Quantum Communications in the Maritime Environment

Jeffrey Uhlmann
University of Missouri-Columbia
201 EBW, Columbia, MO 65211
uhlmannj@missouri.edu

Marco Lanzagorta
US Naval Research Laboratory
Washington, DC 20375
marco.lanzagorta@nrl.navy.mil

Salvador E. Venegas-Andraca
Tecnológico de Monterrey - ECI
Edo. México, 52926, México.
salvador.venegas-andraca@keble.oxon.org

***Abstract*—In this paper we describe research relating to the potential use of quantum key distribution (QKD) protocols for secure underwater communications. We briefly summarize the BB84 QKD protocol, its implementation and use in free-space applications, and then describe recent theoretical considerations of its use in the maritime domain. We also consider alternatives to QKD that offer security and bandwidth utilization advantages when applicable.**

I. Introduction

The deployment of efficient and secure communication links with underwater vehicles is among the most significant technological challenges presently confronted by the world's naval forces and, increasingly, by industry [1]. To this end, recent research efforts have explored the feasibility of free-space optical communication links connecting underwater vehicles with airborne platforms. These optical links are typically implemented with blue-green lasers, which are fine-tuned to work at the frequency of minimal optical attenuation produced by oceanic water. Problems related to the tracking of optical devices and the effect of the air-water interface are currently being investigated.

At the same time, one of the major scientific thrusts in recent years has been to try to harness quantum phenomena to dramatically increase the performance of a wide variety of classical information processing systems. These efforts in *quantum information science* have produced a variety of promising theoretical and experimental results with a considerable impact on the development of *perfectly secure quantum communications*. In this regard, "perfectly secure" communication is understood to imply an encryption protocol with mathematically provable security guarantees that do not rely on assumptions about the amount of computational resources available to potential adversaries. More specifically, *Quantum Key Distribution* (QKD) protocols provide security guaranteed by the laws of physics rather than assumed resource requirements, e.g., to perform prime factorization, that underpin classical key distribution methods that are currently used.

While the feasibility of QKD over optical fibers and the atmosphere is well understood, the underwater environment offers a variety of new challenges. In this paper we will present a general overview of our efforts to study the feasibility of an underwater quantum channel to enable QKD protocols. In particular, we will discuss how free-space QKD performs in the underwater environment in the three major Jerlov water types. For instance, theoretical analysis has shown that, under certain conditions, a QKD protocol that guarantees the perfect security of underwater blue-green optical communications appears to be feasible with a key generation rate of about 170 kb/s over 100m in clear oceanic waters (Jerlov type I). Notice that this represents about 600 times more bandwidth than current VLF systems. Furthermore, 100m 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.

Theoretical quantum key distribution (QKD) protocols have been developed that offer security guarantees which rest on fundamental laws of physics rather than assumptions about the computational limitations of potential adversaries [2], [3], [4], [5], [6]. Physical realizations of such protocols have demonstrated their feasibility. Examples include QKD over optical fiber[7], free-space communication between two ground stations [8], and free-space communications between a satellite and a ground station [9], [10], [11]. To date, however, there has been little if any examination of the practical feasibility of QKD to support secure underwater communications [1].

In this paper we consider potential applications of the BB84 QKD protocol for subsurface communications in oceanic waters. Our objective is not to provide a complete overview of quantum information [2], [3], [4], [5], [6] and quantum cryptography [2], [12], [13], [14]; rather, our goal is to present the basic principles required to understand the operation and security of quantum cryptographic devices so that we may consider their use in underwater applications.

A. Quantum Information

The fundamental unit of quantum information is the *qubit*, which has properties that generalize those of its classical counterpart, the bit [12], [13]. A classical bit is a binary variable that can only assume a value of 0 or a value of 1. Its value is unique, deterministic, and unambiguous. By contrast, a qubit can assume a state of 0, 1, or a probabilistic mixture – or *superposition* – of those two states. The state of a qubit is represented by a pair of complex numbers, $\{a, b\}$, which are related to classical 0-1 binary states as:

$$qubit = \{a, b\} \;=\; a \cdot 0_{bit} \;+\; b \cdot 1_{bit} \;, \qquad (1)$$

978-0-933957-43-5 ©2015 MTS

where $|a|^2$ is the probability that the qubit will be found in state 0 and $|b|^2$ is the probability that the qubit will be found in state 1. By a physical process which has no classical analog, the state of a qubit only becomes equivalent to that of a classical bit *after* it has been read/measured.

Bra-ket notation is a generalization of common vector notation in which $\langle\Psi|$ is a row vector (read as "bra psi") and $|\Psi\rangle$ is a complex conjugate column vector (read as "ket psi"), and the inner product $\langle\Psi|\Psi\rangle$ is referred to as a "bracket" (which is the origin of the root terms "bra" and "ket") [15]. In this notation the state of a single qubit can be written as:

$$|\Psi\rangle = a|0\rangle + b|1\rangle \tag{2}$$

or

$$\langle\Psi| = a^*\langle 0| + b^*\langle 1| \ , \tag{3}$$

where the condition

$$|a|^2 \ + \ |b|^2 \ = \ 1 \tag{4}$$

is critical for the interpretation of the squared norms of a and b as probabilities. In other words, a reading/measurement of the qubit $|\Psi\rangle$ will result in 0 with probability $|a|^2$ and 1 with probability $|b|^2$.

It is important to understand that $|0\rangle$ is not a zero vector; rather, "0" is just a label for one unit vector and "1" is a label for another unit vector, $|1\rangle$. In other words, one basis vector is arbitrarily labeled or interpreted as corresponding to the classical state 0 and the other basis vector is interpreted as corresponding to the classical state 1. If the context were classical True/False Boolean logic then the two basis states might be labeled $|\mathtt{T}\rangle$ and $|\mathtt{F}\rangle$, where the choice of which basis vector is interpreted as "T", and which is interpreted as "F", is entirely arbitrary.

Even the choice of the basis vectors is arbitrary. All that matters is that they are orthogonal and span a two-dimensional space. Once they are chosen they are then referred to as the *computational basis*. The most common choice of vectors for the computational basis is:

$$\begin{aligned} \langle 0| &= (1,0) \\ \langle 1| &= (0,1) \end{aligned} \tag{5}$$

and

$$\begin{aligned} |0\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} . \end{aligned} \tag{6}$$

Because $|0\rangle$ and $|1\rangle$ are orthogonal:

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \tag{7}$$

and

$$\langle 0|1\rangle = \langle 1|0\rangle = 0 \ . \tag{8}$$

In summary, $|0\rangle$ should be interpreted as being equivalent to a classical bit in the 0 state and $|1\rangle$ should be interpreted as being equivalent to a classical bit in the 1 state. The state of qubit is therefore a complex linear combination of classical 0-1 states.

It has been mentioned already that the state of a qubit becomes equivalent to that of a classical bit after it has been measured. This is true because the quantum process of measuring a superposition is unavoidably destructive and results in the "collapse" of the superposition to a classical bit value. After this collapse of the superposition the qubit is essentially a classical bit, so all subsequent read operations will produce the same value. Prior to measurement, however, the superposition can be non-destructively transformed in a variety of ways that permit the relative probabilities of measuring a classical 0 or 1 to be controlled.

Another critical property of a quantum superposition is that it cannot be copied/cloned. Unlike the state of a classical bit, a superposition stored in one qubit cannot be copied and stored in another qubit. The laws of quantum mechanics allow the state of one qubit to be moved to another qubit, but it can be shown that the process necessarily destroys the state of the original qubit. In other words, quantum information cannot be copied – it can only be *teleported* from one place to another. Quantum cryptography exploits the destructive-measurement and no-cloning properties of quantum information to permit detection of surreptitious measurements by an eavesdropper. For example, assume that instead of encoding bits using the computational basis, Alice and Bob communicate using an encoding in which 0 and 1 values are encoded using the *diagonal basis*:

$$\begin{aligned} |0\rangle_D &\equiv |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |1\rangle_D &\equiv |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \ . \end{aligned} \tag{9}$$

Alice and Bob could have mutually chosen any pair of orthogonal vectors to represent 0 and 1 values, so their choice of the diagonal basis instead of the computational basis (or any other basis) is entirely arbitrary. Once the choice of basis has been made, Alice can send her bit-string message, say "1001010001", as a sequence of basis vectors: $|1\rangle_D$, $|0\rangle_D$, $|0\rangle_D$, $|1\rangle_D$, ..., $|0\rangle_D$, $|1\rangle_D$. In order for Bob to properly receive her message he must know to interpret each $|0\rangle + |1\rangle/\sqrt{2}$ as a 0 and each $|0\rangle - |1\rangle/\sqrt{2}$ as a 1. In other words, Bob has to measure the qubits in the exact same basis to know what logical information was sent to him by Alice.

Let $P(x|y)$ denote the probability of measuring a logical bit x given receipt of a logical bit y. If Alice and Bob use the same basis, then for Bob:

$$\begin{aligned} P(0_D|0_D) &= |{}_D\langle 0|0\rangle_D|^2 = 1 \\ P(0_D|1_D) &= |{}_D\langle 0|1\rangle_D|^2 = 0 \\ P(1_D|0_D) &= |{}_D\langle 1|0\rangle_D|^2 = 0 \\ P(1_D|1_D) &= |{}_D\langle 1|1\rangle_D|^2 = 1 \ . \end{aligned} \tag{10}$$

On the other hand, if an eavesdropper, Eve, measures a qubit in the wrong basis, say, the computational basis, then she will

measure a 0 or a 1 with equal probability:

$$\begin{aligned} P(0|0_D) &= |\langle 0|0\rangle_D|^2 = \frac{1}{2}|\langle 0|0\rangle + \langle 0|1\rangle|^2 = \frac{1}{2} \quad (11) \\ P(0|1_D) &= |\langle 0|1\rangle_D|^2 = \frac{1}{2}|\langle 0|0\rangle - \langle 0|1\rangle|^2 = \frac{1}{2} \\ P(1|0_D) &= |\langle 1|0\rangle_D|^2 = \frac{1}{2}|\langle 1|0\rangle + \langle 1|1\rangle|^2 = \frac{1}{2} \\ P(1|1_D) &= |\langle 1|1\rangle_D|^2 = \frac{1}{2}|\langle 1|0\rangle - \langle 1|1\rangle|^2 = \frac{1}{2} \ . \end{aligned}$$

That is, Eve is unable to extract any information from the transmission because she is measuring in the wrong basis, i.e., she cannot properly interpret the sequence of signals sent by Alice to obtain the correct sequence of logical bits comprising the message ("1001010001").

Now suppose Eve thinks that she can distinguish bits constituting "a message" from a random sequence of bits, and she measures Alice's transmissions using different basis pairs in hopes of identifying the one that Alice is using to encode information sent to Bob. In principle this could be done, but each incorrect measurement will irretrievably destroy a part of the message because Eve is unable to create a copy of the original qubit before it is destroyed by her measurement. Thus, if Alice and Bob have suitable expectations based on a predefined protocol, Bob should be able to detect that he has not received all of Alice's transmissions or that the transmissions he has received are not encoded properly.

B. QKD Protocols

It was assumed in the example of the previous section that Alice and Bob had already agreed upon a secret basis set for encoding their communications, but it is often the case that communications need to be established between agents who have not previously communicated. This requires a means for them to somehow derive secret keys for encoding while initially communicating over an unsecure channel accessible to an eavesdropper. This can be achieved using any of several quantum key distribution (QKD) protocols such as BB84 and E91 [2], [3], [4], [5], [6].

All QKD protocols are similar in the sense that Alice (the transmitter) and Bob (the receiver) begin by exchanging quantum and classical information to generate secret keys. This requires two channels: a quantum channel for the transmission of quantum information (usually in the form of photons) and a classical public channel. The classical public channel is what Alice and Bob use to establish non-sensitive details of the protocol and to exchange information to verify the integrity of information obtained through the quantum channel.

In theory, the security of QKD protocols is guaranteed by the laws of physics. As is the case for classical protocols, however, unavoidably-imperfect physical implementations may introduce potential vulnerabilities. In general, the unconditional security of QKD protocols can only be guaranteed if:

- The eavesdropper cannot access the encoding and decoding devices used by the authorized parties.
- The random numbers required by the protocol are truly random.
- The classical channel is authenticated using an unconditionally secure scheme.
- The ciphertext is encrypted using a perfectly secure cipher.
- Alice and Bob have *perfect* quantum and classical technology.

Given the realistic practical limitations of any quantum or classical protocol, probably all that can be said is that in the limit of increasing engineering refinement the theory behind QKD offers a higher degree of security than is possible for any classical alternative.

QKD using optical fiber is relatively mature [7] and is even commercially available [16], [17], [18]. Free-space QKD has also been successfully implemented, including a 2007 experiment carried out between the islands of La Palma and Tenerife in the Canary Islands [8]. This demonstrated that free-space QKD is possible at a distance of 144 km with a key generation rate of 12.8 bits per second. This distance is approximately the same as that from a low Earth orbit to a ground station. That is, the experiment showed that QKD is feasible between a satellite and a ground station. Despite significant practical and theoretical consideration of free-space satellite applications [9], [10], [11], almost no attention has been paid to applications of QKD in underwater environments [1], [20], [21], [22].

C. The BB84 QKD Protocol

The BB84 QKD protocol was developed by C.H. Bennett and G. Brassard in 1984 [23]. The following is a summary of the protocol for a noiseless channel [2]:

1) Alice chooses at random the encoding basis for the qubits that she will send to Bob. Let us denote by "+" the computational basis and by "×" the diagonal basis.
2) Alice creates a random binary string: a random bit associated to each selection of the basis.
3) Alice uses this table to encode qubits with the logical value of the random binary string in the respective basis. She sends these qubits to Bob through the quantum channel.
4) Bob selects at random a basis for the measurement of the qubits that he receives from Alice.
5) Bob performs measurements of the qubits that Alice sent to him using the basis that he selected. As some of the times Bob is using a different basis than Alice, in these instances he will measure a completely random number (called the *raw key*).
6) Alice and Bob use the classical (public) channel to tell each other what bases they used during the protocol. They *do not* reveal the results of the measurements. They know that their results are perfectly correlated in those instances where both used the same basis. In any other case, Bob's measurements only give random numbers. In those instances where both used the same basis, Alice and Bob can use their correlated bits to create a *sifted key*.

7) If there are no eavesdroppers, then Alice and Bob will hold perfectly correlated sifted keys. Alice and Bob can determine the presence of an eavesdropper by randomly testing elements of their sifted keys and comparing their values. That is, Alice and Bob publicly agree on what bits they will use for testing, and publicly compare the values of the test bits. If the values are different, then they can presume the presence of an eavesdropper. The remaining bits form the *secret key* shared by Alice and Bob.

II. Quantum Bit Error Rate

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 (DOS) attack.

The quantum bit error rate (QBER) as defined by

$$QBER = \frac{\text{Probability of False Detection}}{\text{Total Probability of Detection Per Pulse}} \quad (12)$$

is used to quantify the security of the QKD system [3], [24]. In particular, for the case of BB84 it has been shown that if

$$QBER \leq 25\% \quad (13)$$

then the system is secure against a simple intercept-resend attack[1]. On the other hand, if

$$QBER \leq 10\% \ , \quad (14)$$

then it can be shown that the system is secure against a sophisticated quantum attack[2].

For a typical BB84 QKD system, the QBER is given by:

$$QBER = \frac{I_{dc} + \frac{R_d \ A \ \Delta t' \ \lambda \ \Delta\lambda \ \Omega}{4 \ h \ c \ \Delta t}}{\frac{\mu \ \eta}{2\Delta t} \ e^{-\chi_c r} + 2 \ I_{dc} + \frac{R_d \ A \ \Delta t' \ \lambda \ \Delta\lambda \ \Omega}{2 \ h \ c \ \Delta t}} \ , \quad (15)$$

where I_{dc} is the dark current, 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, R_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 [25].

[1]This is the most simple type of quantum attack: Eve intercepts some or all of the qubits that are being sent to Bob, then she sends these or other qubits to Bob.

[2]A sophisticated quantum attack is one where the eavesdropper has access to a fast quantum computer with a large quantum memory and a substantial number of quantum gates.

P_t	10 W	D	0.5 m
ϕ	10°	θ	10°
$\Delta\nu$	1 Mb/s	Δf	$\pi\Delta\nu/2$
Ω	$2\pi(1-\cos\phi)$	R_d	0.0125
I_d	1440 W/m^2	γ	333
λ	480 nm	$\Delta\lambda$	0.12×10^{-9} nm
η_{SPD}	0.6	k_{eff}	0.1
M	100	NEP_{dcsn}	0.4×10^{-12} $W/\sqrt{Hz}$
κ	0.1	η_{BQP}	0.9

TABLE I
VALUES OF PARAMETERS THAT CHARACTERIZE THE CLASSICAL CHANNEL OF THE UNDERWATER OPTICAL COMMUNICATIONS SYSTEM.

Δt	35 ns	$\Delta t'$	200 ps
μ	0.1 Hz	η_{SPD}	0.3
I_{dc}	60 Hz	A	30 cm^2

TABLE II
VALUES OF PARAMETERS THAT CHARACTERIZE THE QUANTUM CHANNEL OF THE UNDERWATER OPTICAL COMMUNICATIONS SYSTEM.

III. Performance of an Underwater Quantum Channel

In this section we examine the performance of a quantum channel in the water column above an underwater vehicle traveling under the mixed layer at a depth of 100m. Although the budget link should include atmospheric effects and the correct variation of the attenuation coefficient with depth, our objective is simply to assess 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 [25], which are presented in Tables 1 (those common to the classical channel) and 2 (those exclusive to the quantum channel). 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 35ns, and a maximum dark count rate of 60Hz.

A. Clear Ocean Waters

Figure 1 shows the QBER as a function of depth for clear ocean waters (Jerlov Type I). The horizontal blue line is the maximum security bound $QBER = 0.1$ and the grey horizontal line is the minimum security bound $QBER = 0.25$. It can be observed that maximally secure single photon underwater BB84 QKD is feasible with SPD up to about 60m in clear ocean waters. In addition, BB84 QKD secure against simple intercept-resend attacks is feasible up to about 110m deep in clear ocean waters using SPD.

On the other hand, it appears feasible to have maximally secure single photon BB84 QKD up to about 100m in clear ocean waters using the BQP detector. And it is also feasible to have BB84 QKD secure against simple intercept-resend attacks up to about 140m deep in clear ocean waters.

At this point it is worthwhile to consider what the desirable target value for QBER should be in the maritime environment. On the one hand, lasers are not highly susceptible to passive detection and interception because they are highly directional, and in principle a satellite could detect the possible presence of

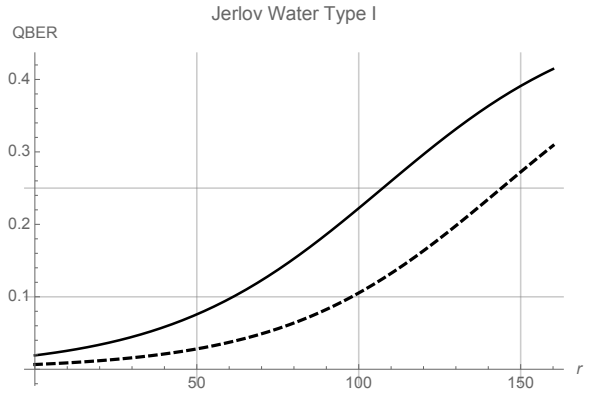

Fig. 1. QBER as a function of depth for SPD (solid) and BQP (dashed) in clear ocean waters (Jerlov Type I).

an eavesdropper on the line-of-sight to the underwater vehicle and respond appropriately (e.g., stop the transmission).

On the other hand, it is known that if enough light is recovered, Scattered Signal Reconstruction (SSR) techniques could reconstruct the original signal from the light that has been scattered from the laser beam. This means that an optical channel, even if highly directional, requires some level of encryption. Furthermore, assuming that the eavesdropper has limited computational and sensing resources to successfully achieve SSR in the maritime environment would imply that the optical system is no longer perfectly secure. In such a case only computational security could be achieved. Therefore, in a practical scenario in the maritime environment the optimal value of QBER will be somewhere between 10% and 25%.

As a consequence, 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 range for SPD and BPQ are shown in Figure 2. The shaded areas indicate the range of values that satisfy a QBER security constrained between 10% and 25%. Then, for example, SPD with a QBER bound of 25% operating in oceanic waters with $\chi_c \approx 0.16m^{-1}$ has a maximum range of about 20m. At the same time, it is not possible to have secure underwater quantum communications beyond a range of 20m if the attenuation coefficient is greater than 0.17 m^{-1}.

As the electromagnetic properties of the ocean may 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 $\chi_c \approx 0.03m^{-1}$. However, even in case when the photosensor is out of range, it is always possible to deploy a small buoy from the underwater vehicle carrying the optical transmitter and receiver. Even though this system becomes more cumbersome, it provides an ability to transmit and receive messages with higher bandwidth and perfect security.

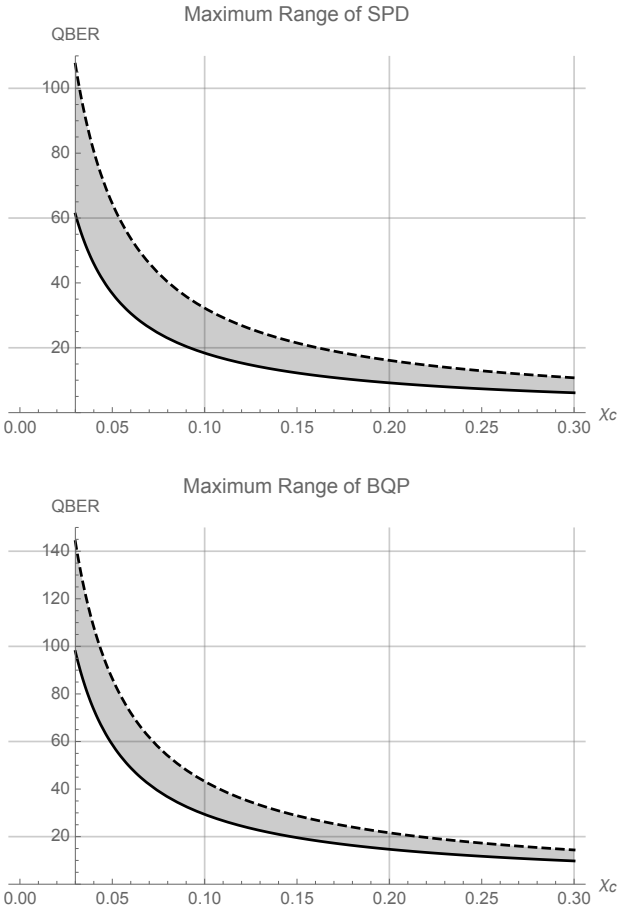

Fig. 2. **Top**: maximum range (m) of SPD for QBER security bounds of 10% (solid) and 25% (dashed) as a function of the attenuation coefficient $\chi_c(m^{-1}$. **Bottom**: maximum range of BQP for QBER security bounds of 10% (solid) and 25% (dashed). Shading indicates the range of values that satisfy QBER security constraint between 10% and 25%.

B. Intermediate and Murky Ocean Waters

As expected, the performance of the channel is degraded in other types of oceanic water as shown in Figure 3. For instance, maximal secure single photon BB84 QKD is only possible up to about 6m in murky ocean waters using SPD (Jerlov Type III). At the same time, maximal secure single photon BB84 QKD is only possible up to about 10m in murky ocean waters using BQP.

C. Quantum Efficiency

The functional dependency between QBER and the quantum efficiency of the photodetector for clear ocean waters is shown in Figure 4. The QBER is shown for 50m (cyan), 100m (purple), and 150m (black) depth. Thus, for example, as $\eta \leq 1$, it appears that there is no detector that can enable secure BB84 QKD communications at 150m depth (assuming all the other system parameters are fixed to the values in Tables 1 and 2).

D. Field of View

As we have seen, even though the BQP detector has nearly perfect quantum efficiency, its performance is borderline with

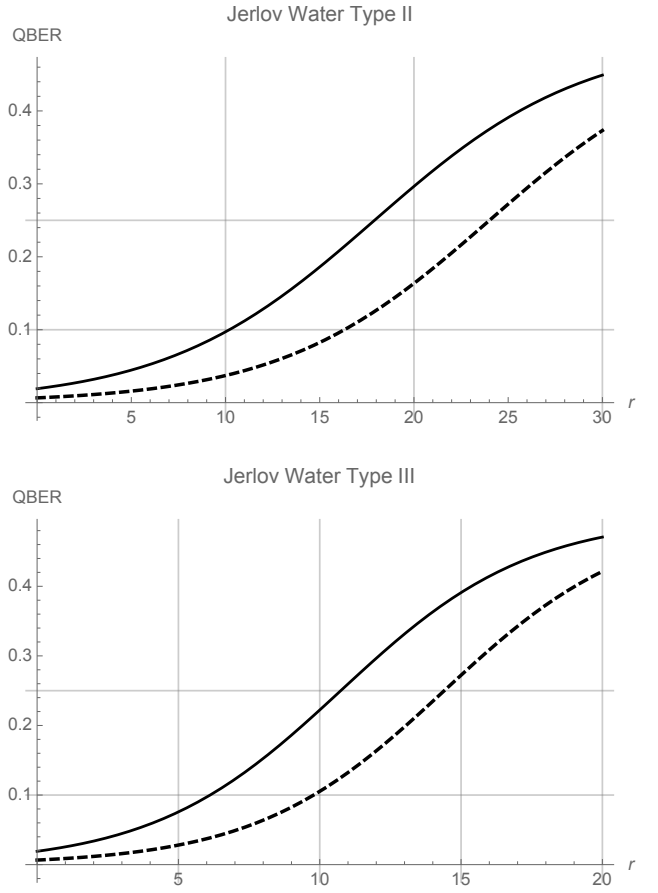

Fig. 3. QBER in terms of the depth for intermediate and murky ocean waters for SPD (solid) and BQP (dashed).

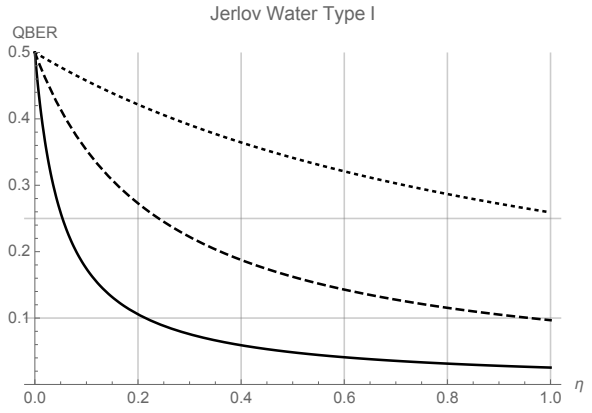

Fig. 4. QBER vs. quantum efficiency in clear ocean waters at depth 50m (solid), 100m (dashed), and 150m (dotted).

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 Figure 5, the QBER depends strongly on the angle that determines the field of view of the detector. The values are taken at 100m deep 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.

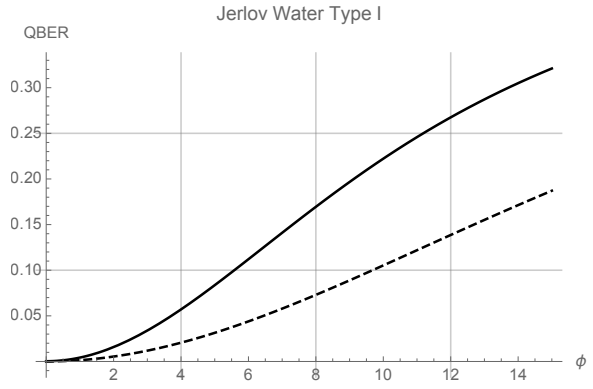

Fig. 5. QBER as a function of the field of view of the detector (in degrees) for SPD (solid) and BQP (dashed) at 100m in clear ocean waters.

Figure 6 shows QBER as function of the range for SPD with $\phi = 10°$ and with $\phi = 1°$, as well as BQP with $\phi = 10°$ (green) and with $\phi = 1°$. Therefore, with a field of view of $\phi = 1°$ it is feasible to have secure BB84 QKD using SPD up to about 230m. Of course, the problem of a detector with a small field of view is to accurately point and track the transmitting laser.

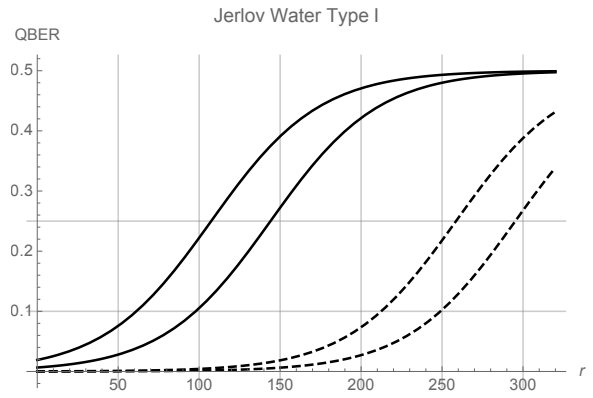

Fig. 6. QBER as function of the range in clear ocean waters for SPD with $\phi = 10°$ (left solid) and with $\phi = 1°$ (left dashed), as well as BQP with $\phi = 10°$ (right solid) and with $\phi = 1°$ (right dashed).

Inspection of Equation (14) reveals 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 current I_{dc}, or the wavelength bandpass $\Delta\lambda$.

E. Attenuation Coefficient

The variation of QBER with the attenuation coefficient χ_c at 100m deep in clear ocean waters is plotted in Figure 7, which shows the performance of SPD with $\phi = 10$ and $\phi = 0.00001°$ and the BQP with $\phi = 10°$ and $\phi = 0.00001°$. The small value of ϕ may not be achievable, but it is used to show the theoretical limits of the system.

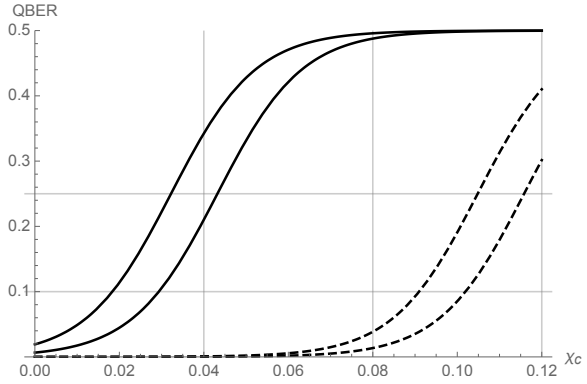

Fig. 7. QBER as function of χ_c at depth 100m in clear ocean waters for SPD with $\phi = 10^\circ$ (left solid) and with $\phi = 0.00001^\circ$ (left dashed), as well as BQP with $\phi = 10^\circ$ (right solid) and with $\phi = 0.00001^\circ$ (right dashed).

	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

TABLE III
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. R_M IS THE MAXIMUM DEPTH IN METERS THAT ACHIEVES THE QBER BOUND.

For example, if $\chi_c = 0.12m^{-1}$ then there is no possible value of ϕ or η that can ensure a secure quantum channel at 100m deep. Similarly, if $\chi_c = 0.10m^{-1}$ then the system requires an extraordinarily small value of ϕ (which may not be practically achievable) in order to establish a secure quantum channel at 100m deep. Therefore, this appears to indicate that it may not be possible to have a secure quantum channel at 100m deep in intermediate or murky ocean waters.

F. Maximum Capacity of the Classical Channel

Table III shows 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.

Thus, for example, using SPD in clear ocean waters it is possible to have secure BB84 QKD at 60m deep, and at this depth it is possible to have the classical channel transmitting information at a capacity of 24 megabits per second. Similarly, it is possible to have BB84 QKD secure against intercept-resend attacks at up to 110m deep, and a classical channel with a capacity of 20 megabits per second. Note that even though the maximum operational range varies considerably (between 6m and 110m), the channel capacity remains varies only between 20 and 31 megabits per second.

IV. SECRET KEY GENERATION RATE

If one desires unconditionally secure communications then one needs to generate private keys as large as the plaintext message. In such a case, the bandwidth of the system will be limited by the secret key generation rate. In general, the secret key generation rate will depend on the specific error correction and privacy amplification algorithms used during the QKD protocol. Assuming a system similar to the free-space QKD system at NIST, one can express the secret key generation rate as:

$$\rho_s \approx 2.8 \times e^{-28 \times QBER} \tag{16}$$

where ρ_s is expressed in megabits per second [25]. Thus, for the two bounding scenarios we have been considering:

$$\begin{aligned} \rho_s(10\%) &= 170\ kb/s \\ \rho_s(25\%) &= 3\ kb/s \end{aligned} \tag{17}$$

which reflects the fact that the higher the noise level allowed, the smaller the secret key generation rate.

Figure 9 shows the secret key generation rate in megabits per second as a function of depth in clear ocean waters. In can be observed, for instance, that the maximum secret key generation rate for the SPD is of about 1.6 megabits per second at extremely short distances.

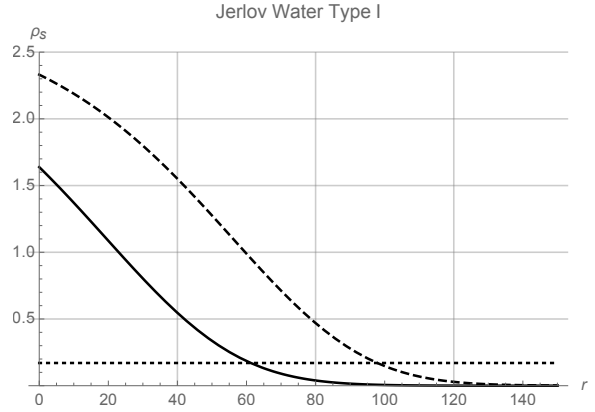

Fig. 8. Secret key generation rate as a function of depth in clear ocean waters for SPD (red) and BQP (green) detectors.

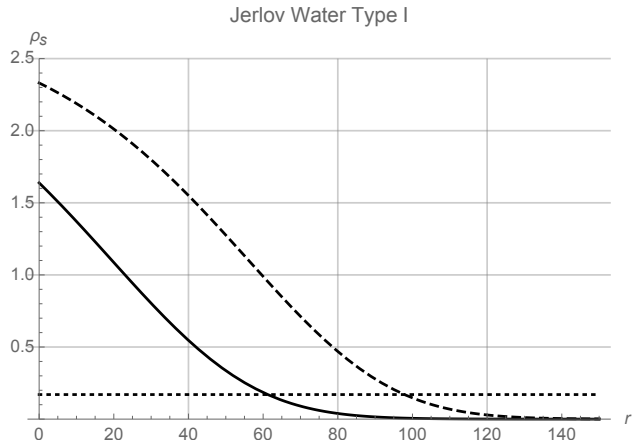

Fig. 9. Secret key generation rate in Mb/s as a function of depth in clear ocean waters for SPD (solid) and BQP (dashed) detectors.

As the depth is increased, the rate of secret key generation decreases, and it reaches a limiting value of 170 kilobits per second at 60m. In other words, using SPD in clear ocean waters it is possible to have a perfectly secure channel at 60m deep with a throughput of 170 kilobits per second. Similar results can be derived for the case of intermediate and murky ocean waters from the curves shown in Figure 10.

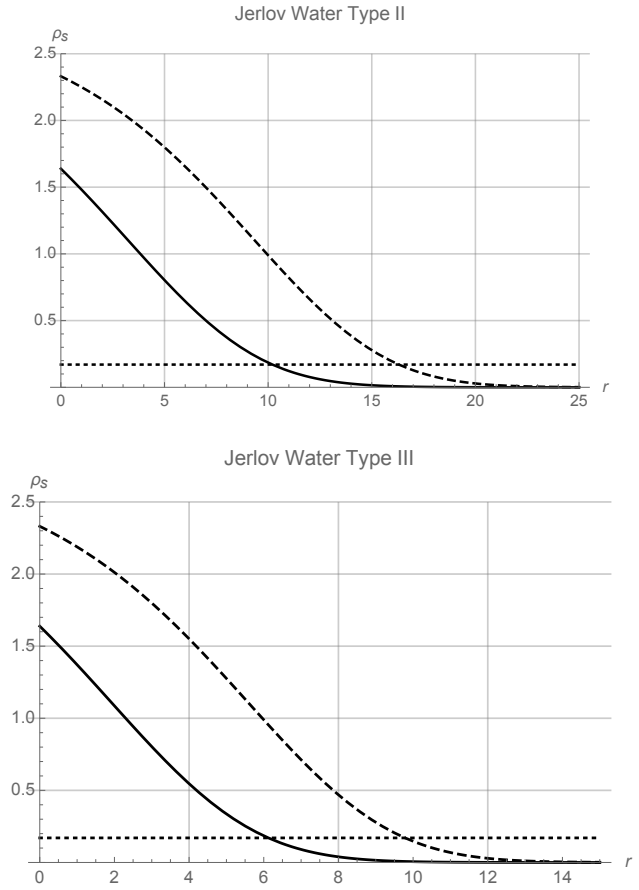

Fig. 10. Secret key generation rate in Mb/s as a function of depth in intermediate and murky ocean waters for SPD (solid) and BQP (dashed) detectors.

Furthermore, as seen in Figure 11, 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 Figure 12, this in turn increases the operational range of the system.

V. Quantum Shrinking One-Time Pads

The BB84 protocol represents a particular solution to the public key encryption problem, which demands a means for two parties to initiate and undertake secure communications in the presence of a *passive* eavesdropper. The reason why the eavesdropper is assumed to be passive is because *any* public key encryption protocol is vulnerable to a man-in-the-middle (MITM) attack in which the eavesdropper actively – though surreptitiously – mediates all communications between the two parties.

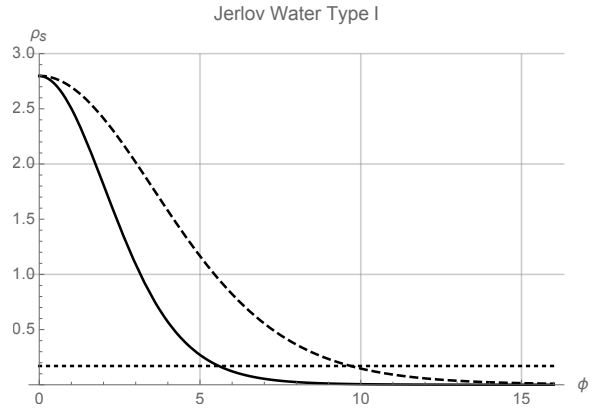

Fig. 11. Secret key generation rate as a function of the field of view for SPD (solid) and a BQP (dashed).

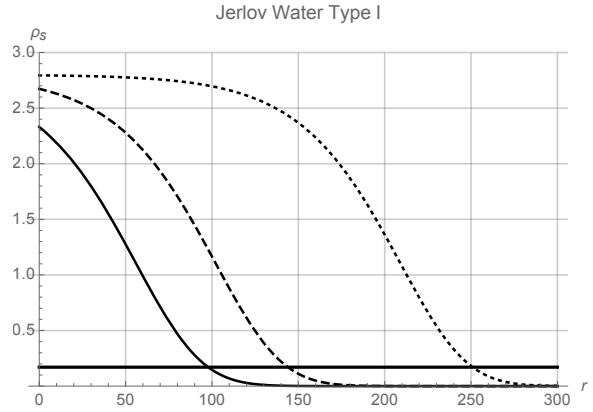

Fig. 12. Secret key generation rate as a function of depth in clear ocean waters for a BQP detectors with a field of view of $\phi = 10^\circ$ (solid), 5° (dashed), and 1° (dotted).

For example, if Eve were to engage in such an attack she would intercept Alice's attempt to initiate communications with Bob and then represent herself as Alice to Bob. She would then intercept Bob's communications and represent herself as Bob to Alice. Because Eve will be communicating separately with Alice and Bob, using whatever encryption protocol is chosen, she will be privy to the information content of every message they exchange. Eve can even alter the communications in any way she pleases, e.g., by sending a message that appears to be from Bob asking Alice for information that Eve wants to know. In principle there is no way Alice and Bob can detect Eve's middleman activities, so all security is lost without additional assumptions involving restrictions on Eve's capabilities or on the existence of pre-existing private information shared by Alice and Bob.

The most general, unconditionally secure, encryption protocol involves the use of a *one-time pad* [26], which is destroyed after use. A one-time pad is just a large sequence of random bits shared by the communicating parties that are sequentially used to encrypt their messages. If Alice and Bob share a one-time pad, P, of length n, they can exchange a sequence of messages of total length n with complete security. For

example, when Alice initiates communications with Bob she will exclusive-or (XOR, $\oplus$) her message of length r with the random binary values P_1 through P_r. Upon receipt, Bob will invert the encryption by applying the same operation using his copy of P. When Bob replies with his message of length s he will XOR it with the values P_{r+1} through P_{r+s}, and Alice will do the same upon receiving it, and the process can be repeated until all n bits of P have been exhausted.

Although not commonly used, OTP encryption is becoming increasingly practical with advances in mass storage technologies. Specifically, current (August 2015) SSDs have capacities up to 16TB [27], and in most practical contexts a one-time pad of this size would likely be sufficient to facilitate unconditionally secure communications for many years. As with any protocol, however, OTP has potential vulnerabilities when implemented in practice. One of these, of course, is that Alice and Bob must preserve the physical security of their respective copies of the OTP because if Eve were able to access one of their devices she could copy the OTP and decrypt any of their subsequent communications.

Compromise of the OTP threatens the security of future messages, but there is a related vulnerability for previously-sent messages. We call this the *Post-Communication Vulnerability* (PCV), and it refers to an eavesdropper's ability to store encrypted communications in anticipation of a possible compromise of the OTP in the future. Classical resource-based security protocols depend on an assumption that while Eve may be able to apply some amount of computational resources to break the encryption, the time required to do so would extend beyond the point at which the information of the communications has any value (e.g., centuries in the future). OTP-encrypted messages, by contrast, are potentially vulnerable only as long as a copy of the OTP exists, hence the OTP must be destroyed after use. In the case of large OTPs with content that is consumed on a per-message basis, however, it is necessary to incrementally destroy the consumed bits.

PCV security can be achieved by enhancing the communication protocol to include a step in which the use of each OTP bit is immediately followed by destruction of that bit, rather than waiting until the entire OTP is exhausted. Thus, Alice would erase (e.g., set to zero) the bits used to encrypt her message and Bob would similarly erase his copy of the same bits after decrypting the message. We refer to this use of an incrementally-erased OTP as a *Shrinking One-Time Pad* (S-OTP) protocol. Thus, Eve may retain surreptitiously-obtained copies of all communications between Alice and Bob, but she can never decrypt them. This ensures that any subsequent discovery of unencrypted messages in Eve's possession must have come from a security breach involving direct access to the unencrypted messages (or OTP) of Alice or Bob.

A cryptographic protocol is only effective if both parties can trust each other to implement it correctly, i.e., to destroy OTP bits immediately after use, and if the physical security of the each OTP is continuously maintained prior to use. A more powerful quantum-based variant, the Quantum S-OTP (QS-OTP), provides an additional level of security by replacing the copies of a shared OTP of classical bits with a pair of quantum OTPs of entangled qubits (EPR pairs), i.e., Alice has random qubits $P_1^A ... P_n^A$ and Bob has essentially identical qubits (by construction, not cloning) $P_1^B ... P_n^B$. Thus, when Alice measures her qubit P_i^A, and Bob measures his corresponding qubit P_i^B using the same previously-chosen *secret measurement basis*, the two are guaranteed to obtain the same binary value b.

The QS-OTP protocol for the exchange of message bit m_i from Alice to Bob includes the following steps:

1) Alice measures P_i^A using the secret measurement basis to obtain binary value b.
2) Alice erases the measurement result (and message-related content, as appropriate).
3) Alice sends classical bit $m_i \oplus b \rightarrow \tilde{m}_i$ to Bob.
4) Bob receives $\tilde{m}_i$ and measures P_i^B using the secret measurement basis to obtain binary value b.
5) Bob obtains Alice's original message bit as $\tilde{m}_i \oplus b \rightarrow m_i$.
6) Bob erases the measurement result (and message-related content, as appropriate)..

The key feature of this protocol is that the QS-OTPs, P^A and P^B, are more secure than their classical counterparts because quantum no-cloning ensures that they cannot be surreptitiously copied without knowledge of the secret measurement basis, and any effort by Eve to read them in a different basis will produce potentially detectable consequences when Alice and Bob attempt to communicate. This provides an additional layer of security for the OTPs prior to deployment[3].

One-time pads are attractive because they exploit a tradeoff between the amount of static resources that Alice and Bob must maintain and the amount of bandwidth required for them to communicate. In the maritime application the static resource consists of the data storage device containing an OTP of size sufficient to process all communications until the submarine is able to physically receive a fresh OTP. Although the security of the protocol depends on the physical security of the OTPs, the OTP protocol benefits from requiring significantly less bandwidth overhead compared to QKD.

VI. Summary

The results discussed in this paper relating to maritime implementations of QKD are based largely on theoretical work [1], but they strongly suggest that it is potentially feasible to use secure single photon BB84 QKD up to about 60m 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 110m 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 [19], [1]

[3]Additional layers of security can of course also be added to the classical S-OTP protocol, so in some sense the use of quantum resources in this context offers only a proportional rather than absolute advantage.

may provide detection sensitivity sufficient to permit secure single photon BB84 QKD up to about 100m in clear oceanic waters and, for the simpler security bound, up to 140m.

If the keys are not reused then the maximum channel capacity is limited by the secret key generation rate at about 170 kilobits per second at the maximum range of the maximally secure system. Nevertheless, this represents nearly 600 times more bandwidth than current VLF systems.

These results suggest that secure public-key protocols between satellites and underwater vehicles can be effectively used when physical constraints (e.g., provable direct line-of-sight security) are available to prevent man-in-the-middle compromise of communications links. For security against active adversaries, we have introduced and discussed the use of shrinking one-time-pads (S-OTPs), as well as their implementation using quantum resources, as alternatives to QKD. One-time pad protocols not only offer powerful security guarantees, they also incur significantly less bandwidth overhead compared to QKD and are becoming increasingly more practical as the capacities of data storage devices continue to increase.

ACKNOWLEDGMENT

SEVA would like to thank his family for their support as well as to gratefully acknowledge the financial support of Tecnológico de Monterrey - Escuela de Ciencias e Ingeniería, CONACyT (SNI member number 41594), and RAS project on: "Modeling the uncertainty: quantum theory and imaging processing", LR 7/8/2007.

REFERENCES

[1] M. Lanzagorta, *Underwater Communications*, Morgan & Claypool, 2014.
[2] D. Bouwmeester, A. Ekert, and A. Zelinger, (eds.), *The Physics of Quantum Information*, Springer, 2000.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", *Rev. Mod. Phys.* 74, 175, 2001.
[4] C. Kollmitzer and M. Pivk (eds.), *Applied Quantum Cryptography*, Springer, 2010.
[5] A.V. Sergienko (ed.), *Quantum Communications and Cryptography*, Taylor & Francis, 2006.
[6] G. Van Assche, *Quantum Cryptography and Secret Key Distillation*, Cambridge University Press, 2006.
[7] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Millar, and J.E. Nordholt, "Long-distance quantum key distribution in optical fibre", *New Journal of Physics*, 8, 193, 2006.
[8] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J.G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km", *Phys. Rev. Lett.* 98, 010504, 2007.
[9] R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, "Quantum cryptography for secure satellite communications," in *Proceedings of the IEEE Aerospace Conference* 2000, (IEEE, Piscataway, NJ, 2000) 1803 Vol. 1, 2000.
[10] J.G. Rarity, P.R. Tapster, P.M. Gorman, P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics* 4, 82.1-82.9, 2002.
[11] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri, "Space-to-ground quantum-communication using an optical ground station: a feasibility study", *Proceedings of SPIE*, 5551, 113, 2004.
[12] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
[13] M. Lanzagorta and J. Uhlmann, *Quantum Computer Science*, Morgan & Claypool, 2008.
[14] V. Vedral, *Introduction to Quantum Information Science*, Oxford University Press, 2006.
[15] P.A.M. Dirac, *The Principles of Quantum Mechanics*, 4th Edition, Oxford University Press, 1958.
[16] IDQuantique, http://www.idquantique.com/
[17] MagiQ, http://www.magiqtech.com/
[18] Smart Quantum, http://smartquantum.co.uk/
[19] M. Lanzagorta, J. Uhlmann, and S. Venegas-Andraca, "Quantum Sensing in the Maritime Environment," Proc. MTS/IEEE Oceans Conference, 19-22 October, 2015.
[20] J. Aron, "Quantum Keys Let Submarines Talk Securely", *New Scientist*, No. 2836, 2011.
[21] C. Dillow, "Quantum Scheme Could Allow Submarines to Communicate Securely", *Popular Science*, 2011. http://www.popsci.com/technology/article/2011-10/quantum-communication-scheme-could-allow-submerged-subs-communicate-securely
[22] N. Gilbert, "Photons Can Quantum Encrypt Submarine Comms", *Australian Popular Science*, 2011. http://www.popsci.com.au/technology/military/photons-can-be-used-to-encrypt-submarine-communications
[23] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, p. 175, 1984.
[24] 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.* 81, 1301-1350, 2009.
[25] D.J. Rogers, J.C. Bienfang, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, L. Ma, D.H. Su, C.J. Williams, and C.W. Clark, "Free-Space Quantum Cryptography in the H-alpha Fraunhofer Window", *Proceedings of SPIE*, Vol 6304, 630417, 2006.
[26] C. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, 28 (4): 656715, 1949.
[27] J. Newman, "Samsung Takes 'Worlds Largest Storage Drive' Crown with 16TB SSD", *PC World*, August 14, 2015 (http://www.pcworld.com/article/2971268/storage/samsung-takes-worlds-largest-storage-drive-crown-with-16tb-ssd.html).