Digital Object Identifier: 10.1109/JOE.2019.2894477

Assessing Feasibility of Secure Quantum Communications Involving Underwater Assets

Marco Lanzagorta and Jeffrey Uhlmann

***Abstract*—In this paper, we apply a mathematical model of the quantum bit error rate to assess the viability of quantum key distribution (QKD) protocols for secure and covert underwater communications. We consider scenarios that may include passive sensor arrays, coordinated underwater vehicles, and surface and aerial assets. This analysis suggests that single-photon QKD can potentially be used effectively at depths between 60 and 110 m in clear waters, with the precise depth depending in part on ambient illumination levels. We discuss how diurnal variations in background illumination can be exploited in some applications to achieve improved communications rate and/or reliability when using QKD or other secure optical protocol.**

***Index Terms*—Quantum cryptography, quantum information, submarine technology, underwater communications.**

I. Introduction

ONE of the most formidable environments for conducting secure communications involves one or more transmitters and/or receivers located under water, especially in deepwater ocean applications. Such applications may involve communications among underwater vehicles or between above-water airborne assets and/or satellites with below-water vehicles and/or passive surveillance systems [7], [16], [35] (see Fig. 1). In the case of underwater vehicles, simple acoustical transmissions with timestamps can allow vehicles to determine distance estimates to each other based on time delays so that a relative or absolute map of their locations can be deduced. In a covert setting, however, communications must be directional to avoid ambient detection outside of a given line-of-sight (LOS) channel. Such covert LOS channels can be established using optical links implemented with blue-green lasers tuned to the ambient transmission characteristics of the local waters. Unfortunately, even when optical links are optimally tailored to minimize attenuation, the efficiency is often insufficient to satisfy practical requirements, especially when the overhead of secure communications protocols is considered. This motivates examination of quantum-based methods to simultaneously provide provably secure communications and improved bandwidth capacity compared to purely classical channels.

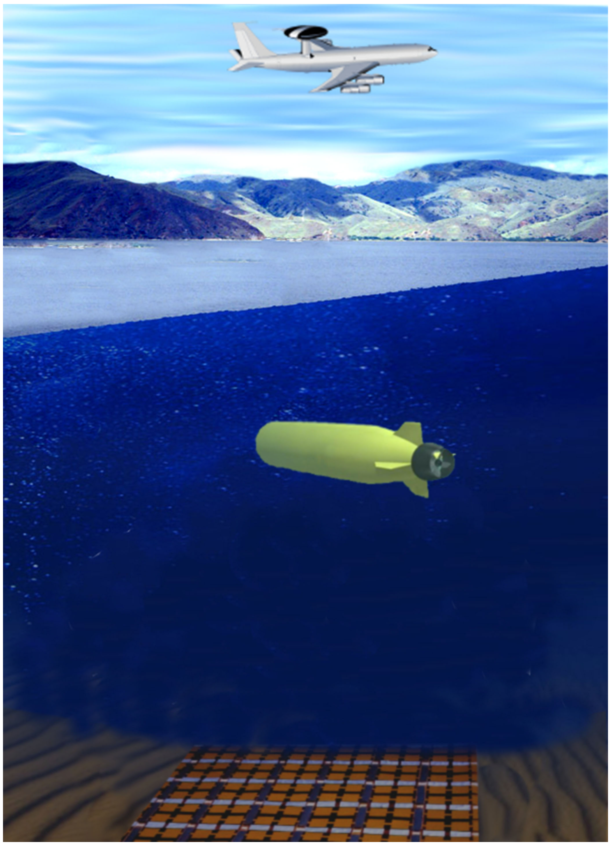

Fig. 1. Notional depiction of a deepwater sensor array, an unmanned underwater vehicle (UUV), and an above-water communications-relay aircraft.

Quantum key distribution (QKD) protocols have been developed, which offer security guarantees that are founded on fundamental laws of physics rather than assumed computational hardness of algorithmic problems such as prime factorization [2], [6], [12], [29], [34], and physical implementations of such protocols have corroborated theoretical predictions in practical demonstrations involving QKD over optical fiber [8], free-space communication between two ground stations [28], and free-space communications between a satellite and a ground station [9], [21], [33]. While the feasibility of QKD over optical fibers and in free-atmosphere contexts has been demonstrated, the underwater environment introduces significant challenges that have not been as rigorously examined [14]. In this paper, we apply a mathematical model for the quantum bit error rate

Manuscript received January 9, 2018; revised November 13, 2018 and December 18, 2018; accepted January 17, 2019. This work was presented in part at the MTS/IEEE OCEANS Conference, Washington, DC, USA, October 19-22, 2015. *(Corresponding author: Marco Lanzagorta.)*

Associate Editor: A. Morozov.

M. Lanzagorta is with the Naval Research Laboratory, Washington, DC 20375 USA (e-mail: marco.lanzagorta@nrl.navy.mil).

J. Uhlmann is with the University of Missouri, Columbia, MO 65211 USA (e-mail: juhlmann@missouri.edu).

Digital Object Identifier 10.1109/JOE.2019.2894477

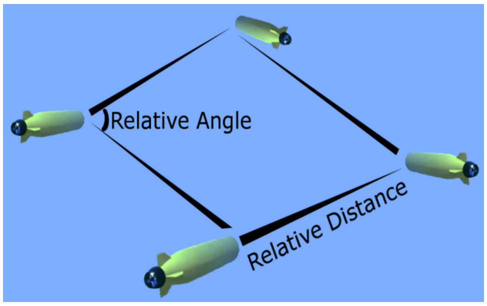

Fig. 2. UUVs can use optical or sonar sensing to measure relative range and bearing to other UUVs.

(QBER) to examine potential underwater performance characteristics of free-space BB84 QKD when applied in the three major Jerlov water types.[1] Specifically, we provide theoretical analysis to show that under certain conditions it can guarantee perfect security for underwater blue-green optical communications with a key generation rate of about 170 kb/s over 100 m in clear oceanic waters (Jerlov type I), which represents about 600 times more bandwidth than current very low frequency (VLF) systems. Furthermore, 100 m is the average depth of the thermocline, the required minimum depth for the stealth navigation of an underwater vehicle. In principle, these results suggest that it may be feasible to establish a quantum channel between an underwater vehicle and an airborne platform.

II. Coordinated UUV Scenarios

Applications of interest in this paper involve secure communications among unmanned underwater vehicles (UUVs), ocean-floor static sensor arrays, surface ships and buoys, and above-water aircraft and satellite assets. In some contexts, communications can be scheduled to occur at specific times while in others they are dynamically initiated as needed to achieve specific objectives. A particularly important example of the latter is the coordination of a team of UUVs for which each is able to obtain relative range and bearing measurements to others within proximity to it (see Fig. 2).

More generally, a team of UUVs may need to construct a map of underwater features to support precise subsequent navigation of the seafloor. If the true state (e.g., position and orientation) of a UUV is denoted as $\mathbf{x}$, and the true position of feature i is denoted as $\mathbf{p}_i$, then the goal is to simultaneously maintain and update (filter) estimates $\hat{\mathbf{x}}$ and $\hat{\mathbf{p}}_i$ of the UUV and feature, respectively.

Unfortunately, the computational complexity required to reliably construct such a map of N features is $O(N^2)$. This quadratic complexity derives from the fact that there exist correlated errors between the UUV estimate and every feature estimate, and between every pair of feature estimates, and these error terms must be maintained to avoid an introduction of estimation bias and consequent loss of information [11], [19]. This can be seen from the joint covariance between the error in the UUV state estimate, $\tilde{\mathbf{x}} = \mathbf{x} - \hat{\mathbf{x}}$, and the error associated with each feature i, $\tilde{\mathbf{p}}_i = \mathbf{p}_i - \hat{\mathbf{p}}_i$

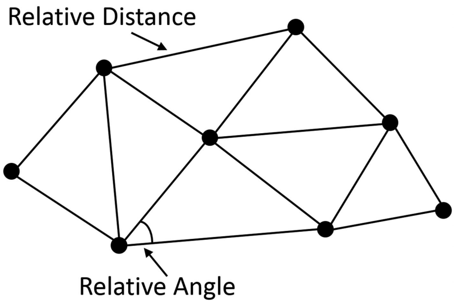

Fig. 3. Relative map only maintains estimates of the relative positions of features. Without absolute position information to "anchor" these relative estimates to a global coordinate frame there is no way to identify the location of a given feature except in terms of its distance and bearing with respect to other features.

$$\mathrm{E}\begin{bmatrix} \tilde{\mathbf{x}}\tilde{\mathbf{x}}^{\mathrm{T}} & \tilde{\mathbf{x}}\tilde{\mathbf{p}}_i^{\mathrm{T}} \\ \tilde{\mathbf{p}}_i\tilde{\mathbf{x}}^{\mathrm{T}} & \tilde{\mathbf{p}}_i\tilde{\mathbf{p}}_i^{\mathrm{T}} \end{bmatrix} \neq 0 \tag{1}$$

and from the joint covariance between feature estimates

$$\mathrm{E}\begin{bmatrix} \tilde{\mathbf{p}}_i\tilde{\mathbf{p}}_i^{\mathrm{T}} & \tilde{\mathbf{p}}_i\tilde{\mathbf{p}}_j^{\mathrm{T}} \\ \tilde{\mathbf{p}}_j\tilde{\mathbf{p}}_i^{\mathrm{T}} & \tilde{\mathbf{p}}_j\tilde{\mathbf{p}}_j^{\mathrm{T}} \end{bmatrix} \neq 0, \ \text{for}\ i \neq j \tag{2}$$

both of which involve $O(N^2)$ cross-covariance terms.

An alternative to creating a map of *absolute* position estimates in an arbitrary global coordinate frame is to create a *relative* map by exploiting the fact that relative position estimates can be independently produced and maintained using a standard Kalman filter [3], [4] (see Fig. 3).

Relative position information is sufficient for local coordination to perform some activities, but for other activities it is necessary to have absolute position information, e.g., so that a UUV can be routed to a location specified in global coordinates. For this it is necessary for relative map information from the UUVs to be communicated to a surface or aerial asset that can fuse the relative maps (using directional information from transmissions) to produce a single map in global coordinates. In practice, this typically requires frequent communications with the above-surface fusion asset to ensure that it is possible to associate features observed by one UUV with the corresponding features observed by another UUV when their respective estimates are only defined in terms of relative positions. As will be discussed, in some applications the ability (or inability) to schedule communications can impact the data rate that can be achieved when using a secure protocol.

III. Quantum Key Distribution

The fundamental unit of quantum information is the *qubit*, which generalizes the classical notion of a bit [13], [20], [32]. A classical bit is a binary variable that can only assume a value of 0 or 1, and its value is unique, deterministic, and unambiguous. A qubit, by contrast, can assume a state of 0, 1, or a probabilistic mixture—or *superposition*—of those two states. The state of a

[1] BB84, developed by Charles Bennett and Giles Brassard in 1984, is probably the simplest QKD protocol [20]. While there are more robust and sophisticated QKD protocols, we have decided to focus on the simplest implementation of BB84 to conduct the present feasibility study.

qubit is represented by a pair of complex numbers, $\{a, b\}$, that can be thought of as weights relating to the likelihood that the qubit will be in the 0 or 1 state when measured

$$\text{qubit} \doteq \{a, b\} = a \cdot 0_{\text{bit}} + b \cdot 1_{\text{bit}} \tag{3}$$

where $|a|^2$ is the probability that the qubit will be in the 0 state and $|b|^2$ is the probability that the qubit will be in the 1 state. Unlike the case for a classical bit, a qubit has no defined state until it is measured, at which point it assumes a binary state and is equivalent to a classical bit.

Although a superposition can be transformed in various ways, the state of a qubit cannot in general be copied to another qubit. This no-cloning property derives from the fundamental laws of quantum mechanics and represents both a limiting constraint and a powerful tool, depending on the application. From a computational perspective it represents a challenge because it prevents the use of temporary copies of quantum variables during intermediate steps of an algorithm. From a security perspective, however, it offers a means for encrypting information in a way that provides inviolable security guaranteed by the laws of physics. This provides the basis for multiple QKD protocols for secure communications between entities that have not previously communicated. Examples include BB84 and E91 [2], [6], [12], [29], [34]. QKD over optical fiber has been implemented in practice [8] and has even been offered commercially [10], [18], [30]. Free-space satellite applications have also been examined [9], [21], [33] and practical demonstrations have been achieved at a distance of 144 km with a key generation rate of 12.8 b/s [28], which is comparable to the distance from a ground station to a satellite. Until recently, however, comparatively little attention has been paid to underwater applications [14]. In Section IV,[2] we consider use of the BB84 QKD protocol under various models of underwater transmission.

It is important to remark that even though we are going to consider the BB84 QKD protocol, we are not interested in the specific implementation details. For instance, BB84 in atmospheric free space is often implemented with polarization states. However, other quantum variables need to be used in the situation where the environment is likely to change the polarization. These alternative encodings of quantum information include phase encoding, compensated polarization encoding, and single-sideband frequency encoding [15]. A more detailed analysis of how the oceanic environment affects photonic qubits is necessary to fully determine the type of QKD protocol and encoding necessary for successful underwater quantum communications.

IV. QBER in Underwater Channels

Because quantum measurements are destructive, any attempt by an eavesdropper to obtain information from the quantum channel will introduce noise into the system in the form of missing or corrupted qubits. It is not generally possible to distinguish noise due to eavesdropping from noise introduced by other error processes, e.g., sporadic environmental effects. Thus, the system's tolerance to noise must ensure that an eavesdropper is not able to extract information at a level that may be mistaken to be random noise. Alternatively, if the eavesdropper intercepts and reads content from the quantum channel without regard to possible detection by the communicating parties then the communication process must terminate, which essentially transforms the adversary's actions from eavesdropping to a denial-of-service attack.

TABLE I
Parameter Values Characterizing an Underwater Quantum Channel in the Optical Domain

$\phi = 10°$	$\Omega = 2\pi(1 - \cos\phi)$
$\lambda = 480$ nm	$\Delta\lambda = 0.12 \times 10^{-9}$ m
$\Delta t = 35$ ns	$\Delta t' = 200$ ps
$\mu = 0.1$	$\eta_{SPD} = 0.3$
$D = 60$ Hz	$\mathrm{A} = 30\ cm^2$
$\eta_{BQP} = 0.9$	$I_d = 1440\ W/m^2$

The QBER is defined by

$$\text{QBER} = \frac{\text{Probability of False Detection}}{\text{Total Probability of Detection Per Pulse}} \tag{4}$$

and is used to quantify the security of a QKD system [6], [27]. In the case of BB84, it has been shown that if

$$\text{QBER} \leq 25\% \tag{5}$$

then the system is secure against a simple intercept-resend attack, and if

$$\text{QBER} \leq 10\% \tag{6}$$

then it can be shown that the system is secure against more sophisticated quantum attacks.

For a typical BB84 QKD system we can model the QBER as [23]

$$\text{QBER} = \frac{D + \frac{I_d\, A\, \Delta t'\, \lambda\, \Delta\lambda\, \Omega}{4\, h\, c\, \Delta t}}{\frac{\mu\, \eta}{2\Delta t}\, e^{-\chi_c\, r} + 2\, D + \frac{I_d\, A\, \Delta t'\, \lambda\, \Delta\lambda\, \Omega}{2\, h\, c\, \Delta t}} \tag{7}$$

where D is the dark counts, Ω is the field of view of the detector, h is Planck's constant, c is the speed of light, η is the quantum efficiency of the detector, χ_c is the attenuation coefficient (i.e., $(1 - e^{-\chi_c L})$ is the fraction of photons lost due to absorption and scattering by the environment after traversing a distance L), I_d is the irradiance of the environment, $\Delta\lambda$ is the filter spectral width, Δt is the bit period, $\Delta t'$ is the receiver gate time, A is the receiver aperture, and μ is the mean photon number per pulse.

We now examine the performance of a quantum channel in the water column above an underwater asset transmitting from below the mixed layer at a depth of 100 m. Although the budget link should include atmospheric effects and the correct variation of the attenuation coefficient with depth, our focus is only on nominal effectiveness for purposes of feasibility assessment. To this end, we will assume the typical parameter values used for currently available free-space BB84 QKD systems [23], which are presented in Table I [14]. We note that, (7) only relates to the quantum channel and the values in Table I are exclusive to this channel. As mentioned before, the quantum channel is only used to generate a pair of secure keys that subsequently are employed to encrypt a message. Thus, a classical channel is assumed to

[2] Some content in this section expands on results previously presented in [31].

accompany the quantum channel for the actual transmission of the encrypted message. Characteristics of classical channels in the underwater domain, e.g., optical signal modulation, have been extensively examined in the literature and thus are not considered here [14].

We assume use of a single photon detector (SPD) operating in Geiger mode with detection probability 0.3 for $\lambda \approx 480$ nm, a blind time of 35 ns, and a maximum dark count rate of 60 Hz. In addition, we assume a theoretical biologically inspired quantum photo detector (BQP) with a detection probability of 0.6 and otherwise similar parameters as the SPD.[3] Furthermore, the NIST QKD system uses filters as wide as 1.2Å at 656 nm and a field of view of 16°, which are commercially available and can be adapted for this type of applications [23]. Thus, we assume that similar filters for the blue-green regime are not impossible to manufacture.

The inquisitive reader may notice that, (7) does not include a term that accounts for beam divergence losses. The reason is simple, assuming current technology it is possible to generate optical beams with a diameter of 0.25 m and a divergence angle of approximately 40 μrad, and a 2-m diameter receiver [22]. In this case, a laser pointed exactly at the detector at a distance R will not suffer losses due to beam divergence as long as

$$R < \frac{2\sqrt{\sigma/\pi} - w}{\theta} \tag{8}$$

where θ is the beam divergence angle, σ is the cross section of the detector, and w is the beamwidth. For the parameters considered, this happens at around 17 000 m. However, we are just considering short range communications on the order of 100 m. As a consequence, losses due to beam divergence are negligible.

In this regard, it is important to note that the pointing accuracy of the laser may not be a strong function of the field of view of the detector, but instead of the effective aperture and the beam spread of the laser in the medium. Indeed, a fully collimated laser requires a high degree of accuracy as it needs to point directly into the effective aperture of the detector. That is, it would be necessary to know the relative viewing angles of the communicating nodes with a high degree of accuracy throughout the entire communication process. On the other hand, a larger laser beam spread will ease the pointing and tracking requirements.

Another potential limiting factor to the proposed system is jitter in the timing. That is, the precision with which we can synchronize clocks for effective QKD distribution. In this text, we have assumed a phase lock loop to synchronize both clocks with the exact same performance as an operational atmospheric free space QKD system [23]. That is, as given in Table I, we have considered a receiver gate time of $\Delta t' = 200$ ps and a bit period of $\Delta t = 35$ ns. Even though we have not considered the practical constraint of carrying out this gating process underwater, we expect similar performance.

It is important to remark that, we have overestimated the effect of the environmental radiance in (7) and the values given in Table I. Also, notice that the environmental irradiance is asymmetric for the communication link between an underwater and an airborne vehicle, as the first one is looking up, whereas the second is looking down. We have done this for the sake of simplicity as at this point we are only interested in a proof of concept analysis.

Also, in addition to the absorption and scattering produced by water molecules, the ocean has a wide variety of scatterers in the form of suspended particles, plankton, and gelbstoffe [14]. A full and detailed analysis of the contributions of these scatterers is very complex because it would imply the incorporation of Mie scattering. However, we have included some of the effects of these scatterers in the values of the attenuation coefficient. Thus, we can notice from (7) that at short distances the dominant term driving the total probability of detection per pulse is the attenuated beam term (first term in the denominator), followed by the dark counts and irradiance terms. For the parameters used, in clear ocean waters ($\chi_w \approx 0.03$ m^{-1}) the dark counts term dominates only after about 105 m. However, in intermediate ($\chi_w \approx 0.18$ m^{-1}) and murkiest waters ($\chi_w \approx 0.3$ m^{-1}), the dark counts dominate after about 15 m. In all these cases, the irradiance term is much smaller.

In any event, clearly (7) includes many nontrivial parameters that affect the QBER. As such, finding the optimal set of parameters that minimize the QBER is not a trivial task. This is particularly true when we consider that the attenuation coefficient and the environment irradiance are highly variable parameters, which may dramatically change with the depth, oceanic region, the time of day, and the season. Clearly, an optimal determination of these parameters is outside the scope of this paper but should be address in future research. As has been observed, however, the attenuation beam term is dominant for short range communications (under 100 m). Thus, we will study the performance of the proposed QKD system in those values where this attenuation is minimal (i.e., in the blue-green regime where water attenuation is minimal [24]).

At this point, it is worth considering the expected maximum coherence lifetime of a photon that carries quantum information underwater. A detailed analysis of the decoherence processes would involve an intractably complicated calculation, but we know that attenuation of a quantum state due to absorption and scattering can be easily modeled by changing the creation/annihilation operations, $\hat{a}^\dagger$ and $\hat{a}$ of a photon to operators of the form

$$\begin{aligned} \hat{a} &\longrightarrow e^{(ikz-\chi/2)z}\hat{a} + i\sqrt{\chi}\int_0^z e^{(ik-\chi/2)(z-x)}\,\hat{b}(x)\,dx \\ \hat{a}^\dagger &\longrightarrow e^{(-ikz-\chi/2)z}\hat{a}^\dagger - i\sqrt{\chi}\int_0^z e^{(-ik-\chi/2)(z-x)}\,\hat{b}^\dagger(x)\,dx \end{aligned} \tag{9}$$

where $k = \omega\eta/c, \eta$ is the refraction index of the medium, χ is the attenuation coefficient that includes absorption and scattering loses, while $\hat{b}$ and $\hat{b}^\dagger$ represent all the possible contributions from the medium to the light field [25].

[3] BQP are photo detectors inspired by the quantum transport observed in the photosynthesis process. That is, they use novel materials able to synthesize the photosynthetic energy transport process observed in plants and bacteria. The manufacturing of these materials is a work in progress, but they appear to be feasible to design and engineer [17].

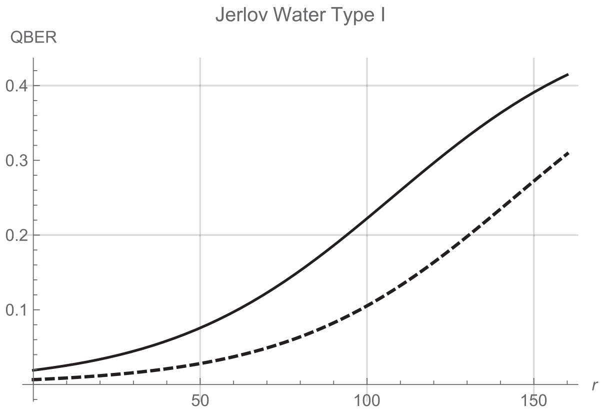

Fig. 4. QBER as a function of depth r in meters for SPD (solid) and BQP (dashed) in clear ocean waters (Jerlov Type I) with mid-day background illumination.

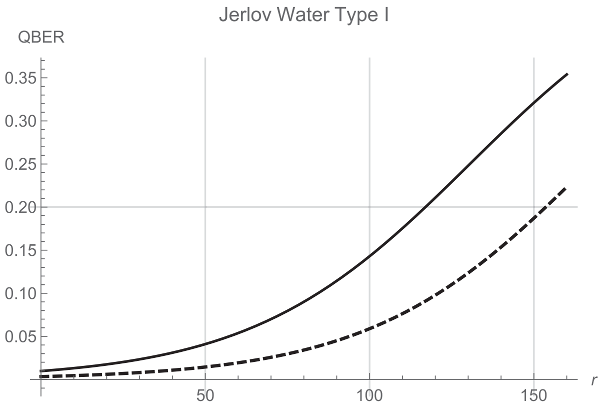

Fig. 5. QBER as a function of depth r in meters for SPD (solid) and BQP (dashed) in clear ocean waters (Jerlov Type I) with background illumination from $I_d = 1440$ (mid-day) to $I_d = 720\ \mathrm{W/m^2}$.

These expressions suggest that losses in the photonic quantum field scale in a similar way as classical light and can be used to give a rough estimate of the maximum coherence lifetime of a photon traveling underwater. A successful long range free-space atmospheric communications experiment conducted in the Canary Islands had a distance of about 144 km [26], and a similar attenuation underwater occurs when

$$e^{-\chi_w r} \approx e^{-\chi_a R} \Longrightarrow r \approx \frac{\chi_a}{\chi_w} R \tag{10}$$

where $R \approx 144 \times 10^3$ m is the maximum atmospheric distance, $\chi_w \approx 0.03\ \mathrm{m^{-1}}$ is the water attenuation coefficients for Jerlov Type I waters, and $\chi_a \approx 0.0002\ \mathrm{m^{-1}}$ is a typical value for the atmospheric attenuation coefficient. Therefore, we can expect that the photon states traveling underwater will be able to survive for a range of about 960 m.

Finally, let us mention that (7) implicitly assumes that coaxial alignment of transmitter and receiver can be maintained with fidelity that is independent of separation distance, which in practice can only be achieved over large distances with some form of active control. A separate sequence of photons can be used to facilitate this purely classical process, but for present purposes we will not make any assumptions about the precise means by which alignment is maintained.

A. Jerlov Type I—Clear Ocean Waters

Fig. 4 shows the QBER as a function of depth for clear ocean waters (Jerlov Type I) and mid-day background illumination ($I_d = 1440\ \mathrm{W/m^2}$). Assuming a maximum security bound QBER $= 0.1$ and a minimum security bound QBER $= 0.25$, Fig. 4 reveals that maximally secure single photon underwater BB84 QKD is feasible with SPD up to approximately 60 m in clear oceans, and remains secure against simple intercept-resend attacks to a depth of approximately 110 m. Using a BQP detector, however, appears to provide maximally-secure single photon BB84 QKD up to approximately 100 m in clear ocean waters with security against simple intercept-resend attacks to a depth of 140 m.

Fig. 5 shows the QBER under the same conditions as Fig. 4 but with a 50% reduction in the assumed background illumination ($I_d = 720\ \mathrm{W/m^2}$). As should be expected, the feasible depths for both SPD and BQP are commensurately increased/improved. This fact can be exploited if communications from underwater assets can be scheduled to be performed at night. In the case of a sensor array, the ability to schedule communications depends critically on whether it is intended to provide real-time detection information or whether it is intended only to record information for later retrospective analysis.

In the case of UUVs, there may be need for communications to be performed at regular intervals with a surface or aerial asset that can provide them with absolute position updates based on transmitted relative information. Because the ability to exploit diurnal effects on QBER is application-specific, all subsequent examples will assume average mid-day illumination with the understanding that QBER correlates strongly with assumed background illumination. However, it must be noted that, an assumed mean value $I_d = 1440$ does not capture QBER volatility due to surface caustics (see Fig. 6).

It is now possible to consider the range of desirable QBER values for an underwater asset. While lasers are minimally susceptible to interception away from the LOS, methods exist for scattered signal reconstruction (SSR) of signals based on light scattered along the transmission path. Thus, even a highly directional optical channel requires some level of encryption. If it is assumed that the eavesdropper has sufficient computational and sensing resources to perform effective SSR then optical security cannot be achieved and computational security would be required. Therefore, in a practical scenario in the maritime environment the optimal value of QBER will be somewhere between 10% and 25%.

Thus, the maximum range of the system as a function of the attenuation coefficient χ_c will depend on the selected value for the QBER security bound. The maximum ranges for SPD and BPQ are shown in Fig. 7. The shaded areas indicate the range of values that satisfy a QBER security constrained between 10% and 25%. Assuming SPD with a QBER bound of 25% in oceanic waters with $\chi_c \approx 0.16\ \mathrm{m^{-1}}$, for example, gives a

Fig. 6. Caustics due to reflected light can produce significant local deviations in levels of illumination that can lead to QBER underestimates.

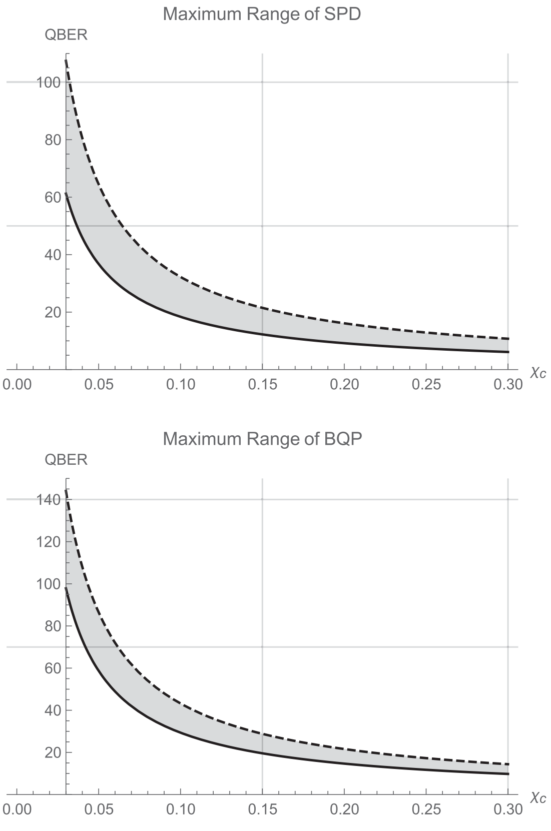

Fig. 7. (Top) Maximum range (m) of SPD for QBER security bounds of 10% (solid) and 25% (dashed) as a function of the attenuation coefficient $\chi_c\,(m^{-1})$. (Bottom) Maximum range of BQP for QBER security bounds of 10% (solid) and 25% (dashed). Shading indicates the range of values that satisfy QBER security constraint between 10% and 25%.

maximum range of about 20 m. At the same time, it is not possible to have secure underwater quantum communications beyond a range of 20 m if the attenuation coefficient is greater than 0.17 m^{-1}.

Because the electromagnetic properties of the ocean can change dramatically according to season, hydrography, and weather, it may be unreasonable to assume that the communications system will always operate in an environment characterized by the smallest value of $\chi_c \approx 0.03\ \text{m}^{-1}$. In the case when the photosensor is out of range, it may be possible to deploy a small buoy capable of conducting optical communications. The practical cost of this option may be mitigated in some applications by the buoy's potentially greater communications bandwidth.

B. Jerlov Type II and III—Intermediate/Murky Waters

As expected, the performance of the channel is degraded in murkier waters, and this is evident in Fig. 8 where maximal secure single photon BB84 QKD is only possible up to about 6 m in murky ocean waters using SPD (Jerlov Type III), and BQP only increases the effective depth to around 10 m.

C. Quantum Efficiency

The functional dependence between QBER and the quantum efficiency of the photodetector for clear ocean waters is shown in Fig. 9. The QBER is shown for 50-m (cyan), 100-m (purple), and 150-m (black) depth. This indicates that for $\eta \leq 1$ at a depth of 150 m no detector can enable secure BB84 QKD communications (assuming all the other system parameters are fixed to the values in Table I).

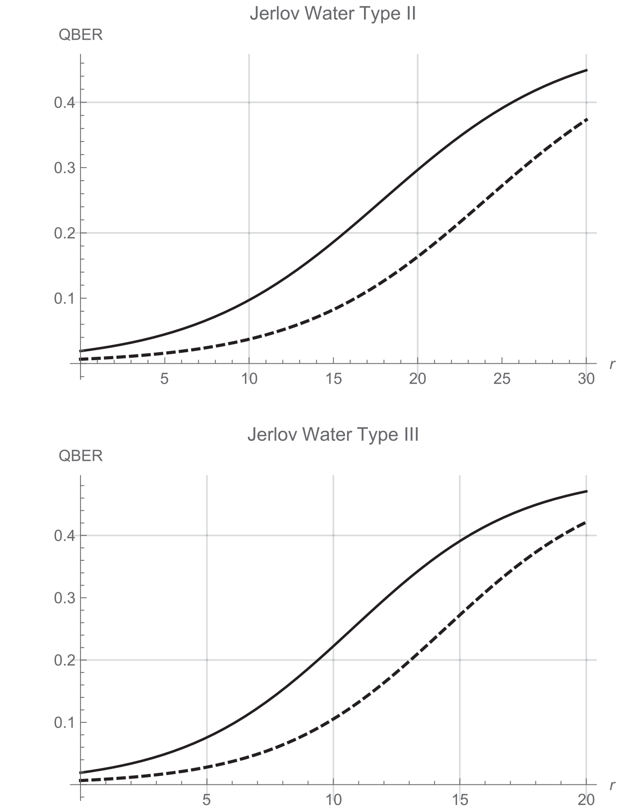

Fig. 8. QBER as a function of the depth r in meters for intermediate and murky waters for SPD (solid) and BQP (dashed).

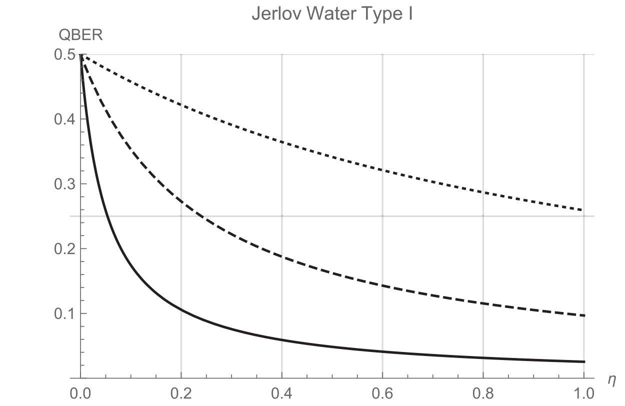

Fig. 9. QBER versus quantum efficiency in clear ocean waters at depth 50 m (solid), 100 m (dashed), and 150 m (dotted).

D. Field of View

The previous results show that even though the BQP detector has nearly perfect quantum efficiency, its performance is borderline with respect to the desired capabilities of an underwater communications system. However, there is another system parameter that could be improved to enhance the performance of these systems. As shown in Fig. 10, the QBER depends strongly on the angle that determines the field of view of the detector. The values are taken at 100-m depth for clear ocean waters. Therefore, as the field of view is decreased, the value of QBER is decreased, which in turn increases the range of the system.

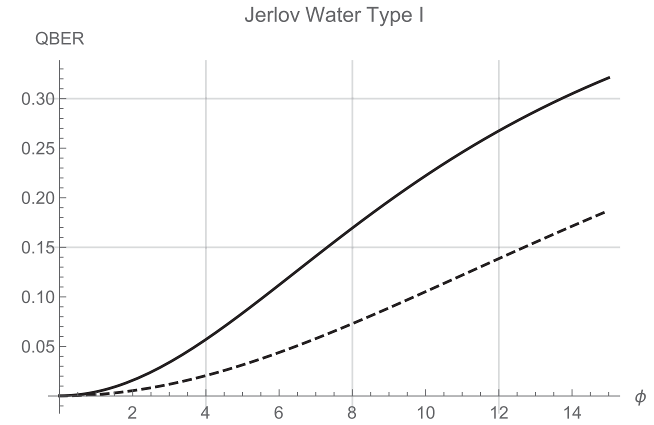

Fig. 10. QBER as a function of the field of view of the detector (in degrees) for SPD (solid) and BQP (dashed) at 100 m in clear ocean waters.

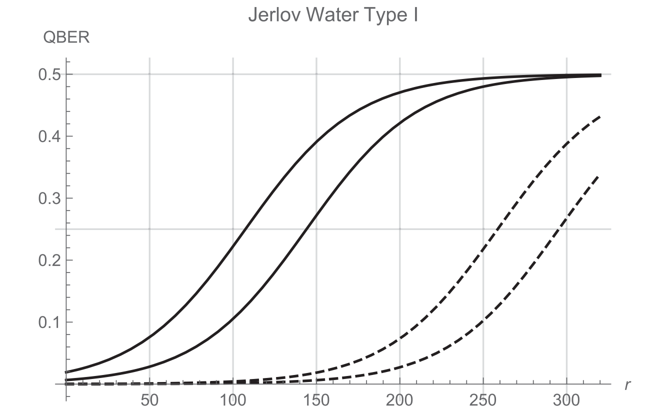

Fig. 11. QBER as function of the range r (in meters) in clear ocean waters for SPD with $\phi = 10^\circ$ (left solid) and with $\phi = 1^\circ$ (left dashed), as well as BQP with $\phi = 10^\circ$ (right solid) and with $\phi = 1^\circ$ (right dashed).

Fig. 11 shows QBER as a function of the range r in meters for SPD with $\phi = 10^\circ$ and with $\phi = 1^\circ$, as well as BQP with $\phi = 10^\circ$ (green) and with $\phi = 1^\circ$. Therefore, with a field of view of $\phi = 1^\circ$ it is feasible to have secure BB84 QKD using SPD up to about 230 m. Of course, the problem of a detector with a small field of view is to accurately point and track the transmitting laser.

Equation (6) suggests that it may also be possible to decrease the value of QBER by reducing the value of the receiver gate time $\Delta t'$, the dark counts D, or the wavelength bandpass $\Delta\lambda$.

E. Attenuation Coefficient

The variation of QBER with the attenuation coefficient χ_c at 100-m depth in clear ocean waters is plotted in Fig. 12, which shows the performance of SPD with $\phi = 10$ and $\phi = 0.00001^\circ$ and the BQP with $\phi = 10^\circ$ and $\phi = 0.00001^\circ$. The small value of ϕ may not be achievable, but it is used to show the theoretical limits of the system.

In the case of $\chi_c = 0.12\ \mathrm{m}^{-1}$, there is no possible value of ϕ or η that can ensure a secure quantum channel at a depth of 100 m. Similarly, in the case of $\chi_c = 0.10\ \mathrm{m}^{-1}$ the system requires an impractically small value of ϕ to establish a secure

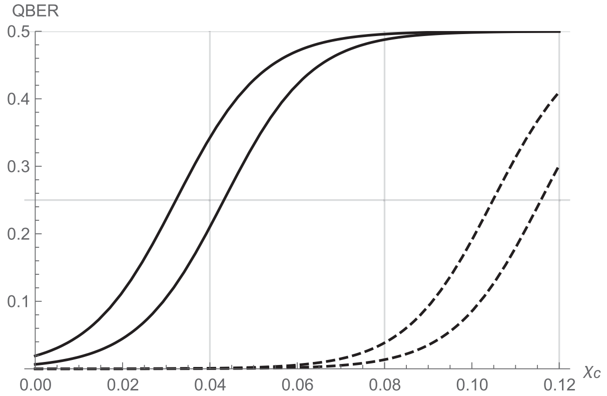

Fig. 12. QBER as function of χ_c (in m^{-1}) at depth 100 m in clear ocean waters for SPD with $\phi = 10°$ (left solid) and with $\phi = 0.00001°$ (left dashed), as well as BQP with $\phi = 10°$ (right solid) and with $\phi = 0.00001°$ (right dashed).

TABLE II
MAXIMUM CHANNEL CAPACITY C_M IN MEGABITS PER SECOND OF THE CLASSICAL CHANNEL FOR SPD AND BQP AT SECURITY ERROR BOUNDS OF 10% AND 25% FOR THE THREE MAJOR TYPES OF OCEANIC WATER

	SPD				BQP			
	10%		25%		10%		25%	
Jerlov	R_M	C_M	R_M	C_M	R_M	C_M	R_M	C_M
I	60	24	110	20	100	25	145	22
II	10	29	17	26	16	30	24	27
III	6	30	11	26	10	31	14	29

R_M is the maximum depth in meters that achieves the QBER bound.

quantum channel at a depth of 100 m. This suggests that it may not be possible to establish a secure quantum channel at a depth of 100 m in intermediate or murky ocean waters.

F. Maximum Capacity of the Classical Channel

Table II gives the maximum capacity C_M of the classical channel for SPD and BQP at security error bounds of 10% and 25% for the three major types of oceanic water. R_M is the maximum depth that achieves the QBER bound.

It is possible using SPD in clear ocean waters to have secure BB84 QKD communications at a depth of 60 m and to have the classical channel transmitting information at a capacity of 24 Mb/s. It is similarly possible to have BB84 QKD communications secure against intercept-resend attacks at a depth of 110 m and a classical channel with a capacity of 20 Mb/s. Note that although the maximum operational range varies considerably (between 6 and 110 m), the channel capacity varies only between 20 and 31 Mb/s.

V. SECRET KEY GENERATION RATE

To establish unconditionally secure communications it is necessary to generate private keys as large as the plaintext message. In that case the bandwidth of the system will be limited by the secret key generation rate, which depends on the specific error correction and privacy amplification algorithms used during the QKD protocol. Assuming a system similar to those used in demonstrations of free-space QKD, the secret key generation rate can be expressed as

$$\rho_s \approx \alpha \times e^{-\beta \times \mathrm{QBER}} \tag{11}$$

where ρ_s is expressed in megabits per second [23].

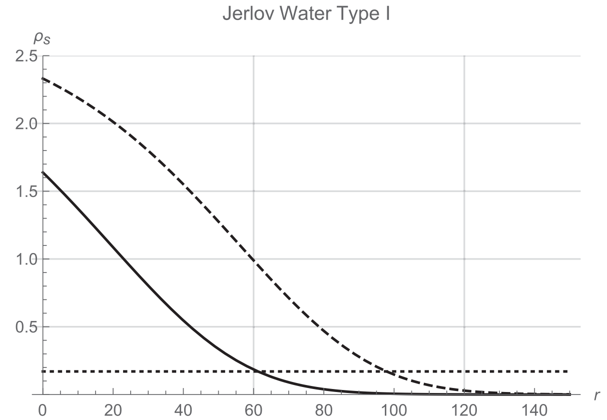

Fig. 13. Secret key generation rate in megabits per second as a function of depth r in meters in clear ocean waters for SPD (solid) and BQP (dashed) detectors.

It is important to remark that (8) is empirically derived. However, the parameters involved have very particular origins. Indeed, the effect of the environment and the characteristics of the technological system implementation are accounted for in the expression for QBER. As shown in (7), the QBER fully accounts for the environment attenuation, photodetection efficiency, dark counts, signal photon frequency, etc. On the other hand, the parameters α and β exclusively depend on the specific QKD protocol, error-correction methods, and privacy amplification algorithms used. In particular, if we use the same protocols, methods and algorithms as those used for free space QKD in air, then we have

$$\rho_s \approx 2.8 \times e^{-28 \times \mathrm{QBER}} \tag{12}$$

expressed in megabits per second [23]. Of course, optimal QKD in the underwater environment may require of different protocols, methods, and algorithms.

Thus, for the two bounding scenarios that have been considered thus far

$$\begin{aligned} \rho_s(10\%) &= 170\ \mathrm{kb/s} \\ \rho_s(25\%) &= 3\ \mathrm{kb/s} \end{aligned} \tag{13}$$

which reflects the fact that allowing higher the noise levels leads to reduced secret key generation rates.

Fig. 13 shows the secret key generation rate in megabits per second as a function of depth r (meters) in clear ocean waters. In can be observed, for example, that the maximum secret key generation rate for the SPD is of about 1.6 Mb/s at extremely short distances.

As the depth is increased, the rate of secret key generation decreases, and it reaches a limiting value of 170 kb/s at 60 m. In other words, using SPD in clear ocean waters it is possible to have a perfectly secure channel at 60-m depth with a throughput of 170 kb/s. Similar results can be derived for the case of

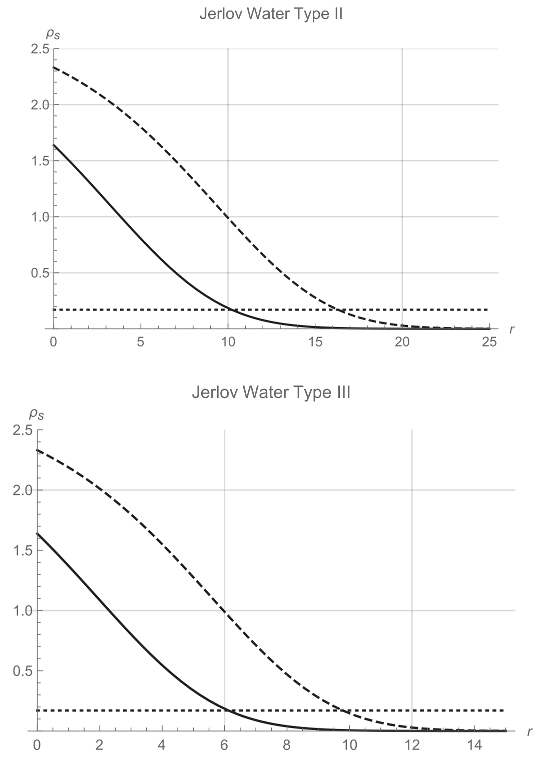

Fig. 14. Secret key generation rate in megabits per second as a function of depth (in meters) in intermediate and murky ocean waters for SPD (solid) and BQP (dashed) detectors.

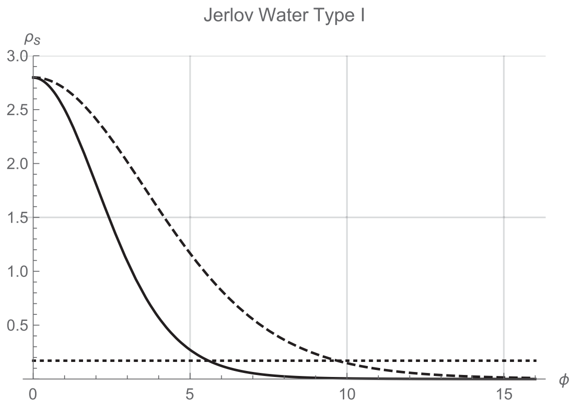

Fig. 15. Secret key generation rate as a function of the field of view (in degrees) for SPD (solid) and a BQP (dashed).

intermediate and murky ocean waters from the curves shown in Fig. 14.

Furthermore, as seen in Fig. 15, the rate of secret key generation also depends on the field of view. As expected, the rate increases as the field of view of the receiver decreases. As shown in Fig. 16, this in turn increases the operational range of the system.

VI. Discussion

In this paper, we have applied a mathematical model of the QBER to assess maritime implementations of QKD in applications involving underwater vehicles and sensors that must communicate with surface or aerial (or space) platforms. These results suggest that it is potentially feasible to use secure single photon BB84 QKD up to about 60 m in clear ocean waters using current SPD technology. Furthermore, it appears possible to have BB84 QKD secure against simple intercept and resend attacks up to about 110 m in the same type of water. On the other hand, these estimates are based on the limitations of current SPD technologies. Biologically inspired photosensors currently under investigation [14], [17] may provide detection sensitivity sufficient to permit secure single photon BB84 QKD up to about 100 m in clear oceanic waters and, for the simpler security bound, up to 140 m. If the keys are not reused, then the maximum channel utilization is limited by the secret key generation rate at about 170 kb/s at the maximum range of the maximally secure system, which represents nearly 600 times more bandwidth than current VLF systems. These results suggest that secure public-key protocols between satellites and underwater vehicles can potentially be used when physical constraints (e.g., provable direct LOS security) are available to prevent man-in-the-middle compromise of communications links.

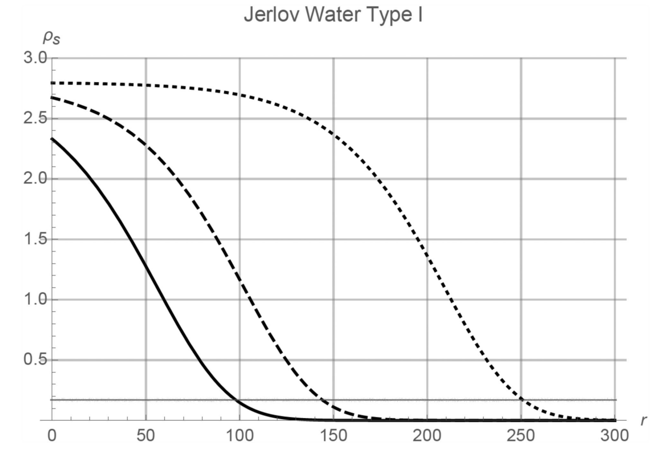

Fig. 16. Secret key generation rate as a function of depth r in meters in clear ocean waters for a BQP detectors with a field of view of $\phi = 10^\circ$ (solid), 5° (dashed), and 1° (dotted).

It is important to clarify that even though our work is entirely theoretical, recent experimental efforts have shown that polarization states of single and entangled photons can survive after traveling kilometers underwater [36]. Clearly further work is necessary to establish the best quantum encodings and system parameters for optimal underwater QKD.

The results presented have used the standard qubit representation. However, we are also considering the use of information theoretic representations of qubit channels that could enhance our understanding of the protocols involved and how to improve the transmission rates [37]–[40].

In terms of practical applications, we have discussed the limitations of QBER estimates that are based on an assumed constant background illumination. On the other hand, we have also suggested that it may be possible in some applications to achieve significantly reduced QBER by optimizing the scheduling of communications to exploit diurnal variations in ambient illumination, i.e., by communicating at night. For applications involving assets that must maintain regular communications with surface and/or aerial assets, e.g., UUVs that construct relative maps during intervals between communications with global positioning assets, assets may be able to dynamically adjust the amount of error-correction overhead applied by the protocol based on real-time monitoring of the background illumination. Whether this can provide practical benefit will be the subject of future work.

Acknowledgment

The authors are thankful to the many insightful comments and corrections suggested by the reviewers. In addition, they would also like to thank Dr. K. Martin for interesting discussions regarding the optical properties of blue lasers in the benthic region of the Sargasso Sea.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.

[2] D. Bouwmeester, A. Ekert, and A. Zelinger, Eds., *The Physics of Quantum Information*. Berlin, Germany: Springer, 2000.

[3] M. Csorba, J. K. Uhlmann, and H. F. Durrant-Whyte, "A sub-optimal algorithm for automatic map building," in *Proc. Amer. Control Conf.*, 1997, pp. 537–541.

[4] M. Csorba, J. K. Uhlmann, and H. F. Durrant-Whyte, "A new approach to simultaneous localization and dynamic map building," in *Proc. SPIE 10th Annu. Int. Symp. Aerosp./Defense Sens., Simul., Controls*, 1996, doi: 10.1117/12.241084.

[5] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed. London, U.K.: Oxford Univ. Press, 1958.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, p. 175, 2001.

[7] R. Headrick and L. Freitag, "Growth of underwater communication technology in the U.S. Navy," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 80–82, Jan. 2009.

[8] P. A. Hiskett *et al.*, "Long-distance quantum key distribution in optical fibre," *New J. Phys.*, vol. 8, p. 193, 2006.

[9] R. J. Hughes *et al.*, "Quantum cryptography for secure satellite communications," in *Proc. IEEE Aerosp. Conf.*, 2000, pp. 191–200.

[10] ID Quantique. 2019. [Online]. Available: http://www.idquantique.com/

[11] S. J. Julier and J. K. Uhlmann, "Building a million beacon map," in *Proc. SPIE Sens. Fusion Decentralized Control Robot. Syst.*, 2000, vol. 4571, doi: 10.1117/12.444158.

[12] C. Kollmitzer and M. Pivk, Eds., *Applied Quantum Cryptography*. Berlin, Germany: Springer, 2010.

[13] M. Lanzagorta and J. K. Uhlmann, *Quantum Computer Science*. San Rafael, CA, USA: Morgan & Claypool, 2008.

[14] M. Lanzagorta, *Underwater Quantum Communications*. San Rafael, CA, USA: Morgan & Claypool, 2014.

[15] D. Rogers, *Broadband Quantum Cryptography*. San Rafael, CA, USA: Morgan & Claypool, 2010.

[16] M. Lanzagorta and J. K. Uhlmann, "Quantum imaging in the maritime environment," in *Proc. MTS/IEEE OCEANS Conf.*, Anchorage, AK, USA, Sep. 18–21, 2017, pp. 1–10.

[17] M. Lanzagorta, J. K. Uhlmann, and S. Venegas-Andraca, "Quantum sensing in the maritime environment," in *Proc. MTS/IEEE OCEANS Conf.*, Oct. 19–22, 2015, doi: 10.23919/OCEANS.2015.7401973.

[18] MagiQ. 2019. [Online]. Available: http://www.magiqtech.com/

[19] M. Montemerlo and S. Thrun, *The FastSLAM Algortihm for Simultaneous Localization and Mapping*. Berlin, Germany: Springer, 2007.

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[21] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, pp. 82.1–82.9, 2002.

[22] T. Crowder and M. Lanzagorta, "Detection and communication with entanglement," in *Proc. IEEE Conf. Antenna Meas. Appl.*, 2018, doi: 10.1109/CAMA.2018.8530549.

[23] D. J. Rogers *et al.*, "Free-space quantum cryptography in the H-alpha Fraunhofer window," *Proc. SPIE*, 2006, vol. 6304, Paper 630417.

[24] N. G. Jerlov, *Marine Optics*. Amsterdam, The Netherlands: Elsevier, 1976.

[25] J. R. Jeffers, N. Imoto, and R. Loudon, "Quantum optics of traveling-wave attenuators and amplifiers," *Phys. Rev. A*, vol. 47, no. 4, 1993, Art. no. 3346.

[26] X.-S. Ma *et al.*, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, pp. 269–273, 2012.

[27] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.

[28] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, 2007, Art. no. 010504.

[29] A. V. Sergienko, Ed., *Quantum Communications and Cryptography*. New York, NY, USA: Taylor & Francis, 2006.

[30] Smart Quantum. 2019. [Online]. Available: http://smartquantum.co.uk/

[31] J. K. Uhlmann, M. Lanzagorta, and S. Venegas-Andraca, "Quantum communications in the maritime environment," in *Proc. MTS/IEEE OCEANS Conf.*, Washington, DC, USA, Oct. 19–22, 2015, doi: 10.23919/OCEANS.2015.7401974.

[32] V. Vedral, *Introduction to Quantum Information Science*. London, U.K.: Oxford Univ. Press, 2006.

[33] P. Villoresi *et al.*, "Space-to-ground quantum-communication using an optical ground station: A feasibility study," *Proc. SPIE*, vol. 5551, p. 113, 2004.

[34] G. Van Assche, *Quantum Cryptography and Secret Key Distillation*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[35] M. Zhao *et al.*, "Passive ghost imaging using caustics modeling," in *Proc. SPIE Signal Process., Sens./Inf. Fusion, Target Recognit.*, 2017, vol. 10200, doi: 10.1117/12.2262656.

[36] L. Ji *et al.*, "Towards quantum communications in free-space seawater," *Opt. Express*, vol. 25, pp. 19795–19806, 2017.

[37] T. Crowder and K. Martin, "Classical representations of qubit channels," *Electron. Notes Theor. Comput. Sci.*, vol. 270, no. 2, pp. 37–58, Feb. 14, 2011.

[38] T. Crowder and K. Martin, "Information theoretic representations of qubit channels," *Found. Phys.*, vol. 42, p. 976, 2012.

[39] T. Crowder, "A Quantum Representation for Involution Groups," *Electron. Notes Theor. Comput. Sci.*, vol. 276, pp. 145–158, Sep. 29, 2011.

[40] T. Crowder, "Representations of quantum channels," Ph.D. dissertation, Dept. Math., Howard Univ., Washington, DC, USA, 2013.

Marco Lanzagorta received the Ph.D. degree in theoretical physics from Oxford University, Oxford, U.K., in 1996.

He was the Technical Fellow and the Director of the Quantum Technologies Group of ITT Exelis (currently Harris Corporation), and worked at the European Organization for Nuclear Research (CERN) in Switzerland, and at the International Centre for Theoretical Physics in Italy. He is currently a Research Physicist with the U.S. Naval Research Laboratory, Washington, DC, USA. He is a recognized authority on the research and development of advanced information technologies and their application to combat and scientific systems. In addition, he has authored or coauthored more than 100 publications in the areas of physics and computer science, and authored the books *Quantum Information in Gravitational Fields* (Morgan & Claypool, 2013), *Quantum Radar* (Morgan & Claypool, 2011), and *Underwater Communications* (Morgan & Claypool, 2012).

Jeffrey Uhlmann received the Ph.D. degree in robotics from Oxford University, Oxford, U.K., in 1996.

For 13 years, he was a Research Scientist with the Naval Research Laboratory, Washington, DC, USA, where he developed key technologies for multiple-target tracking systems. He has authored or coauthored extensively in areas relating to quantum computing and quantum sensing as well as in the mathematics of system estimation and control. He is currently a Faculty Member with the Department of Electrical Engineering and Computer Science, University of Missouri, Columbia, MO, USA.