Performance analysis of decoy state quantum key distribution over underwater turbulence channels

Performance Analysis of Decoy State Quantum Key Distribution over Underwater Turbulence Channels

Amir Hossein Fahim Raouf, *Student Member, IEEE,*
Majid Safari, *Member, IEEE,* Murat Uysal, *Fellow, IEEE*

Abstract

Decoy state quantum key distribution protocols have been earlier studied for atmospheric, fiber and satellite links, however those results are not directly applicable to underwater environments with different channel characteristics. In this paper, we investigate the fundamental performance limits of decoy state BB84 protocol over turbulent underwater channels and provide a comprehensive performance characterization. We adopt a near field analysis to determine the average power transfer over turbulent underwater path and use this to obtain a lower bound on secret key rate. We quantify the performance of decoy BB84 protocol in different water types assuming various turbulence conditions. We further investigate the effect of system parameters such as transmit aperture size and detector field of view on the performance.

I. Introduction

Unlike classical cryptosystems which build upon the formulation of some intractable computational problems, quantum cryptography has the promise to enable unconditional data security [1]. The concept of quantum key distribution (QKD) has been introduced by Bennett and Brassard who propose the well-known BB84 protocol [2]. QKD has been so far successfully applied to fiber optic, atmospheric and satellite links [3]–[5]. Another potential application domain for QKD is underwater sensor networks (USNs). The increasing deployment of USNs for underwater applications with sensitive data such as surveillance of critical infrastructure such as harbor, port, pipelines and maritime border protection have sparked interest in underwater QKD [6]–[15].

Monte Carlo simulations were conducted in [6] to demonstrate that the polarization of scattered photons was preserved in underwater environments. The maximum secure communication distance for BB84 protocol to achieve a targeted level of quantum bit error rate (QBER) was derived in [7], [8] using the Beer-Lambert path loss model. The effect of underwater turbulence on QBER and the maximum achievable distance were further investigated in [9] based on a near field analysis. In addition to these theoretical and simulation results, some experimental demonstrations of BB84 QKD protocol were further conducted in [10]–[13]. The performance of other QKD protocols based on entanglement [14] and continuous-variable approaches [15] were further investigated in underwater environments.

The discrete-variable QKD protocols such as the BB84 build upon the assumption of the availability of a single photon source. However, in practice, attenuated laser sources are used instead which occasionally emit more than one photon. This opens up the possibility of sophisticated eavesdropping attacks such as photon number splitting attack, where an adversary stops all single-photon signals and splits multi-photon signals, keeping one copy herself and resending the rest to the legitimate receiver. The decoy method [16] can be employed to combat such attacks. In this method, the transmitter employs multiple intensity levels, i.e., one signal state and several decoy states which result in varying photon number statistics throughout the channel. The main idea behind decoy protocols is that the transmitter sends the decoy state pulse sequence (which contains no useful information) accompanying the single photon pulse sequence. Since the adversary cannot distinguish whether a photon state is from a signal or a decoy, its attempts on photon number splitting attack leads to a variation on the expected yield of signal and decoy states. As a result, the presence of photon-number-dependent loss in the quantum channel can be detected.

The decoy QKD protocols were earlier studied for atmospheric, fiber and satellite links [17]–[19], however those results are not directly applicable to underwater environments with different channel characteristics. There have been only some sporadic efforts on investigating the performance of underwater decoy state BB84 QKD [20]–[24]. Specifically, in [20], an underwater quantum channel model was developed based on Monte Carlo simulations and some preliminary analysis on QBER and secret key rate (SKR) were presented. In [21], Li *et al.* considered the use of decoy state BB84 QKD system for air-to-underwater transmission. In addition to the theoretically analyzing the impact of fluctuating sea surface, they implemented a controlled lab experiment for a distance of 0.5 m and achieved an SKR of approximately 6.82 b/s with an error

rate of 3.74%. Another experiment [22] was conducted in a 10 m water tank with extinction coefficient of 0.08 m^{-1} and reported a SKR of 711.29 kb/s by employing two decoy-state BB84 QKD. In [23], the key generation rate for decoy state BB84 QKD over an underwater channel of 30 m was studied and reported an average QBER of 2.48% where the average sifted and final key rate are 427.3 b/s and 220.5 b/s, respectively.

The effect of underwater turbulence on decoy QKD was only addressed in [24] where Hufnagel *et al.* conducted the experiments in a 30.5 meter flume tank. The QBER and SKR were measured for link distances of 0.5, 10.5, 20.5, and 30.5 meters and the maximum distance for secure communication was predicted as 80 m for the QKD system under consideration. As the above literature survey points out, there is not yet a comprehensive analytical study to demonstrate the effect of turbulence on decoy state BB84 protocol. To address this gap, we investigate the fundamental performance limits of decoy state BB84 protocol over turbulent underwater channels and provide a comprehensive performance characterization. As path loss model, we consider a modified version of Beer-Lambert formula, which takes into account the effect of scattering. Based on the near field analysis [25], we utilize the wave structure function to determine the average power transfer over turbulent underwater path and use this to obtain a lower bound on SKR. Based on this bound, we present the performance of decoy BB84 protocol in different water types. We further investigate the effect of system parameters such as transmit aperture size and detector field of view (FOV) on the performance.

The remainder of this paper is organized as follows. In Section II, we describe the system model under consideration. In Section III, we derive a lower bound on SKR for decoy BB84 protocol in the presence of turbulence. In Section IV, we present numerical results and finally, we conclude in Section V.

II. System Model

Fig. 1 illustrates a schematic diagram of a decoy state BB84 QKD system under consideration. The system is built upon BB84 protocol with two decoy states[1] (i.e., vacuum and weak decoy state) which aims to create a secret key between the authorized parties (Alice and Bob) such that eavesdropper (Eve) fails to acquire meaningful information.

[1]It is shown in [26] that two decoy states are sufficient for practical use and provides almost the same capability to detect an eavesdropper with an infinite number of decoy states.

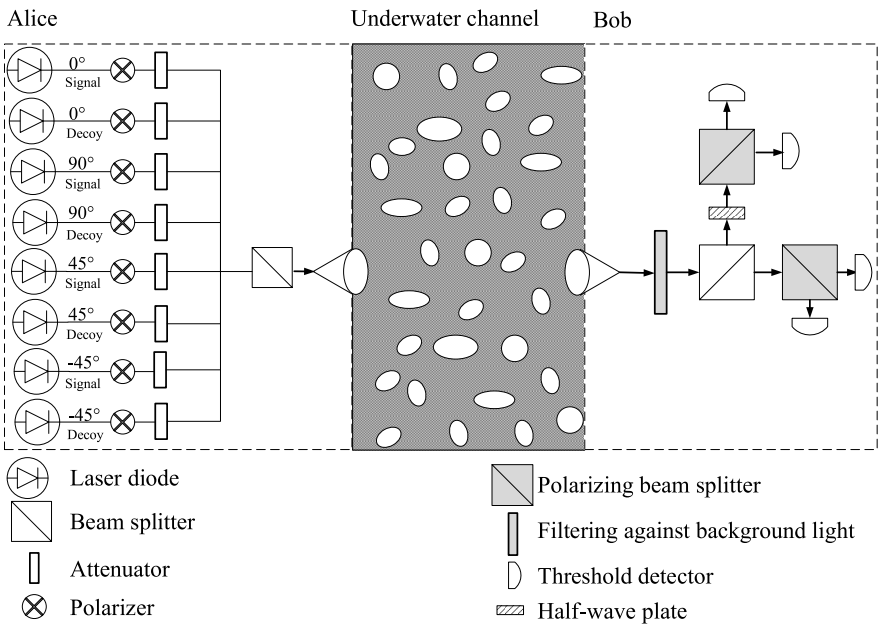


Fig. 1: Underwater decoy BB84 QKD system under consideration

In this protocol, Alice prepares a qubit by choosing the intensity and the basis to encode her bit. She randomly selects from three possible intensities, namely, vacuum state, weak decoy, and signal state. The photon number of each pulse follows a Poisson distribution with the expected photon number of μ for signal and v ($v < \mu$) for weak decoy. In the vacuum decoy state, Alice switches off her photon source. In the other two states (i.e., weak decoy and signal state), the basis is chosen randomly between two linear polarization bases namely rectilinear (denoted by $\oplus$) or diagonal (denoted by $\otimes$) for every bit she wants to send. She selects a random bit value "0" or "1" and uses polarization encoding of photons where polarization of $0^{\circ}/-45^{\circ}$ represents 0 and polarization of $+90^{\circ}/+45^{\circ}$ represents 1.

A threshold detector at Bob's side enables him to differentiate between vacuum and non-vacuum states [26]. Bob further measures the arriving photon randomly in either $\oplus$ or $\otimes$ bases. Through the public channel, Bob announces the basis used to measure each qubit. Alice responds by announcing which bases are correct along with the state information for each pulse, i.e., signal, decoy, or vacuum. Alice and Bob perform sifting process on both the signal and decoy state qubits for the matched bases. Alice announces the encoded bit values of the sifted decoy state qubits to Bob through an authenticated public channel. This information will be used later for analyzing the statistical characteristics (e.g., the gain and QBER) and to determine possible Eve's

attack which will inevitably alter these statistics. Alice and Bob perform error correction for the sifted signal state qubits. Based on these sifted qubits, a shared one-time pad key is created to use for secure communication [27].

Alice uses a weak coherent state laser source with a circular exit pupil and a diameter of d_1 as the transmitter. Bob collects the light received from Alice with a diameter of d_2 in the $z = l$ plane. The effects of diffraction, turbulence, and attenuation loss lead to a reduction in Bob's collected photons. In addition, Bob's receiver will collect n_B background photons per polarization on average, and each of his detectors will be subject to an average equivalent dark current photon number of n_D. By considering the dark current and irradiance of the environment, the total average number of noise photons reaching all four Bob's detector can be expressed [25], [28]

$$Y_0 = 4\left(n_B/2 + n_D\right) = 4I_{dc}\Delta t + \frac{\pi R_d A \Delta t' \lambda \Delta\lambda \left(1 - \cos\left(\Omega\right)\right)}{h_p c_{light}} \tag{1}$$

where I_{dc} is the dark current, A is the receiver aperture area, Ω is the field of view of the detector, h_p is Planck's constant, c_{light} is the speed of light, R_d is the irradiance of the environment, $\Delta\lambda$ is the filter spectral width, Δt is the bit period and $\Delta t'$ is the receiver gate time. It is convenient to write the depth dependence of $R_d\left(\lambda, z_d\right)$ as

$$R_d\left(\lambda, z_d\right) = R_d\left(\lambda, 0\right)\exp\left(-K_\infty z_d\right) \tag{2}$$

where K_∞ is the asymptotic value of the spectral diffuse attenuation coefficient for spectral downwelling plane irradiance [29].

III. Performance Analysis

The attenuated laser source generates a pulse having a finite probability of multiple photons described by the Poisson distribution. The probability for a pulse containing i photons is given by $\Pr_i^\mu = \mu\exp\left(-\mu\right)/i!$ where μ denotes the average photon number per pulse. The yield of an i-photon pulse (denoted by Y_i) represents the probability that Bob detects conclusively an i-photon pulse sent by Alice. Let η denote the received fraction of transmitted photons. Assuming independent behavior of travelling between the i photons in an i-photon pulse, the transmittance and yield of the i-photon pulse are given by [26] $\eta_i = 1-\left(1-\eta\right)^i$ and $Y_i \cong Y_0 + \eta_i$, respectively. The gain of an i-photon pulse is defined as the product of probability of emitting an i-photon

pulse and Y_i represents a weighted average of all detected photons including the vacuum pulses, i.e., $i = 0$ [30]. Thus, the overall gains for signal and weak decoy state are respectively given as [26]

$$\begin{aligned} Q_\mu &= \sum_{i=0}^{\infty} Q_i^\mu = \sum_{i=0}^{\infty} \left(Y_0 + 1 - (1-\eta)^i\right) \frac{\mu^i}{i!} \exp\left[-\mu\right] \\ &= Y_0 + 1 - \exp\left[-\eta\mu\right] \end{aligned} \tag{3}$$

$$\begin{aligned} Q_v &= \sum_{i=0}^{\infty} Q_i^v = \sum_{i=0}^{\infty} \left(Y_0 + 1 - (1-\eta)^i\right) \frac{v^i}{i!} \exp\left[-v\right] \\ &= Y_0 + 1 - \exp\left[-\eta v\right] \end{aligned} \tag{4}$$

Furthermore, let $f\left(x\right)$ and $H_2\left(x\right)$ denote respectively the bidirectional error correction efficiency, and the binary Shannon information function. The latter is defined as $H_2\left(x\right) = -x\log_2\left(x\right) - \left(1-x\right)\log_2\left(1-x\right)$. A lower bound on the SKR for BB84 protocol with two decoy states is then obtained as (see Appendix for main derivation steps summarized from [31])

$$\begin{aligned} R &\geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1^\mu\left[1 - H_2\left(e_1\right)\right]\right\} \\ &\geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1^{L,\nu,0}\left[1 - H_2\left(e_1^{U,\nu,0}\right)\right]\right\} \end{aligned} \tag{5}$$

where $q = 1/2$ is the basis reconciliation factor, $Q_1^{L,v,0}$ is the lower bound on the gain of single photon state, E_μ is the overall QBER, and $e_1^{U,v,0}$ is the upper bound on error rate of single photon state. In (5), $Q_1^{L,v,0}$, and $e_1^{U,v,0}$ are respectively given by [26]

$$Q_1^{L,v,0} = \frac{\mu^2 \exp\left[-\mu\right]}{\mu\nu - \nu^2}\left(Q_\nu \exp\left[v\right] - Q_\mu \frac{\nu^2}{\mu^2} \exp\left[\mu\right] - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{6}$$

$$e_1^{U,\nu,0} = \frac{E_\nu Q_\nu \exp\left[v\right] - e_0 Y_0}{Y_1^{L,\nu,0}\nu} \tag{7}$$

where the lower bound on the yield of single photon state (i.e., $Y_1^{L,\nu,0}$) can be expressed as [26]

$$Y_1^{L,v,0} = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu \exp\left[v\right] - Q_\mu \frac{\nu^2}{\mu^2} \exp\left[\mu\right] - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{8}$$

The overall QBER can be then expressed as [26]

$$E_\mu = \frac{\sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} \exp\left[-\mu\right]}{Q_\mu} = \frac{e_0 Y_0 + e_{\text{det}} \left(1 - \exp\left[-\eta\mu\right]\right)}{Q_\mu} \tag{9}$$

where e_i is the error rate of i-photon pulse and is given by [26] $e_i = (e_0 Y_0 + e_{\text{det}}\eta_i)/Y_i$. Here, e_{det} denotes the probability that a photon hits the erroneous detector and under the assumption of random background noise $e_0 = 0.5$ is the error rate of noise [26]. We assume e_{det} is constant and independent of the link distance [26].

Calculation of SKR depends on the operation environment through its dependence on η. To find the performance bounds for the decoy state BB84 QKD, it is required to find the fraction of received photons taking into account the effect of path loss and turbulence experienced in underwater channels which will be discussed in the following. For collimated light sources, the geometrical loss is negligible; therefore, the path loss for a laser diode transmitter only depends on the attenuation loss including the effects of absorption and scattering. Let $h\left(l\right)$ denote the deterministic path loss. Furthermore, let $0 \leq \widehat{\alpha} \leq 1$ denote the so-called "power transfer" term [9], [25] which defines the probability of transmitted photon being reliably received in the presence of turbulence. Therefore, we can write the received fraction of transmitted photons as $\eta = h\left(l\right)\widehat{\alpha}\eta_{\text{Bob}}$ where η_{Bob} is the receiver efficiency, i.e., including the internal transmittance of optical components and detector efficiency [26].

Based on the modified version of Beer-Lambert formula [32], the underwater path loss can be expressed as

$$h\left(l\right) = \exp\left[-\varsigma l\left(\frac{d_2}{\theta l}\right)^T\right] \tag{10}$$

where ς is extinction coefficient, l is transmission distance, θ is the full-width transmitter beam divergence angle and T is a correction coefficient based on water type [32]. Extinction coefficient depends on the wavelength and water type. Typical values of extinction coefficients for $\lambda = 532$ nm (green color) in different water types can be found in [33].

Finding a statistical description of $\widehat{\alpha}$ and, therefore η, is a formidable task and a closed-form expression is not available in the literature for near field propagation. As an alternative, a lower bound on the average power transfer can be expressed as [25]

$$\mathrm{E}\left(\widehat{\alpha}\right)=\int\widehat{\alpha}P\left(\widehat{\alpha}\right)d\widehat{\alpha}\geq\alpha=\frac{8\sqrt{F}}{\pi}\int_{0}^{1}\exp[-W\left(dx,l\right)/2]\left(\cos^{-1}\left(x\right)-x\sqrt{1-x^{2}}\right)J_{1}\left(4x\sqrt{F}\right)dx \tag{11}$$

where $P\left(\widehat{\alpha}\right)$ is the probability density function (pdf) of $\widehat{\alpha}$, $J_1(\cdot)$ is the first-order Bessel function of the first kind and F is the Fresnel number product of transmit and receive diameters given by $F=\left(\pi d^2/4\lambda l\right)^2$. In (11), $W(\cdot,\cdot)$ is the underwater wave structure function. For a given transmission distance of l and given separation distance between two points on the phase front transverse to the axis of propagation (denoted by ρ), it is expressed as [9]

$$W\left(\rho,l\right)=1.44\pi k^{2}l\left(\frac{\alpha_{\mathrm{th}}^{2}\chi}{\omega^{2}}\right)\varepsilon^{-\frac{1}{3}}\left(1.175\eta_{K}^{2/3}\rho+0.419\rho^{\frac{5}{3}}\right)\left(\omega^{2}+d_{r}-\omega\left(d_{r}+1\right)\right) \tag{12}$$

where $k=2\pi/\lambda$ is the wave number, ω is the relative strength of temperature and salinity fluctuations, ε is the dissipation rate of turbulent kinetic energy per unit mass of fluid, α_{th} is the thermal expansion coefficient, χ is the dissipation rate of mean-squared temperature and d_r is the eddy diffusivity ratio. In (12), η_K is Kolmogorov microscale length and given by $\eta_K=\left(\upsilon^3/\varepsilon\right)^{1/4}$ with υ referring to the kinematic viscosity.

The negative exponential function $\exp\left[-x\right]$ in (3) and (4) is a convex function with negative derivative. By inserting $\eta=h\left(l\right)\widehat{\alpha}\eta_{\mathrm{Bob}}$ therein, averaging the right hand side of (3) and (4) over $\widehat{\alpha}$ and utilizing Jensen's inequality, we can express the lower bound on the Q_v and Q_μ respectively as

$$\begin{aligned}\mathrm{E}\left\{Q_{\nu}\right\}&=Y_{0}+1-\int_{0}^{1}\exp\left[-\nu\eta_{Bob}h\left(l\right)\widehat{\alpha}\right]P\left(\widehat{\alpha}\right)d\widehat{\alpha}\\&\geq Y_{0}+1-\left(\int_{0}^{1}\left(1-\widehat{\alpha}+\widehat{\alpha}\exp\left[-\nu\eta_{\mathrm{Bob}}h\left(l\right)\right]\right)P\left(\widehat{\alpha}\right)d\widehat{\alpha}\right)\\&=Y_{0}+1-\left(1-E\left(\widehat{\alpha}\right)+E\left(\widehat{\alpha}\right)\exp\left[-\nu\eta_{\mathrm{Bob}}h\left(l\right)\right]\right)\\&\geq Q_{\nu}^{L}\triangleq Y_{0}+\alpha-\alpha\exp\left[-\nu\eta_{\mathrm{Bob}}h\left(l\right)\right]\end{aligned} \tag{13}$$

$$\mathrm{E}\left\{Q_{\mu}\right\}\geq Q_{\mu}^{L}\triangleq Y_{0}+\alpha-\alpha\exp\left[-\mu\eta_{\mathrm{Bob}}h\left(l\right)\right] \tag{14}$$

Ignoring the effects of diffraction and turbulence (i.e., $\widehat{\alpha}=1$), we can obtain an upper bound on Q_μ as

$$Q_{\mu}|_{\widehat{\alpha}=1} = Q_{\mu}^{U} \triangleq Y_0 + 1 - \exp\left[-\mu\eta_{\text{Bob}} h\left(l\right)\right] \tag{15}$$

Therefore, the upper bound on the overall QBER can be expressed as

$$E_{\mu}^{U} \triangleq \frac{e_0 Y_0 + e_{\text{det}}\left(1 - \exp\left[-\mu\eta_{\text{Bob}} h\left(l\right)\right]\right)}{Q_{\mu}^{L}} \tag{16}$$

Employing (13), (14), (15), and (16), we can write the lower bounds on $Y_1^{L,v,0}$ and $Q_1^{L,v,0}$, and the upper bound on $e_1^{U,v,0}$ respectively as

$$Y_1^{L,\nu,0} \geq Y_1^{L} \triangleq \frac{\mu}{\mu\nu - \nu^2}\left(Q_{\nu}^{L}\exp\left[v\right] - Q_{\mu}^{U}\frac{\nu^2}{\mu^2}\exp\left[\mu\right] - \frac{\mu^2 - \nu^2}{\mu^2}Y_0\right) \tag{17}$$

$$Q_1^{L,\nu,0} \geq Q_1^{L} \triangleq \frac{\mu^2\exp\left[-\mu\right]}{\mu\nu - \nu^2}\left(Q_{\nu}^{L}\exp\left[v\right] - Q_{\mu}^{U}\frac{\nu^2}{\mu^2}\exp\left[\mu\right] - \frac{\mu^2 - \nu^2}{\mu^2}Y_0\right) \tag{18}$$

$$e_1^{U,\nu,0} \leq e_1^{U} \triangleq \frac{\left(e_0 Y_0 + e_{\text{det}}\left(1 - \exp\left[-v\eta_{\text{det}} h\left(l\right)\right]\right)\right)\exp\left[v\right] - e_0 Y_0}{Y_1^{L}\nu} \tag{19}$$

Thus, we obtain the final expression for the lower bound on SKR as

$$R^{L} = q\left\{-Q_{\mu}^{U} f\left(E_{\mu}^{U}\right) H_2\left(E_{\mu}^{U}\right) + Q_1^{L}\left[1 - H_2\left(e_1^{U}\right)\right]\right\} \tag{20}$$

Special case: As a benchmark, we consider a QKD system which uses classical BB84 protocol for key distribution. By considering an *"ideal"* single-photon transmitter, the gain of the signal states will be equal to the gain of single photon state (i.e., $Q_{\mu} = Q_1^{\mu} = \left(Y_0 + \eta\right)\mu\exp\left[-\mu\right]$) and the overall QBER will reduce to $E_{\mu} = e_1$. By substituting these parameters in (5) and after some simple mathematical manipulations, we obtain the lower bound on the SKR as

$$R \geq R_{\text{BB84}}^{L} \triangleq \frac{Q_1}{2}\left\{1 - H_2\left(e_1\right)\left[1 + f\left(e_1\right)\right]\right\} \tag{21}$$

which coincides with Eq. (45) of [34] when the probability of multi photon emission is 0 (denoted as p_m in [34]). In (21), the first term (i.e., $Q_1/2$) indicates the probability of sift and the second term (see Eq. (3) in [35]) is due to the error correction process for removing the residual information that Eve might have. Substituting $i = 1$ in (9), the QBER for the ideal single photon transmitter can be expressed as

TABLE I: System and channel parameters

Parameter	Definition		Numerical Value
μ	Expected photon number for signal		0.48 [26]
v	Expected photon number for decoy state		0.05 [26]
η_{Bob}	Transmittance in Bob's side		0.045 [26]
e_{det}	System error		3.3% [26]
Ω	Field of view		180° [32]
$\Delta\lambda$	Filter spectral width		30 nm [28]
λ	Wavelength		530 nm [32]
Δt	Bit period		35 ns [28]
$\Delta t'$	Receiver gate time		200 ps [28]
d_1	Transmitter aperture diameter		5 cm [25]
d_2	Receiver aperture diameter		5 cm [25]
I_{dc}	Dark current count rate		60 Hz [28]
K_∞	Asymptotic diffuse attenuation coefficient		0.08 m^{-1} [29]
z_d	Depth		100 m [28]
θ	Transmitter beam divergence angle		6° [32]
ς	Extinction coefficient	Clear water	0.151 m^{-1} [33]
		Coastal water	0.339 m^{-1} [33]
T	Correction coefficient	$\theta = 6^\circ,\ d_1 = 5\,\text{cm}$	0.13 [32]
		$\theta = 6^\circ,\ d_1 = 10\,\text{cm}$	0.16 [32]
		$\theta = 6^\circ,\ d_1 = 20\,\text{cm}$	0.21 [32]
		$\theta = 6^\circ,\ d_1 = 30\,\text{cm}$	0.26 [32]

$$E_\mu = \frac{e_1 Y_1}{Y_0 + \eta} = \frac{e_0 Y_0 + e_{\text{det}}\eta}{Y_0 + \eta} \tag{22}$$

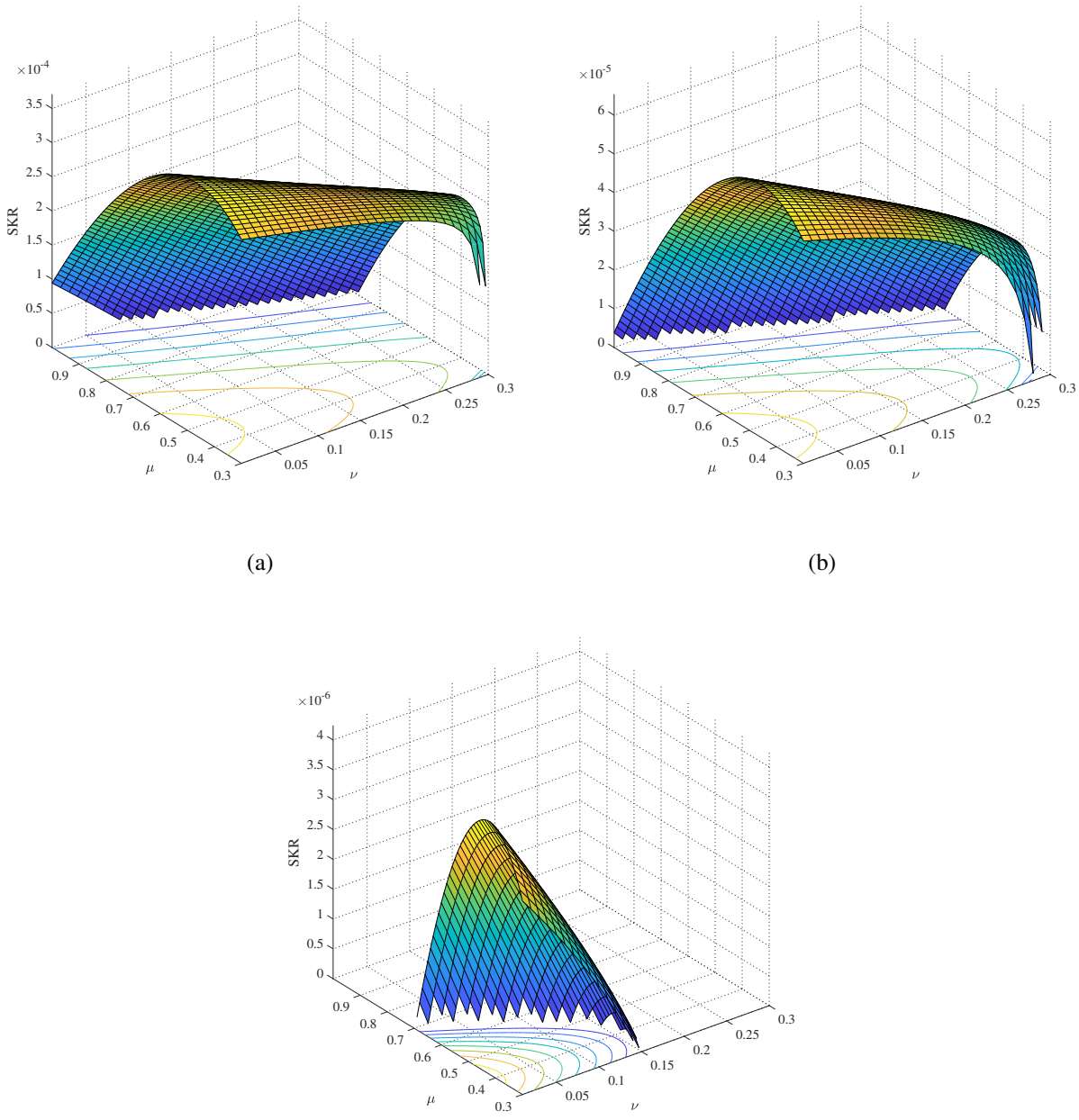
Substituting $Y_0 = 4\left(n_B/2 + n_D\right)$ and $e_0 = 0.5$ into (22), and for $e_{\text{det}} = 0$ (i.e., ignoring system error) and $\eta_{\text{Bob}} = 1$ (i.e., no transmittance in Bob's detector), (22) reduces to

$$E_\mu = \frac{n_B/2 + n_D}{h\left(l\right)\widehat{\alpha}/2 + n_B + 2n_D} \tag{23}$$

which coincides with Eq. (17) of [36] which is the QBER for classical BB84 protocol.

IV. Numerical Results

In this section, we demonstrate the performance of underwater QKD scheme under consideration. We assume the transmitter beam divergence angle of $\theta = 6^\circ$, the system error of $e_{\text{det}} = 3.3\%$, the dark current count rate of $I_{dc} = 60$ Hz, filter spectral width of $\Delta\lambda = 30$ nm, bit period of $\Delta t = 35$ ns, receiver gate time of $\Delta t' = 200$ ps, and the transmittance in Bob's side of $\eta_{Bob} = 0.045$. In this paper, we assume the error correction efficiency of $f\left(E_\mu\right) = 1.22$ regardless of the error rate [26]. Unless otherwise stated, we assume the transmitter and receiver aperture



(a) (b)

(c)

Fig. 2: Effect of expected photon number for signal and decoy state on SKR over clear ocean with weak turbulence conditions for **(a)** l = 20 m **(b)** l = 40 m and **(c)** l = 60 m

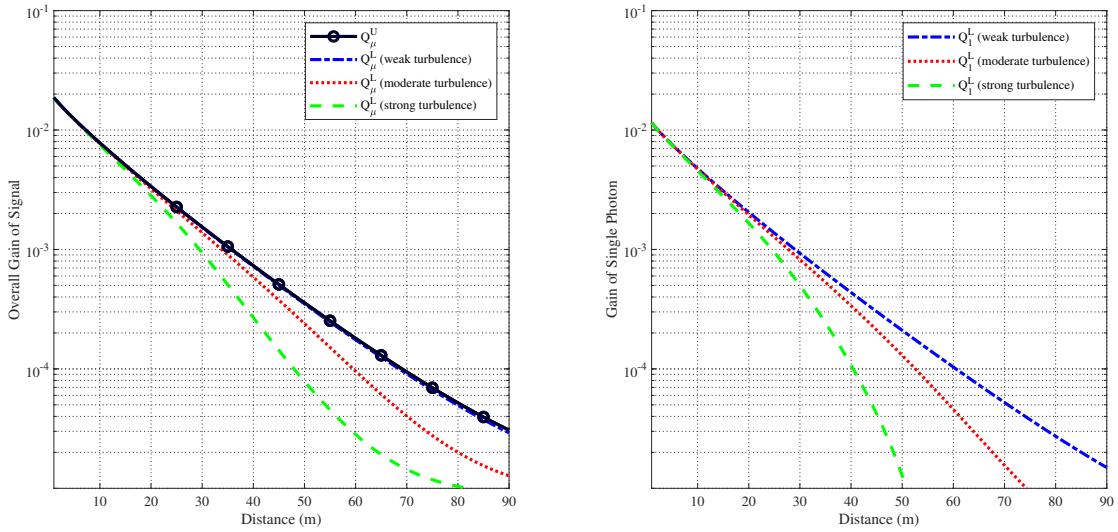
diameters of $d_1 = d_2 = 5$ cm, FOV of $\Omega = 180^{\circ}$, clear atmospheric conditions at night with a full moon, i.e., $R_d(\lambda, 0) = 10^{-3}\,\mathrm{W/m^2}$ [37], and the expected photon number of $\mu = 0.48$ and $v = 0.05$ for signal and weak decoy state, respectively. As for channel parameters, we assume $\alpha_{th} = 2.56 \times 10^{-4}$ 1/deg, and $\upsilon = 1.0576 \times 10^{-6}\ \mathrm{m^2 s^{-1}}$ [38]. We consider three representative cases for turbulence strength. Specifically, we assume $\omega = -2.2$, $\chi_T = 2 \times 10^{-7}\ \mathrm{K^2 s^{-3}}$ and $\varepsilon = 2 \times 10^{-5}\ \mathrm{m^2 s^{-3}}$ for weak turbulence, $\omega = -2.2$, $\chi_T = 10^{-6}\ \mathrm{K^2 s^{-3}}$ and $\varepsilon = 5 \times 10^{-7}\ \mathrm{m^2 s^{-3}}$ for moderate turbulence and $\omega = -2.2$, $\chi_T = 10^{-5}\ \mathrm{K^2 s^{-3}}$ and $\varepsilon = 10^{-5}\ \mathrm{m^2 s^{-3}}$ [39]. For the convenience of the reader, the channel and system parameters are summarized in Table I.

In Fig. 2, we investigate the effect of expected photon number for signal and decoy states. We assume clear ocean with weak turbulence and consider three distinctive link distances; i.e., l = 20, 40, and 60 m. We assume the expected photon numbers for signal and decoy state vary respectively as $0.3 < \mu \leq 1$ and $0 < v \leq 0.3$. It is observed that choosing the proper values for the expected photon number of signal and decoy becomes critical as the link distance increases. For example, the QKD system with $\mu > 0.68$ and $v > 0.16$ fails to provide a non-zero SKR at link distance of l = 60 m (see Fig. 2c). These observations indicate the dependency of optimal values for such parameters on the link distance.

Fig. 3 presents the overall gain of signal state, i.e., (14) and (15), and the gain of single photon state, i.e., (18), over clear ocean with weak, moderate, and strong turbulence conditions. The upper bound on the overall gain of signal state is calculated by ignoring the effects of diffraction and turbulence and is identical regardless of turbulence conditions. As it can be observed from Fig. 3a, the upper bound and lower bound on the overall gain of signal for weak turbulence behave almost the same. As the link distance and turbulence strength increase, the difference between upper and lower bounds on the overall gain of signal becomes more noticeable. It can be further observed from Fig. 3b that the effect of turbulence on the lower bound of single photon gain is more significant compared to the overall gain of signal.

In Fig. 4, we present the lower bound on SKR for decoy BB84 protocol and compare it with the classical BB84 protocol. Note that we consider an ideal single photon transmitter for BB84 protocol, whereas this condition cannot be met in practice. As the water type, we assume clear ocean and non-turbulent conditions. As expected, there is significant difference between the achievable distances for these two protocols. The achievable distance to obtain non-zero SKR for BB84 protocol is around 87 m while it decreases to 65 m for the decoy scheme.

In Fig. 5, we investigate the effect of turbulence on the performance of decoy BB84 protocol.



(a) (b)

Fig. 3: **(a)** The upper bound and lower bound on the overall gain of signal and **(b)** The lower bound on the single photon gain for clear ocean with weak, moderate, and strong turbulence conditions.

We consider clear ocean, and coastal water. For each water type, we assume weak, moderate and strong turbulence. The lower bound on SKR for non-turbulent case is also included as a benchmark. It can be observed from Fig. 5 that the turbulence effect in coastal water is small and the path loss is the dominant factor. The achievable distance to obtain non-zero SKR in coastal water with weak turbulence conditions is around 25 m which is the same as non-turbulent case. The achievable distance reduces to 23 m and 19 m for moderate and strong turbulence conditions, respectively. As turbidity decreases, the achievable distance increases and the effect of turbulence is more pronounced. While the achievable distance to maintain positive SKR for clear ocean and non-turbulent conditions is around 65 m, it decreases to 62 m for weak turbulence conditions. The achievable distance reduces to 39 m and 23 m for moderate and strong turbulence, respectively.

In Fig. 6, we study the effect of aperture size on the performance of decoy BB84 protocol. We assume clear ocean with weak turbulence at night time with a full moon. We assume receiver aperture sizes of $d_2 = 5$ cm, 10 cm and 20 cm and the transmitter pupil has the same diameter as the receiver. It is observed that the achievable distance increases as the diameter size increases. For example, the achievable distance for $d_2 = 5$ cm is around 62 m, while it climbs up to 66

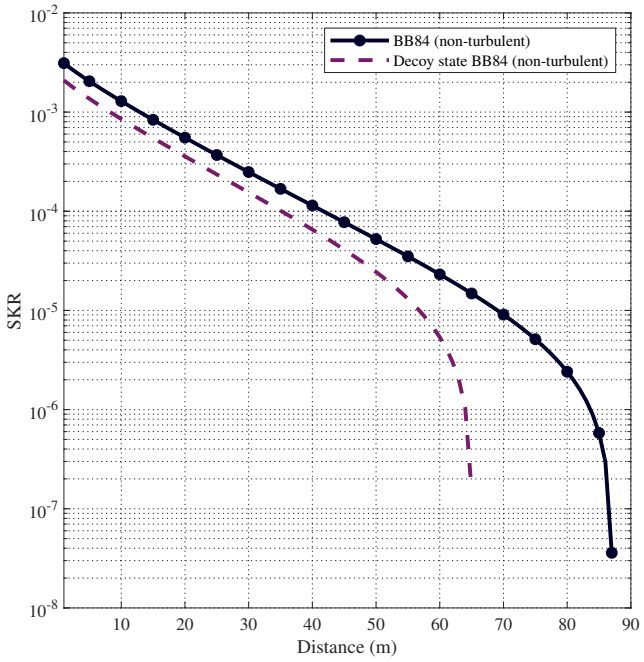


Fig. 4: SKR of the QKD system over clear ocean for BB84 and decoy BB84 protocols.

m and 71 m for $d_2 = 10$ cm and 20 cm, respectively. It should be emphasized that the increase in background noise as a result of increasing the diameter size is negligible at night, however, larger diameter results in an increase of collected photons coming from Alice.

In Fig. 7, we investigate the effect of FOV on the performance of decoy BB84 protocol. We assume clear ocean with weak turbulence and consider two atmospheric cases. These are clear weather night with a full moon and heavy overcast when sun is near the horizon. We assume Ω = $10°$, $60°$ and $180°$. It is observed that at night time, the effect of FOV is practically negligible and the SKR remains the same for all FOV values under consideration. Benefit of choosing a proper value of FOV becomes clear as the environment irradiance increases. In daylight, we observe that the achievable distance significantly improves as the FOV decreases. This improvement is due to the decrease in background noise as the FOV decreases. Mathematically speaking, the achievable distance for Ω = $180°$ is around 7 m, while it increases to 23 m and 56 m for $\Omega = 60°$ and $180°$, respectively.

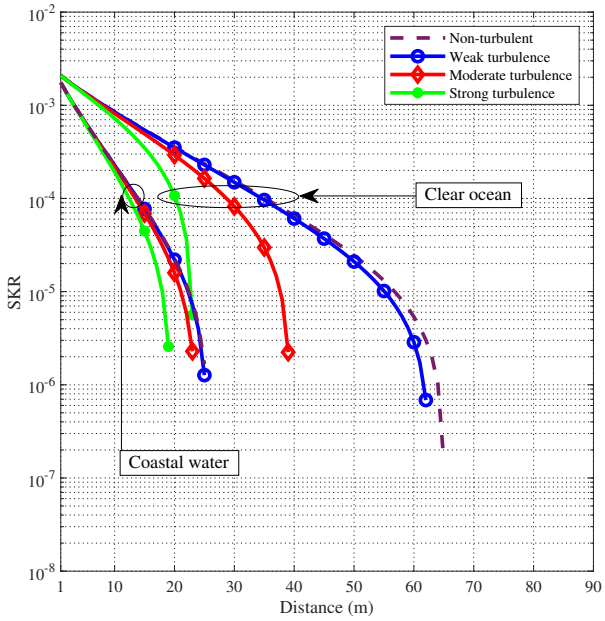


Fig. 5: SKR of the QKD system over clear ocean and coastal water for non-turbulent, weak, moderate, and strong turbulence conditions.

V. Conclusions

The classical BB84 protocol builds upon the assumption of the availability of a single photon source. However, in practice, attenuated laser sources are used instead which occasionally emit more than one photon. Decoy state BB84 protocol has been proposed to combat photon number splitting attacks and widely used in practice. In this paper, we have investigated the performance of the decoy state BB84 protocol over underwater channels. Our results have demonstrated that there is a significant difference between the achievable distances for *ideal* BB84 and decoy BB84 protocol. We have investigated the effect of expected photon number for signal and decoy states and demonstrated the dependency of optimal values for such parameters on the link distance. Our analysis has further revealed that turbulence effect becomes more pronounced as the water turbidity decreases. We have also investigated the effect of system parameters such as aperture size and FOV on SKR performance. At night time when the background noise is limited, the achievable distance increases as the diameter size increases. The effect of FOV has been found to be practically negligible at night time, and the performance remains the same for all FOV values under consideration. In daylight, the achievable distance significantly improves as the

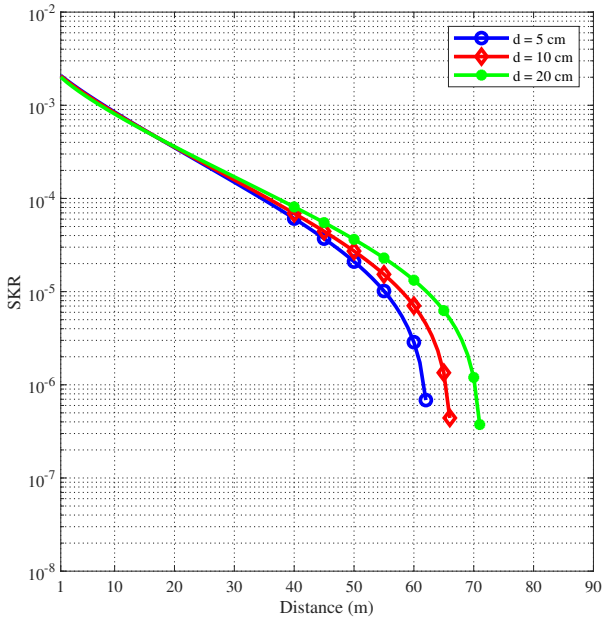


Fig. 6: SKR of the QKD system over clear ocean with weak turbulence conditions for different diameter size.

FOV decreases as a result of reduced background noise.

Disclosures. The authors declare no conflicts of interest.

Data availability. No data were generated or analyzed in the presented research.

APPENDIX

APPENDIX

In standard BB84 protocol, only signals generated from single photon pulse are guaranteed to be secure. From Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [40] argument, the secret SKR can be expressed as

$$R \geq Q_{\mu}\left\{-H_2\left(E_{\mu}\right)+\Omega_1\left[1-H_2\left(e_1\right)\right]\right\} \tag{A1}$$

where Ω_1 and e_1 are respectively the fraction and QBER of detection events from single-photon signals. The fraction of Bob's detection events from single-photon signals emitted by Alice is given by $\Omega_1 = Q_1/Q_{\mu}$ where Q_1 denotes the gain for the single photon state. The derivation of

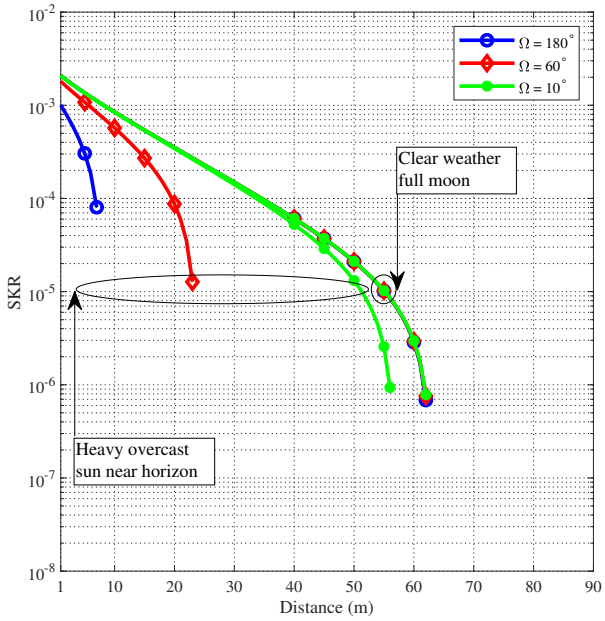


Fig. 7: SKR of the QKD system over clear ocean with weak turbulence conditions for different FOV.

(A1) assumes that error correction protocols can achieve the Shannon limit. However, practical error correction protocols are generally inefficient. Introducing $f(\mathrm{QBER})$ as the error correction efficiency and substituting $\Omega_1 = Q_1/Q_\mu$ in (A1), the SKR can be expressed as

$$R \geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\} \tag{A2}$$

where $q = 1/2$ for the BB84 protocol as a result of sifting process. By substituting the lower bound on the gain of single photon state and the upper bound on error rate of single photon state in (A2), a lower bound on the SKR for decoy state BB84 can be calculated as

$$R \geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1^{L,\nu,0}\left[1 - H_2\left(e_1^{U,\nu,0}\right)\right]\right\} \tag{A3}$$

REFERENCES

[1] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, 1984)*, 1984, pp. 175–179.

[3] C. Gobby, a. Yuan, and A. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Applied Physics Letters*, vol. 84, no. 19, pp. 3762–3764, 2004.

[4] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New journal of physics*, vol. 4, no. 1, p. 43, 2002.

[5] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[6] P. Shi, S.-C. Zhao, Y.-J. Gu, and W.-D. Li, "Channel analysis for single photon underwater free space quantum key distribution," *JOSA A*, vol. 32, no. 3, pp. 349–356, 2015.

[7] S.-C. Zhao, X.-H. Han, Y. Xiao, Y. Shen, Y.-J. Gu, and W.-D. Li, "Performance of underwater quantum key distribution with polarization encoding," *JOSA A*, vol. 36, no. 5, pp. 883–892, 2019.

[8] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE Journal of Oceanic Engineering*, vol. 45, no. 3, pp. 1138–1147, 2019.

[9] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *JOSA B*, vol. 37, no. 2, pp. 564–573, 2020.

[10] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," *Quantum*, vol. 2, p. 111, 2018.

[11] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang *et al.*, "Experimental investigation of quantum key distribution over a water channel," *Applied optics*, vol. 58, no. 14, pp. 3902–3907, 2019.

[12] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-Q. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang *et al.*, "Transmission of photonic polarization states through 55-m water: Towards air-to-sea quantum communication," *Photonics Research*, vol. 7, no. 8, pp. A40–A44, 2019.

[13] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs *et al.*, "Characterization of an underwater channel for quantum communications in the Ottawa river," *Optics express*, vol. 27, no. 19, pp. 26 346–26 354, 2019.

[14] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Optics express*, vol. 27, no. 3, pp. 3055–3064, 2019.

[15] Y. Mao, X. Wu, W. Huang, Q. Liao, H. Deng, Y. Wang, and Y. Guo, "Monte Carlo-based performance analysis for underwater continuous-variable quantum key distribution," *Applied Sciences*, vol. 10, no. 17, p. 5744, 2020.

[16] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[17] X. Sun, I. B. Djordjevic, and M. A. Neifeld, "Secret key rates and optimization of BB84 and decoy state protocols over time-varying free-space optical channels," *IEEE Photonics Journal*, vol. 8, no. 3, pp. 1–13, 2016.

[18] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Physical review letters*, vol. 98, no. 1, p. 010503, 2007.

[19] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," *Physical Review A*, vol. 84, no. 6, p. 062326, 2011.

[20] M. Lopes and N. Sarwade, "Optimized decoy state QKD for underwater free space communication," *International Journal of Quantum Information*, vol. 16, no. 02, p. 1850019, 2018.

[21] D.-D. Li, Q. Shen, W. Chen, Y. Li, X. Han, K.-X. Yang, Y. Xu, J. Lin, C.-Z. Wang, H.-L. Yong *et al.*, "Proof-of-principle demonstration of quantum key distribution with seawater channel: Towards space-to-underwater quantum communication," *Optics Communications*, vol. 452, pp. 220–226, 2019.

[22] Z. Feng, S. Li, and Z. Xu, "Experimental underwater quantum key distribution," *Optics Express*, vol. 29, no. 6, pp. 8725–8736, 2021.

[23] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-M. Li, H. Zhou, J.-P. Dou, and X.-M. Jin, "Decoy-state quantum key distribution over a long-distance high-loss air-water channel," *Physical Review Applied*, vol. 15, no. 2, p. 024060, 2021.

[24] F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. J. Sussman, and E. Karimi, "Investigation of underwater quantum channels in a 30 meter flume tank using structured photons," *New Journal of Physics*, vol. 22, no. 9, p. 093074, 2020.

[25] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Physical Review A*, vol. 67, no. 2, p. 022309, 2003.

[26] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[27] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[28] M. Lanzagorta, *Underwater Communications*. Morgan & Claypool Publishers, 2012.

[29] C. D. Mobley, *Light and Water: Radiative Transfer in Natural Waters*. Academic press, 1994.

[30] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[31] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[32] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 543–552, 2018.

[33] F. Hanson and S. Radic, "High bandwidth underwater optical communication," *Applied optics*, vol. 47, no. 2, pp. 277–283, 2008.

[34] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Information & Computation*, vol. 7, no. 5, pp. 431–458, 2007.

[35] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *2009 IEEE International Symposium on Information Theory*. IEEE, 2009, pp. 1879–1883.

[36] H. V. Nguyen, P. V. Trinh, A. T. Pham, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "Network coding aided cooperative quantum key distribution over free-space optical channels," *IEEE Access*, vol. 5, pp. 12 301–12 317, 2017.

[37] C. Mobley, E. Boss, and C. Roesler, "Ocean optics web book," http://www.oceanopticsbook.info, 2010.

[38] M. Elamassie, M. Uysal, Y. Baykal, M. Abdallah, and K. Qaraqe, "Effect of eddy diffusivity ratio on underwater optical scintillation index," *JOSA A*, vol. 34, no. 11, pp. 1969–1973, 2017.

[39] T. Wu, X. Ji, H. Zhang, X. Li, L. Wang, and X. Fan, "Rytov variance of spherical wave and performance indicators of laser radar systems in oceanic turbulence," *Optics Communications*, vol. 434, pp. 36–43, 2019.

[40] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* IEEE, 2004, p. 136.