Research Article Vol. 33, No. 3 / 10 Feb 2025 / Optics Express 5696
Optics EXPRESS

Security of AUV-carried OIRS-assisted quantum key distribution links in underwater channels subject to misalignment

WEINA PANG,[1] PING WANG,[1,*] BO BAI,[1,2] WENWEN CHEN,[1] SHUANG LI,[1] AND KAILE WANG[1]

[1]School of Telecommunications Engineering, Xidian University, Xi'an 710071, China
[2]National Key Laboratory of Air-based Information Perception and Fusion, Luoyang 471000, China
[*]pingwang@xidian.edu.cn

Abstract: To establish a secure and high-bandwidth communication link between the gateway node and the central node in the internet of underwater things (IoUwT), it is meaningful to introduce quantum key distribution (QKD) protocols into underwater wireless optical communication (UWOC) systems. However, the line-of-sight (LOS) requirement for photon transmission will pose an inevitable challenge to the QKD-based UWOC system. In this work, an optical intelligent reflecting surface (OIRS) array mounted on an autonomous underwater vehicle (AUV) is utilized for the first time to alleviate the LOS blockage and enable more reliable underwater wireless optical quantum link for both discrete-variable quantum key distribution (DV-QKD) and continuous-variable quantum key distribution (CV-QKD). To begin with, a novel statistical model of the aggregated channel transmissivity experienced by the OIRS-based quantum states in underwater link is derived by combing the effects of oceanic absorption, scattering, turbulence and OIRS misalignment, where the oceanic turbulence-induced irradiance fluctuation is modeled by exponential and generalized gamma (EGG) distribution, and the jitter angle associated with AUV-carried OIRS misalignment is characterized by a Rayleigh distribution. Then, on the basis of this statistical model and the Gauss-Chebyshev quadrature, the quantum bit error rate and the lower bound secret key rate (SKR) for the AUV-carried OIRS-assisted DV-QKD link are obtained with weak coherent optical source and decoy state idea by utilizing Gottesman-Lo-Lütkenhaus-Preskill. In terms of univariate Fox-H function, the average Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound over the bosonic pure-loss channel, as well as the thermal upper and lower bounds over the thermal-loss channel are both derived for the AUV-carried OIRS-assisted CV-QKD link. Additionally, the achievable SKR for a practical GG02 CV-QKD protocol in underwater channels is also presented through the worst-case analysis. Furthermore, the impacts of the number of OIRS elements, OIRS positioning, jitter variances, the probability of erroneous detection and link distance on the security performance of the proposed links are studied with different water types, thereby offering valuable insights for the QKD-based UWOC system in IoUwT.

1. Introduction

As maritime activities expand to environmental monitoring, resource exploration, military defense, and disaster prevention, the internet of underwater things (IoUwT) has increasingly emerged as a prominent focus in ocean engineering [1,2]. Typically, the IoUwT consist of underwater sensor networks (USN) that gather data, central nodes for data aggregation, and gateway nodes for forwarding the collected information to onshore or offshore systems [3]. With the growing of confidential data used for monitoring critical infrastructure such as naval bases, undersea pipelines, and marine border security systems, one of the main challenges in IoUwT is how to ensure seamless data transmission between central and gateway nodes. This requires the communication link to be high-bandwidth, reliable, flexibly movable and secure. In this context,

#545449 https://doi.org/10.1364/OE.545449
Journal © 2025 Received 4 Nov 2024; revised 19 Dec 2024; accepted 20 Jan 2025; published 4 Feb 2025

Optics EXPRESS

underwater wireless optical communication (UWOC) stands out as a promising candidate for the IoUwT due to its attractive features. It can offer high data rates, unlicensed bandwidth, and less energy consumption compared to radio frequency (RF) and acoustic communications, while providing greater flexibility and cost efficiency than optical fiber communication [4]. Additionally, the narrow laser beam in UWOC system greatly improves security. Nevertheless, the safe signal transmission in UWOC system is not always feasible [5]. On one hand, the inherent divergence angle and geometric spreading of the beam would cause the spot size at the receiver to expand with increasing distance, thereby raising the risk that the confidential information could be intercepted by the eavesdroppers located within the expanded beam footprint [6]. On the other hand, as the beam propagates through seawater, it is highly susceptible to scattering effects. The interaction between suspended particles and photons will alter the direction of photon propagation, leading to significant spatial dispersion [7]. As a result, some scattered photons may not reach the field of view (FOV) of the legitimate receivers and could even enter the FOV of eavesdroppers.

In recent years, quantum key distribution (QKD) has garnered interest of researchers [8–11]. Based on the fundamental principles of quantum physics, it enables data confidentiality by using quantum states to transmit information. Any attempt by an eavesdropper to intercept the transmission will alter the quantum states and then alert the parties to the intrusion. This inherent security feature makes QKD more secure than the classical cryptography schemes relying on complex computations. The experimental results in [12] have demonstrated the feasibility of implementing secure quantum communication with submersibles in the open sea. Additionally, several theoretical studies on QKD in underwater channels have also been conducted [13–17]. For example, the authors in [13] investigated the quantum bit error rate (QBER) and secret key rate (SKR) performances of the well-known Bennett-Brassard 1984 (BB84) protocol over underwater turbulent path modeled by the average power transfer. Then, to overcome the range limitations due to absorption, scattering, and turbulence, passive relays is deployed to help the key distribution with BB84 protocol in [14]. In [15], the performance of the decoy state BB84 protocol was analyzed over underwater channels modeled by the average transmittance. In addition to the above discrete variable QKD (DV-QKD), recent studies have also explored continuous variable QKD (CV-QKD) in UWOC [16,17]. These experimental and theoretical studies on QKD generally assume the existence of a line-of-sight (LOS) link between the two quantum parties. However, this requirement may not always be satisfied in oceanic environment due to obstacles such as aquatic animals, seamounts, and underwater vehicles, etc. Consequently, a cost-effective solution is then needed to avoid blockage and maintain LOS connectivity for QKD-based quantum links in UWOC system.

The deployment of optical relay nodes is a traditional solution to overcome the limitation of LOS blockage in optical links, but such relay nodes are expensive and inconvenient as they normally require substantial additional hardware [18]. In recent years, optical intelligent reflecting surface (IRS) or reconfigurable intelligent surfaces (RIS) is emerging as a more efficient alternative, which can simply enhance signal propagation by reflecting the incident wave in the desired direction without a dedicated energy source [19–24]. Besides, it can be designed in various shapes and sizes, with implementations including conventional mirrors, software defined metasurfaces, phase-change materials (PCM), or liquid crystal surfaces [18]. Thus, it is a highly cost-effective, easily deployable and energy-efficient technology. For the first time, the authors in [25] introduced the concept of RIS to UWOC links, and applied the central limit theorem to evaluate the performance metrics such as average bit error rate (ABER), outage probability (OP), and channel capacity over Gamma-Gamma channels combining with misalignment from both beam jitter and IRS jitter. Besides, utilizing the approximate distribution of the sum of Gamma-Gamma random variables, the OP of RIS-assisted UWOC system were derived for IoUwT [26]. Then, the OP of an IRS-assisted UWOC system was studied under log-normal

Optics EXPRESS

channels with beam jitter-induced misalignment modeled by Rayleigh distribution in [27], as well as over exponentiated-Weibull (EW) turbulent channels with beam jitter-induced misalignment characterized by Hoyt distribution in USN [28]. In [29], the average spectral efficiency, average energy efficiency, OP, and ABER for IRS-assisted UWOC were analyzed using exponential and generalized gamma (EGG) distributions, without considering misalignment. In the rest of this paper, the optical IRS/RIS is uniformly referred to as OIRS. These aforementioned studies have shown that OIRS not only extends the coverage area but also enhances the SNR gain for UWOC links with different channel models. Nevertheless, those reports on OIRS mainly focused on enhancing the performance of classical UWOC links, leaving its potential role in underwater wireless optical quantum links unexplored. Very recently, although some studies [30–32] related to the OIRS-based FSO quantum links have been conducted, those results cannot be directly applied to underwater environments because of different channel characteristics. Actually, the deployment of OIRS in the oceanic environment will have various configurations depending on its location, such as being attached to the seabed, shore, or autonomous underwater vehicles (AUVs) and floating beneath the surface [33]. Among them, AUVs are expected to serve the deployed nodes of the IoUwT by moving from one node to another. While the primary task is to ensure a better connectivity and recharge the batteries of the distant nodes, AUVs are still quite suitable for carrying OIRS, whose high mobility could offer deployment flexibility and be adjusted to achieve optimal positioning of OIRS [33–35].

Motivated by the above analysis, in this work, an AUV-carried OIRS array is incorporated into QKD for the first time to establish a stable underwater wireless optical quantum link between the gateway node and the central node in the IoUwT, even in the obstructed underwater environment. A comprehensive evaluation is then conducted on the security of the AUV-carried OIRS-assisted DV-QKD and CV-QKD links in underwater channels subject to misalignment. Specifically, assuming that oceanic turbulence-induced irradiance fluctuation is modeled by EGG distribution, the irradiance attenuation triggered by oceanic absorption and scattering is depicted as Beer-Lambert's law, and the jitter angle corresponding to the optical beam offset in the receiving plane is characterized by a Rayleigh distribution, the novel statistics of this aggregated channel transmissivity experienced by quantum states in underwater links are derived. For the AUV-carried OIRS-assisted DV-QKD link, its QBER for weak coherent optical source is obtained and the lower bound SKR under the decoy state is established on the basis of these statistics and Gauss-Chebyshev quadrature (GCQ) method. For the AUV-carried OIRS-assisted CV-QKD link, the average Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound under the bosonic pure-loss channel, as well as the thermal upper bound (TUB) and thermal lower bound (TLB) under the thermal-loss channel are derived in terms of univariate Fox-H function. Besides, the achievable SKR for a practical GG02 CV-QKD protocol is also presented through the worst-case analysis. Furthermore, the security performances of the proposed underwater wireless optical quantum links are discussed by numerical analysis.

2. System and channel models

In this work, an AUV-carried OIRS-assisted underwater wireless optical quantum link is proposed to reliably distribute secret keys between the central node and the gateway node within the IoUwT. Typically, the link comprises a central node, an OIRS, and a gateway node, as illustrated in Fig. 1. The central node plays a critical role as the primary data aggregator, responsible for collecting data from USN and forwarding it to the gateway node via the UWOC link. The gateway node then receives the information and transmits it to onshore or offshore systems. Due to the open nature of the UWOC link, the collecting private data is susceptible to malicious eavesdropping. To this end, the DV-QKD and CV-QKD protocols are separately employed to provide quantum-level security for this link. In particular, an OIRS mounted on the AUV is used to flexibly avoid the LOS blockages caused by obstacles such as aquatic animals, seamounts, and underwater vehicles,

Optics EXPRESS

thereby maintaining the LOS connectivity in QKD-based UWOC links. Here, it is assumed that the AUV-carried OIRS is equipped with M reflecting elements. In the reminder of paper, the quantum link from the central node to the OIRS and then to the gateway node is referred to as the AUV-carried OIRS-assisted underwater wireless optical quantum link.

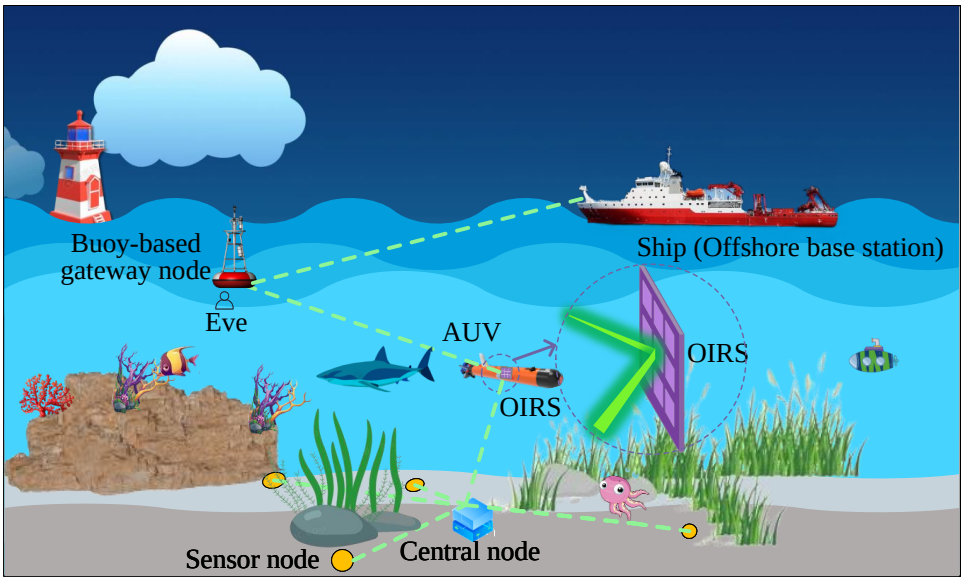

Fig. 1. A schematic of AUV-carried OIRS-assisted QKD link in IoUwT.

2.1. AUV-carried OIRS misalignment

In the underwater wireless optical quantum link, the misalignment usually refers to the deviation of the beam on the receiver plane caused by the jitter from both the transmitter and the AUV-carried OIRS. When the optical beam reflected by the AUV-carried OIRS travels to the gateway node at distance l, the received power can be approximately expressed as [36]

$$h^{PE}(u) \approx A_0 \exp\left(-\frac{2\|\mathbf{u}\|^2}{\omega_{zeq}^2}\right). \tag{1}$$

The approximation in (1) is accurate if w_Z/a_p >6, where a_p is the size of the receiving aperture and $\omega_z = \phi\left(l_{C,OIRS} + l_{OIRS,G}\right)$ describes the increase of the beam radius with the link distance. Here, ϕ is the divergence angle of beam, $l_{C,OIRS}$ is the link distance from the central node to the OIRS, and $l_{OIRS,G}$ is the link distance from the OIRS to the gateway node. $\|\mathbf{u}\|$ represents the instantaneous displacement from the receiver center to receiving light spot, which can be expressed as $\|\mathbf{u}\| = \tan\|\mathbf{\Theta}\|\, l_{OIRS,G} \approx \|\mathbf{\Theta}\|\, l_{OIRS,G}$ according to the geometric relationships in [24,37,38]. $\|\mathbf{\Theta}\|$ represents the superimposed pointing error angle and is characterized by a Rayleigh distribution. A_0 is the fraction of power collected by the receiver at its center and ω_{zeq} is the equivalent beam width. We have $A_0 = erf^2(\upsilon)$ and $\omega_{zeq}^2 = \omega_z^2\sqrt{\pi}erf\,(\upsilon)/2\upsilon\exp\left(-\upsilon^2\right)$, where $\upsilon = \sqrt{\pi/2}\,a_p/\omega_z$ is the ratio between aperture radius and the beam width. Furthermore, utilizing the properties of a monotonic function and letting $\zeta = \omega_{zeq}^2/4\sigma_\theta^2\left(l_{C,OIRS} + l_{OIRS,G}\right)^2 + 16\sigma_\beta^2 l_{OIRS,G}^2$, the probability

Optics EXPRESS

density function (PDF) of misalignment h^{PE} can be derived as [24]

$$f_{h^{PE}}\left(h^{PE}\right) = \frac{\zeta}{A_0{}^{\zeta}}\left(h^{PE}\right)^{\zeta-1},\ 0<h^{PE}<A_0, \tag{2}$$

where σ_θ^2 is the variance of the beam jitter angle at the transmitter, and σ_β^2 is the variance of the jitter angle of AUV-carried OIRS, ranging on the order of 10^{-6} rad^2.

2.2. Oceanic irradiance attenuation

As the optical beam propagates through the OIRS-assisted underwater channel, its mean irradiance will be attenuated. According to the well-known Beer-Lambert law, the oceanic irradiance attenuation can be calculated as [6]

$$L(\lambda, l) = \exp\left[-c(\lambda)\, l\right], \tag{3}$$

where l is the total transmission distance, i.e., $l = l_{C,OIRS} + l_{OIRS,G}$. $c(\lambda)$ denotes the extinction coefficient, which depends on the laser wavelength λ and water types, and is defined as the linear combination of absorption and scattering coefficients, i.e., $c(\lambda) = a(\lambda) + b(\lambda)$.

2.3. Oceanic irradiance fluctuation

To estimate the security of AUV-carried OIRS-assisted QKD links in underwater channels, it is crucial to select a suitable statistical model that can accurately describe the oceanic irradiance fluctuation caused by oceanic turbulence. Over the years, several models such as the Log-Normal, Generalized Gamma, Mixture Exponential-Lognormal and EGG distributions were proposed [39–42]. Among them, the EGG distribution stands out as a unified turbulence fading model, offering an excellent goodness of fit under various physical variations. It efficiently and statistically describes air bubbles and temperature-induced irradiance fluctuations from weak to strong turbulence conditions using fresh as well as salty waters. Furthermore, this model has a less complicated mathematical form, making it analytically tractable and more convenient for performance analysis. Based on reference [42], the unified statistical of irradiance fluctuation can be characterized as

$$f_{h^{Tur}}(h^{Tur}) = \frac{\omega}{\delta}\exp\left(-\frac{h^{Tur}}{\delta}\right) + \frac{(1-\omega)c{h^{Tur}}^{ac-1}}{b^{ac}}\frac{\exp\left(-\left(h^{Tur}/b\right)^{c}\right)}{\Gamma(a)}, \tag{4}$$

where ω is the mixture weight or mixture coefficient of the distribution, satisfying $\omega \in [0, 1]$, δ is the parameter of the Exponential distribution, a, b and c are the parameters of the Generalized Gamma distribution, and $\Gamma(\cdot)$ represents the Gamma function.

2.4. Statistics of the aggregated channel transmissivity

For the AUV-carried OIRS-assisted underwater wireless optical quantum link, the aggregated channel transmissivity can be written as $\eta_g = \eta L \sum_{m=1}^{M} \mathcal{H}_m$, where η is the responsivity of the detector, M corresponds to the number of the OIRS elements and $\mathcal{H}_m$ denotes the channel fading coefficient of central node-the mth OIRS element-gateway node link. Mathematically, the PDF

Optics EXPRESS

of $\mathcal{H}_m$ can be calculated as

$$f_{\mathcal{H}_m}(\mathcal{H}) = \int f_{\mathcal{H}_m|h^{Tur}}\left(\mathcal{H}\left|h^{Tur}\right.\right) f_{h^{Tur}}\left(h^{Tur}\right) dh^{Tur}. \tag{5}$$

Here, $f_{\mathcal{H}_m|h^{Tur}}\left(\mathcal{H}\left|h^{Tur}\right.\right)$ is the conditional probability defined as

$$f_{\mathcal{H}_m|h^{Tur}}\left(\mathcal{H}\left|h^{Tur}\right.\right) = \zeta \frac{\mathcal{H}^{\zeta-1}}{{A_0}^{\zeta}\left(h^{Tur}\right)^{\zeta}}, \tag{6}$$

where $0<\mathcal{H}_m/h_a<A_0$. Then, substituting (4) and (6) into (5) and utilizing (07.34.03.0228.01) in [43], the PDF of $\mathcal{H}_m$ can be achieved as

$$f_{\mathcal{H}_m}(\mathcal{H}_m) = \frac{\omega\zeta}{\mathcal{H}_m} G_{1,2}^{2,0}\left[\frac{\mathcal{H}_m}{\delta A_0}\middle| \begin{matrix}\zeta+1\\ 1,\zeta\end{matrix}\right] + \frac{(1-\omega)\zeta}{\Gamma(a)\mathcal{H}_m} G_{1,2}^{2,0}\left[\left(\frac{\mathcal{H}_m}{bA_0}\right)^c\middle| \begin{matrix}\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c}\end{matrix}\right]. \tag{7}$$

With the definition of the Meijer G function which is given as (9.301) in [44], the cumulative distribution function (CDF) of $\mathcal{H}_m$ can be obtained as

$$F_{\mathcal{H}_m}(\mathcal{H}_m) = \omega\zeta\, G_{2,3}^{2,1}\left[\frac{\mathcal{H}_m}{\delta A_0}\middle| \begin{matrix}1,\zeta+1\\ 1,\zeta,0\end{matrix}\right] + \frac{(1-\omega)\zeta}{c\Gamma(a)} G_{2,3}^{2,1}\left[\left(\frac{\mathcal{H}_m}{bA_0}\right)^c\middle| \begin{matrix}1,\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c},0\end{matrix}\right]. \tag{8}$$

Assuming that random variables $\mathcal{H}_1,\ldots\mathcal{H}_m,\ldots\mathcal{H}_M$ are independent and identically distributed, the aggregated channel transmissivity becomes $\eta_g = \eta LM\mathcal{H}$ [28]. Thus, with the aid of the probability density function transformation theorem, the PDF and CDF of η_g can be derived as

$$f_{\eta_g}(\eta_g) = \frac{\omega\zeta}{\eta_g} G_{1,2}^{2,0}\left[\frac{\eta_g}{\delta A_0\eta LM}\middle| \begin{matrix}\zeta+1\\ 1,\zeta\end{matrix}\right] + \frac{(1-\omega)\zeta}{\Gamma(a)\,\eta_g} G_{1,2}^{2,0}\left[\left(\frac{\eta_g}{bA_0\eta LM}\right)^c\middle| \begin{matrix}\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c}\end{matrix}\right], \tag{9}$$

$$F_{\eta_g}(\eta_g) = \omega\zeta\, G_{2,3}^{2,1}\left[\frac{\eta_g}{\delta A_0\eta LM}\middle| \begin{matrix}1,\zeta+1\\ 1,\zeta,0\end{matrix}\right] + \frac{(1-\omega)\zeta}{c\Gamma(a)} G_{2,3}^{2,1}\left[\left(\frac{\eta_g}{bA_0\eta LM}\right)^c\middle| \begin{matrix}1,\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c},0\end{matrix}\right]. \tag{10}$$

3. SKR of the AUV-carried OIRS-assisted DV-QKD link

The DV-QKD protocol typically employs polarization or time-bin encoding schemes and relies on single photon sources and detectors [45]. However, widespread deployment and integration of DV-QKD in the existing UWOC systems of IoUwT are hindered by the technological challenges in producing efficient single photon sources and detectors. In this context, we use weak laser pulses with less-than-unity average photon numbers instead of single photon, incorporating the decoy state idea first proposed by [46] to combat eavesdropping attacks, such as a photon number splitting attack. Furthermore, to maintain the quantum coherence of the photons reflected by the AUV-carried OIRS, we implement a time-bin encoding scheme in this section.

With Gottesman-Lo-Lütkenhaus-Preskill (GLLP) framework, the secure key generation rate formula for DV-QKD protocol under decoy state idea can be achieved as [9]

$$r_d \geq q\{Q_1[1-H(e_1)] - fQ_\mu H(e_\mu)\}, \tag{11}$$

where q depends on the implementation (1/2 for the BB84 protocol due to the fact that half of time Alice and Bob bases are not compatible, and if one uses the efficient BB84 protocol,

Optics EXPRESS

$q \approx 1.$), and f is the bidirectional error correction efficiency satisfying $f \geq 1$. The subscript μ represents the expected intensity of signal states and satisfies the condition $\mu \in (0, 1]$. This implies that the photon number of each weak laser pulse follows a Poisson distribution with the parameter μ. $Q_1 = Y_1 \mu e^{-\mu} \approx \eta_g \mu e^{-\mu}$ is the gain of single-photon states and $Q_\mu = \eta_g \mu$ is the overall gain of weak coherent pulse. $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Furthermore, e_1 is the error rate of single-photon state. e_μ denotes the overall QBER. Mathematically, e_1 and e_μ are given by $e_1 = e_{\text{det}} + Y_0/2\,\eta_g$ and $e_\mu = e_{\text{det}} + Y_0/2\,\eta_g\,\mu$, respectively [9,15]. Here, e_{det} is the probability that a photon hits the erroneous detector, and Y_0 is the dark count rate of the detector.

By applying Jensen's inequality, we can obtain a lower bound of $\mathbb{E}[r_d]$ as

$$\mathbb{E}[r_d] > \widetilde{r}_d = q\{\overline{Q}_1[1 - H(\bar{e}_1)] - f\overline{Q}_\mu H(\bar{e}_\mu)\}. \tag{12}$$

Consequently, the lower bound of the SKR in bits per second (bps) can be achieved as $R_d = \widetilde{r}_d/T$, where T is the pulse duration. $\overline{Q}_1 = \mathbb{E}\left[\eta_g \mu e^{-\mu}\right] = \overline{\eta}_g \mu e^{-\mu}$ and $\overline{Q}_\mu = \mathbb{E}\left[\eta_g \mu\right] = \overline{\eta}_g \mu$. $\bar{e}_1$ is the average error rate of single-photon states and $\bar{e}_\mu$ is the average overall QBER. On the basis of the statistic of aggregated channel transmissivity η_g, $\bar{e}_1$ and $\bar{e}_\mu$ can be calculated as

$$\bar{e}_1 = e_{\text{det}} + \frac{Y_0}{2}\int_0^\infty {\eta_g}^{-1} f_{\eta_g}(\eta_g)\, d\eta_g, \tag{13}$$

$$\bar{e}_\mu = e_{\text{det}} + \frac{Y_0}{2\mu}\int_0^\infty {\eta_g}^{-1} f_{\eta_g}(\eta_g)\, d\eta_g. \tag{14}$$

Then, using the GCQ-based computing method, the integral term $I_{\bar{e}} = \int_0^\infty {\eta_g}^{-1} f_{\eta_g}(\eta_g)\, d\eta_g$ in (13) and (14) can be obtained as

$$I_{\bar{e}} = \sum_{n=1}^{N}\left\{\frac{A_n \omega \zeta}{{u_n}^2} G_{1,2}^{2,0}\left[\frac{u_n}{\delta A_0 \eta L M}\,\middle|\,\begin{matrix}\zeta+1\\ 1,\zeta\end{matrix}\right] + \frac{A_n(1-\omega)\zeta}{\Gamma(a){u_n}^2} G_{1,2}^{2,0}\left[\left(\frac{u_n}{bA_0\eta L M}\right)^c\,\middle|\,\begin{matrix}\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c}\end{matrix}\right]\right\}, \tag{15}$$

where $A_n = \pi^2 \sin\left(\frac{2n-1}{2N}\pi\right)/\left[4N\cos^2\left(\frac{\pi}{4}\cos\left(\frac{2n-1}{2N}\pi\right)+\frac{\pi}{4}\right)\right]$ and $u_n = \tan\left(\frac{\pi}{4}\cos\left(\frac{2n-1}{2N}\pi\right)+\frac{\pi}{4}\right)$. By comparing the QBER expressions in Eq. (13) and Eq. (14), it can be concluded that the QBER of the single-photon optical source is greater than that of the weak coherent light source in the AUV-carried OIRS-assisted DV-QKD link due to $\mu \in (0, 1]$.

4. SKR of the AUV-carried OIRS-assisted CV-QKD link

The CV-QKD protocol can be effectively implemented using standard coherent optical sources in conjunction with homodyne/heterodyne detectors. Consequently, it can be seamlessly integrated with classical coherent UWOC systems in the IoUwT. First, we explore the ultimate information-theoretic bounds of the SKR for the AUV-carried OIRS-assisted CV-QKD link in underwater channel, without restrictions on their local operations and classical communication.

Bosonic pure-loss channel: The optical beam transmitted through AUV-carried OIRS-assisted underwater channel will inevitably experience losses and therefore the standard model to describe this scenario is the lossy channel. More concretely, this is a bosonic Gaussian channel characterized by a transmissivity parameter, which can be represented as a beam splitter mixing the signals with a zero-temperature environment while neglecting the background thermal noise. Utilizing the convexity properties of the relative entropy of entanglement in [47], the PLOB

Optics EXPRESS

bound of AUV-carried OIRS-assisted CV-QKD link over the lossy channel is given by

$$\bar{C} = \int_0^{\frac{1}{\eta LM}} -\log_2\left(1-\eta LM\mathcal{H}\right) f_{\mathcal{H}}\left(\mathcal{H}\right) d\mathcal{H}. \tag{16}$$

Substituting (7) into (16), one obtains

$$\begin{aligned}\bar{C} = &-\frac{\omega\zeta}{\ln 2}\underbrace{\int_0^{\frac{1}{\eta LM}} \ln\left(1-\eta LM\mathcal{H}\right)\mathcal{H}^{-1}\, G_{1,2}^{2,0}\left[\frac{\mathcal{H}}{\delta A_0}\,\middle|\, \begin{matrix}\zeta+1\\ 1,\zeta\end{matrix}\right] d\mathcal{H}}_{I_{\bar{C}}^{(1)}} \\ &-\frac{(1-\omega)\zeta}{\ln 2\Gamma(a)}\underbrace{\int_0^{\frac{1}{\eta LM}} \ln\left(1-\eta LM\mathcal{H}\right)\mathcal{H}^{-1}\, G_{1,2}^{2,0}\left[\left(\frac{\mathcal{H}}{bA_0}\right)^c\,\middle|\, \begin{matrix}\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c}\end{matrix}\right] d\mathcal{H}}_{I_{\bar{C}}^{(2)}}.\end{aligned} \tag{17}$$

Then, using the Taylor series expansion of $\ln(1-y) = -\sum_{k=1}^{\infty} y^k/k$ for $0 \le y<1$ and the properties of Fox-H function, along with (1.16.4) in [48], the integral terms $I_{\bar{C}}^{(1)}$ and $I_{\bar{C}}^{(2)}$ in (17) can be derived as

$$I_{\bar{C}}^{(1)} = -\sum_{k=1}^{\infty} \frac{D_{\bar{C}}{}^k}{k} F_{\bar{C}}^{(k,1)}\left(\frac{1}{D_{\bar{C}}}\right), \tag{18}$$

$$I_{\bar{C}}^{(2)} = -\sum_{k=1}^{\infty} \frac{D_{\bar{C}}{}^k}{k} F_{\bar{C}}^{(k,2)}\left(\frac{1}{D_{\bar{C}}}\right), \tag{19}$$

where $D_{\bar{C}} = \eta LM$ and the unified expression for $F_{\bar{C}}^{(k,i)}(y)$ can be written as

$$F_{\bar{C}}^{(k,i)}(y) = \frac{1}{A_{\bar{C}2}^{(i)}} y^k\, H_{2,3}^{2,1}\left[A_{\bar{C}1}^{(i)}\, {}^{\frac{1}{A_{\bar{C}2}^{(i)}}} y\,\middle|\, \begin{matrix}(1-k,1),\left(B_{\bar{C}1}^{(i)},\frac{1}{A_{\bar{C}2}^{(i)}}\right)\\ \left(B_{\bar{C}2}^{(i)},\frac{1}{A_{\bar{C}2}^{(i)}}\right),\left(B_{\bar{C}1}^{(i)}-1,\frac{1}{A_{\bar{C}2}^{(i)}}\right),(-k,1)\end{matrix}\right]. \tag{20}$$

We have $A_{\bar{C}1}^{(1)} = 1/(\delta A_0), A_{\bar{C}2}^{(1)} = 1, B_{\bar{C}1}^{(1)} = \zeta+1, B_{\bar{C}2}^{(1)} = 1$ for $i=1$ and $A_{\bar{C}1}^{(2)} = (1/bA_0)^c, A_{\bar{C}2}^{(2)} = c, B_{\bar{C}1}^{(2)} = \zeta/c+1, B_{\bar{C}2}^{(2)} = a$ for $i=2$.

Thermal-loss channel: In practice, the additional thermal noise will be introduced into the AUV-carried OIRS-assisted underwater wireless optical quantum link, normally due to laser noise. Hence, it is crucial to identify the SKR for these more general thermal-loss channels with a nonzero environmental thermal photon number. By applying the reduction method in [47], the TUB is given by

$$\mathcal{U}\left(\eta_g,\bar{n}\right) = \begin{cases} -\log_2\left(1-\eta_g\right) - \bar{n}\log_2\left(\eta_g\right) - h\left(\bar{n}\right), & \eta_g \ge \bar{n} \\ 0, & otherwise \end{cases} \tag{21}$$

Here, $h(x) := (1+x)\log_2(1+x) - x\log_2(x)$. $\bar{n}$ represents the total number of thermal photons and can be calculated as $\bar{n} = \eta_g\,\bar{n}_B + \bar{n}_d$, where $\bar{n}_B$ denotes the number of background thermal photons per mode, ranging between 10^{-8} photons/mode (at night) and 10^{-3} photons/mode (during day). $\bar{n}_d$ is the number of detector thermal photons composed of electronic noise, local oscillator noise, and other factors in the underwater wireless optical quantum link. For a pure-loss channel, the

Optics EXPRESS

environmental mode is in a vacuum state with $\bar{n} = 0$. On the basis of (7), the average TUB of AUV-carried OIRS-assisted CV-QKD link can be expressed as

$$\mathcal{U} = \begin{cases} I_{\bar{\mathcal{U}}}^{(1)} + I_{\bar{\mathcal{U}}}^{(2)} + I_{\bar{\mathcal{U}}}^{(3)}, & \eta_g \geq \bar{n} \\ 0, & otherwise \end{cases} \tag{22}$$

By performing operations similar to solving $I_{\bar{C}}^{(1)}$ and $I_{\bar{C}}^{(2)}$, the integral term $I_{\bar{\mathcal{U}}}^{(1)}$ can be achieved as

$$\begin{aligned} I_{\bar{\mathcal{U}}}^{(1)} &= -\int_{\bar{n}/\eta LM}^{1/\eta LM} \log_2\left(1-\eta LM\mathcal{H}\right) f_{\mathcal{H}}\left(\mathcal{H}\right) d\mathcal{H} \\ &= \frac{\omega\zeta}{\ln 2}\sum_{k=1}^{\infty}\frac{(\eta LM)^k}{k}\left[F_{\bar{C}}^{(k,1)}\left(\frac{1}{\eta LM}\right) - F_{\bar{C}}^{(k,1)}\left(\frac{\bar{n}}{\eta LM}\right)\right] \\ &\quad + \frac{(1-\omega)\zeta}{\ln 2\Gamma(a)}\sum_{k=1}^{\infty}\frac{(\eta LM)^k}{k}\left[F_{\bar{C}}^{(k,2)}\left(\frac{1}{\eta LM}\right) - F_{\bar{C}}^{(k,2)}\left(\frac{\bar{n}}{\eta LM}\right)\right], \end{aligned} \tag{23}$$

where $F_{\bar{C}}^{(k,i)}(y)$ has been presented in (20). $I_{\bar{\mathcal{U}}}^{(2)}$ can be further expressed as

$$\begin{aligned} I_{\bar{\mathcal{U}}}^{(2)} &= -\frac{\bar{n}\omega\zeta}{\ln 2}\underbrace{\int_{\bar{n}/\eta LM}^{1/\eta LM}\ln\left(\eta LM\mathcal{H}\right)\mathcal{H}^{-1}\, G_{1,2}^{2,0}\left[\frac{\mathcal{H}}{\delta A_0}\middle|\begin{matrix}\zeta+1\\ 1,\zeta\end{matrix}\right] d\mathcal{H}}_{I_{\bar{\mathcal{U}}}^{(2,1)}} \\ &\quad -\bar{n}\frac{(1-\omega)\zeta}{\ln 2\Gamma(a)}\underbrace{\int_{\bar{n}/\eta LM}^{1/\eta LM}\ln\left(\eta LM\mathcal{H}\right)\mathcal{H}^{-1}\, G_{1,2}^{2,0}\left[\left(\frac{\mathcal{H}}{bA_0}\right)^c\middle|\begin{matrix}\frac{\zeta}{c}+1\\ a,\frac{\zeta}{c}\end{matrix}\right] d\mathcal{H}}_{I_{\bar{\mathcal{U}}}^{(2,2)}}. \end{aligned} \tag{24}$$

Then, using integration by parts and with the aid of (1.16.4) in [48], the integral terms in (24) can be derived as

$$I_{\bar{\mathcal{U}}}^{(2,1)} = -\ln\left(\bar{n}\right) F_{\bar{C}}^{(0,1)}\left(\bar{n}/\eta LM\right) - \mathcal{F}_{\bar{\mathcal{U}}}^{(0,1)}\left(1/\eta LM\right) + \mathcal{F}_{\bar{\mathcal{U}}}^{(0,1)}\left(\bar{n}/\eta LM\right), \tag{25}$$

$$I_{\bar{\mathcal{U}}}^{(2,2)} = -\ln\left(\bar{n}\right) F_{\bar{C}}^{(0,2)}\left(\bar{n}/\eta LM\right) - \mathcal{F}_{\bar{\mathcal{U}}}^{(0,2)}\left(1/\eta LM\right) + \mathcal{F}_{\bar{\mathcal{U}}}^{(0,2)}\left(\bar{n}/\eta LM\right). \tag{26}$$

The unified expression of $\mathcal{F}_{\bar{\mathcal{U}}}^{(0,i)}(y)$ is given by

$$\mathcal{F}_{\bar{\mathcal{U}}}^{(0,i)}(y) = \frac{1}{A_{\bar{\mathcal{U}}2}^{(i)}} H_{3,4}^{2,2}\left[A_{\bar{\mathcal{U}}1}^{(i)\,\frac{1}{A_{\bar{\mathcal{U}}2}^{(i)}}} y\middle|\begin{matrix}(1,1),(1,1),\left(B_{\bar{\mathcal{U}}1}^{(i)},\frac{1}{A_{\bar{\mathcal{U}}2}^{(i)}}\right)\\ \left(B_{\bar{\mathcal{U}}2}^{(i)},\frac{1}{A_{\bar{\mathcal{U}}2}^{(i)}}\right),\left(B_{\bar{\mathcal{U}}1}^{(i)}-1,\frac{1}{A_{\bar{\mathcal{U}}2}^{(i)}}\right),(0,1),(0,1)\end{matrix}\right] \tag{27}$$

We have $A_{\bar{\mathcal{U}}1}^{(1)} = 1/\delta A_0$, $A_{\bar{\mathcal{U}}2}^{(1)} = 1, B_{\bar{\mathcal{U}}1}^{(1)} = \zeta + 1, B_{\bar{\mathcal{U}}2}^{(1)} = 1$ for $i = 1$ and $A_{\bar{\mathcal{U}}1}^{(2)} = (1/bA_0)^c, A_{\bar{\mathcal{U}}2}^{(2)} = c, B_{\bar{\mathcal{U}}1}^{(2)} = \zeta/c + 1, B_{\bar{\mathcal{U}}2}^{(2)} = a$ for $i = 2$. $I_{\bar{\mathcal{U}}}^{(3)}$ can be calculated as

$$I_{\bar{\mathcal{U}}}^{(3)} = -h\left(\bar{n}\right)\int_{\bar{n}/\eta LM}^{1/\eta LM} f_{\mathcal{H}}\left(\mathcal{H}\right) d\mathcal{H} = h\left(\bar{n}\right)\left[F_H\left(\frac{\bar{n}}{\eta LM}\right) - F_H\left(\frac{1}{\eta LM}\right)\right], \tag{28}$$

Optics EXPRESS

where $F_H(.)$ can be obtained in (8). In addition to the TUB, the TLB of AUV-carried OIRS-assisted CV-QKD link is given by [47]

$$\mathcal{L}\left(\eta_g, \bar{n}\right) = -\log_2\left(1-\eta_g\right) - h\left(\bar{n}\right). \tag{29}$$

Corresponding, the average TLB can be expressed as

$$\bar{\mathcal{L}} = I_{\bar{\mathcal{L}}}^{(1)} + I_{\bar{\mathcal{L}}}^{(2)}. \tag{30}$$

Thus, the solution of the integral term $I_{\bar{\mathcal{L}}}^{(1)}$ can be derived as

$$\begin{aligned} I_{\bar{\mathcal{L}}}^{(1)} &= -\int_0^{1/\eta LM} \log_2\left(1-\eta LM\mathcal{H}\right) f_{\mathcal{H}}\left(\mathcal{H}\right) d\mathcal{H} \\ &= \frac{\omega\zeta}{\ln 2}\sum_{k=1}^{\infty}\frac{(\eta LM)^k}{k} F_{\bar{C}}^{(k,1)}\left(\frac{1}{\eta LM}\right) + \frac{(1-\omega)\zeta}{\ln 2\Gamma(a)}\sum_{k=1}^{\infty}\frac{(\eta LM)^k}{k} F_{\bar{C}}^{(k,2)}\left(\frac{1}{\eta LM}\right). \end{aligned} \tag{31}$$

$I_{\bar{\mathcal{L}}}^{(2)}$ can be further achieved as

$$I_{\bar{\mathcal{L}}}^{(2)} = -h\left(\bar{n}\right)\int_0^{1/\eta LM} f_{\mathcal{H}}\left(\mathcal{H}\right) d\mathcal{H} = -h\left(\bar{n}\right) F_H\left(\frac{1}{\eta LM}\right). \tag{32}$$

Subsequently, a practical Gaussian-modulated CV-QKD protocol also known as the GG02 protocol is adopted in the AUV-carried OIRS-assisted underwater wireless optical quantum link. We assume that the legitimate communicating parties utilize reverse reconciliation while the eavesdropper employs a Gaussian collective attack to extract the maximum information from the key. Besides, the eavesdropper has sufficient capability to acquire all the background photons, leaked photons from imperfect detectors, and to manipulate the detector noise. This worst-case analysis establishes a lower bound for the SKR, effectively ensuring perfect secrecy. According to Ref. [31], the achievable SKR of the GG02 protocol can be expressed as

$$r_c = \frac{\xi}{2}\log_2\left(1+\frac{\eta_g\left(V-1\right)}{2\bar{n}+1}\right) - h^{'}\left(\lambda_1\right) - h^{'}\left(\lambda_2\right) + h^{'}\left(\lambda_3\right), \tag{33}$$

where ξ is the reconciliation efficiency, V is the variance of the transmitted mode in shot noise units (SNU). $h^{'}(x)$ is defined as

$$h^{'}(x) := \frac{(x+1)}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right). \tag{34}$$

In addition, $\lambda_{1/2}$ and λ_3 are defined as

$$\lambda_{1/2} = \frac{1}{2}\left(\sqrt{(V+\beta)^2 - 4\eta_g\left(V^2-1\right)} \pm (\beta - V)\right), \tag{35}$$

$$\lambda_3 = \sqrt{V^2 - \frac{V\eta_g\left(V^2-1\right)}{\beta}}, \tag{36}$$

where $\beta = \eta_g\left(V-1\right) + 2\bar{n} + 1$. Consequently, the achievable SKR in bits per use (bits/use) can be achieved as $R_c = r_c/T$, where T is the pulse duration.

Optics EXPRESS

Table 1. Monte Carlo Simulation Parameters

Parameters of Link and Channel	Value	Parameters of Link and Channel	Value
Receiving aperture, a_p	20cm	Source wavelength, λ	532nm
The divergence angle of beam, ϕ	10mrad	Pulse duration, T	1 ns
The ratio of the distance from the central node to the OIRS relative to the total link distance, $l_{S,OIRS}/l$	0.8	The absorption and scattering coefficient in clear water and coastal water, respectively $[a(\lambda), b(\lambda)]$	(0.014,0.037) (0.179,0.22)
The optical-to-electrical conversion coefficients, η	0.8	The parameters of EGG turbulence distribution, $[\omega, \delta, a, b, c]$	(0.213,0.3291, 1.4299,1.1817, 17.1984)
Signal rate, R_s	1Gbps	The variance of the beam jitter angle at the transmitter and AUV-carried OIRS, $\sigma_\theta^2 = \sigma_\beta^2$	1×10^{-6} rad^2
Parameters of DV-QKD protocol	Value	Parameters of CV-QKD protocol	Value
Weak laser pulse with Poisson parameter , μ	0.5	The reconciliation efficiency, ξ	0.95
The probability that a photon hits the erroneous detector, e_{det}	0	The variance of the transmitted mode in shot noise units, V	5 SNU
The dark count rate of the detector, Y_0	10^{-7}	The number of background thermal photons per mode, $\bar{n}_B$	4.75×10^{-7}
The bidirectional error correction efficiency, f	1.22	The number of detector thermal photons, $\bar{n}_d$	0.05

5. Numerical results and discussion

In this section, the numerical results are presented to demonstrate the security performance of the AUV-carried OIRS-assisted QKD links in underwater channels with misalignment. Specifically, Monte Carlo (MC) simulations are utilized to validate and evaluate the QBER and SKR metrics. The acceptance/rejection method is adopted to generate random fading channel with the EGG turbulence distribution, while the analytical transform method is applied to generate random fading of AUV-carried OIRS misalignment model. During the process, a total of 10^8 Monte Carlo trials are conducted. Unless otherwise specified, the default MC simulation parameters are provided in Table 1.

Figure 2 illustrates the QBER of the AUV-carried OIRS-assisted DV-QKD link under different jitter variances and OIRS element numbers in underwater channel. The analytical results have excellent agreement with the corresponding MC simulation results, thereby confirming the correctness of our QBER models. As shown in Figs. 2(a) and 2(b), the QBER for a single-photon optical source increases steadily with link distance in both clear water and coastal water, and the increase is more pronounced in coastal water. This is mainly because the oceanic irradiance

Optics EXPRESS

attenuation is proportional to both the link distance and the extinction coefficient. Coastal water, with a higher extinction coefficient, will make photon detection more challenging, ultimately leading to a decline in QBER performance. As the jitter variances σ_θ^2 and σ_β^2 increase, the QBER rises. This effect becomes more significant over longer transmission distances, such as at l>15 m. Specifically, increasing the number of OIRS elements can effectively reduce the QBER values. For instance, in clear water at a transmission distance of l = 41 m, the QBERs for three different jitter variances are about 4.5×10^{-6}, 5.8×10^{-6} and 7.1×10^{-6} when M = 1, and 4.5×10^{-7}, 5.8×10^{-7} and 7.1×10^{-7} when M = 10. This further confirms the effectiveness of the AUV-carried OIRS in enhancing the performance of DV-QKD within the underwater wireless optical quantum links. That is to say, the AUV-carried OIRS can not only help to overcome LOS blockages caused by underwater obstacles but also significantly enhance the reliability of the quantum links. Notably, the performance improvements provided by the AUV-carried OIRS are not limitless. Once the number of elements surpasses a certain threshold, the QBER will reach saturation. Comparing Figs. 2(c) and 2(d), it is evident that as the water quality deteriorates, the overall QBER performance degrades for the weak coherent source. For given values of l = 31 m, M = 5 and $\sigma_\theta^2 = \sigma_\beta^2 = 5 \times 10^{-6}$, the overall QBER is 5.97×10^{-7} in clear water, whereas it is 1.3×10^{-3} in coastal water. Additionally, as the link distance increases, the overall QBER performance continues to worsen. Meanwhile, the beam jitter at the transmitter and AUV-carried OIRS jitter further exacerbate the overall QBER at longer transmission distances. In coastal water at a transmission distance of l = 31 m, the overall QBERs are 3.9×10^{-3} and 3.9×10^{-4} for M = 1 and M = 10, respectively, when $\sigma_\theta^2 = \sigma_\beta^2 = 1 \times 10^{-6}$. And the overall QBERs are 6.5×10^{-3} and 6.5×10^{-4} for M = 1 and M = 10 when $\sigma_\theta^2 = \sigma_\beta^2 = 5 \times 10^{-6}$. Fortunately, increasing the number of AUV-carried OIRS elements can effectively mitigate these adverse effects and reduce the performance demands on components, such as the sensitivity of photodetectors. Besides, under the same link, the DV-QKD utilizing a single-photon optical source exhibits better QBER performance than that with a weak coherent light source, further supporting the conclusions drawn in Section3.

Figure 3 shows the SKR of the AUV-carried OIRS-assisted DV-QKD link with the decoy state idea in underwater channel. As can be observed, the SKR exhibits a marked decline as the underwater wireless optical quantum link distance increases. This decline is attributed to the inverse relationship between the SKR and the overall QBER, as described in (12), and the overall QBER values will rise as the link distance increases. In Fig. 3(a), the impact of the AUV-carried OIRS position on the SKR is compared by varying $l_{C,OIRS}/l$ for different link distances. At longer link distance, the SKR increases as $l_{C,OIRS}/l$ increases, where $l_{C,OIRS}/l$ varies within $(0, 1)$. For instance, at l = 25 m, the SKR is 1.27 Mbps when $l_{C,OIRS}/l = 0.2$, while it is 1.67 Mbps when $l_{C,OIRS}/l = 0.8$. As demonstrated, the improvement in SKR resulting from the increase of $l_{C,OIRS}/l$ is not very pronounced, and this can be explained as follows. In the aggregated channel transmissivity, the parameter related to $l_{C,OIRS}/l$ is $\zeta = \omega_{zeq}^2 \Big/ \left[4\sigma_\theta^2 \left(l_{C,OIRS} + l_{OIRS,G}\right)^2 + 16\sigma_\beta^2 l_{OIRS,G}^2\right]$ of the AUV-carried OIRS misalignment model, where ζ will vary with changes in $l_{OIRS,G}$, thereby affecting the misalignment. Clearly, $l_{OIRS,G}$ will change more noticeably as the link distance l increases when $l_{C,OIRS}/l$ rises in equal increments. Thus, the improvement in SKR can be observed at longer link distance. However, the aggregated channel transmissivity is on the order of 10^{-6}, while $l_{OIRS,G}$ is on the order of 10 m, therefore the improvement is not very pronounced. From the above analysis, it could be concluded that the link distance has a substantial impact on the SKR, whereas the position of the AUV-carried OIRS has a negligible effect. This insight offers some guidance for the placement of the OIRS in practical systems, suggesting that the shortest available path can serve as the optimal installation location in real applications. In Fig. 3(b), a comparative analysis of the SKR under varying jitter variances and different OIRS element numbers is provided. As can be found,

Optics EXPRESS

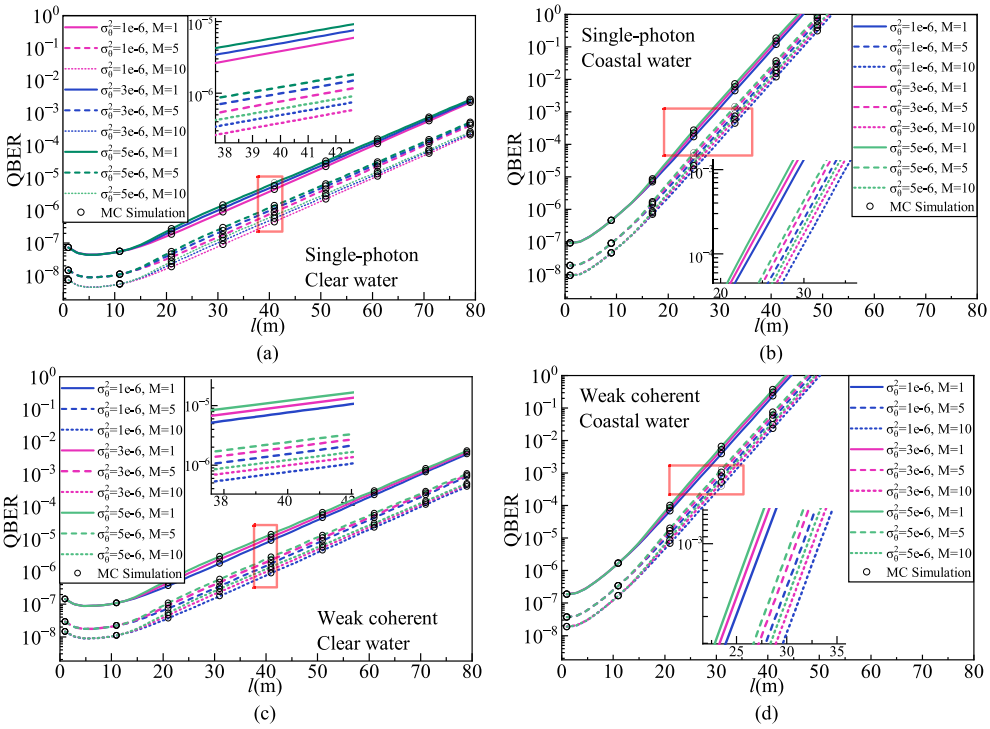

Fig. 2. QBER versus link distance for the AUV-carried OIRS-assisted DV-QKD link with (a) single-photon optical source in clear water, (b) single-photon optical source in coastal water, (c) weak coherent optical source in clear water and (d) weak coherent optical source in coastal water under different jitter variances and OIRS element numbers.

an increase in σ_θ^2 and σ_β^2 also negatively affects the SKR, especially in the medium-distance range, such as (15 m, 30 m). Given $M = 1$ and $l = 21$ m, the SKR values are 3.7 Mbps for $\sigma_\theta^2 = \sigma_\beta^2 = 1 \times 10^{-6}$ and 2.5 Mbps for $\sigma_\theta^2 = \sigma_\beta^2 = 5 \times 10^{-6}$. Consistent with the results in Fig. 2, increasing the number of AUV-carried OIRS elements can effectively mitigate the adverse effects of link distance and misalignment, thereby improving the SKR performance of the AUV-carried OIRS-assisted DV-QKD link in underwater channel. Figures 3(c) and 3(d) demonstrate the impacts of the probability of erroneous detection e_{det} and OIRS element numbers on the SKR for the AUV-carried OIRS-assisted DV-QKD protocol across varying link distances in clear water and coastal water, respectively. As e_{det} increases, the SKR for the protocol decreases. For instance, in clear water at a transmission distance of $l = 21$ m, the SKR values are 3.70 Mbps for $e_{\text{det}} = 0$ and 1.36 Mbps for $e_{\text{det}} = 3.3\%$ when $M = 1$. The AUV-carried OIRS-assisted DV-QKD link can achieve better security performance in clear water. For given parameters $e_{\text{det}} = 0$ and $M = 5$, the SKR decreases from 155.23 Mbps to 58.81 Mbps in clear water, and from 16.69 Mbps to 1.43 Mbps in coastal water, as the link distance extends from 9 m to 15 m. Additionally, the detrimental impact of increasing e_{det} on the SKR is more pronounced in clear water, whereas the influence of increasing link distance is more significant in coastal water. This is because that the end-to-end aggregated channel transmissivity primarily depends on the effects of oceanic absorption and scattering for the given jitter variance and oceanic turbulence. Compared to coastal water, clear water has a smaller extinction coefficient, resulting in relatively lower irradiance attenuation and a smaller impact on the SKR. In this case, the SKR exhibits a strong dependency on e_{det}. In coastal water, the larger extinction coefficient will result in

Optics EXPRESS

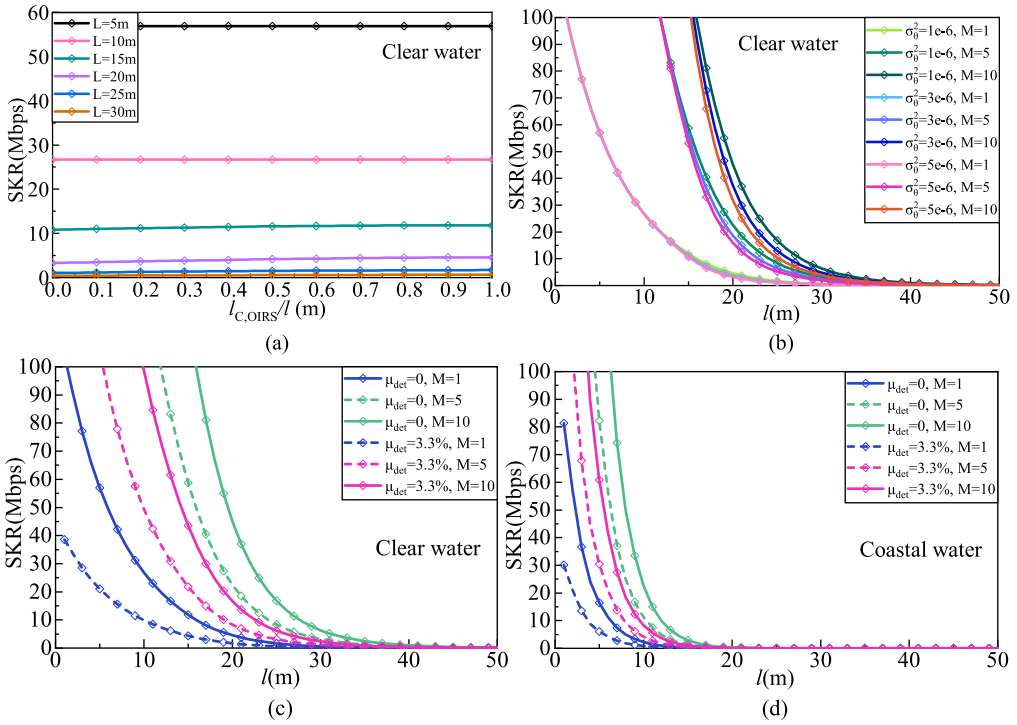

Fig. 3. SKR of the AUV-carried OIRS-assisted DV-QKD link versus (a) $l_{S,IRS}/l$ with different link distances and (b) l for varying jitter variances and OIRS element numbers in clear water, (c) l for different e_{det} and OIRS element numbers in clear water and (d) l for different e_{det} and OIRS element numbers in coastal water.

more significant irradiance attenuation as the link distance increases, thus leading to a faster decline in the SKR. Although increasing the number of OIRS elements can enhance the SKR to some extent, this effect will become limited as the link distance increases, regardless of the medium is clear water or coastal water. Consequently, in practical communication scenarios, the effective transmission distance should be determined in conjunction with the quality-of-service requirements and the number of OIRS elements.

Figures 4(a) and 4(b) present the PLOB, TUB, and TLB of the AUV-carried OIRS-assisted CV-QKD link in underwater channel and illustrate the impacts of different jitter variances and link distances on these SKR metrics in both clear water and coastal water. An excellent agreement between the analytical results and MC simulations is achieved, therefore validating the derived closed-form expressions of the PLOB, TUB and TLB. For given water type and jitter variance, the TUB and TLB are lower than the PLOB, indicating that the background thermal noise has a significant impact on the SKR performance. For example, the PLOB, TUB, and TLB are 0.036 bits/use, 0.027 bits/use and 0.018 bits/use in clear water at a transmission distance of 21 m when $\sigma_\theta^2 = \sigma_\beta^2 = 1 \times 10^{-6}$. As the link distance increases, these SKR metrics drop significantly and the decline will be more obvious in coastal water compared to clear water. For instance, when l increases from 9 m to 15 m, the PLOB values in clear water and coastal water decrease by 66.7% and 91.6%, respectively. Meanwhile, these SKR metrics will decrease as the jitter variance increases and this effect is more noticeable in clear water. This is because the lower irradiance attenuation in clear water has less effect on the security of the proposed quantum link, making the impact of misalignment on its security more obvious. Figure 4(c) depicts the achievable SKR

Optics EXPRESS

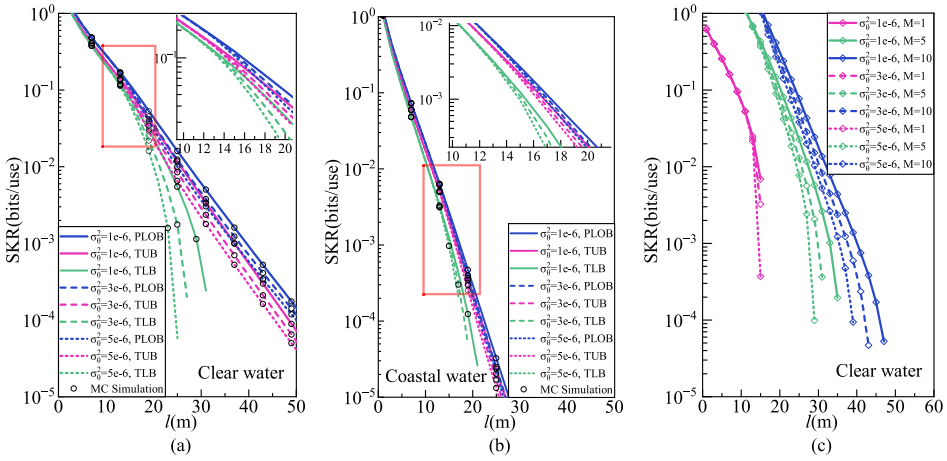

Fig. 4. PLOB, TUB and TLB of AUV-carried OIRS-assisted CV-QKD link (a) in clear water and (b) in coastal water versus link distance for different jitter variances, and (c) achievable SKR of GG02 versus link distance under different jitter variances and OIRS element numbers in clear water.

of the AUV-carried OIRS-assisted GG02 link for different jitter variances and link distances in clear water. The achievable SKR of the AUV-carried OIRS-assisted GG02 protocol steadily declines as the link distance increases in the underwater channel. Additionally, the influence of σ_θ^2 and σ_β^2 on the achievable SKR becomes more significant as the link distance increases. For example, when $\sigma_\theta^2 = \sigma_\beta^2$ increases from 1×10^{-6} to 5×10^{-6}, the achievable SKR for $M = 5$ decreases by 0.15% and 14.2% in $l = 9$ m and $l = 15$ m, respectively. In particular, increasing the number of AUV-carried OIRS elements can effectively enhance the achievable SKR, thereby further improving the confidentiality of the GG02 protocol.

6. Conclusion

In this work, an AUV-carried OIRS-assisted QKD link was proposed for the gateway and central nodes of the IoUwT system and its security was investigated over EGG turbulence channel combining oceanic absorption, scattering and OIRS misalignment. Specifically, the statistics of the aggregated channel transmissivity experienced by the AUV-carried OIRS-assisted quantum states in underwater link were derived. With the help of GCQ-based computing method, the overall QBER and the lower bound SKR were also obtained for the AUV-carried OIRS-assisted DV-QKD link employing weak coherent optical source and decoy state idea. Besides, for the AUV-carried OIRS-assisted CV-QKD link, the ultimate information-theoretic bounds of the SKR were derived in terms of univariate Fox-H function. The achievable SKR for a practical GG02 protocol over the aggregated channel transmissivity was also presented. Furthermore, the influences of the number of OIRS elements, OIRS positioning, jitter variances, the probability of erroneous detection, link distance and water types on the security performance of the proposed quantum links were studied. Results showed that the security performance of the AUV-carried OIRS-assisted DV-QKD and CV-QKD links degrades with deteriorating water quality as well as with increased link distances and jitter variances in underwater channels. The position of the AUV-carried OIRS has a negligible impact on the security performance, suggesting that the shortest available path could serve as the optimal installation location for the quantum links. As the probability of erroneous detection increases, the SKR for the AUV-carried OIRS-assisted DV-QKD link decreases, with the detrimental impact being more pronounced in clear water.

Optics EXPRESS

The background thermal noise significantly affects the SKR performance of the AUV-carried OIRS-assisted CV-QKD link. Interestingly, the AUV-carried OIRS can not only help to overcome LOS blockages caused by underwater obstacles but also significantly enhance the security performance of the quantum links by increasing the number of OIRS elements for both DV-QKD and CV-QKD protocols across various underwater conditions. This work could serve as reference for the design and research of underwater wireless optical quantum links in IoUwT system.

Funding. National Natural Science Foundation of China (62071365); Key Research and Development Projects of Shaanxi Province (2017ZDCXL-GY-06-02, 2022GY-103); Fundamental Research Funds for the Central Universities and the Innovation Fund of Xidian University (YJS2203); Aeronautical Science Foundation of China and National Key Laboratory of Air-based Information Perception and Fusion (20230001081001)

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. I. Ahmad, R. Narmeen, Z. Kaleem, *et al.*, "Machine-learning-based optimal cooperating node selection for internet of underwater things," IEEE Internet Things J. **11**(12), 22471–22482 (2024).
2. T. Qiu, Z. Zhao, T. Zhang, *et al.*, "Underwater internet of things in smart ocean: System architecture and open issues," IEEE Trans. Ind. Inf. **16**(7), 4297–4307 (2020).
3. M. C. Domingo, "An overview of the internet of underwater things," J. Netw. Comput. Appl. **35**(6), 1879–1890 (2012).
4. Z. Zeng, S. Fu, H. Zhang, *et al.*, "A survey of underwater optical wireless communications," IEEE Commun. Surv. Tutorials **19**(1), 204–238 (2017).
5. B. Zhou, P. Wang, W. Pang, *et al.*, "Effective secrecy throughput optimization for GTLS-based UWOC systems with eavesdropper outage constraint," Opt. Express **32**(18), 32079–32093 (2024).
6. L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media* (Society of Photo-Optical Instrumentation Engineers, 2005).
7. R. Boluda-Ruiz, P. Salcedo-Serrano, B. Castillo-Vázquez, *et al.*, "Impact of scattering on secrecy outage probability of underwater optical wireless links," IEEE J. Oceanic Eng. **48**(4), 1362–1372 (2023).
8. D. Gottesman, L. O. Hoi-Kwonglo, N. Lutkenhaus, *et al.*, "Security of quantum key distribution with imperfect devices," Quantum Informat. Comput. **4**(5), 325–360 (2004).
9. X. Ma, B. Qi, Y. Zhao, *et al.*, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
10. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photonics **12**(4), 1012–1236 (2020).
11. S. Pirandola, "Limits and security of free-space quantum communications," Phys. Rev. Res. **3**(1), 013279 (2021).
12. C.-Q. Hu, Z.-Q. Yan, J. Gao, *et al.*, "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," Photonics Res. **7**(8), A40–A44 (2019).
13. A. H. Fahim Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," J. Opt. Soc. Am. B **37**(2), 564–573 (2020).
14. A. H. Fahim Raouf, M. Safari, and M. Uysal, "Multi-hop quantum key distribution with passive relays over underwater turbulence channels," J. Opt. Soc. Am. B **37**(12), 3614–3621 (2020).
15. A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of decoy state quantum key distribution over underwater turbulence channels," J. Opt. Soc. Am. B **39**(6), 1470–1478 (2022).
16. Y. Xiang, Y. Wang, X. Ruan, *et al.*, "Improving the discretely modulated underwater continuous-variable quantum key distribution with heralded hybrid linear amplifier," Phys. Scr. **96**(6), 065103 (2021).
17. Z. Zuo, Y. Wang, Y. Mao, *et al.*, "Security of quantum communications in oceanic turbulence," Phys. Rev. A **104**(5), 052613 (2021).
18. V. Jamali, H. Ajam, M. Najafi, *et al.*, "Intelligent reflecting surface assisted free-space optical communications," IEEE Commun. Mag. **59**(10), 57–63 (2021).
19. H. Ajam, M. Naja, V. Jamali, *et al.*, "Channel modeling for IRS-assisted FSO systems," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, (2021), pp. 1–7.
20. M. Najafi and R. Schober, "Intelligent reflecting surfaces for free space optical communications," in *2019 IEEE Global Communications Conference (GLOBECOM)*, (2019), pp. 1–7.
21. A. R. Ndjiongue, T. M. N. Ngatched, O. A. Dobre, *et al.*, "Analysis of RIS-based terrestrial-FSO link over G-G turbulence with distance and jitter ratios," J. Lightwave Technol. **39**(21), 6746–6758 (2021).
22. J.-H. Noh and B. Lee, "Phase-shift design and channel modeling for focused beams in IRS-assisted FSO systems," IEEE Trans. Veh. Technol. **72**, 10971–10976 (2023).
23. J. Sipani, P. Sharda, and M. R. Bhatnagar, "Modeling and design of IRS-assisted FSO system under random misalignment," IEEE Photonics J. **15**(4), 1–13 (2023).

Optics EXPRESS

24. H. B. Wang, Z. C. Zhang, B. C. Zhu, *et al.*, "Performance analysis of multi-branch reconfigurable intelligent surfaces-assisted optical wireless communication system in environment with obstacles," IEEE Trans. Veh. Technol. **70**(10), 9986–10001 (2021).
25. R. P. Naik and W. Y. Chung, "Evaluation of reconfigurable intelligent surface-assisted underwater wireless optical communication system," J. Lightwave Technol. **40**(13), 4257–4267 (2022).
26. Q. Zhang, D. W. Yue, and X. Y. Xu, "Performance analysis of reconfigurable intelligent surface-assisted underwater wireless optical communication systems," IEEE Photonics J. **16**(4), 1–14 (2024).
27. Y. Ata, H. Abumarshoud, L. Bariah, *et al.*, "Intelligent reflecting surfaces for underwater visible light communications," IEEE Photonics J. **15**(1), 1–10 (2023).
28. Y. Ata, M. C. Gökçe, and Y. Baykal, "Intelligent reflecting surface aided vehicular optical wireless communication systems using higher-order mode in underwater channel," IEEE Trans. Veh. Technol. **73** 11196–11208 (2024).
29. R. Salam, A. Srivastava, V. A. Bohara, *et al.*, "An optical intelligent reflecting surface-assisted underwater wireless communication system," IEEE Open J. Commun. Soc. **4**, 1774–1786 (2023).
30. S. Kisseleff and S. Chatzinotas, "Trusted reconfigurable intelligent surface for multi-user quantum key distribution," IEEE Commun. Lett. **27**(8), 2237–2241 (2023).
31. N. K. Kundu, M. R. McKay, R. Murch, *et al.*, "Intelligent reflecting surface-assisted free space optical quantum communications," IEEE Trans. Wireless Commun. **23**(5), 5079–5093 (2024).
32. M. Chehimi, M. Elhattab, W. Saad, *et al.*, "Reconfigurable intelligent surface (RIS)-assisted entanglement distribution in FSO quantum networks," arXiv (2024).
33. S. Kisseleff, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces in challenging environments: Underwater, underground, industrial and disaster," IEEE Access **9**, 150214–150233 (2021).
34. Z. Wei, Z. Wei, J. Fang, *et al.*, "Impulse response modeling and dynamic analysis for SIMO UOWC systems enhanced by RIS-equipped UUV," IEEE Trans. Veh. Technol. **73**, 1540–1553 (2023).
35. B. Zhou, P. Wang, T. Cao, *et al.*, "Performance analysis of AUV-carried RISs-aided multihop UWOC convergent with RF MRC systems over WGG oceanic turbulence," Vehicular Commun. **45**, 100722 (2024).
36. A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," J. Lightwave Technol. **25**(7), 1702–1710 (2007).
37. H. Wang, Z. Zhang, B. Zhu, *et al.*, "Space division multiple access based on OIRS in multi-user FSO system," IEEE Trans. Veh. Technol. **71**(12), 13403–13408 (2022).
38. Y. Wang, H. Wang, and X. Jiang, "Performance of reconfigurable-intelligent-surface-assisted satellite quasi-stationary aircraft–terrestrial laser communication system," Drones **6**(12), 405 (2022).
39. F. Hanson and M. Lasher, "Effects of underwater turbulence on laser beam propagation and coupling into single-mode optical fiber," Appl. Opt. **49**(16), 3224–3230 (2010).
40. H. M. Oubei, E. Zedini, R. T. ElAfandy, *et al.*, "Simple statistical channel model for weak temperature-induced turbulence in underwater wireless optical communication systems," Opt. Lett. **42**(13), 2455–2458 (2017).
41. Z. Vali, A. Gholami, Z. Ghassemlooy, *et al.*, "Modeling turbulence in underwater wireless optical communications based on monte carlo simulation," J. Opt. Soc. Am. A **34**(7), 1187–1193 (2017).
42. E. Zedini, H. M. Oubei, A. Kammoun, *et al.*, "Unified statistical channel model for turbulence-induced fading in underwater wireless optical communication systems," IEEE Trans. Commun. **67**(4), 2893–2907 (2019).
43. M. Amer and Y. Al-Eryani, "Underwater optical communication system relayed by α-μ fading channel: outage, capacity and asymptotic analysis," arXiv (2019).
44. I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products* (Academic Press, 2014).
45. M. Razavi, "Multiple-access quantum key distribution networks," IEEE Trans. Commun. **60**(10), 3071–3079 (2012).
46. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**(5), 057901 (2003).
47. S. Pirandola, R. Laurenza, C. Ottaviani, *et al.*, "Fundamental limits of repeaterless quantum communications," Nat. Commun. **8**(1), 15043 (2017).
48. A. P. Prudnikov, I. A. Brychkov, J. A. Bryckov, *et al.*, *Integrals and Series: Special Functions* (CRC Press, 1986).