor networks and submarines. In this work, we propose two wavelength attack schemes on underwater discrete modulated (DM) CV-QKD protocol, which is effective for the case with and without local oscillator (LO) intensity monitor, respectively. In terms of the transmittance properties of the fused biconical taper (FBT) BS, two sets of wavelengths are determined for Eve's pulse manipulation, which are all located in the so-called blue–green band. The derived successful criterion shows that both attack schemes can control the estimated excess noise of Alice and Bob close to zero by selecting the corresponding condition parameters based on channel transmittance. Additionally, our numerical analysis shows that Eve can steal more bits when the wavelength attack controls the value of the estimated excess noise closer to zero.

Keywords: wavelength attack; continuous-variable quantum key distribution; discrete modulated; underwater

Citation: Feng, K.; Wang, Y.; Li, Y.; Wang, Y.; Zuo, Z.; Guo, Y. Underwater Wavelength Attack on Discrete Modulated Continuous-Variable Quantum Key Distribution. *Entropy* **2024**, *26*, 515. https://doi.org/10.3390/e26060515

Academic Editors: Mohsen Razavi, Masoud Ghalaii, Federico Grasselli and Mirko Pittaluga

Received: 9 May 2024
Revised: 6 June 2024
Accepted: 12 June 2024
Published: 14 June 2024

1. Introduction

One of the most famous applications of quantum mechanics is quantum key distribution (QKD), which can protect distant communication with unconditional security [1]. Generally, QKD has two main categories: the discrete-variable (DV) version [2–4] and the continuous-variable (CV) version [5–7]. In detail, DV-QKD encodes the information on the polarization of a photon and uses a single-photon detector for receiver detection, while CV-QKD encodes the information on the quadrature of the optical field and uses coherent detection. Compared with the DV version, CV-QKD is a younger category but has the advantages of lower cost detection and higher compatibility with the current optical communication system [8–10].

To date, many CV-QKD protocols have been proposed. By using different quantum states, CV-QKD has a coherent-state protocol and a squeezed-state protocol [5,11]. By using various modulation formats, CV-QKD has a Gaussian-modulated protocol and a discrete modulated (DM) protocol [5,12]. Among these protocols, research on the Gaussian-modulated coherent-state (GMCS) protocol, whose security has been proven under individual attacks [13], collective attacks [14], and coherent attacks [15], is the most advanced. However, unbounded Gaussian modulation can only be implemented to a certain degree in practice. Moreover, for the GMCS protocol, it is hard to achieve highly efficient error correction at a low signal-to-noise ratio (SNR). Therefore, the DM protocol was first proposed in 2009 to improve error correction efficiency in low-SNR cases [16]. In detail, the discrete

signals are loaded symmetrically on the quadrature phase, similar to phase-shift keying (PSK) in digital communication systems.

When we develop a security proof, no matter the GMCS protocol or DM protocol, we assume that all devices follow their ideal mathematical models. In the real world, however, the device may deviate from the ideal model and introduce practical security loopholes because of Eve's manipulation, such as saturation attacks [17], Trojan-horse attacks [18], and so on. In Ref. [19], the authors proposed a local oscillator (LO) calibration attack, where Eve manipulates the linear relationship between the variance in the measurement and the intensity of the LO by changing the shape of the LO signal. In detail, the calibration attack makes the legitimate users overestimate the shot noise so that they underestimate the channel excess noise. Therefore, Eve can perform an intercept–resend attack without being detected. To defend systems against this attack, the authors suggest randomly attenuating the signal intensity to monitor the shot noise [19]. However, this defense method was demonstrated not to hold when the wavelength attack was proposed [20]. The wavelength attack uses the imperfection of the beam splitter (BS) to make the users overestimate the shot noise again and even perform shot noise monitoring. Recently, the wavelength attack on CV-QKD in a free-space atmospheric channel, as well as in the fiber case, was analyzed and proven to be effective [21]. As discussed in many papers [22–25], the atmospheric channel is an important part of building a global quantum network, especially at present, when quantum relay technology is not yet mature [26].

The free-space seawater channel, like the atmospheric channel, is also an important part of the global quantum network, as it can be used for ocean exploitation and modern communication [27]. Even if the communication capability of the seawater quantum channel has been discussed in Ref. [28], seawater research lags behind that of the atmosphere. In fact, the seawater channel is a promising channel for quantum tasks, as free-space water is a uniform isotropic medium which does not lead to massive polarization rotation or depolarization of single photons [29]. Motivated by the previous idea, in this work, we explore the wavelength attack on CV-QKD in a seawater channel. We consider the four-state DM protocol with homodyne detection, while the central wavelength of Alice and Bob is located in the blue–green band for lower attenuation [30]. In terms of the determined central wavelength and the transmittance properties of fused biconical taper (FBT) BSs, we determine two sets of wavelengths for Eve, which are randomly selected by Eve when she manipulates the pulse. Numerical analysis shows that the wavelength attack can steal the secret key without being detected by manipulating the estimated excess noise of Alice and Bob.

The paper is organized as follows: In Section 2, we show the influences of horizontal seawater links, including extinction losses and ocean turbulence. In Section 3, we review the principle of the four-state protocol and FBT BSs and then propose two wavelength attack schemes. In Section 4, we derive the successful criteria of both attack schemes. In Section 5, we show the impact of wavelength attack on the security of the four-state protocol. Finally, Section 6 draws a conclusion.

2. Seawater Channel

In this section, we present a brief introduction to transmittance in seawater channels. The channel model used in our manuscript has been discussed in our previous works [28]. Specifically, this model considers the effects caused by extinction and turbulence in a horizontal seawater link.

2.1. Extinction Losses

The extinction-induced losses are caused by the absorption and scattering of both soluble and insoluble impurities, such as chlorophyll, inorganic salts, sediment particles, microorganisms, etc. Specifically, absorption causes energy loss while scattering leads to the divergence of the laser beam [31,32], and they are quantified by absorption coefficient $a(\lambda)$ and scattering coefficient $b(\lambda)$, respectively. Here, λ denotes the wavelength of quantum

light, while the details of $a(\lambda)$ and $b(\lambda)$ are shown in Appendix A of Ref. [28]. In detail, $a(\lambda)$ and $b(\lambda)$ are related to both the ocean type and the submarine depth d. The total extinction coefficient $\beta(\lambda)$ is defined as the sum of $a(\lambda)$ and $b(\lambda)$. Finally, extinction-induced transmittance is characterized by the Lambert–Beer law given by [28].

$$\eta_{\text{ext}} = e^{-\beta(\lambda)L}, \tag{1}$$

where L is the transmission distance. For less attenuation, we use a 532 nm laser in the blue–green band in the following. In addition, the ocean type of our manuscript is set to S6 as an example.

2.2. Ocean Turbulence

In general, ocean turbulence is caused by the combined effect of two fluctuating scalars: temperature and salinity. In our manuscript, these scalars can be characterized by the classical Kolmogorov power spectrum given by [33].

$$\Phi(\kappa) = \mathbb{A}\omega\xi^{-\frac{1}{3}}\kappa^{-\frac{11}{3}}, \tag{2}$$

where $\mathbb{A}$ is the order of unity, ω is related to the dissipation rate of temperature or salinity variance, ξ is the kinetic energy dissipation rate, and κ is the spatial frequency. In terms of this power spectrum, the elliptical model of free-space quantum light can be used for analyzing the beam evolution of ocean turbulent channels. Finally, transmittance in a seawater channel with an initial beam radius w_0 can be estimated as

$$\eta_{\text{ch}} = \eta_{\text{ext}}\eta_0 \exp\left\{-\left[\frac{r/a}{\mathcal{Q}(\frac{2}{w_{\text{eff}}(\phi-\varphi)})}\right]^{\mathcal{Y}\left(\frac{2}{w_{\text{eff}}(\phi-\varphi)}\right)}\right\}, \tag{3}$$

where η_0 is the transmittance without either extinction and beam wandering effects, r is the beam-centroid vector, a is the receiver telescope radius, $w_{\text{eff}}(\cdot)$ is the effective spot-radius with deformation effects, ϕ is the beam–ellipse orientation angle, φ denotes the angle between vector r and the x-axis, and $\mathcal{Q}(\cdot)$ and $\mathcal{Y}(\cdot)$ are scale and shape functions, respectively. The details of the above parameters are shown in Appendix B of Ref. [28]. In our manuscript, the value of the above parameters are a = 0.25 m, w_0 = 80 mm, $\omega = 10^{-11}$, and $\xi = 10^{-3}$.

3. Seawater Wavelength Attack on Discrete Modulated CV-QKD

In this section, we have a quick review of the four-state DM protocol and the principle of FBT BSs. Then, two wavelength attack schemes in seawater channels are proposed.

3.1. The Four-State Protocol

The four-state protocol with homodyne detection will be used in the following, and its steps can be described as follows:

(1) *State preparation and transmission:* For the j-th round, Alice randomly prepares one of the quantum states from $|\phi_j\rangle \in \{|\alpha e^{i(2k-1)\pi/4}\rangle : k \in 1,2,3,4\}$ and sends it to Bob via a thermal-loss channel, which is characterized by transmittance η_{ch} and excess noise ε. Here, α is the amplitude of the quantum state, and the states $|\alpha e^{i(\pi/4)}\rangle$, $|\alpha e^{i(3\pi/4)}\rangle$, $|\alpha e^{i(4\pi/4)}\rangle$, and $|\alpha e^{i(7\pi/4)}\rangle$ correspond to the data 00, 10, 11, and 01, respectively. Along with the quantum state, Alice also prepares and sends a strong LO by multiplexing technology for homodyne detection on Bob's side.

(2) *Measurement:* With the help of the multiplexed LO, Bob performs homodyne detection on the q or p quadrature of the arriving quantum state for the raw key. In detail, Bob generates a uniform random number $b_j \in \{1,2\}$ so that $b_j = 0$ ($b_j = 1$) measures q (p).

(3) *Parameter estimation:* To obtain a practical secret key rate, Alice and Bob choose a part of the data for parameter estimation. In detail, Alice publishes part of the quantum states she sends, and Bob publishes the corresponding measurement results. Based on the public information, both parties can estimate the practical secret key rate. If this secret key rate is below zero, both parties abort the protocol; otherwise, they proceed to the data post-processing.

(4) *Data post-processing:* General data post-processing has two steps: error correction and privacy amplification. Error correction is to correct the keys that are inconsistent between the two parties. Private amplification reduces the amount of information to which Eve has access to with the secret key. After the appropriate private amplification, Alice and Bob generate the final secret key.

Note that the above description is based on the prepare-and-measure scheme, which is widely used in experiments. For the security analysis, one usually uses an equivalent entanglement-based (EB) scheme, as shown in Section 5.

3.2. The Principle of Beam Splitters

Generally, the BS used in the CV-QKD system is an FBT BS, which combines the ends of two bare fibers in a high-temperature environment to form a biconical waveguide structure. The splitting ratio of this BS is related to the wavelength of the input, which can be expressed as [34]

$$T(\lambda) = F^2 \sin^2\left(\frac{c\lambda^{2.5}w}{F}\right), \tag{4}$$

where F^2 denotes the fraction of power coupled, $c\lambda^{2.5}$ represents the coupling coefficient of the FBT BS, and w is the width of the heat source. As discussed in Section 2.1, our manuscript uses a central wavelength λ_0 = 532 nm for less attenuation. Therefore, we have $T(\lambda_0) = \sin^2\left(c{\lambda_0}^{2.5}w\right) = 0.5$. Here, we set F = 1 for simplicity. Based on Equation (4), we find that only when the input is located at the central wavelength, the splitting ratio of the BS is 50:50. In other words, the splitting ratio is no longer balanced when the input's wavelength deviates from the center wavelength. In what follows, we will discuss how Eve uses the wavelength dependence of such BS for the so-called wavelength attack.

3.3. Wavelength Attack Scheme

Figure 1 shows the general wavelength attack scheme. To implement the wavelength attack, Eve first intercepts and measures both the q and p quadrature of Alice's quantum states $|\phi_j\rangle$ by heterodyne detection. Then, Eve prepares and sends two groups of pulses at the same time to Bob: $\{F^s, F^{lo}\}$ and $\{P^s, P^{lo}\}$. In detail, the wavelength of $\{F^s, F^{lo}\}$ is the same as Alice, while the wavelength of $\{P^s, P^{lo}\}$ is changed by Eve. In the first group, the signal pulse F^s is modulated according to Eve's measurement results $\{q_E, p_E\}$, and the LO pulse F^{lo} is manipulated by Eve in terms of Bob's monitoring method. In the second group, the wavelengths of $\{P^s, P^{lo}\}$ (i.e., λ^s and λ^{lo}) are randomly selected from two sets of wavelengths with equal probability. In terms of the central wavelength λ_0, the two sets of wavelengths in our manuscript are shown in Table 1, which also shows the corresponding transmittance, i.e., T^s and T^{lo} [35].

Table 1. Two sets of wavelengths with corresponding transmittance.

Set	λ^s(nm)	T^s	λ^{lo}(nm)	T^{lo}
1	526	0.47805	632	0.47837
2	538	0.52233	637	0.52199

On the receiver side, the differential current measured by the homodyne detector comes from the signal photocurrent i^s and LO photocurrent i^{lo}, whose intensities are I^s and I^{lo}, respectively. In general, Bob will attenuate the quantum signal with randomly

selected coefficient r_i ($i = 1, 2$), which equals 0 or 1, to resist the LO calibration attack [19]. In detail, when $r_1 \approx 0$, the differential current is primarily contributed by i^{lo}. If $T^{lo} = 0.5$, which correspond to Bob measuring $\{F^s, F^{lo}\}$, only the differential current remains.

$$i^{sn} = \sqrt{\eta^{lo} I^{lo}} \left(\sqrt{\eta^{lo}} \delta \hat{X}_\phi + \sqrt{1 - \eta^{lo}} \frac{\hat{X}_{v2} - \hat{X}_{v1}}{\sqrt{2}} \right), \tag{5}$$

where $\delta \hat{X}_\phi$, $\hat{X}_{v1}$, and $\hat{X}_{v2}$ are irrelevant vacuum states and η^{lo} is the detection efficiency when the wavelength is λ_{lo}. Note that the variance in Equation (5) is used as the normalized shot noise unit given by

$$N_0 = \eta^{lo} I^{lo} = \eta^{lo} \alpha_{\mathrm{lo}}^2, \tag{6}$$

where $\alpha_{\mathrm{lo}} = \sqrt{I_{lo}}$ is the amplitude of the LO. If $T^{lo} \neq 0.5$, which means that Bob measures $\{P^s, P^{lo}\}$, the differential current (without shot noise part) is approximately equal to [20]

$$D^{lo} = \left(2T^{lo} - 1\right) \eta^{lo} I^{lo}. \tag{7}$$

When $r_2 \approx 1$, the differential current is contributed by both i^s and i^{lo}. If Bob measures $\{F^s, F^{lo}\}$, we have $T^s = T^{lo} = 0.5$ and obtain the q_E or p_E quadrature. If Bob measures $\{P^s, P^{lo}\}$, we have $T^s \approx T^{lo} \neq 0.5$ (see Table 1), and the differential current (without shot noise part) is approximately equal to

$$D^s = (1 - 2T^s) \eta^s I^s, \tag{8}$$

where η^s is the detection efficiency when wavelength is λ_s.

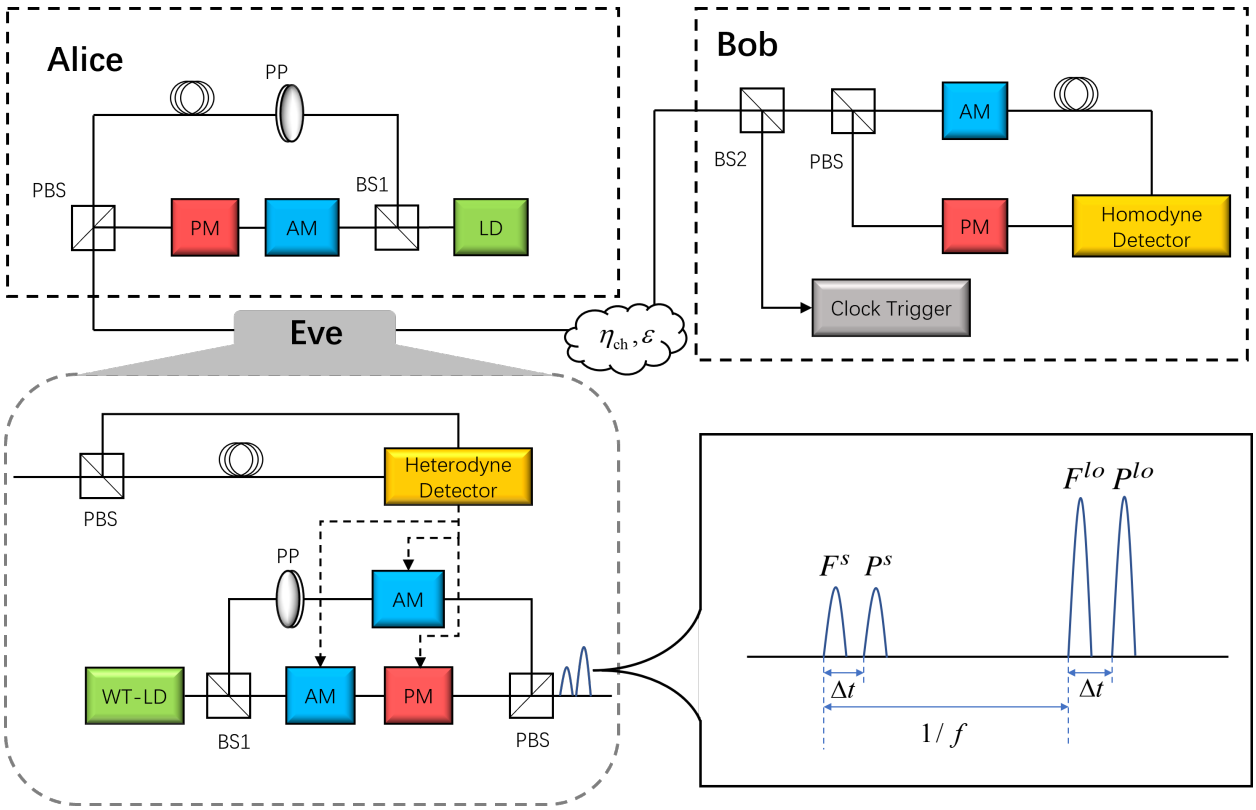

Figure 1. Seawater wavelength attack scheme using homodyne detector. LD, laser diode; WT-LD, wavelength-tunable laser diode; PP, polarizing prism; BS1, 1:99 beam splitter; BS2, 10:90 beam splitter; PBS, polarization beam splitter; AM, amplitude modulator; PM, phase modulator; Δt, a very small time interval; f, repetition rate.

As mentioned above, the LO pulse F^{lo} is manipulated by Eve in terms of Bob's monitoring method. Next, we discuss two attack schemes where Bob is without and with LO intensity monitoring ability, i.e., attack scheme A and attack scheme B, respectively. Figure 2 shows the differences in Eve's manipulation between attack scheme A and attack scheme B. In attack scheme A, both the amplitudes of the signal and the LO are manipulated, while attack scheme B only manipulates the wave shape of the LO.

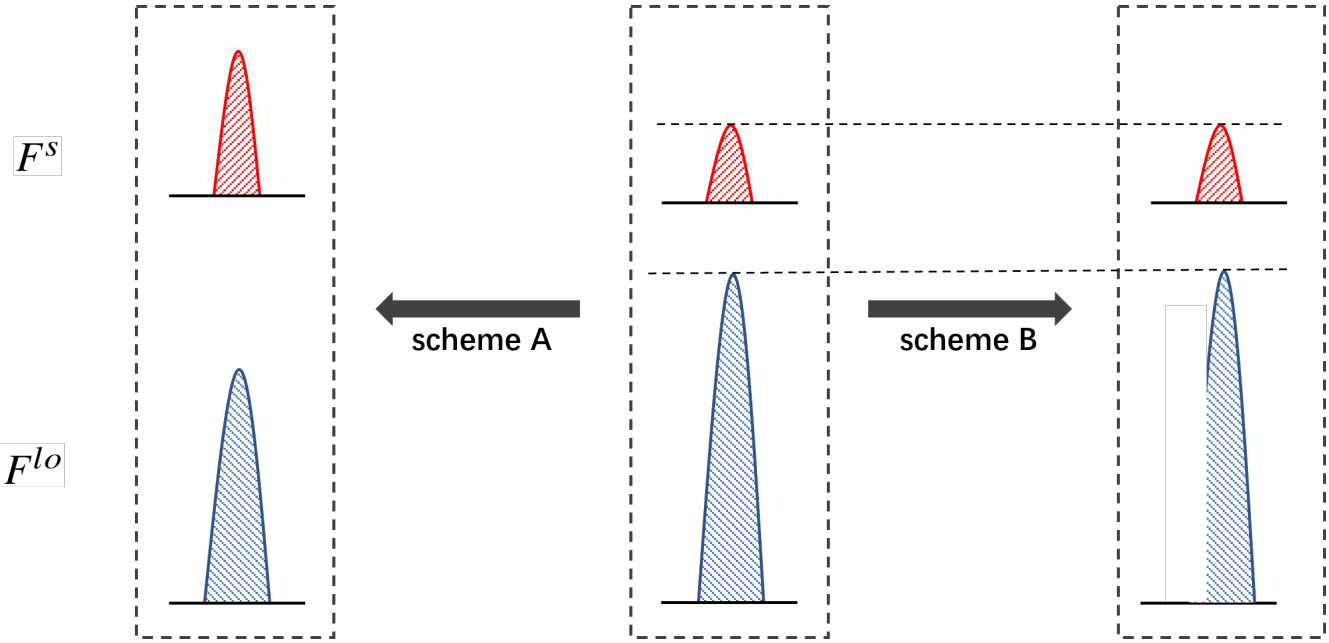

Figure 2. Differences in Eve's manipulation between attack scheme A and attack scheme B. Red and blue colors represent signal pulse and LO pulse, respectively.

Attack scheme A: If Bob does not measure the intensity of the LO, Eve performs the intercept–resend attack along with the wavelength attack. In this case, Bob uses the shot noise unit obtained before key distribution to normalize the measurement result. This scheme has two parts, as follows.

Part 1: Eve performs the intercept–resend attack and obtains the heterodyne detection results $\{q_E, p_E\}$. Then, Eve sends $\{F^s, F^{lo}\}$ according to $\{q_E, p_E\}$ and keeps their polarization unchanged. The amplitude of F^s is set to $\sqrt{N\eta_{\mathrm{ch}}}(q_E + ip_E)/2$, where N is larger than 1. For the amplitude of F^{lo}, Eve changes it from α_{lo} to $\alpha_{\mathrm{lo}}/\sqrt{N}$.

Part 2: Eve sends $\{P^s, P^{lo}\}$ at the same time as $\{F^s, F^{lo}\}$, and the wavelengths of $\{P^s, P^{lo}\}$ are chosen randomly from Table 1.

In Part 1, Eve reduces the amplitude of F_{lo}, which will decrease the shot noise unit. In this case, Bob can detect Eve's attack by shot noise monitoring if Eve has no other steps. Therefore, Eve needs to add $\{P^s, P^{lo}\}$ in Part 2 to compensate the total shot noise unit to a normal level, i.e., N_0. In detail, the variance in these pulses' differential current is considered the added shot noise. However, if Eve only uses one set of wavelengths, such as Set 1, the variance in the corresponding differential current D_1^{lo} will equal zero. This is the reason why we use two sets of wavelengths with random selection. In addition to the variance, the mean value of D^{lo} should be zero because a normal shot noise quadrature is considered a random variable with zero mean value. Therefore, we set $T_1^{lo} \approx 1 - T_2^{lo}$ to make $D_1^{lo} = -D_2^{lo}$ so that $\langle D^{lo} \rangle = \langle D_1^{lo} \rangle + \langle D_2^{lo} \rangle = 0$. Finally, the mean value of D^s should also be zero, so that we set $D_1^s = -D_2^s$. In total, we can make $D_1^s = -D_1^{lo} = -D_2^s = D_2^{lo} \equiv D$ for simple.

Attack scheme B: If Bob measures the intensity of the LO, Eve cannot reduce the amplitude of F^{lo} anymore. In this case, Eve combines the LO calibration attack and

wavelength attack. Note that attack scheme B also uses $D_1^s = -D_1^{lo} = -D_2^s = D_2^{lo} \equiv D$ to meet the requirements mentioned above. The two parts of this scheme are as follows.

Part 1: Eve performs the intercept–resend attack and sends F^s according to $\{q_E, p_E\}$, whose amplitude is $\sqrt{\eta_{\mathrm{ch}}}(X_E + iP_E)/2$. Then, Eve performs an LO calibration attack, which changes the shape of the LO to delay Bob's detector response time. This change makes Bob overestimate the shot noise unit with the correct LO intensity.

Part 2: Same as Part 2 in attack scheme A.

4. The Successful Criterion of the Wavelength Attack

Considering the random coefficient r_i, the variance in Bob's homodyne detection data under the linear channel assumption is

$$\langle \hat{y}^2 \rangle_i = r_i \eta \eta_{\mathrm{ch}} (V_A + \varepsilon) N_0 + N_0 + v_{\mathrm{el}} N_0, \tag{9}$$

where V_A is the modulation variance and v_{el} is the electronic noise. Then, Bob can estimate the shot noise unit and the excess noise as

$$\hat{N}_0 = \left[\frac{r_2 \langle \hat{y}^2 \rangle_1 - r_1 \langle \hat{y}^2 \rangle_2}{r_2 - r_1} \right] / (1 + v_{\mathrm{el}}), \tag{10}$$

$$\tilde{\varepsilon} = \left[\frac{\langle \hat{y}^2 \rangle_2 - \langle \hat{y}^2 \rangle_1}{(r_2 - r_1)\eta \eta_{\mathrm{ch}}} - V_A \hat{N}_0 \right] / \hat{N}_0. \tag{11}$$

To ensure the success of the attack without being detected, the following two conditions must be met: $\hat{N}_0 = N_0$ and $\tilde{\varepsilon} \leq \varepsilon$. Next, we derive the specific success criteria of the two attack schemes. In the following, the values of the parameters are $V_A = 0.3$ [36], $\varepsilon = 0.1$, $v_{\mathrm{el}} = 0.01$, $\eta_1^s = \eta_2^s = \eta_1^{lo} = \eta_2^{lo} = \eta = 0.5$, $I^{lo} = 1 \times 10^8$, $r_1 = 0.001$, $r_2 = 1$, and $N_0 = \eta I^{lo} = 5 \times 10^7$.

4.1. Attack Scheme A

The differential current measured by the homodyne detector is the sum of the currents from two parts, which can be expressed as

$$\hat{\delta} i_{\mathrm{tot},i} = \hat{\delta} i_{\mathrm{part1},i} + \hat{\delta} i_{\mathrm{part2},i}, \tag{12}$$

where $i = \{1, 2\}$ corresponds to the coefficients $\{r_1, r_2\}$, respectively. In detail, the variance in $\hat{\delta} i_{\mathrm{part1},i}$ is given by

$$\begin{aligned} V^A_{\mathrm{part1},i} &= \eta \frac{\alpha^2_{LO}}{N} [r_i \eta \eta_{\mathrm{ch}} N (V_A + 2) + 1] + r_i \eta \eta_{\mathrm{ch}} \varepsilon N_0 + v_{el} N_0 \\ &= r_i \eta \eta_{\mathrm{ch}} (V_A + 2 + \varepsilon) N_0 + \frac{N_0}{N} + v_{\mathrm{el}} N_0. \end{aligned} \tag{13}$$

Then, the variance in $\hat{\delta} i_{\mathrm{part2},i}$ can be expressed as

$$V^A_{\mathrm{part2},i} = (1 - r_i)^2 D^2 + \eta \langle I_j^{lo} \rangle + \eta r_i^2 \langle I_j^s \rangle, \tag{14}$$

where $\langle I_j^{lo} \rangle$ and $\langle I_j^s \rangle$ denote the mean values of I_j^{lo} and I_j^s in the seawater channel, respectively. Since we randomly select the coefficient r_i, $\langle I_j^{lo} \rangle$ and $\langle I_j^s \rangle$ are given by

$$\langle I_j^{lo} \rangle = \frac{I_1^{lo}}{2} + \frac{I_2^{lo}}{2} = \frac{D_1^{lo}}{2\eta(2T_1^{lo} - 1)} + \frac{D_2^{lo}}{2\eta(2T_2^{lo} - 1)} = 45.854D, \tag{15}$$

$$\langle I_j^s \rangle = \frac{I_1^s}{2} + \frac{I_2^s}{2} = \frac{D_1^s}{2\eta(1 - 2T_1^s)} + \frac{D_2^s}{2\eta(1 - 2T_2^s)} = 45.170D. \tag{16}$$

Therefore, Equation (14) can be rewritten as

$$V^A_{\text{part2},i} = (1-r_i)^2 D^2 + \left(22.927+22.585 r_i^2\right) D. \tag{17}$$

Thus, the variance in the differential current can be expressed as

$$\begin{aligned} \langle \hat{y}^2 \rangle_i^A &= V^A_{\text{part1},m} + V^A_{\text{part2},m} \\ &= r_m \eta \eta_{\text{ch}} (V_A + 2 + \varepsilon) N_0 + \frac{N_0}{N} + v_{\text{el}} N_0 + (1-r_m)^2 D^2 + \left(22.927 + 22.585 r_m^2\right) D. \end{aligned} \tag{18}$$

Finally, Bob estimates the shot noise unit and excess noise by Equations (10) and (11), which can be expressed as

$$\begin{aligned} \hat{N}_0 &= \frac{\left(\frac{1}{N} + v_{\text{el}}\right) N_0 + (1 - r_1 r_2) D^2 + (22.927 - 22.585 r_1 r_2) D}{1 + v_{\text{el}}}, \\ \tilde{\varepsilon} &= \left[(2+\varepsilon) \frac{N_0}{\hat{N}_0} + V_A \left(\frac{N_0}{\hat{N}_0} - 1 \right) + \frac{(r_1 + r_2 - 2) D^2}{\eta \eta_{\text{ch}} \hat{N}_0} + \frac{22.585 (r_1 + r_2) D}{\eta \eta_{\text{ch}} \hat{N}_0} \right]. \end{aligned} \tag{19}$$

To make the wavelength attack successful, the parameters N and D should satisfy

$$N = -\frac{N_0}{(1 - r_1 r_2) D^2 + (22.927 - 22.585 r_1 r_2) D - N_0}, \tag{20}$$

$$-(2+\varepsilon) \eta \eta_{\text{ch}} \hat{N}_0 < (r_1 + r_2 - 2) D^2 + 22.585 (r_1 + r_2) D \leq -2 \eta \eta_{\text{ch}} \hat{N}_0. \tag{21}$$

We find that these two formulas are not related to V_A, which implies that Eve can perform the attack without knowing the modulation variance.

4.2. Attack Scheme B

In this scheme, since Eve performs the LO calibration attack, the shot noise unit is γN_0 ($\gamma < 1$). Then, the variance in $\hat{\delta i}_{\text{part1},m}$ is given by

$$V^B_{\text{part1},m} = \gamma \left[r_m \eta \eta'_{\text{ch}} (V_A + 2 + \varepsilon) + 1 \right] N_0 + v_{\text{el}} N_0, \tag{22}$$

where $\eta'_{\text{ch}} = \eta_{\text{ch}} / \gamma$ can be considered the virtual channel transmittance simulated by Eve. Next, the expression of $V^B_{\text{part2},m}$ is the same as that in attack scheme A. Therefore, the variance in the differential current is

$$\begin{aligned} \langle \hat{y}^2 \rangle_i^B &= V^B_{\text{part1},m} + V^B_{\text{part2},m} \\ &= \gamma \left[r_m \eta \eta'_{\text{ch}} (V_A + 2 + \varepsilon) + 1 \right] N_0 + v_{\text{el}} N_0 + (1-r_m)^2 D^2 + \left(22.927 + 22.585 r_m^2\right) D. \end{aligned} \tag{23}$$

Based on Equation (10), Bob estimates the variance in the shot noise given by

$$\hat{N}_0 = \frac{(\gamma + v_{\text{el}}) N_0 + (1 - r_1 r_2) D^2 + (22.927 - 22.585 r_1 r_2) D}{1 + v_{\text{el}}}; \tag{24}$$

thus, γ should satisfy

$$\gamma = 1 - \frac{(1 - r_1 r_2) D^2 + (22.927 - 22.585 r_1 r_2) D}{N_0}. \tag{25}$$

Based on Equation (11), we find that the estimation of $\tilde{\varepsilon}$ is the same as that of attack scheme A. We find that the above formulas are still not related to V_A.

5. Simulation

In this section, we first show the effectiveness of our two attack schemes. Then, the secret key rate and Holevo bound of the four-state protocol are discussed. The simulation parameters are the same as in Section 4. As discussed in Section 4, the condition parameters in attack scheme A and attack scheme B are N and γ, respectively. Figure 3 shows the relationship of these two parameters with various $\tilde{\varepsilon}$ and transmittance η_{ch}. Here, the green lines represent the case $\tilde{\varepsilon} = \varepsilon = 0.1$, which means Eve cannot obtain more information by the wavelength attack. We find that both schemes can control $\tilde{\varepsilon}$ close to zero. To a target $\tilde{\varepsilon}$, the corresponding N of attack scheme A increases as the transmittance increases, as shown in Figure 3a. Moreover, for each transmittance value, Eve needs to use a lager N for a lower $\tilde{\varepsilon}$. In contrast, Figure 3b shows that the required value of γ decreases as the transmittance grows, while a lower γ obtains a lower $\tilde{\varepsilon}$ for each transmittance.

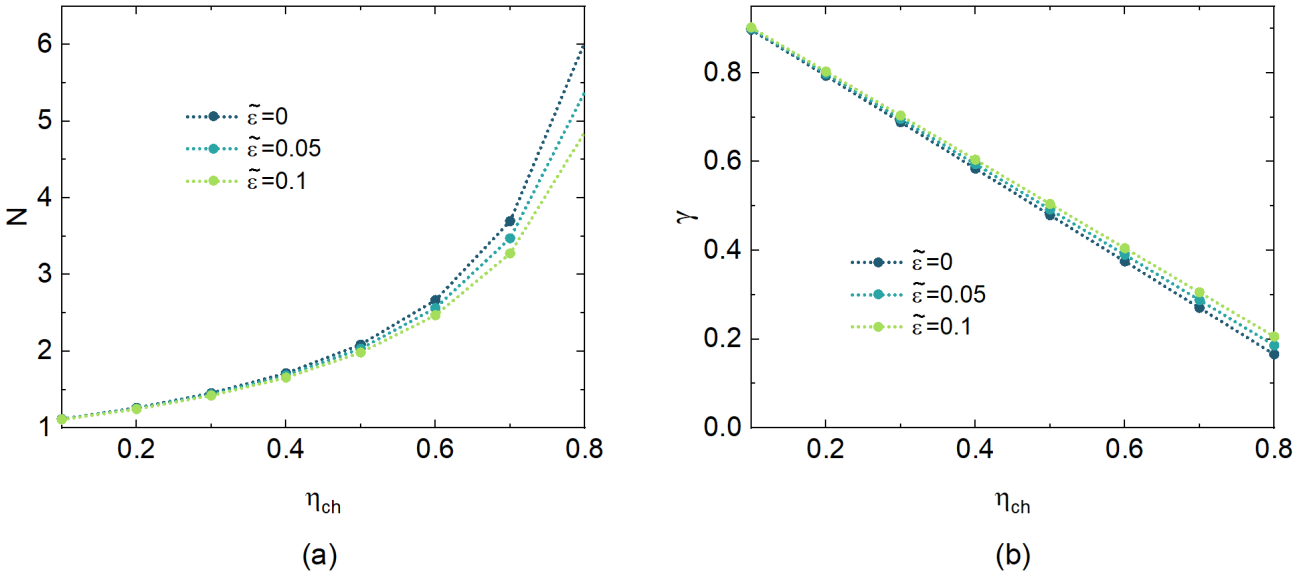

Figure 3. (**a**) N of attack scheme A vs. transmittance for various $\hat{\varepsilon}$. (**b**) γ of attack scheme B vs. transmittance for various $\hat{\varepsilon}$.

As described in Section 3.1, in parameter estimation, Bob calculates the practical secret key rate according to the estimated channel parameters. Here, we use the equivalent EB scheme instead of the prepare-and-measure scheme for security analysis. In the equivalent EB scheme, Alice generates a two-mode entangled state, which can be characterized by its covariance matrix given by [36].

$$\gamma_{AB} = \begin{bmatrix} VI_2 & Z_4\sigma_z \\ Z_4\sigma_z & VI_2 \end{bmatrix}, \tag{26}$$

where $I_2 = \mathrm{diag}(1,1)$, $\sigma_z = \mathrm{diag}(1,1)$, $V = V_A + 1$, and

$$Z_4 = 2\alpha^2\left(\frac{p_0^{3/2}}{p_1^{1/2}} + \frac{p_1^{3/2}}{p_2^{1/2}} + \frac{p_2^{3/2}}{p_3^{1/2}} + \frac{p_3^{3/2}}{p_0^{1/2}}\right), \tag{27}$$

with

$$p_{0,2} = \frac{1}{2}e^{-\alpha^2}\left[\cosh\left(\alpha^2\right) \pm \cos\left(\alpha^2\right)\right], \tag{28}$$

$$p_{1,3} = \frac{1}{2}e^{-\alpha^2}\left[\sinh\left(\alpha^2\right) \pm \sin\left(\alpha^2\right)\right]. \tag{29}$$

Then, mode A of the entangled state stays on Alice's side for heterodyne measurement, while mode B is transferred to Bob by the quantum channel. When mode B reaches Bob, the covariance matrix of the arriving entangled states can be expressed as [36]

$$\gamma_{AB} = \begin{bmatrix} VI_2 & \langle\sqrt{\eta_{\mathrm{ch}}}\rangle Z_4\sigma_z \\ \langle\sqrt{\eta_{\mathrm{ch}}}\rangle Z_4\sigma_z & [\langle\eta_{\mathrm{ch}}\rangle(V-1)+1+\langle\eta_{\mathrm{ch}}\rangle\tilde{\varepsilon}]I_2 \end{bmatrix}. \tag{30}$$

In the asymptotic case with reverse reconciliation, the secret key rate can be expressed as

$$K(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}) = \beta_0 I_{AB}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}) - \chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}), \tag{31}$$

where $\langle\cdot\rangle$ means the mean value, I_{AB} is the classic mutual information between Alice and Bob, χ_{BE} is the Holevo bound, and β is the reconciliation efficiency (see Appendix A for details).

Figure 4 shows the relationship between the stolen bits, i.e., $K(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}) - K(\langle\eta_{\mathrm{ch}}\rangle,\varepsilon)$, and transmission distance L when using the four-state protocol with submarine depth d = 200 m. Here, we use reverse reconciliation with reconciliation efficiency β_0 = 0.95, while the real excess noise is ε = 0.1. We find that Alice and Bob cannot generate a secret key when ε = 0.1. However, after the wavelength attack, Alice and Bob use the estimated excess noise $\tilde{\varepsilon}$ for the estimation of the secret key rate. In this case, the users will believe the keys are secure when the estimation result is above zero. For example, when Eve reduces the estimated excess noise to zero, the users will believe that the secure transmission distance is above 30 m. In fact, the real secure transmission distance is zero so that Eve can obtain these secret keys without being detected. In addition, the estimated secret key rate increases when $\tilde{\varepsilon}$ decreases. For example, the estimated secure transmission distance increases from 2 m to above 30 m when $\tilde{\varepsilon}$ decreases from 0.03 to 0. Figure 5 shows the relationship of the real Holevo bound $\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle,\varepsilon)$ and the estimated Holevo bound $\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon})$ under different seawater types with various submarine depth d and transmission distance L. Here, the estimated Holevo bound is calculated with an estimated excess noise $\tilde{\varepsilon}$ = 0. We find that there is a big difference in the performance of the two seawater types.

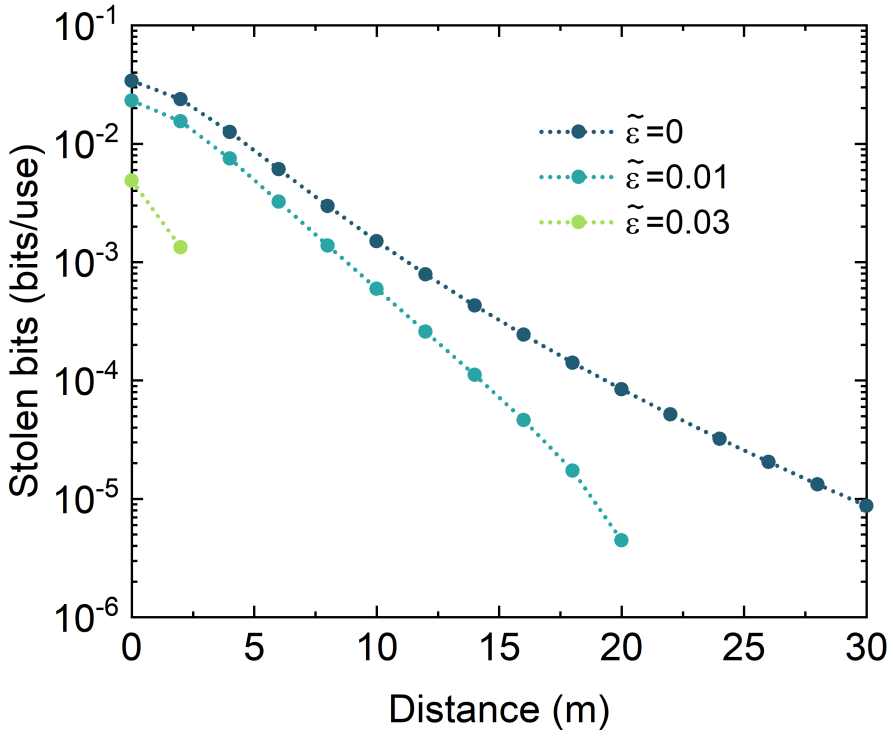

Figure 4. The stolen bits in the S6 ocean for various estimated excess noise values $\tilde{\varepsilon}$. The submarine depth is set to d = 200 m.

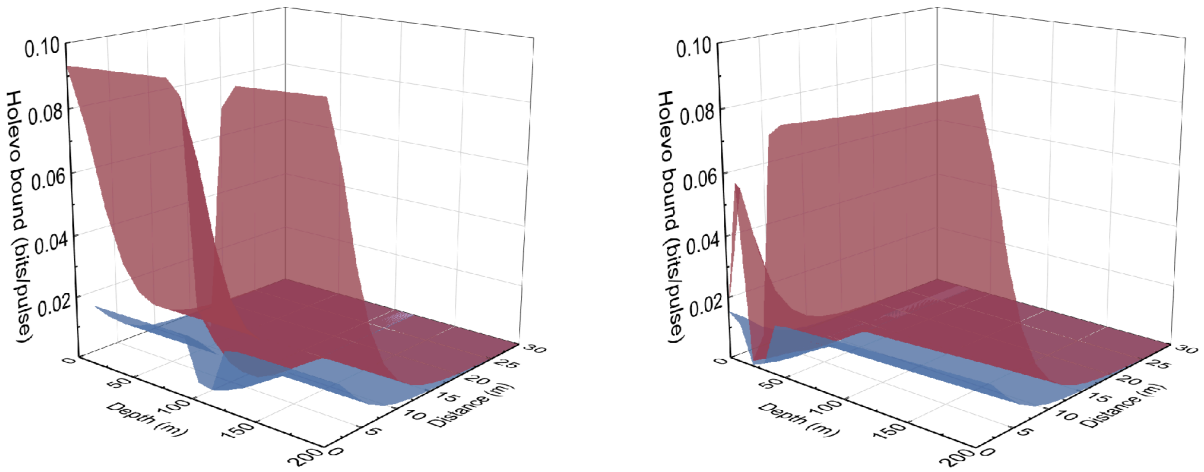

Figure 5. The relationship of the real Holevo bound $\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle, \varepsilon)$ (red surface) and the estimated Holevo bound $\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle, \tilde{\varepsilon})$ (blue surface) with various submarine depths and transmission distances. The estimated excess noise is set to $\tilde{\varepsilon} = 0$. (**a**) S1 seawater. (**b**) S6 seawater.

6. Conclusions and Discussion

In this paper, we have proposed two wavelength attack schemes for the underwater four-state protocol with and without LO intensity monitoring. Transmittance in underwater channels is affected by both extinction and ocean turbulence, so it fluctuates randomly over time. Different from both the fiber and atmosphere cases, the communication wavelength of underwater channels is not 1550 nm but is located in the so-called blue–green band. To meet this change, we have proposed two sets of wavelengths for Eve's pulse manipulation based on the transmittance properties of FBT BSs. We have calculated the successful criteria of both attack schemes and found that Eve can manipulate the estimated excess noise of Alice and Bob close to zero by slightly changing the corresponding condition parameters, i.e., N or γ. Numerical analysis shows that the secure transmission distance is overestimated by Alice and Bob when Eve performs the wavelength attack.

To avoid the wavelength attack, a direct idea is that one can design and use a wavelength-independent BS instead of a wavelength-dependent one. In addition, narrow wavelength filtering on Bob's side can also avoid the wavelength attack. Note that wavelength filtering needs LO intensity monitoring to work together. This is because practical wavelength filtering has an upper limit of attenuation for any specific wavelength so that Eve can beat it by increasing the pulse intensity. Moreover, Ref. [20] has proposed a method by using a third attenuation ratio in the shot noise monitoring module. In this method, Alice and Bob ensure they avoid a wavelength attack when the polynomial function of the total noise-to-attenuation ratio is almost linear. To avoid increasing the complexity and decreasing the final secret key rate in the above method, Ref. [37] has proposed another data post-processing method via peak–valley seeking and Gaussian postselection.

Author Contributions: Conceptualization, Y.W. (Yuang Wang) and Y.L.; writing—original draft preparation, K.F.; writing—review, Y.G. and Z.Z.; writing—editing, Y.W. (Yijun Wang) and Y.W. (Yuang Wang). All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by National Natural Science Foundation of China (grant No. 61871407) and Special Funds for the Construction of an Innovative Province in Hunan (grant No. 2022GK2016).

Data Availability Statement: All data generated or analyzed during this study are included in this article.

Acknowledgments: We would like to thank Jingzheng Huang and Zhe He for the helpful discussion.

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

Appendix A

In terms of Equation (30), when using homodyne detection, the mutual information between Alice and Bob can be expressed as

$$I_{AB}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}) = \frac{1}{2}\log_2\frac{1}{1-\frac{\langle\sqrt{\eta_{\mathrm{ch}}}\rangle^2(V-1)}{\langle\eta_{\mathrm{ch}}\rangle(V+\chi_{\mathrm{tot}})}}, \tag{A1}$$

where $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/\langle\eta_{\mathrm{ch}}\rangle$ with the total channel-added noise $\chi_{\mathrm{line}} = 1/\langle\eta_{\mathrm{ch}}\rangle - 1 + \tilde{\varepsilon}$ and the detection-added noise $\chi_{\mathrm{hom}} = (1-\eta+v_{\mathrm{el}})/\eta$. Then, the estimated Holevo bound $\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon})$ can be expressed by

$$\chi_{BE}(\langle\eta_{\mathrm{ch}}\rangle,\tilde{\varepsilon}) = \sum_{i=1}^{2} G\left(\frac{\lambda_i-1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i-1}{2}\right), \tag{A2}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and λ_i represents the symplectic eigenvalues given by

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}\left(A \pm \sqrt{A^2-4B}\right), \\ \lambda_{3,4}^2 &= \frac{1}{2}\left(C \pm \sqrt{C^2-4D}\right), \\ \lambda_5 &= 1, \end{aligned} \tag{A3}$$

where

$$\begin{aligned} A &= V^2 + \langle\eta_{\mathrm{ch}}\rangle^2\left(V + \frac{1-\langle\eta_{\mathrm{ch}}\rangle}{\langle\eta_{\mathrm{ch}}\rangle} + \tilde{\varepsilon}\right)^2 - 2\langle\sqrt{\eta_{\mathrm{ch}}}\rangle^2 Z_4^2, \\ B &= \left[\langle\eta_{\mathrm{ch}}\rangle V^2 + \langle\eta_{\mathrm{ch}}\rangle\chi_{\mathrm{line}}V - \langle\sqrt{\eta_{\mathrm{ch}}}\rangle^2 Z_4^2\right]^2, \\ C &= \frac{A\chi_{\mathrm{hom}} + V\sqrt{B} + \langle\eta_{\mathrm{ch}}\rangle(V+\chi_{\mathrm{line}})}{\langle\eta_{\mathrm{ch}}\rangle(V+\chi_{\mathrm{tot}})}, \\ D &= \frac{\sqrt{B}V + B\chi_{\mathrm{hom}}}{\langle\eta_{\mathrm{ch}}\rangle(V+\chi_{\mathrm{tot}})}. \end{aligned} \tag{A4}$$

References

1. 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. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef] [PubMed]
3. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef] [PubMed]
4. 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]
5. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
6. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402. [CrossRef]
7. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726–730. [CrossRef]
8. 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. [CrossRef]
9. Qi, B. Simultaneous classical communication and quantum key distribution using continuous variables. *Phys. Rev. A* **2016**, *94*, 042340. [CrossRef]
10. Jain, N.; Chin, H.M.; Mani, H.; Lupo, C.; Nikolic, D.S.; Kordts, A.; Pirandola, S.; Pedersen, T.B.; Kolb, M.; Ömer, B.; et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **2022**, *13*, 4740. [CrossRef]

11. Derkach, I.; Usenko, V.C.; Filip, R. Squeezing-enhanced quantum key distribution over atmospheric channels. *New J. Phys.* **2020**, *22*, 053006. [CrossRef]
12. Ghalaii, M.; Ottaviani, C.; Kumar, R.; Pirandola, S.; Razavi, M. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 506–516. [CrossRef]
13. Grosshans, F.; Cerf, N.J. Continuous-variable quantum cryptography is secure against non-Gaussian attacks. *Phys. Rev. Lett.* **2004**, *92*, 047905. [CrossRef] [PubMed]
14. Navascués, M.; Grosshans, F.; Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
15. Renner, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504. [CrossRef] [PubMed]
16. 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]
17. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [CrossRef]
18. Pereira, J.; Pirandola, S. Hacking Alice's box in continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *98*, 062319. [CrossRef]
19. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
20. Huang, J.Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304. [CrossRef]
21. Tan, X.; Guo, Y.; Zhang, L.; Huang, J.; Shi, J.; Huang, D. Wavelength attack on atmospheric continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, *103*, 012417. [CrossRef]
22. Sidhu, J.S.; Joshi, S.K.; Gündoğan, M.; Brougham, T.; Lowndes, D.; Mazzarella, L.; Krutzik, M.; Mohapatra, S.; Dequal, D.; Vallone, G.; et al. Advances in space quantum communications. *IET Quantum Commun.* **2021**, *2*, 182–217. [CrossRef]
23. Zuo, Z.; Wang, Y.; Huang, D.; Guo, Y. Atmospheric effects on satellite-mediated continuous-variable quantum key distribution. *J. Phys. A Math. Theor.* **2020**, *53*, 465302. [CrossRef]
24. Pirandola, S. Satellite quantum communications: Fundamental bounds and practical security. *Phys. Rev. Res.* **2021**, *3*, 023130. [CrossRef]
25. Ghalaii, M.; Bahrani, S.; Liorni, C.; Grasselli, F.; Kampermann, H.; Wooltorton, L.; Kumar, R.; Pirandola, S.; Spiller, T.P.; Ling, A.; et al. Satellite-Based Quantum Key Distribution in the Presence of Bypass Channels. *PRX Quantum* **2023**, *4*, 040320. [CrossRef]
26. Azuma, K.; Economou, S.E.; Elkouss, D.; Hilaire, P.; Jiang, L.; Lo, H.K.; Tzitrin, I. Quantum repeaters: From quantum networks to the quantum internet. *Rev. Mod. Phys.* **2023**, *95*, 045006. [CrossRef]
27. 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]
28. Zuo, Z.; Wang, Y.; Mao, Y.; Ruan, X.; Guo, Y. Security of quantum communications in oceanic turbulence. *Phys. Rev. A* **2021**, *104*, 052613. [CrossRef]
29. Chen, Y.; Shen, W.G.; Li, Z.M.; Hu, C.Q.; Yan, Z.Q.; Jiao, Z.Q.; Gao, J.; Cao, M.M.; Sun, K.; Jin, X.M. Underwater transmission of high-dimensional twisted photons over 55 meters. *PhotoniX* **2020**, *1*, 1–11. [CrossRef]
30. Kaushal, H.; Kaddoum, G. Underwater optical wireless communication. *IEEE Access* **2016**, *4*, 1518–1547. [CrossRef]
31. Wiscombe, W.J. Improved Mie scattering algorithms. *Appl. Opt.* **1980**, *19*, 1505–1509. [CrossRef]
32. Lock, J.A.; Gouesbet, G. Generalized Lorenz–Mie theory and applications. *J. Quant. Spectrosc. Radiat. Transf.* **2009**, *110*, 800–807. [CrossRef]
33. Hou, W.W. A simple underwater imaging model. *Opt. Lett.* **2009**, *34*, 2688–2690. [CrossRef] [PubMed]
34. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]
35. Available online: http://www.thorlabschina.cn (accessed on 1 April 2024).
36. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312. [CrossRef]
37. Huang, P.; Huang, J.; Wang, T.; Li, H.; Huang, D.; Zeng, G. Robust continuous-variable quantum key distribution against practical attacks. *Phys. Rev. A* **2017**, *95*, 052302. [CrossRef]