Hindawi
Quantum Engineering
Volume 2023, Article ID 7185329, 26 pages
https://doi.org/10.1155/2023/7185329

Review Article

A Primer on Underwater Quantum Key Distribution

Pietro Paglierani,[1] **Amir Hossein Fahim Raouf**,[2,3] **Konstantinos Pelekanakis**,[1] **Roberto Petroccia**,[1] **João Alves**,[1] **and Murat Uysal**[4]

[1]*NATO STO Centre for Maritime Research and Experimentation, La Spezia 19126, Italy*
[2]*Department of Electrical and Electronics Engineering, Ozyegin University, Istanbul 34794, Türkiye*
[3]*Department of Electrical & Computer Engineering, North Carolina State University, Raleigh, NC 27695, USA*
[4]*Engineering Division, New York University Abu Dhabi (NYUAD), Abu Dhabi 129188, UAE*

Correspondence should be addressed to Pietro Paglierani; pietro.paglierani@cmre.nato.int

Received 4 July 2023; Revised 31 October 2023; Accepted 20 November 2023; Published 23 December 2023

Academic Editor: YuBo Sheng

The growing importance of underwater networks (UNs) in mission-critical activities at sea enforces the need for secure underwater communications (UCs). Classical encryption techniques can be used to achieve secure data exchange in UNs. However, the advent of quantum computing will pose threats to classical cryptography, thus challenging UCs. Currently, underwater cryptosystems mostly adopt symmetric ciphers, which are considered computationally quantum robust but pose the challenge of distributing the secret key upfront. Post-quantum public-key (PQPK) protocols promise to overcome the key distribution problem. The security of PQPK protocols, however, only relies on the assumed computational complexity of some underlying mathematical problems. Moreover, the use of resource-hungry PQPK algorithms in resource-constrained environments such as UNs can require nontrivial hardware/software optimization efforts. An alternative approach is underwater quantum key distribution (QKD), which promises unconditional security built upon the physical principles of quantum mechanics (QM). This tutorial provides a basic introduction to free-space underwater QKD (UQKD). At first, the basic concepts of QKD are presented, based on a fully worked out QKD example. A thorough state-of-the-art analysis of UQKD is carried out. The paper subsequently provides a theoretical analysis of the QKD performance through free-space underwater channels and its dependence on the key optical parameters of the system and seawater. Finally, open challenges, points of strength, and perspectives of UQKD are identified and discussed.

1. Introduction

Secure underwater communications (UCs) play a key role in mission-critical activities at sea; hence, effective cryptosystems, specifically tailored to underwater applications, are needed [1–4]. Classical encryption techniques can provide confidentiality, integrity, and authentication in underwater networks [4–6]. However, the advent of quantum computing will pose threats to classical cryptography and will thus challenge also the security of UCs [7, 8]. In principle, a quantum computer running the Shor algorithm can efficiently solve the complex mathematical problems currently used in the most popular public key distribution schemes [9]. As a consequence, these schemes, which are computationally robust to classical computer-based attacks, are vulnerable to quantum attacks [10–12]. Conversely, it is widely acknowledged that symmetric block ciphers will offer computational quantum robustness until 2050 and beyond [8, 13]. The Grover quantum algorithm can speed up brute force attacks to these schemes. In particular, it can reduce the required number of steps to perform the full search of an n-bit secret key in an unstructured space of 2^n elements, from $\mathcal{O}(2^n)$ to $\mathcal{O}(2^{n/2})$ over classic algorithms [14]. Nonetheless, the security of symmetric ciphers can be easily restored by increasing the secret key length n [8, 13]. Symmetric key cryptography, however, relies on the fundamental

requirement that legitimate communicating nodes must share the secret key in advance. This requirement has opened the key distribution problem (KDP), which is challenging in terrestrial networks and can be critical or even insurmountable in the harsh environments, such as those in which underwater networks operate [2–4]. To overcome the KDP, standardization bodies and security agencies presently recommend the use of post-quantum public-key (PQPK) protocols [10–12]. These schemes do not require any preshared information; conversely, they can establish asymmetric pairs of keys through an authenticated public channel, based only on some complex mathematical problems, which neither classical nor quantum computers are known to efficiently solve [10, 12]. To counteract quantum threats, in 2016, the National Institute of Standards and Technology (NIST) started the "Post Quantum Cryptography" contest, with the aim of selecting and standardizing cryptographic schemes capable to withstand both quantum and classical attacks [11]. This initiative recently completed the third round of its evaluation process [11]. As a result of this contest, one public key algorithm was selected for standardization, and four additional public key schemes were chosen as candidates for standardization in the next round [15]. The security of PQPK algorithms, however, cannot be theoretically proved; it only relies on the experimental evidence that a given mathematical problem is computationally hard both for known quantum-enabled and classic algorithms to solve (four weeks after NIST announced the results of the third round of evaluation [15], a practical attack to SIKE (one of the four candidate public key algorithms selected for potential standardization in the fourth round) was published [16]. The software used for the attack could obtain the secret key in about one hour time, when executed on a single core of a standard computer running at 2.6 GHz. An attack to Rainbow, a digital signature scheme also included in the Post Quantum Cryptography standardization contest, had been published just a few months earlier [17]) [12, 16, 18]. Furthermore, PQPK schemes typically operate on power-hungry computers and servers. Therefore, using them in resource-constrained networks, such as underwater acoustics, may necessitate additional complex software or hardware optimization efforts in order to be practical [12]. Ongoing research and standardization efforts are being devoted to solve this problem. For instance, in [19], the authors present a memory-optimized version of the quantum-safe public key Classic McEliece cryptosystem, a NIST candidate for future standardization, which necessitates a one-megabyte public key. The proposed implementation can run on a memory-constrained processor like an ARM Cortex-M4, by streaming small chunks of the public key calculated at run time from the private key. This way, the algorithm memory footprint can be significantly reduced. Nonetheless, the transmission of such a large public key in an underwater acoustic network remains a daunting problem [4]. With the widespread diffusion of Internet of Things (IoT) devices and sensor networks, the deployment of computationally demanding cryptographic algorithms onto processors with constrained resources has become a compelling problem also outside the UC domain. The NIST Lightweight Cryptography project focuses on authenticated encryption and hashing schemes suitable for computationally and bandwidth-constrained environments. However, this standardization initiative does not include any proposal for lightweight public key cryptography, at least in its first phase [20].

Physical layer security (PLS) is another potential way for key generation and distribution in underwater acoustic networks. PLS utilizes the physical characteristics of wireless acoustic channels to enable two legitimate parties to share a secret key [21–23]. It assumes that the two unidirectional wireless channels connecting two legitimate nodes are highly correlated and unique, so that a shared secret key can be originated by suitably processing their impulse responses. An eavesdropping adversary attempting to obtain the secret key will not possess sufficient knowledge about the state of the environment to accurately reproduce those unique channels on a computer and thus will be unable to calculate the secret key.

Quantum key distribution (QKD) addresses KDP in a different way. Specifically, it allows two legitimate parties that can transmit photons through a quantum channel to securely share a secret key, by exploiting the physical principles of quantum mechanics (QM) [8]. Any adversary trying to obtain the secret key will unavoidably alter the quantum states of the transmitted photons and will thus reveal its activity to the legitimate users. Moreover, a QKD system can continuously generate additional secret key bits, starting from a short initial secret key [8]. As a result, the newly generated secret bits can be used by a One Time Pad (OTP) cipher to transmit unconditionally secure messages, i.e., their confidentiality is independent from the amount and quality of resources available to attackers and cannot be harmed by technological advances [8, 24]. In the case of using the OTP, it is important to emphasize that in order to transmit n data bits, an equally long secret key of n is necessary. Alternatively, QKD can be combined with a classic symmetric block cipher, with the advantage of using the same short secret key to encrypt a large number of different messages. This latter combination cannot provide unconditional security [8]. Nevertheless, existing quantum algorithms currently lack the efficiency required to compromise its security. Moreover, it allows the potential bottlenecks due to the low secret key generation rates currently achievable by existing QKD systems to be overcome [8].

In 1984, Bennet and Brassard presented BB84, the first QKD protocol [25]. Since then, QKD has become a very active and fast-growing research field in fiber cable and satellite communications. The practical security of QKD systems in real-life scenarios is still debated, due to some well-identified limitations (such limitations originate from the need of entity authentication on the QKD public channel, the challenge of securing and validating real-life QKD systems, the lack of flexibility, the costs and risks associated with the use of bespoke hardware equipment, and the sensitivity to denial of service attacks [26]) [10, 26]. Nonetheless, terrestrial QKD is rapidly evolving towards in-field testing and industrial prototypes [18, 27]. Conversely, the application of QKD over free-space underwater channels

is at an earlier stage. The first experiment showing free-space underwater QKD (UQKD) feasibility was carried out in 2017, at a distance of 3.3 m [28]. Furthermore, the first UQKD system implementing the complete BB84 protocol was successfully demonstrated in 2019, at a distance of 2.37 m [29]. At present, UQKD is confined to lab experiments and proof-of-concept prototypes. The current limitations of UQKD systems in terms of achievable data rates and operating distance make their use in real-life scenarios still an open problem. Nonetheless, theoretical studies and extrapolation of experimental results indicate that UQKD can be successfully achieved at distances of tens to hundreds of meters, thus rendering this technique a potentially attractive solution in various undersea applications.

1.1. Tutorial Outline and Contributions. UQKD is a multidisciplinary technology, ranging from QM and information theory, to ocean optics and underwater networking. This tutorial aims at presenting selected concepts and results from these disciplines, so as to provide the reader with a complete and homogeneous view on UQKD. Specifically, the paper focuses on the problem of distributing a secret key using free-space UQKD. We stress that the problem of using the shared secret key to securely transmit data through classic free-space underwater channels (optical or acoustic) is not covered in the tutorial.

The paper is organized as follows. Section 2 summarizes the fundamental concepts of QKD. Specifically, it presents an overview of the major QKD protocols available today, with a particular focus on BB84, owing to the specific relevance of this protocol to UQKD. For a deep and practical understanding of BB84, the reader is guided through all the steps of a simple but complete key generation example. We then discuss the performance of BB84 in terms of two fundamental indexes, i.e., the quantum bit error rate (QBER) and the secret key (SK) generation rate (SKGR), for which simple analytical bounds are given in closed form. Section 3 guides the reader through the analysis of UQKD performance limitations. In particular, we express the general bounds on QBER and SKGR as functions of typical seawater optical parameters. The underwater quantum channel is analyzed, a model used in this development is introduced and discussed, and all the steps to obtain the closed-form expressions of the UQKD performance bounds are explained. The section provides links to selected bibliographic references, offering interested readers direct access to a wider and deeper view on this subject, and then proceeds to discuss the effects of the most relevant system and channel parameters on overall performance. This session also provides a discussion about the classification of ocean waters based on their optical properties. Section 4 introduces the reader to the UQKD state-of-the-art. A thorough survey of UQKD simulation-based studies, UQKD experimental activities, and UQKD systems is presented. Finally, we briefly go through the few works on underwater continuous variable QKD techniques currently available in the literature. Section 5 introduces the challenges and prospects of UQKD. The technology readiness level (TRL) of UQKD is compared to the TRL of fiber cable and satellite QKD. We also identify and discuss some UQKD ancillary functions, such as pointing acquisition and tracking (PAT) and synchronization, which are mandatory for the practical deployment of UQKD systems at sea. We then discuss the problem of providing authentication capabilities over the underwater QKD public channel. Section 6 outlines the conclusions of this work.

2. QKD Fundamentals

In this section, we offer a concise survey of the most extensively studied and promising QKD protocols, with a particular emphasis on the popular BB84 protocol. Subsequently, we present a numerical illustration and define QBER and SKGR as two pivotal performance metrics in this domain.

2.1. QKD Protocols. Based on the wave-particle duality of light, discrete variable or continuous variable protocols can be developed, which treat light either as photons or waves. Discrete variable QKD protocols exploit the particle nature of light and encode information at the single photon state. Continuous variable QKD protocols build upon the wave nature of light and encode information onto its amplitude and/or phase.

Discrete variable QKD schemes are of two types, specifically, prepare and measure (PaM) protocols and entanglement-based (EB) protocols [30]. The earliest QKD protocols utilized the PaM method, which involves creating a qubit (in quantum computing, a quantum bit (qubit) is the counter-representations of classical bit. Unlike a classical bit which can be either 0 or 1, a qubit is a superposition of 0 and 1) state and subsequently transmitting it to the recipient party. These types of approaches require that one legitimate party possesses a trusted device to send the qubits and has access to a true random number generator to originate the initial bit string [31]. Subsequently, EB protocols emerged, in which two parties can originate the secret key by performing measurements on a shared quantum state [7]. This approach does not require that one communicating node possesses the joint state source, nor that this source is trusted. In fact, the quantum correlations between the measurements performed by the legitimate parties on the joint states can be tested, by using the inequalities given by Bell's theorem (for the sake of simplicity, the authors briefly summarize here Bell's theorem version based on the so-called Clauser–Horne–Shimony–Holt (CHSH) inequality [7]. The Bell theorem assumes that Alice and Bob perform repeated independent measurements on a sequence of joint states, each choosing randomly one out of two possible measurement setups. Assuming that (i) the observed physical quantities exist independently of observation (realism), and (ii) Alice's measurements do not influence Bob's measurements and vice versa (locality), one can evaluate a statistical index S as a function of the obtained measurement correlations, such that the CHSH inequality $S \leq 2$ is always satisfied. Conversely, using the laws of QM, one obtains $S = 2\sqrt{2}$, which is a result clearly in contrast with the CHSH inequality [7, 32]. Assumptions (i) and (ii)

together are usually referred to as local realism. Thus, QM is incompatible with the assumption of local realism. Experimental results are all in favour of QM [7]). A malicious adversary manipulating the joint states would alter such quantum correlations and could thus be detected [31, 32]. While EB protocols provide an extra layer of security since there is no need for trusted quantum source, PaM protocols are more prevalent owing to their greater simplicity. Table 1 summarizes the major QKD protocols.

The initial proposal for a QKD protocol, presented by Bennett and Brassard, has become widely recognized in academic circles as BB84 [25]. BB84 is a PaM protocol, founded on the principle of quantum coding first introduced by Wiesner [42]. It employs polarization to map information bits into orthogonal photon quantum states. It is worth noting that, besides polarization encoding, the techniques of time-phase encoding and phase encoding have also captured the interest of numerous researchers in the field. In particular, time-phase encoding in QKD involves encoding quantum states in specific time bins and using interference-based measurements to recover the time-encoded information at the receiver's end. This approach enhances security by making eavesdropping attempts detectable and enables the establishment of a secure cryptographic key between Alice and Bob. Due to the possible multiple scattering events and propagation delay of the emitted photons, time-phase encoding may be a challenging task for underwater environment [43]. Phase encoding in QKD involves encoding quantum states with specific phase information. The randomness of the phase encoding and the security properties of quantum mechanics ensure that eavesdropping efforts can be detected, allowing for the establishment of a secure cryptographic key between Alice and Bob. The main drawback of phase-encoded QKD systems is the inherent phase drift caused by environmental changes and the system's nonlinearity [44]. In this paper, we mainly focus on polarization encoding.

Initially, the transmitter (i.e., Alice) randomly chooses a random bit string. For each bit, she prepares a qubit, by selecting between the rectilinear polarization basis $\oplus$ (with polarizations 0° or $+90^\circ$, corresponding to the bit values 0 or 1, respectively), and the diagonal polarization basis $\otimes$ (-45° or $+45^\circ$, corresponding to 0 or 1). She then transmits to the legitimate receiver (i.e., Bob) the sequence of prepared qubits. Bob determines the potential incoming qubit by randomly selecting either the $\oplus$ or $\otimes$ basis. If both Alice and Bob use the same basis, they will both obtain the same bit value. If Alice sends a qubit in the $\oplus$ basis and Bob measures it using the $\otimes$ basis, there is a 50%–50% chance that Bob gets -45° or $+45^\circ$. Furthermore, if Alice sends the qubit in the $\otimes$ basis and Bob measures it using the $\oplus$ basis, there is a 50%–50% chance that Bob obtains either 0° or $+90^\circ$. After all the photons have been transmitted, Alice and Bob determine which qubits were successfully received, and which were measured in the correct bases, by exchanging messages through a public classic channel. The secure key is constructed only from those qubits that both Alice and Bob measure on the same basis. The process of retaining only the bits measured on the same basis, usually referred to as "sifting," will be described in detail in the following.

Since the BB84 protocol needs to operate at single photon level, laser pulses should be attenuated in practical implementation. These sources sometimes produce pulses containing two or more photons. In case of multiphoton emission, an adversarial eavesdropper (usually referred as Eve) is able to launch the photon-number-splitting (PNS) attack. In a PNS attack, Eve intercepts and blocks all single-photon signals. Additionally, she splits multiphoton signals by retaining one portion, and forwarding the remainders to the intended recipient. The retained photon can reveal its actual polarization to Eve, if she can perform her polarization measurement using the proper basis. To this end, Eve could keep the photons in a quantum memory and perform her measurements after Alice has publicly discussed with Bob the used bases. This way, an eavesdropper could in principle obtain full information about the generated key. The most common counter measure to protect QKD systems from PNS attacks combines BB84 with the decoy-state method [45]. The decoy-state method requires the variation of intensity during pulse generation, so as to create signal states and decoy states [46]. Decoy states were first introduced by Hwang in [35]. In 2005, Lo et al. provided the first comprehensive security proof of the decoy method, considering an infinite number of intensities [47]. In a decoy-state protocol, the sender transmits a sequence of decoy-state pulses (which do not contain any useful information) along with the signal pulse sequence. As Eve cannot discriminate between decoy states from useful signals, her attempts at performing a PNS attack result in variations in the expected yields of both the signal and decoy states. In the decoy-state protocol, Alice can originate the useful signal pulses at a higher intensity μ than in the original BB84 protocol [45]. For instance, in the UQKD system described in [48], BB84 was implemented with $\mu = 0.1$, while in the decoy-state protocol the signal pulse intensity was chosen equal to $\mu = 0.9$, with a mixture of signal and decoy-state signals equal to 50%–50%. As a result, in the experiments, the secret key generation ratio was equal to 563 kbps with the BB84 protocol, to 711 kbps with the decoy-state protocol. In general, it has been shown that [45] the decoy state can substantially increase both the distance and the key generation rate of QKD in lossy channels.

In 1992, Bennett proposed B92 protocol, i.e. a protocol with only two polarization states (i.e., 0° to encode "0" and $+45^\circ$ to encode "1") [33]. As in BB84, Bob randomly decides in which basis he will measure the qubit, i.e., in the $\oplus$ or in the $\otimes$ basis. As an example, assume Alice sends a qubit with polarization $+45^\circ$, and Bob has made the decision to take measurements of it using the $\oplus$ basis, with possible outcomes 0° or $+90^\circ$. If the measurement outcome is $+90^\circ$, Bob can infer that Alice sent the polarization state $+45^\circ$; otherwise, he will discard the qubit because the outcome is inconclusive. In a high loss environment, however, Eve could intercept and measure all the qubits sent by Alice, discarding those on which she obtained inconclusive measurements, and resending to Bob correct copies of the others. As a countermeasure to this attack, Alice and Bob can encode the phase of the qubits with respect to a strong reference pulse, also transmitted from Alice to Bob. If Eve tries to suppress the

Table 1: Major QKD protocols.

Signal type	Protocol type	Name	Year
Discrete variable QKD	Prepare and measure protocols	BB84 [25]	1984
		B92 [33]	1992
		Six-state [34]	1998
		Decoy-state [35]	2003
		SARG04 [36]	2004
	Entanglement based	E91 [37]	1991
		BBM92 [38]	1992
		MDI-QKD [39]	2012
		TF-QKD [40]	2018
		PM-QKD [41]	2018
Continuous variable QKD	Gaussian modulation		2003
	Discrete modulation		2011

strong pulse or the qubits, she will originate errors, so that she will be detected [45]. Tamaki et al. explored the security of B92 under the assumption of single-photon source in [49, 50]. Koashi also examined the B92 implementation using strong phase-reference coherent light in [51]. Additionally, it was demonstrated in [52] that B92 provides better eavesdropper detection compared to BB84.

Scarani et al. [36] proposed the SARG04 protocol which has a robust performance against PNS attacks. The SARG04 protocol uses two nonorthogonal quantum states, similar to the B92 protocol. However, the bit is encoded in the basis rather than the state in SARG04. Furthermore, in distinction to BB84, Alice does not disclose her basis to Bob. In the sifting phase, Bob reveals the bits he measured from the incoming qubits. If a bit revealed by Bob is different from the corresponding bit sent by Alice, then Alice and Bob can conclude that they used different polarization bases to prepare and measure that bit. In this case, Alice tells Bob to accept the bit, and Bob chooses the bit value associated to the basis that he did not use in that measurement. This protocol was further generalized to n quantum states in [53].

In [34], Bruß presented a six-state protocol that utilizes three conjugate bases. Such states lie on the positive and negative directions of the x-, y-, and z-axes on the Bloch sphere (the Bloch Sphere is a unit three-dimensional sphere that effectively visualizes the state of any qubit. In the Bloch Sphere, qubit "0" and "1" usually lie on the z-axis, with coordinates $(x, y, z) = (0, 0, 1)$ and $(x, y, z) = (0, 0, -1)$, respectively). It was shown that this protocol is more secure than BB84 protocol since Eve possesses less mutual information. However, the key distribution rate is reduced by 2/3 compared to 1/2 reduction in BB84 [54].

Bennett, Brassard, and Mermin developed BBM92, a version of BB84 based on entanglement [38]. In this protocol, Alice and Bob carry out measurements on the photons received from a central source. If they use the same basis, they will obtain perfectly correlated results. However, if they choose different bases (for example, Alice chooses $\otimes$ and Bob chooses $\oplus$), their results will not match. Waks et al. analyzed the security of BBM92 against individual attacks, considering a realistic and untrusted source, in [55]. They showed that BBM92 has the same average collision probability as BB84, but it can achieve a higher data rate. The key advantage of BBM92 is that Alice and Bob can detect Eve's malicious interference with the source. It is worth mentioning that the requirement of a trustworthy central source for producing entangled photons is not necessary.

Ekert introduced the E91 protocol [37] by utilizing the generalized Bell's theorem to detect eavesdropping. In E91, a central source sends a series of shared states to Alice and Bob. The following are the definitions of two compatible cases: (1) if Alice (Bob) measures spin up, Bob (Alice) measures spin down; (2) if Alice (Bob) measures spin down, then Bob (Alice) measures spin up. We stress that the measurement order is irrelevant, i.e., whoever measures the first pair will cause the other to collapse accordingly. E91 allows for the detection of Eve by determining whether Alice and Bob's measurement results are perfectly correlated or not. Ekert originally proposed the use of three bases both for Alice (0°, 45°, and 90°) and for Bob (45°, 90°, and 135°), with a probability of measurements with compatible bases equal to 1/3. Like the BB84 protocol, Alice and Bob publicly announce their chosen bases and discard any results obtained from incompatible bases. In a study by Ilic [56], various aspects of error correction, privacy amplification, and violations of Bell's theorem were explored in the context of the E91 protocol. Acin et al. [57] proposed a simplified version of the E91 protocol, where it only involves three bases on one side (e.g., Alice's) and two bases on the other side (e.g., Bob's). A comparative summary of aforementioned QKD protocols is provided in Table 2.

To overcome the secret key capacity of the lossy communication channel [58], known as the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound, the measurement-device-independent (MDI)-QKD protocol has been proposed. This protocol is built upon the concept of correlating measurements of a two-photon state [39]. Despite the technical challenges in practical experiments, the transmission distance of MDI-QKD has almost doubled compared to BB84 [40]. Two variations of MDI-QKD protocols are twin-feld- (TF-) QKD [40] and phase-matching- (PM-) QKD [41] which were proposed to improve the key rate. TF-QKD and PM-QKD share fundamental similarities; TF-QKD pertains to the states used for carrying the keys, while PM-QKD concerns the methodology behind key generation. Based on such results, recent

Table 2: Comparative summary of discrete QKD protocols.

Protocol	Basis	Number of basis	Number of bases states
BB84	Orthogonal	2	4
E91	Nonorthogonal	3	5
BBM92	Orthogonal	2	4
B92	Nonorthogonal	1	2
Six-state	Conjugate	3	6
SARG04	Orthogonal	2	4

research efforts have significantly contributed to narrow the discrepancy between the theoretical security of QKD systems and their practical implementation. In [59], the authors prove the practical security of a four-phase (FP) MDI-QKD protocols against all possible practical flaws of the used photon source. Moreover, they prove the feasibility of the proposed technique through a proof-of-principle implementation of the presented protocol. To further improve the performance of MDI-QKD and simplify its practical implementation, a new variant called asynchronous MDI-QKD has been recently proposed. With respect to TF-QKD, asynchronous MDI-QKD does not require stringent phase tracking capabilities; hence, it is easier to implement and can also extend the maximum achievable distance in fibre-cable QKD networks [60–64].

Continuous variable QKD protocols transmit information using light instead of single photons. The idea was proposed separately by Ralph [65] and Hillery [66]. A continuous version of the BB84 protocol was introduced in [66] that uses squeezed states of light and homodyne detection. Leverrier and Grangier [67] suggested two continuous variable QKD protocols that use discrete modulation and involve two or four coherent states. In [68], Brádler et al. introduce a protocol using ternary-phase-shift keying (TPSK) of coherent states with homodyne detection as an alternative to an earlier protocol using binary-phase-shift keying (BPSK) [69]. Later, in [70], Guo et al. propose a method to boost the maximum secret key rate in eight-state continuous variable quantum key distribution by utilizing optical amplifiers to mitigate imperfections in Bob's equipment with the cost of a minor reduction in transmission range. They further investigate the effectiveness of two types of amplifiers, phase-insensitive amplifiers and phase-sensitive amplifiers, both of which yield approximately equivalent performance enhancements in the eight-state continuous variable QKD system. Recently, Papanastasiou and Pirandola [71] introduced a continuous variable QKD protocol that employs a discrete-alphabet encoding method. In [72], the authors propose a homodyne detection protocol using quadrature phase shift keying, with better tolerance to excess noise.

Most QKD protocols use binary signal formats, represented by qubits, i.e., by two-dimensional quantum systems. To utilize higher dimensional quantum states, orbital angular momentum (OAM) has been applied in designing QKD systems [73, 74]. These systems use quantum states belonging to a higher dimensional Hilbert space, represented by qudits instead of qubits. Different QKD protocols have been demonstrated in successful experiments with different transmission ranges and data rates, as discussed in [75] and references therein.

2.2. BB84 Protocol. As an example to illustrate the principles of QKD, we consider the BB84 protocol, which is also commonly used in commercial QKD products. The schematic diagram in Figure 1 shows a typical QKD transmitter and receiver implementing BB84.

At the transmitter side, a random bit sequence is mapped to a pulse sequence with an average power of n_S photons per pulse. The already introduced rectilinear $\oplus$ and diagonal $\otimes$ polarization bases are used in the encoding phase. The transmitted polarized photons travel through the propagation medium, which might be a wireline or wireless channel. Figure 1(b) illustrates the QKD receiver. In the shown scheme, after filtering against background light, Bob utilizes a passive 50 : 50 beam splitter (BS) to randomly send the received photons towards two different paths. On each path, a polarizing beam splitter (PBS) is connected to two single-photon avalanche photodiodes (APDs), which work in Geiger-mode to count photons. Let γ denote the fraction of received photons at the receiver side. The average signal power per pulse entering each PBS is $\gamma n_S/2$ photons/pulse. The half-wave plate (HWP) in the vertical path properly adjusts the incoming photon polarization, so that the same APDs can be used to detect both bases ($\oplus$ and $\otimes$) of the system.

If a polarized photon entering a PBS and the PBS itself share the same polarization basis, the incoming photon will be systematically forwarded to the designated APD. Consequently, the entire average signal power $p_1 = \gamma n_S/2$ will be forwarded to such APD, while the second APD on the same path will receive a null average signal power $p_2 = 0$. Conversely, if the polarization bases of the incoming photon and of the selected PBS are different, the photon will randomly proceed towards one of the two APDs. In this case, the average signal power will be equally split, resulting in an average signal power of $p_3 = \gamma n_S/4$ at the input of both APDs. In practice, aside from any potential interference by Eve, the raw key also includes errors due to background noise and dark counts in Bob's detectors. The background noise n_B per polarization affects the transmitted pulses, and each APD experiences dark-count noise with an average power of n_D, resulting in an average noise power of $n_N = n_D + n_B/2$ for each APD. The overall average signal power before reaching to an APD can therefore be expressed as

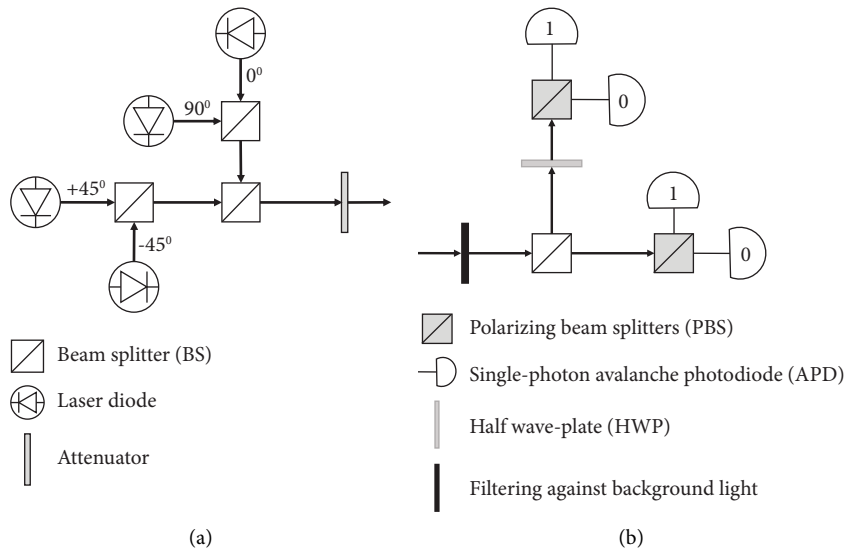

Figure 1: Schematic diagram of transmitter and receiver for the BB84 QKD system. (a) Transmitter. (b) Receiver.

$$a_i = p_i + n_N, \tag{1}$$

where $i \in \{1, 2, 3\}$.

Alice and Bob create a secure key from the bits received during instances where both parties selected the same basis and only one of the two APDs detected a photon. These instances are referred to as "sift" events. Alice and Bob are able to determine the sift events by informing each other of the basis they selected, without revealing the value of their raw keys, through a publicly accessible classical communication channel (e.g., optical or acoustic signaling for underwater use). Any data obtained using different bases is discarded. To assess the system's security against potential eavesdropping, a subset of the sifted key is used to estimate the QBER. If the estimated QBER is suitable for cryptography, the key is established; otherwise, the QKD system ends the key exchange. To ensure that both Alice and Bob have uniform keys, they use public information exchanged over the classic channel to correct errors in the sifted keys. The amount of disclosed information about the key can be reduced to maintain privacy through privacy amplification techniques, but this comes at the cost of key length.

2.3. Numerical Example. As a numerical example to demonstrate how the BB84 protocol works, consider a raw key with the length of 100 bits (see Table 3). Alice prepares the raw key in the form of a bit sequence which is mapped to the pulse sequence (according to the polarization rule) having an average power of $n_S = 1$ photon/pulse. Then, the prepared qubits are sent to Bob through the propagation medium. Due to imperfections associated with the medium, Bob only receives a certain fraction of transmitted photons. The ND notation in Table 3 indicates "no detection" and represents the qubit that has not arrived at Bob side and therefore cannot be detected by the APDs. The corresponding bit is therefore not available at Bob's side, i.e., NA. For the sake of readability, in Table 3, the rectilinear basis ⊕ is indicated as H/V, while the diagonal basis ⊗ is indicated as *D*.

As defined in the previous section, the sifted events are the bit intervals where both Alice and Bob use the same bases for the measurement. Table 4 represents the sift events extracted from Table 3 where the compatible bases are indicated by a yellow box. It can be noted that, in this example, $100 - 52 = 48$ bits were discarded, i.e., almost half of the transmitted bits.

The next step is to estimate the QBER to determine whether the secure key can be established, or the key exchange should be restarted/terminated. In this phase, Alice and Bob announce the value of some measured bits. In this example, we choose 13 qubits (out of 52 sifted bits) for this purpose, which are indicated by a yellow box in Table 4. In this subset, only one measured bit is wrong (bit interval 40). The estimated QBER can then be calculated as $\text{QBER}_{\text{estimate}} = 1/13 = 0.07$. It is widely acknowledged that the BB84 protocol can withstand a complex quantum attack if the QBER is below 0.11 [45]. In our example, this condition is satisfied; therefore the QKD protocol continues to generate the shared key. These 13 qubits used to estimate the QBER are deleted to prevent data leakage.

The process continues with the rest of sifted keys, i.e., $52 - 13 = 39$ bits (see Table 5). In this example, we employ a simple error detection scheme. Alice and Bob calculate the parity bits every 3 bits and announce these values to each other. The parity bit ensures that the total number of 1-bits in the string is even. For example, consider the first 3 bit intervals, i.e., 3, 5, and 9 where their corresponding bit value is "110" and "100" for Alice and Bob, respectively. As a result, the corresponding parity bit for Alice is 0 while it is calculated as 1 from the Bob's measurement which indicates the error occurrence. The error detection is unable to correct the error, and Alice and Bob simply discard the bits with inconsistent parity bits.

Table 3: The shared raw key between Alice and Bob. The yellow boxes indicate the compatible bases.

Bit interval	Alice		Bob		Bit interval	Alice		Bob	
	Bit	Basis	Basis	Bit		Bit	Basis	Basis	Bit
1	0	H/V	D	0	51	0	D	D	0
2	0	D	D	0	52	0	H/V	D	0
3	1	H/V	H/V	1	53	1	D	H/V	1
4	0	H/V	ND	NA	54	1	D	D	1
5	1	D	D	0	55	1	H/V	D	0
6	0	H/V	D	0	56	0	D	D	1
7	1	D	H/V	1	57	1	H/V	H/V	1
8	1	D	H/V	1	58	1	D	H/V	1
9	0	D	D	0	59	0	H/V	ND	NA
10	1	H/V	D	1	60	1	H/V	D	1
11	0	H/V	H/V	0	61	0	D	H/V	0
12	1	D	D	1	62	1	H/V	D	0
13	1	H/V	D	1	63	1	H/V	D	1
14	1	D	H/V	1	64	1	D	H/V	1
15	0	H/V	H/V	0	65	1	H/V	H/V	1
16	0	D	H/V	0	66	0	H/V	H/V	0
17	1	D	D	1	67	1	D	D	1
18	0	H/V	D	0	68	0	D	D	0
19	1	D	D	1	69	1	H/V	ND	NA
20	1	H/V	H/V	1	70	1	D	H/V	1
21	1	D	D	1	71	1	D	D	1
22	0	H/V	H/V	0	72	0	H/V	H/V	0
23	0	D	D	0	73	0	D	D	0
24	1	D	ND	NA	74	1	H/V	H/V	1
25	0	H/V	D	0	75	0	H/V	D	0
26	0	D	D	0	76	0	D	H/V	1
27	0	D	D	0	77	0	H/V	H/V	1
28	1	H/V	H/V	1	78	1	D	H/V	1
29	0	H/V	D	0	79	0	H/V	ND	NA
30	1	H/V	H/V	1	80	1	H/V	H/V	1
31	0	D	D	0	81	0	D	D	0
32	1	H/V	H/V	1	82	1	D	H/V	1
33	1	D	H/V	1	83	1	D	D	1
34	0	H/V	D	0	84	0	H/V	H/V	0
35	1	D	D	1	85	1	D	D	1
36	0	D	H/V	0	86	0	D	H/V	0
37	1	H/V	D	0	87	1	H/V	D	0
38	1	H/V	ND	NA	88	1	D	D	1
39	1	D	H/V	1	89	1	D	H/V	1
40	0	H/V	H/V	1	90	1	D	D	1
41	0	D	H/V	0	91	0	H/V	D	0
42	1	D	D	1	92	1	D	H/V	1
43	0	H/V	D	0	93	0	H/V	H/V	0
44	0	D	D	0	94	1	H/V	H/V	1
45	1	H/V	H/V	1	95	1	D	D	1
46	1	D	D	1	96	0	D	H/V	1
47	1	H/V	H/V	1	97	0	H/V	H/V	0
48	0	H/V	D	0	98	0	D	H/V	0
49	1	D	H/V	1	99	1	D	D	1
50	0	D	D	0	100	0	H/V	D	0

Table 6 represents the 30 bit long shared key after performing the error detection process. Now, the privacy amplification is performed on the error-free bits. In this example, we simply discard the middle bit of every 3 consecutive bits used in the error detection process to cancel any further possible information obtained by Eve. The final shared error-free key is presented in Table 7, with size equal to 20 bits. The SKGR in this example becomes $R = 0.38$ since there are 20 shared error-free key out of 52 sifted key.

2.4. QBER and SKGR Performance. In the performance evaluation of QKD protocols, two key metrics are QBER and SKGR. QBER is calculated as the ratio between the number of incorrectly decoded bits and the bit length of the overall sifted key. SKGR is given by the difference between the

Table 4: The sifted key. The yellow boxes indicate the qubits for QBER estimation.

Bit interval	Alice		Bob		Bit interval	Alice		Bob	
	Bit	Basis	Basis	Bit		Bit	Basis	Basis	Bit
2	0	D	D	0	50	0	D	D	0
3	1	H/V	H/V	1	51	0	D	D	0
5	1	D	D	0	54	1	D	D	1
9	0	D	D	0	56	0	D	D	1
11	0	H/V	H/V	0	57	1	H/V	H/V	1
12	1	D	D	1	65	1	H/V	H/V	1
15	0	H/V	H/V	0	66	0	H/V	H/V	0
17	1	D	D	1	67	1	D	D	1
19	1	D	D	1	68	0	D	D	0
20	1	H/V	H/V	1	71	1	D	D	1
21	1	D	D	1	72	0	H/V	H/V	0
22	0	H/V	H/V	0	73	0	D	D	0
23	0	D	D	0	74	1	H/V	H/V	1
26	0	D	D	0	77	0	H/V	H/V	1
27	0	D	D	0	80	1	H/V	H/V	1
28	1	H/V	H/V	1	81	0	D	D	0
30	1	H/V	H/V	1	83	1	D	D	1
31	0	D	D	0	84	0	H/V	H/V	0
32	1	H/V	H/V	1	85	1	D	D	1
35	1	D	D	1	88	1	D	D	1
40	0	H/V	H/V	1	90	1	D	D	1
42	1	D	D	1	93	0	H/V	H/V	0
44	0	D	D	0	94	1	H/V	H/V	1
45	1	H/V	H/V	1	95	1	D	D	1
46	1	D	D	1	97	0	H/V	H/V	0
47	1	H/V	H/V	1	99	1	D	D	1

Table 5: The remaining sifted key after discarding the bits used for QBER estimation.

Bit interval	Alice		Bob		Bit interval	Alice		Bob	
	Bit	Basis	Basis	Bit		Bit	Basis	Basis	Bit
3	1	H/V	H/V	1	51	0	D	D	0
5	1	D	D	0	56	0	D	D	1
9	0	D	D	0	57	1	H/V	H/V	1
12	1	D	D	1	65	1	H/V	H/V	1
15	0	H/V	H/V	0	67	1	D	D	1
17	1	D	D	1	68	0	D	D	0
20	1	H/V	H/V	1	71	1	D	D	1
21	1	D	D	1	73	0	D	D	0
22	0	H/V	H/V	0	74	1	H/V	H/V	1
26	0	D	D	0	77	0	H/V	H/V	1
27	0	D	D	0	81	0	D	D	0
28	1	H/V	H/V	1	83	1	D	D	1
31	0	D	D	0	84	0	H/V	H/V	0
32	1	H/V	H/V	1	88	1	D	D	1
35	1	D	D	1	90	1	D	D	1
42	1	D	D	1	93	0	H/V	H/V	0
44	0	D	D	0	95	1	D	D	1
45	1	H/V	H/V	1	97	0	H/V	H/V	0
47	1	H/V	H/V	1	99	1	D	D	1
50	0	D	D	0					

mutual information shared by Alice and Bob and the information that Eve might have obtained about the key [76]. In the following, we present the derivations of QBER and SKGR.

Let the polarization of the transmitted qubit be represented by x. Furthermore, let y denote the polarization of an APD, i.e., $x, y \in \{0^\circ, 90^\circ, +45^\circ, -45^\circ\}$ [77]. Table 8 summarizes the average signal power that any APD in the scheme of Figure 1 can receive. In that table, η is the quantum efficiency of Geiger-mode APDs, while the received average signal power A_i is obtained by multiplying η by the PBS output average signal power a_i, which is given by (1).

Table 6: The remaining sifted key after performing error detection.

Bit interval	Alice		Bob		Bit interval	Alice		Bob	
	Bit	Basis	Basis	Bit		Bit	Basis	Basis	Bit
12	1	D	D	1	47	1	H/V	H/V	1
15	0	H/V	H/V	0	50	0	D	D	0
17	1	D	D	1	51	0	D	D	0
20	1	H/V	H/V	1	67	1	D	D	1
21	1	D	D	1	68	0	D	D	0
22	0	H/V	H/V	0	71	1	D	D	1
26	0	D	D	0	81	0	D	D	0
27	0	D	D	0	83	1	D	D	1
28	1	H/V	H/V	1	84	0	H/V	H/V	0
31	0	D	D	0	88	1	D	D	1
32	1	H/V	H/V	1	90	1	D	D	1
35	1	D	D	1	93	0	H/V	H/V	0
42	1	D	D	1	95	1	D	D	1
44	0	D	D	0	97	0	H/V	H/V	0
45	1	H/V	H/V	1	99	1	D	D	1

Table 7: The shared error-free key.

Bit interval	Alice		Bob		Bit interval	Alice		Bob	
	Bit	Basis	Basis	Bit		Bit	Basis	Basis	Bit
12	1	D	D	1	47	1	H/V	H/V	1
17	1	D	D	1	51	0	D	D	0
20	1	H/V	H/V	1	67	1	D	D	1
22	0	H/V	H/V	0	71	1	D	D	1
26	0	D	D	0	81	0	D	D	0
28	1	H/V	H/V	1	84	0	H/V	H/V	0
31	0	D	D	0	88	1	D	D	1
35	1	D	D	1	93	0	H/V	H/V	0
42	1	D	D	1	95	1	D	D	1
45	1	H/V	H/V	1	99	1	D	D	1

Table 8: The average signal power received by the APDs at Bob's side.

Basis and polarization of transmitted and detected photons	The average received power A_i (photons/pulse), $i \in \{1,2,3\}$
$x = y$	$A_1 = \eta(\gamma n_S/2 + n_N)$
$x \neq y$ and $x, y \in \oplus$	$A_2 = \eta n_N$
$x \neq y$ and $x, y \in \otimes$	$A_2 = \eta n_N$
$x \in \oplus$ and $y \in \otimes$	$A_3 = \eta(\gamma n_S/4 + n_N)$
$x \in \otimes$ and $y \in \oplus$	$A_3 = \eta(\gamma n_S/4 + n_N)$

The probability that a pulse contains m photons is provided by the Poisson distribution as $P_\mu(m) = e^{-\mu}\mu^m/m!$ where μ denotes the mean value. Accordingly, the probability of detecting $m = 0$ or $m = 1$ photon in a given pulse can be represented as $P_\mu(0) = e^{-\mu}$ and $P_\mu(1) = \mu e^{-\mu}$, respectively. The sift event can occur in two cases, i.e., error-free sift and erroneous sift events. In the first case, both detectors connected to one of the two PBSs shown in Figure 1 register a photon count of $m = 0$. Specifically, this occurs on the receiver path where the PBS polarization basis and the incoming photon polarization basis are different. Meanwhile, on the other path (where the PBS and the incoming photon polarization bases match), one of the detectors registers a photon count of $m = 1$, while the other one, with differing polarization with respect to the photon, registers a photon count of $m = 0$. As a result, the probability in the case of an error-free sift event can be calculated as

$$\begin{aligned} P_{\text{case1}} &= [P(m=0|A_3)]^2 P(m=1|A_1) P(m=0|A_2) \\ &= e^{-\eta(\gamma n_S + 4n_N)} \eta\left(\frac{\gamma n_S}{2} + n_N\right), \end{aligned} \tag{2}$$

where A_i, with $i \in (1,2,3)$ can assume the values reported in Table 8. In the second case (erroneous sift event), $m = 1$ photon is detected by the APD with the same basis but a different polarization with respect to the incoming photon. Concurrently, the other APD on that path, with the same polarization as the transmitted photon, erroneously detects $m = 0$ photon, while the two APDs on the other path both detect $m = 0$ photon. The error probability $P_{\text{error}} = P_{\text{case2}}$ can be calculated as

$$\begin{aligned} P_{\text{case2}} &= [P(m=0|A_3)]^2 P(m=0|A_1) P(m=1|A_2) \\ &= e^{-\eta(\gamma n_S + 4n_N)} \eta n_N. \end{aligned} \tag{3}$$

The definition of QBER is the error rate in the sifted key, which can be computed as

$$\text{QBER} = \frac{P_{\text{error}}}{P_{\text{sift}}} = \frac{P_{\text{case2}}}{P_{\text{case1}} + P_{\text{case2}}}. \tag{4}$$

Replacing (2) and (3) in (4), we obtain

$$\text{QBER} = \frac{n_N}{\gamma n_S/2 + 2n_N}. \tag{5}$$

As earlier discussed, the BB84 protocol is assumed to be secure against advanced quantum attacks if the QBER value is below 0.11 [45].

In Figure 2, we plot the QBER in (5) as a function of the fraction of received photons (i.e., γ) for an atmospheric channel. We assume $n_S = 1$, $n_B = 10^{-3}$, and $n_D = 10^{-6}$ [78]. As expected, QBER decreases as γ increases. The amount of captured photons is greatly affected by various channel effects, including diffraction, atmospheric turbulence, and losses caused by absorption and scattering. For the sake of simplicity, we assume here that the channel is affected only by attenuation loss (the impact of diffraction and turbulence will be considered in Section 3, in the analysis of the underwater quantum channel). The path loss can be taken into account by the Beer–Lambert law, so that

$$\gamma = \exp[-L\alpha], \tag{6}$$

where L and α denote link distance and extinction coefficient, respectively. Figure 3 illustrates the QBER versus the link distance for $\alpha = 2$ dB/km, i.e., for an atmospheric channel operating in clear weather conditions, with visibility of 10 km [78]. As the link distance increases, the effect of path loss becomes more noticeable, thus increasing the QBER.

The mathematical representation of SKGR can be obtained by modeling the BB84 quantum channel as a binary symmetric channel (BSC), with a QBER crossover probability. The entropy function determines the smallest amount of Shannon information that Alice and Bob must exchange

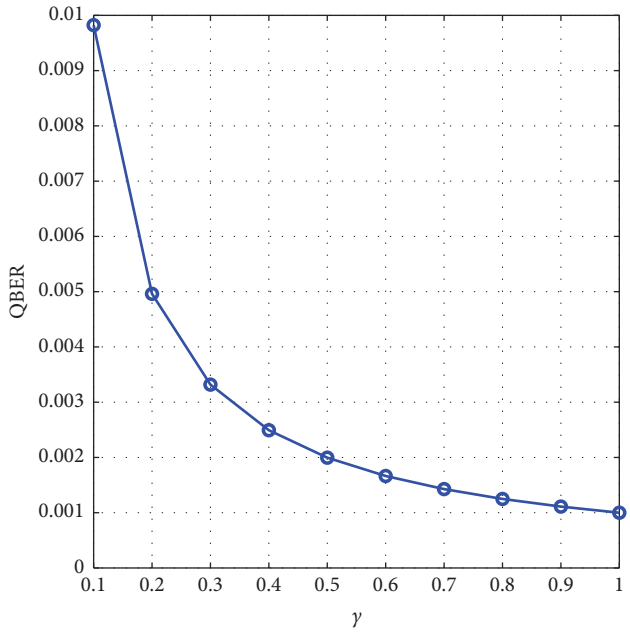

Figure 2: QBER versus the fraction of received photons (i.e., γ).

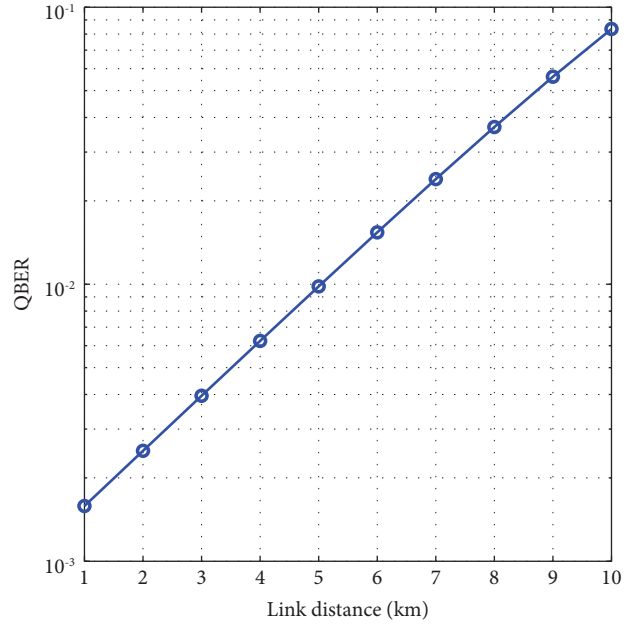

Figure 3: QBER versus link distance.

through a public channel to attain key bit strings that are completely correlated. The entropy function

$$h(\text{QBER}) = -\text{QBER}\log_2(\text{QBER}) - (1-\text{QBER})\log_2(1-\text{QBER}), \quad (7)$$

in fact, accounts for the uncertainty of the legitimate receiver about the sender key string, due to possible transmission errors in the quantum channel [79]. Thus, the sender must disclose through the public channel an equivalent amount of information to let the receiver correct the wrongly received bits. The fraction of perfectly correlated secret bits after the error correction phase will then be $1 - h(\text{QBER})$, which formally corresponds to the mutual information $I(A;B)$ between Alice's and Bob's raw keys [79]. To destroy the additional amount of information that Eve could have gained about the key from the transmitted photons, a fraction I_E of bits must be further removed from $I(A;B)$. Under the assumption of single-photon source, it can be shown that the maximum information achievable by Eve is $I_{E,\text{MAX}} = h(\text{QBER})$ [79]. Finally, SKGR for BB84 can be expressed as (a similar analysis can be performed for the more realistic case of nonsingle photon source and the decoy-state protocol. The interested reader can find the details in [79]):

$$\text{SKGR} = \max(0, R), \quad (8)$$

where the rate R is

$$R = I(A;B) - I_{E,\text{MAX}} = 1 - (1+f)h(\text{QBER}). \quad (9)$$

In (9), $f > 1$ is a parameter accounting for the efficiency of the adopted reconciliation algorithm, and its value is dependent on the error correction code used [79]. Any practical error correction technique, in fact, will require an amount of information greater than $h(\text{QBER})$ to reconcile the raw keys. In the ideal case, i.e., setting $f = 1$ in (9), Eve's information $I_{E,\text{MAX}}$ equals Alice's and Bob's mutual information $I(A;B)$ when $\text{QBER} \geq 0.11$. This QBER value corresponds to the BB84 security threshold already introduced in subsection 2.3. When the quantum channel QBER is higher than this value, any bit shared by Alice and Bob can be known to Eve, and no secure bit can be produced (i.e., $R = 0$). A critical design choice is the type of error correction that determines the reconciliation efficiency of f. As an example, take into account the use of Low Density Parity Check (LDPC) codes, which have been optimized on BSCs, for the error reconciliation phase [79]. The reconciliation efficiency parameter can expressed as [80]

$$f = \frac{1 - R_c}{h(\text{QBER}_{\text{th}})}, \quad (10)$$

with R_c denoting the code rate. Here, the highest possible value of QBER that can be corrected when the length of the code becomes infinite is represented by QBER_{th}. Table 1 in [79] lists the code rates and threshold QBER values for optimized LDPC codes. Under the assumption of LDPC codes, the rate R in (9) takes the form of

$$R = 1 - \left(1 + \frac{1 - R_c}{h(\text{QBER}_{\text{th}})}\right) h(\text{QBER}). \quad (11)$$

3. The Underwater Quantum Channel

Section 2.4 has presented derivations for QBER and SKGR in a generic quantum channel. This section will now provide closed-form bounds for these parameters when applying the BB84 protocol in free-space underwater channels. We consider the impact of diffraction, turbulence, path loss, and other important factors, as reported in studies [81, 82]. We

will then analyze and discuss the effects of various channel and system parameters on the performance of UQKD to practically demonstrate the utility of the provided analytical tools.

3.1. QBER and SKGR Evaluation in Underwater Quantum Channels. Assume that Alice sends her key bit string to Bob by transmitting a normalized beam pattern from a circular exit pupil, denoted as P_0, with a diameter of d_{TX} located on the $z = 0$ plane through a free-space underwater quantum channel. The average photon number to represent a bit value is n_S. On the receiving end, Bob collects a fraction γ of the photons from Alice using a pupil P_1 with diameter d_{RX} located at the plane $z = L$. The reduction in the number of photons collected by Bob, quantified by the fraction γ, is caused by various impairments originating in the underwater environment. Additionally, Bob's receiver will detect an average of n_N noise photons reaching each detector. As discussed in Section 2.4, the secret key transmission performance can be assessed by evaluating the corresponding QBER. To this end, however, we must first evaluate γ and n_N for the quantum underwater channel.

3.1.1. Evaluation of γ. To determine γ, we will consider the impact of diffraction, turbulence, and path loss on the free-space underwater quantum channel (other system impairments related to, e.g., synchronization and alignment, are beyond the scope of this paper and can be found in [45]). We assume that, for laser diode transmitters with collimated light sources, the impact of geometrical loss is negligible, and the path loss only depends on the attenuation loss due to absorption and scattering. Let $\sqrt{P_T}u_0(\mathbf{r})$, $\mathbf{r} \in P_0$, be the optical pattern sent by Alice from her pupil P_0, where P_T is the transmitted power in photons/s, and

$$\int_{P_0} d\mathbf{r}\left|u_0(\mathbf{r})\right|^2 = 1. \tag{12}$$

Based on the extended Huygens–Fresnel principle and the paraxial approximation, the received optical pattern $u(\boldsymbol{\rho})$ at Bob's pupil P_1 is

$$u(\boldsymbol{\rho}) = \sqrt{P_T}\int_{P_0} d\mathbf{r}u_0(\mathbf{r})h(\mathbf{r},\boldsymbol{\rho}), \tag{13}$$

where $\boldsymbol{\rho} \in P_1$, while $h(\mathbf{r},\boldsymbol{\rho})$ is the underwater quantum channel impulse response for a monochromatic waveform of wavelength λ and wavenumber $k = 2\pi/\lambda$ propagating from $z = 0$ to $z = L$ through a turbulent environment, i.e., [77]

$$h(\mathbf{r},\boldsymbol{\rho}) = \sqrt{A(L)}\cdot\frac{e^{\mathrm{jkL}+jk(\mathbf{r}-\boldsymbol{\rho})^2/2L}}{j\lambda L}\cdot e^{\psi(\mathbf{r},\boldsymbol{\rho})+j\chi(\mathbf{r},\boldsymbol{\rho})}. \tag{14}$$

In (14), $A(L)$ is the attenuation loss in the path from $z = 0$ to $z = L$; the second fractional term is the deterministic impulse response of a loss-less, nonturbulent underwater quantum channel, and accounts for diffraction [83]. Finally, $\psi(\mathbf{r},\boldsymbol{\rho})$ and $\chi(\mathbf{r},\boldsymbol{\rho})$ model the random log-amplitude and phase fluctuations induced by turbulence, which (in the weak-turbulence regime) can be described as jointly Gaussian random processes with known first and second moments [77]. The fraction γ of useful photons captured at Bob's side can be obtained from (13) and (16) as

$$\gamma = \frac{\int_{P_1} d\boldsymbol{\rho}|u(\boldsymbol{\rho})|^2}{P_T} = \int_{P_1} d\boldsymbol{\rho}\left|\int_{P_0} d\mathbf{r}u_0(\boldsymbol{\rho})h(\boldsymbol{\rho},\mathbf{r})\right|^2. \tag{15}$$

In the presence of turbulence γ is a random quantity, whose statistical description is very hard to evaluate. To simplify its analysis, we will follow the approach proposed in [77], and express $h(\mathbf{r},\boldsymbol{\rho})$ by its functional singular value decomposition:

$$h(\mathbf{r},\boldsymbol{\rho}) = A(L)\cdot\sum_{i=1}^{\infty}\sqrt{\mu_i}f_i(\mathbf{r})\phi_i(\boldsymbol{\rho}), \tag{16}$$

where $\mathbf{r} \in P_0$, $\boldsymbol{\rho} \in P_1$, and $1 \geq \mu_1 \geq \mu_2 \geq \ldots \geq 0$ are the modal transmittivities, $\{f_i(\mathbf{r})\}$ is a set of complete orthonormal (CON) functions in P_0 (input modes), and $\{\phi_i(\boldsymbol{\rho})\}$ is a set of CON functions in P_1 (output modes) [77, 84]. We remark that, in the presence of turbulence, μ_i, $\{f_i(\mathbf{r})\}$, and $\{\phi_i(\boldsymbol{\rho})\}$ are random quantities. By inserting (16) into (13), one can easily see that the transmission of the i-th input mode (i.e., $\sqrt{P_T}u_0(\mathbf{r}) = \sqrt{P_T}f_i(\mathbf{r})$) originates the field pattern $u(\boldsymbol{\rho}) = \sqrt{A(L)\mu_i P_T}\phi_i(\boldsymbol{\rho})$ at P_1, and the resulting fraction of captured photons (15) is $\gamma = A(L)\cdot\mu_i$. As shown in [77, 81], to find a practical lower bound on the underwater quantum channel QBER, we can limit our efforts to evaluating a lower bound on the expected value of the maximum modal transmittivity μ_1, i.e., a value μ_{turb} such that $E[\mu_1] \geq \mu_{\mathrm{turb}}$ [81]. It can be shown that

$$\mu_{\mathrm{turb}} = \frac{8\sqrt{F}}{\pi}\int_0^1 \exp\left(-W\frac{(d_{\mathrm{TX}}x, L)}{2}\right)\left(\cos^{-1}(x) - x\sqrt{1-x^2}\right)J_1(4x\sqrt{F})\mathrm{d}x, \tag{17}$$

where $F = ((\pi d_{\mathrm{TX}}d_{\mathrm{RX}})/4\lambda L)^2$ is the Fresnel number and $J_1(\cdot)$ is the first-order Bessel function of the first kind [77, 81]. The wave structure function $W(\cdot,\cdot)$ in (17) is associated with the spatial power spectrum of the refractive index [85]. For a spherical wave, a specified transmission distance of L, and a set separation distance ρ between two points on the phase front perpendicular to the axis of propagation, it is expressed as [81, 86]

$$W(\rho, L) = 1.44\pi k^2 L\left(\frac{\alpha_{\text{th}}^2 \chi_T}{\omega^2}\right)\varepsilon^{-1/3}\left(1.175\eta_K^{2/3}\rho + 0.419\rho^{5/3}\right)\left(\omega^2 + d_r - \omega\left(d_r + 1\right)\right), \tag{18}$$

where the variables within (18) are related to the characteristics of the underwater medium and defined in Table 9.

The analysis of the underwater quantum channel carried out so far has focused on the impact of diffraction and turbulence on the achievable QBER, which can be summarized by the parameter μ_{turb} given by (17) and (18). However, the most important and range-limiting effect in both quantum and classical underwater optical communications is the attenuation loss $A(L)$. In the ocean, the attenuation loss is due to the absorption and scattering of the propagating photons by water molecules, dissolved salts, and dead or decaying organic matter, and is typically characterized by the extinction parameter α. The extinction parameter is dependent on the wavelength λ, and results from the sum of the absorption coefficient $a(\lambda)$ and the scattering coefficient $b(\lambda)$, i.e., $\alpha(\lambda) = a(\lambda) + b(\lambda)$ [87, 88]. This parameter was firstly introduced in subsection 2.4, where it was generally related to the attenuation loss through the Beer–Lambert formula (6) [87]. For the underwater propagation medium, the attenuation loss can be expressed as [89]

$$A(L) = \exp\left[-\alpha L\left(\frac{d_{\text{RX}}}{\theta L}\right)^T\right], \tag{19}$$

based on a modified version of the Beer–Lambert formula. In (19), θ represents the full width of the transmitter beam divergence angle and T is a correction factor chosen according to the type of water, as described in [89]. Also, the characterization of the attenuation loss introduced by seawater can be a very challenging problem. The results of extensive studies on light attenuation in the ocean were first summarized by the Jerlov classification scheme, which has been widely used in many works in classical and quantum underwater communications. Thus, for the sake of clarity and completeness, we introduce here Jerlov's taxonomy of seawaters, together with some more recent, alternative classification schemes also used in the literature.

3.1.2. Classification of Water Types. Jerlov's classification of water types is a convenient one-parameter classification scheme to describe ocean water clarity [87, 90]. Proposed in 1951, this scheme is still used in underwater optical communications, e.g., when typical classes of water conditions are considered. Jerlov classification is based on the diffuse attenuation coefficient $K_d(\lambda, \xi)$, which is the vertical attenuation in the ocean of the spectral downward irradiance, expressed as a function of wavelength λ and depth ξ. When averaged over depth, this parameter varies in a systematic way with λ through a wide range of water bodies, from very clear to very turbid, while remaining rather insensitive to external environmental conditions [87, 90]. Consequently, Jerlov proposed to classify ocean waters into two main groups, open ocean waters and coastal waters, based on observed values of the averaged diffuse attenuation coefficient $\overline{K_d}(\lambda)$. He further split open ocean waters into types I, IA, IB, II, and III, and classified coastal waters as 1, 3, 5, 7, and 9 [87]. Type I is the clearest open ocean water, and type III is the most turbid one. Moreover, types 1 and 9 are the clearest and the most turbid coastal waters, respectively. In Table 10, the measured values of $\overline{K_d}(\lambda)$, averaged over a depth of 10 m from the sea surface and multiplied by a factor of 100 (for graphical clarity), are reported for the different water types [87]. In the table, the columns span wavelength values, while the rows correspond to the different water types. As a useful practical reference, the study [87] also provides a geographical map illustrating the distribution of Jerlov water types in the world oceans. An updated map of Jerlov's water types in the Nordic Seas is available in [91].

The relevance of Jerlov classification to UQKD relies on the fact that $\overline{K_d}(\lambda)$ typically results close to the extinction parameter α and can thus be related to the attenuation loss $A(L)$ through (6) or (19).

In [88], Mobley proposed a different classification of sea waters, based on selected measured values of the extinction parameter $\alpha(\lambda)$ at wavelengths corresponding to blue/green light. Such reference values are reported in Table 11, together with the corresponding absorption (a) and scattering (b) coefficients, for four different types of waters. In particular, the measured values given in such table were obtained at wavelength $\lambda = 514$ nm for pure sea water; at $\lambda = 530$ nm for clear ocean, coastal ocean, and turbid harbor waters. This water classification scheme has been adopted in several papers available in the literature, e.g., [82, 89, 92–94]. However, it should be remarked that some works strictly adopt the values proposed by Mobley in [88] for the extinction, absorption, and scattering parameters. Other works (e.g., [82, 89, 93, 94]), conversely, though adopting the same water types, use slightly different numeric values for those coefficients. With respect to Jerlov classification, Mobley classification applies to a narrower interval of the light spectrum, centered at wavelength $\lambda = 530$ nm. Nonetheless, it provides a significantly wider interval of extinction coefficient values, since it goes from $0.043\ \text{m}^{-1}$ for pure seawater to $2.190\ \text{m}^{-1}$ for turbid harbor water, while in Jerkov classification, the averaged diffuse attenuation coefficient $\overline{K_d}(\lambda)$ at $\lambda = 530$ nm assumes a maximum value of $0.78\ \text{m}^{-1}$ for Type 9 water.

3.1.3. Average Number of Noise Photons. To complete the analysis of the underwater quantum channel, we finally need to characterize the effect of noise photons. Bob's receiver will collect n_B background photons per polarization on average, and each of his detectors will be subject to an average equivalent dark current photon number of n_D. Background noise consists of photons that scatter into the receive aperture but are not part of the transmitting signal, while the dark current noise is caused by thermally generated

Table 9: The definition of parameters in (18).

Parameter	Definition
$k = 2\pi/\lambda$	Wavenumber
α_{th}	Thermal expansion coefficient
χ_{T}	Dissipation rate of mean-squared temperature
ω	Relative strength of temperature and salinity fluctuations
ε	Dissipation rate of turbulent kinetic energy per unit mass of fluid
η_K	Kolmogorov microscale length
d_r	Eddy diffusivity ratio

Table 10: Averaged diffuse attenuation coefficient $\overline{K_d} \times 100\,(\text{m}^{-1})$ averaged over a depth from 0 to 10 m.

Water type	Wavelength (nm)															
	310	350	375	400	425	450	475	500	525	550	575	600	625	650	675	700
I	15	6.2	3.8	2.8	2.2	1.9	1.8	2.7	4.3	6.3	8.9	23.5	30.5	36	42	56
IA	18	7.8	5.2	3.8	3.1	2.6	2.5	3.2	4.8	6.7	9.4	24	31	37	43	57
IB	22	10	6.6	5.1	4.2	3.6	3.3	4.2	5.4	7.2	9.9	24.5	31.5	37.5	43.5	58
II	37	17.5	12.2	9.6	8.1	6.8	6.2	7.0	7.6	8.9	11.5	26	33.5	40	46.5	61
III	65	32	22	18.5	16	13.5	11.6	11.5	11.6	12.0	14.8	29.5	37.5	44.5	52	66
1	180	120	80	51	36	25	17	14	13	12	15	30	37	45	51	65
3	240	170	110	78	54	39	29	22	20	19	21	33	40	46	56	71
5	350	230	160	110	78	56	43	36	31	30	33	40	48	54	65	80
7		300	210	160	120	89	71	58	49	46	46	48	54	63	78	92
9		390	300	240	190	160	123	99	78	63	58	60	65	76	92	110

Table 11: Selected reference values of absorption (a), scattering (b), and extinction (α) parameters for different water types.

Water type	a (m^{-1})	b (m^{-1})	α (m^{-1})
Pure sea water	0.0025	0.0405	0.043
Clear ocean water	0.037	0.114	0.151
Coastal ocean water	0.219	0.179	0.398
Turbid harbor water	1.824	0.366	2.190

electrons in the detector. By considering the dark current and the irradiance of the environment, the average number of noise photons reaching each of Bob's detectors can be obtained by [95]

$$n_N = \frac{n_B}{2} + n_D = \frac{1}{2}\frac{\pi E_d A \Delta t' \lambda \Delta\lambda\,(1-\cos(\Omega))}{2h_p c_{\text{light}}} + I_{\text{dc}}\Delta t, \tag{20}$$

where I_{dc} is the dark current count rate, λ is the wavelength, A is the receiver aperture area, Ω is the field of view (FoV) of the detector, h_P is Planck's constant, c_{light} is the speed of light, $\Delta\lambda$ is the filter spectral width, Δt is the bit period, and $\Delta t'$ is the receiver gate time. E_d is the irradiance of the environment and given by $E_d = E_{d,0}e^{-K_\infty \xi}$ where $E_{d,0}$ denotes the irradiance of the underwater environment at the sea surface, ξ denotes the underwater depth, and K_∞ is the asymptotic value of the spectral diffuse attenuation coefficient for spectral downwelling plane irradiance [88]. The typical total irradiances at sea level in the visible wavelength band for some atmospheric conditions are provided in [96].

3.1.4. QBER of the Free-Space Underwater Quantum Channel. Based on the lower and upper bounds for sift and error probabilities obtained in [77] over a turbulent channel, we can finally obtain a lower bound on QBER, given by [81]

$$\text{QBER} \geq \frac{\eta n_N e^{-\eta 4 n_N}\left[1-\mu_{\text{turb}}\right] + \eta n_N \exp\left[-\eta\left(n_S A(L) + 4n_N\right)\right]\mu_{\text{turb}}}{2\eta n_N e^{-\eta 4 n_N}\left[1-\mu_{\text{turb}}\right] + (\eta/2)\left(n_S A(L) + 4n_N\right)\exp\left[-\eta\left(n_S A(L) + 4n_{N|}\right)\right]\mu_{\text{turb}}}. \tag{21}$$

For the sake of clarity, we recall that, in (21), n_N is given by (20), μ_{turb} is given by (17) and (18), and $A(L)$ is given by (19). For the nonturbulent underwater path, it was shown in [81] that QBER can be approximated as

$$\text{QBER} \cong \frac{2n_N}{\mu_{\text{non-turb}} n_S l + 4n_N}, \tag{22}$$

where $\mu_{\text{non-turb}}$ represents the largest eigenvalue obtained from the singular value decomposition of the loss-less,

nonturbulent underwater quantum channel impulse response (which can be obtained from (13) with $\psi(\mathbf{r}, \boldsymbol{\rho}) = \chi(\mathbf{r}, \boldsymbol{\rho}) = 0$), as described in [97].

Alternatively, for short distance links where the Fresnel number (i.e., F) is high (as those considered in UQKD systems), one can assume $\mu_{\text{non-turb}} \approx 1$. We stress that all results relative to nonturbulent water environments presented in the following will be based on (22), with $\mu_{\text{non-turb}} = 1$. A lower bound on SKGR for the BB84 protocol can be straightforwardly calculated by replacing the upper bound on QBER (21) or (22) into (9), for turbulent or nonturbulent channels, respectively.

3.2. Effects of Channel Parameters. Based on the analytical expressions provided in the previous section, we now discuss the effect of various free-space underwater channel parameters, i.e., water type, turbulence, and atmospheric conditions, on the QBER and SKGR performance of BB84. We will consider the Mobley seawater classification, in order to be concise and to include also turbid waters as those observed in harbors. For the purpose of this study, we presume that the transmitter and receiver pupil diameters are both equal to 10 cm, FoV is $\Omega = 180^{\circ}$, and that the atmospheric conditions are clear at night with a full moon unless otherwise indicated [30]. For the sake of clarity and conciseness, Table 12 summarizes the relevant parameters used in the following examples.

3.2.1. Effects of Water Type. Figure 4 illustrates QBER and SKGR results for nonturbulent underwater environments. We consider clear ocean, coastal ocean, and turbid harbor waters as water types, and assume that a QBER less than 0.11 is targeted. Figure 4(a) shows the QBER as a function of the free-space link distance L. Under this performance metric, the achievable distances for turbid harbor, coastal ocean, and clear ocean waters are, respectively, 6.4 m, 59.3 m, and 155.4 m. This clearly demonstrates that the type of water significantly affects the performance. As the turbidity increases, the transmission distance strongly decreases. We highlight that perfect error correction has been assumed to attain the achievable distances mentioned above (i.e., $f = 1$ in (9)). To determine the achievable transmission distances using practical coding methods, the SKGR performance is shown in relation to the link length in Figure 4(b). In the error correction phase, we have used an LDPC code with rate of $R_c = 0.5$, which has been optimized for a BSC with a QBER threshold of approximately 0.11 (calculated as $\text{QBER}_{\text{th}} = 0.1071 \approx 0.11$) [79] (one should note that it is possible to utilize other LDPC codes in [79] designed for lower QBER values to improve SKGR. However, the maximum achievable distance will remain the same since the highest QBER that can be tolerated to obtain nonzero SKGR should be less than 0.11). It can be seen that a nonzero SKGR value can only be achieved over a maximum distance of 6 m in turbid water. The result is slightly lower than the achievable distance of 6.4 m obtained through the QBER analysis performed above assuming perfect error correction. Similar patterns can be seen for other water types and turbulence levels. For instance, the maximum transmission distances for coastal ocean and clear ocean water in nonturbulent conditions are 59 m and 155 m, respectively, when evaluated using SKGR and the LDPC code with rate of $R_c = 0.5$ for practical error correction. The corresponding QBER analysis, performed under the assumption of perfect error correction, gives corresponding distances of 59.3 m and 155.4 m. Thus, since the two analysis approaches reveal similar results, for the sake of simplicity in the following, we will only consider QBER as the performance metric, and we will always assume perfect error correction.

3.2.2. Effects of Turbulence. The optical signal can also be impacted by turbulence, i.e., by sudden changes in the refractive index due to ocean currents causing variations in water temperature and pressure, which leads to fluctuations in the signal known as fading. In Figure 5, we investigate the effect of turbulence on QBER using (21) and by modelling the turbulent channel based on a subset of parameters given in Table 9. We assume $\alpha_{\text{th}} = 2.56 \times 10^{-4}$ 1/deg, $\eta_k = 10^{-4}$ m, $\omega = -2.2$, $\chi_T = 10^{-5}\text{K}^2\text{s}^{-3}$, and $\epsilon = 10^{-5}\text{m}^2\text{s}^{-3}$ which corresponds to strong turbulence. It can be seen from Figure 5 that the impact of turbulence in turbid water is negligible, and the primary factor affecting the signal loss is path loss. As the clarity of the coastal and clear water increases, the distance that can be achieved also increases and the effect of turbulence becomes more apparent. For example, consider the clear ocean. The achievable distance to maintain QBER ≤ 0.11 is around 155.4 m for the case of no turbulence. This reduces to 106.7 m for strong turbulence condition. In coastal water, for the same QBER target, achievable distances are observed as 59.3 m and 53.7 m for the nonturbulent and turbulent cases, respectively.

3.2.3. Effect of Atmospheric Conditions. In Figure 6, the impact of various atmospheric conditions on the performance of the QKD system is explored. The clear ocean with high turbulence is considered and five different atmospheric conditions are taken into account. These are as follows:

(1) Scenario 1: clear atmosphere, full moon near the zenith (i.e., $E_{d,0} = 10^{-3}\text{W/m}^2$)

(2) Scenario 2: heavy overcast, sun near the horizon (i.e., $E_{d,0} = 10\,\text{W/m}^2$)

(3) Scenario 3: hazy atmosphere, sun near the horizon (i.e., $E_{d,0} = 50\,\text{W/m}^2$)

(4) Scenario 4: heavy overcast, sun at the zenith (i.e., $E_{d,0} = 125\,\text{W/m}^2$)

(5) Scenario 5: clear atmosphere, sun at the zenith (i.e., $E_{d,0} = 500\,\text{W/m}^2$)

In particular, the underwater environment irradiance E_d takes different value for each atmospheric condition, which consequently affects the background noise (cf. (20)). It can be observed from Figure 6 that the maximum transmission distance for underwater QKD systems during the day decreases significantly compared to nighttime conditions, resulting from an increase in

Table 12: System and channel parameters under consideration.

Parameter	Definition		Numerical value
R_c	Code rate		0.5 [79]
Ω	Field of view		180° [89]
$\Delta\lambda$	Filter spectral width		30 nm [95]
λ	Wavelength		530 nm [89]
Δt	Bit period		35 ns [95]
$\Delta t'$	Receiver gate time		200 ps [95]
d_{TX}	Transmitter pupil diameter		10 cm [77]
d_{RX}	Receiver pupil diameter		10 cm [77]
η	Quantum efficiency of Geiger-mode APDs		0.5 [77]
I_{dc}	Dark current count rate		60 hz [95]
K_∞	Asymptotic diffuse attenuation coefficient		0.08 m^{-1} [88]
z_d	Depth		100 m [95]
θ	Transmitter beam divergence angle		6° [89]
α	Extinction coefficient	Clear ocean	0.151 m^{-1} [94]
		Coastal ocean	0.339 m^{-1} [94]
		Turbid harbor	2.195 m^{-1} [94]
T	Correction coefficient	$\theta = 6°$, $d_{TX} = 5$ cm	0.13 [89]
		$\theta = 6°$, $d_{TX} = 10$ cm	0.16 [89]
		$\theta = 6°$, $d_{TX} = 20$ cm	0.21 [89]
		$\theta = 6°$, $d_{TX} = 30$ cm	0.26 [89]

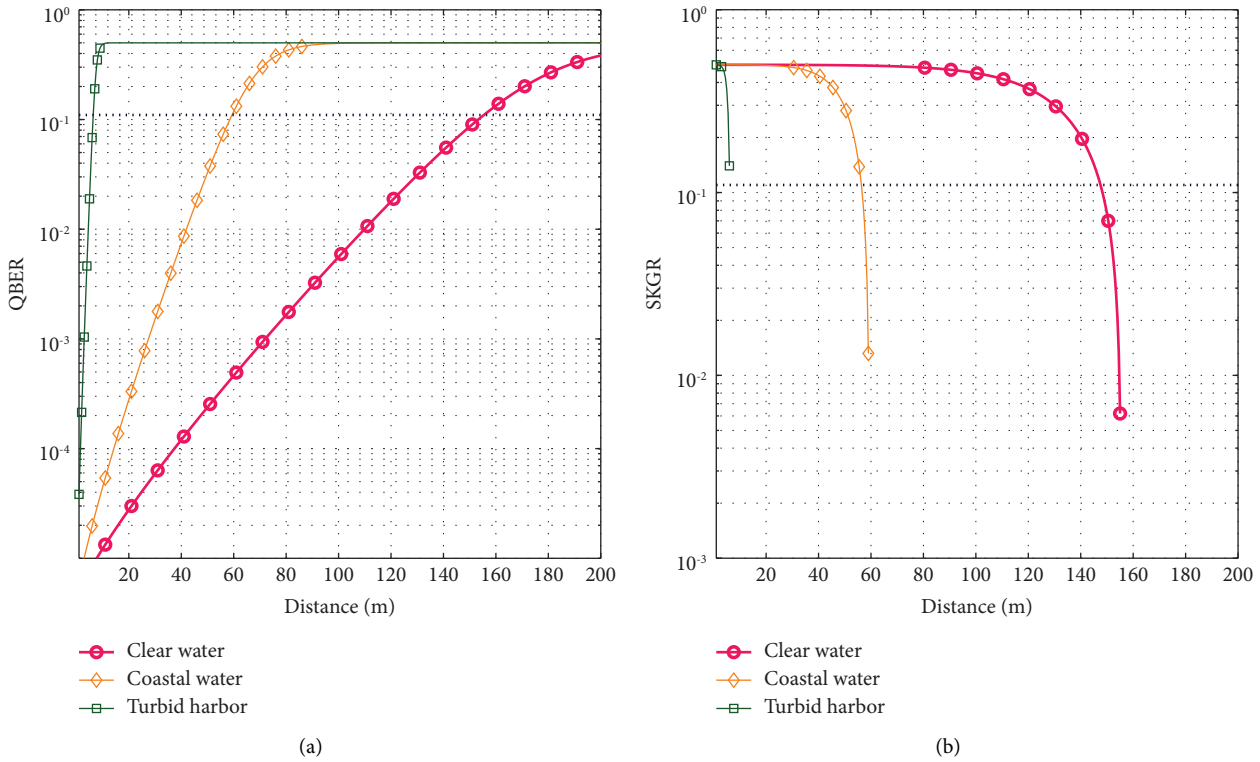

Figure 4: Effect of water types for nonturbulent condition on (a) QBER (i.e., using (22)) and (b) SKGR (i.e., replacing (22) in (11) and then using (8)).

background noise. For instance, the maximum transmission distance in Scenario 2 (heavy overcast with the sun near the horizon) is 49.5 m, while it drops to 22.3 m and 6.7 m for Scenario 4 and Scenario 5 (heavy overcast and clear atmosphere with the sun at the zenith), respectively. These are much shorter than the 106.7 m that can be achieved at night under clear atmosphere conditions with a full moon.

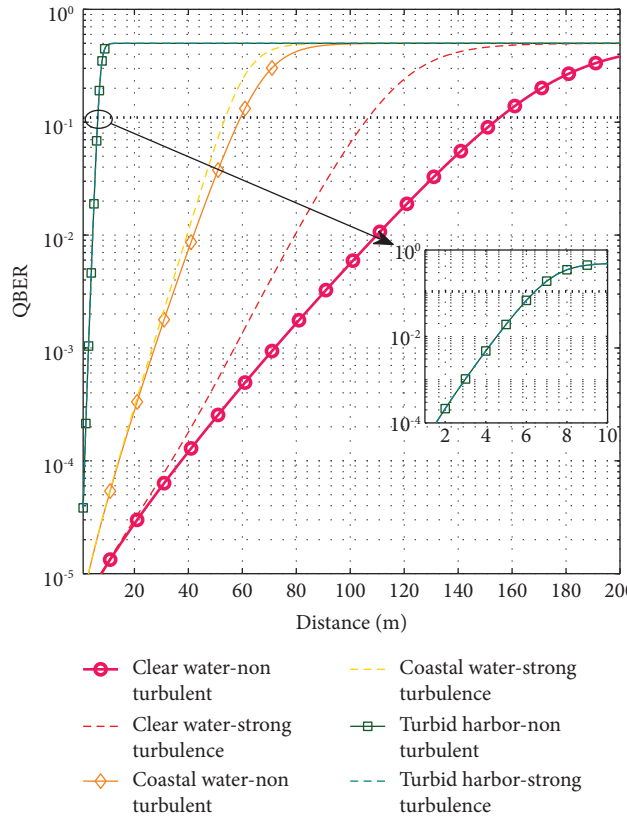

Figure 5: Effect of turbulence on QBER (using (21)) for different water types.

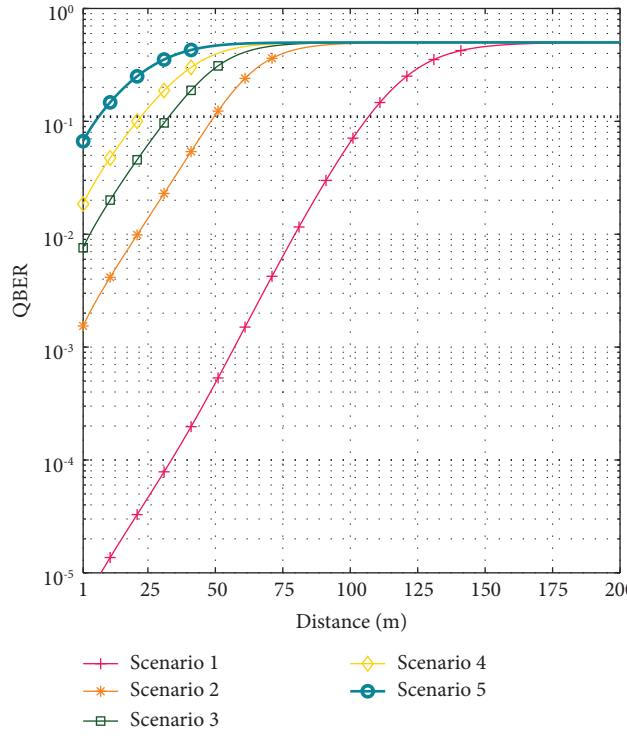

Figure 6: Effect of atmospheric conditions on QBER (using (21)).

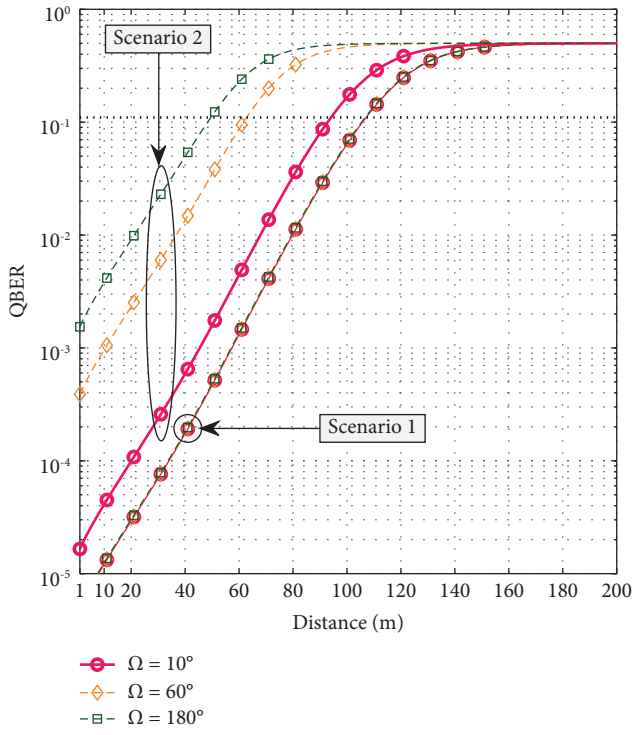

Figure 7: Effect of field of view on QBER (using (21)).

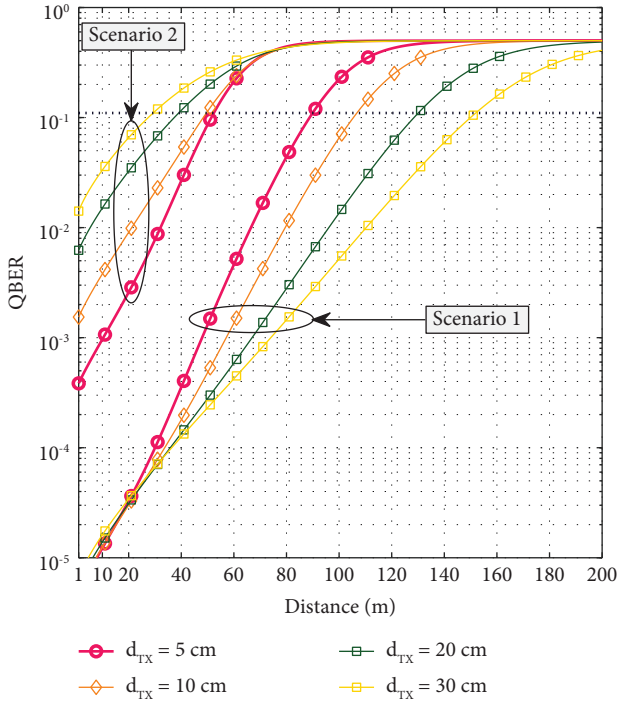

Figure 8: Effect of aperture size on QBER (using (21)).

3.3. Effects of System Parameters. In the previous subsections, we discussed the effect of various channel parameters on the QBER and SKGR performance for given values of system parameters. In this subsection, we now discuss how to select two critical system parameters, namely field-of-view and aperture size.

3.3.1. Effects of FoV. In Figure 7, the impact of FoV on the QKD system performance is explored. The scenario is set with a clear ocean with strong turbulence, and two of the previously studied atmospheric conditions, Scenario 1 and Scenario 2, are taken into consideration. Here, we consider three FoV values, $\Omega = 10^{\circ}$, 60°, and 180°. It is observed from Figure 7 that FoV has minimal effect on the QBER during nighttime, as all three FoV values yielded the same result. However, during daylight, the achievable transmission distance improves as the FoV narrows, due to a reduction in background noise. The maximum transmission distance was found to be 49.5 m for FoV of 180°, increasing to 62.8 m for FoV of 60°, and reaching 94 m for FoV of 10°.

3.3.2. Effects of Aperture Size. The effect of the aperture size on the underwater QKD system's performance is investigated in Figure 8. Both the receiver and transmitter aperture sizes are assumed to be the same, with diameters of $d_{TX} = d_{RX} = 5$, 10, 20, and 30 cm. In the night time, the maximum transmission distance improves as the pupil diameter increases. For example, a maximum transmission distance of 89.9 m is achieved for a 5 cm pupil diameter, while this distance increases to 106.7 m, 130 m, and 151.9 m for pupil diameters of 10, 20, and 30 cm, respectively. The increase in background noise caused by the larger pupil diameter is negligible at night. Conversely, during daylight, the maximum transmission distance decreases as the pupil diameter increases. For example, a maximum transmission distance of 52.3 m is achieved for a 5 cm pupil diameter, while this decreases to 49.5 m, 39 m, and 29.3 m for pupil diameters of 10, 20, and 30 cm, respectively.

4. State-of-the-Art in Underwater QKD

Here, a thorough survey of UQKD is summarized. We will consider separately simulation studies, experimental studies, UQKD systems, and, finally, continuous variable UQKD.

4.1. Simulation Studies. Free-space UQKD was first discussed by Lanzagorta in 2012 [95]. In [98], the authors theoretically investigate the performance of a vertical quantum channel between the sea surface and a submerged vehicle, about 100 m deep. The analysis relies on a closed-form expression of the QBER achievable by BB84 in free space, obtained as a function of depth and some key environmental and system parameters [99]. The results suggest that secure BB84 (i.e., with QBER $\leq 11\%$) [45] can be achieved up to a depth of 60 m in Jerlov Type I ocean water; conversely, BB84 secure only against simple intercept-and-resend attacks (QBER $\leq 25\%$) is possible up to 110 m. In Jerlov Type III water, the maximum achievable distance between two UQKD nodes falls to about 6 m. In the analysis, scenarios with coordinated underwater vehicles and surface/

aerial assets are also considered. In [100], Shi et al. investigate the scattering and absorption properties of photons in seawater by means of Monte Carlo simulations, based on the vector radiative transfer theory. Numerical results confirm that, under environmental conditions of starlight only and Jerlov Type I ocean water, secure BB84 UQKD is feasible up to a depth of 60 m; the corresponding SKGR is equal to 207 kbps. In the considered scenario, if the QBER threshold is relaxed to 25%, UQKD can reach 107 m, with SKGR of 45 kbps. In [101], the authors analyze the QKD performance through the air-water interface. The effects of the photon incident angles to the air-water interface are considered, and performance bounds in different types of water types are evaluated. Further theoretical studies are carried out in [29, 102], where the analysis is extended to the decoy-state protocol applied to UQKD, and in [103], which considers horizontal submarine-to-submarine UQKD. All these works further conclude the feasibility of horizontal/vertical UQKD at distances up to about 100 m, based on the assumption that a stable optical link between Alice and Bob can be established. Moreover, they also confirm that the performance in terms of SKGR can be improved if the decoy-state protocol is adopted. To overcome range limitations due to absorption, scattering, and turbulence, in [82], a multihop UQKD system is investigated, where intermediate nodes support the key distribution process. In [81], the BB84 QBER and SKGR performances in underwater channels are analyzed. To this end, the authors first present an upper bound for the QBER as a function of path loss and average power transfer function. To analytically model the path loss, they use a modified Beer–Lambert formula taking into account also the scattering effect. Furthermore, they evaluate a closed-form expression of the average power transfer function based on the near-field analysis presented in [77]. Similarly, they can obtain a lower bound for the SKGR. This way, the performance of the BB84 protocol in terms of QBER and SKGR can be investigated in different types of water (clear, coastal, and turbid) and under different atmospheric conditions (clear, hazy, and overcast). The effects of system parameters such as aperture size and detector field-of-view on QBER and SKGR are also assessed by numerical simulations. In the considered scenario, for clear ocean waters, the maximum achievable distance is 155 m. The distance reduces to 107 m, under strong turbulence conditions. In turbid water, the prevailing factor is the path loss, and the maximum distance that can be achieved is around 6 m. The main results of the (comparable) simulation studies discussed above are summarized in Table 13. As one can easily see, all studies confirm the feasibility of UQKD in open ocean water, at a distance of at least 60 m.

4.2. Experimental Studies. The first experimental evidence of UQKD feasibility was obtained in 2017. This experiment, as well as all the other experiments reported in this and in the following section, was performed in a laboratory or in a controlled environment, where a stable quantum channel between Alice and Bob had been previously established by an operator by means of a manual alignment procedure. Specifically, in [28], the authors show that certain physical properties of photons, such as polarization and entanglement, can be preserved after the transmission through an artificial tube filled with Jerlov Type I seawater. In the reported experiment, the underwater quantum channel length was 3.3 m. For single photons at 405 nm wavelength in the blue-green window, an average process fidelity above 98% was observed. In [104], the effect of turbulence on the QBER achievable by UQKD was analyzed. To this end, the OAM of light, also known as twisted photons, was used. Since OAM states lie in a Hilbert space with unbounded dimension, they can be used to implement high-dimensionality QKD. This way, 2-, 3-, 4-dimensional BB84 and the six-state protocol could be tested. The experiments were performed in an outdoor pool exposed to temperature variations between 17° and 27°, to create a temperature gradient mixed with built-in water jets. The feasibility of high-dimensional secure QKD was demonstrated through a quantum channel of length equal to about 3 m. The authors could then calculate the corresponding QBER and SKGR values from probability-of-detection matrices obtained during the experiments. In [105], the transmission of optical beams with various polarizations and spatial modes was studied through the Ottawa River. The experiments were carried out through a quantum channel of length equal to 5.5 m. The paper analyzed the effects of turbulence in the underwater channel, due to differences of temperature and salinity through the optical link. In [106], the achievable performance of a UQKD system based on polarization states, BB84, and the decoy-state protocol was analyzed in a laboratory flume tank. In the presence of turbulence, UQKD could be achieved at a distance of 30.5 m, with a SKGR of about 100 kbps, in clear water. Extrapolation of the obtained experimental data shows that a quantum channel length not far from 80 m is achievable, with an estimated key rate between 100 and 1000 bps. Finally, in [107, 108], the persistence of polarization and OAM states of photons were, respectively, verified, by applying quantum tomography techniques, through 55 m long underwater channels.

4.3. UQKD Systems. The results discussed in the previous subsection have been mostly obtained by a combination of ad hoc laboratory setups, commercial instrumentation, and on off-line postprocessing procedures, with the aim of experimentally demonstrating the feasibility of UQKD; hence, they have been classified as experimental feasibility tests in this state-of-the-art survey. Conversely, the first complete underwater UQKD system, capable to autonomously carry out the original BB84 process in view of its practical implementation, was demonstrated only in 2019 [109]. Since then, to the best of the authors' knowledge, five UQKD systems have been presented in the available literature. All these systems are based on the BB84 protocol and polarization encoding. The most relevant aspects of such systems are summarized in Table 14. The first column points at the reference paper that describes the system. The following columns outline the most relevant system features, such as the complete implementation of the BB84 protocol, the real-

Table 13: Summary of UQKD simulation studies.

Ref.	Analyzed protocol	Type of link	Max. distance (m)	Type of water
[98]	BB84	Vertical	60	Jerlov Type I
[100]	BB84	Vertical	60	Jerlov Type I
[101]	BB84	Vertical	281	Jerlov Type I
[102]	BB84	Vertical	60	Jerlov Type I
[81]	BB84	Horizontal	155	Open ocean (Mobley)

Table 14: Summary of UQKD systems.

Ref.	Complete BB84	Real time	λ (nm)	Distance (m)	QBER (%)	SKGR (bps)	Decoy state
[109]	NO	NO	488	2.37	3.5	337.2	NO
[48]	YES	NO	520	10.0	0.36	563410.0	YES
[110]	YES	NO	450	30.0	2.5	595.0	YES
[111]	YES	YES	450	10.4	1.55	1800.0	YES
[112]	YES	YES	405	7.0	10.4	100.0	NO

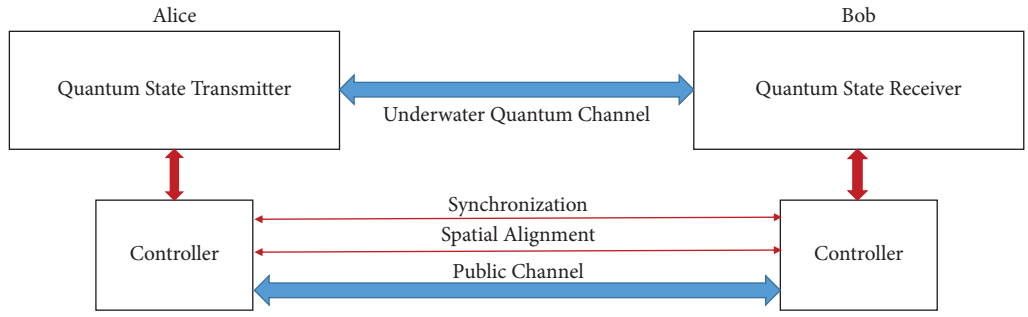

Figure 9: High-level scheme of a typical UQKD system.

time execution of all the protocol phases, the used wavelength, the distance between transmitter and receiver in the system validation experiments, the achieved QBER and SKGR, and the implementation of the Decoy-State protocol in the system. Moreover, a common high-level scheme representing the main functional blocks of all systems is shown in Figure 9. As will be discussed in more detail in Section 5, all systems can be operated only in a lab environment, with the quantum underwater channel implemented by a pipe or a water tank. The quantum state transmitter and receiver are described, at the logical level, in Figure 1. However, the technological solutions adopted in the implementations can be quite different. For instance, the quantum state transmitter in [48] is based on a single laser diode and a rotation controller operating on a half-wave-plate. Conversely, in the system presented in [113], the quantum states are generated by four distinct lasers and the originated light pulses are then collimated onto the same path by the following transmitter optical circuit. Moreover, each system includes a public channel, a synchronization system, and an additional functional block to support the pointing, acquisition, and tracking function. Also, the solutions adopted to implement such functions vary significantly through the five systems. We let the interested reader refer to the literature for the implementation details. In the following, we will briefly describe and discuss each single system of Table 14.

The system in [109] did not include a true quantum random number generator, and the error correction and privacy amplification phases were not executed in real time. Specifically, this paper described an experimental validation of BB84, over a 2.37 m artificial water channel, using a laser in the blue-green optical window (488 nm wavelength), originating photon pulses at a frequency of 1 MHz. The system described, tested through air, gave an experimental SKGR equal to 422.96 bps, with QBER of 1.58%. The SKGR and the QBER were then measured through the water channel, with the water attenuation coefficient ranging from 0.11 m^{-1} to 0.68 m^{-1}. Correspondingly, the SKGR reduced from 337.2 bps to 37.9 bps, while the QBER increased from 1.65% to 3.5%. The obtained QBER values were always below the 11% threshold of BB84; hence, secure QKD could be achieved in all tests. Extrapolation of the obtained experimental data indicated that secure UQKD could potentially reach a maximum distance of about 54 m, with a water attenuation coefficient equal to 0.03 m^{-1} at 488 nm wavelength (Jerlov Type I water); in such a case, SKGR and QBER would be close to 37.9 bps and 3.5%, respectively. The paper in [48] provided useful reference values of the SKGR and QBER for UQKD systems, obtained in a controlled laboratory environment. The described experiments were carried out using the BB84 protocol, at a distance of 10 m through a tank, with a single laser diode transmitter at a wavelength of 520 nm, operating at a pulse rate of 20 MHz. In the

experiments, the outputs of four single photon detectors were collected by means of an oscilloscope, for off-line signal processing. The measured path loss in the tank at 520 nm wavelength was equal to 0.08 m^{-1}, close to Jerlov Type II water. The UQKD system presented could run with or without the support of the decoy-state protocol. Without decoy-state, the system achieved a lower bound SKGR of 563.41 kbps, with QBER of 0.0036. Conversely, using the decoy-state protocol, the SKGR could arrive up to 711.29 kbps, with QBER equal to 0.0095. With Jerlov Type II water, the maximum transmission distance, predicted by simulations, equalled to 19.2 m. Nonetheless, extrapolating the achieved SKGR from Jerlov Type II water to Jerlov Type I water (attenuation coefficient equal to 0.03 m^{-1} at 520 nm), the authors claimed that the system could operate up to 237 m. The work in [110] describes a UQKD system implementing BB84 with a 3-decoy-state protocol (with blue-green lasers at 450 nm originating photon pulses at 50 MHz) achieving an average SKGR of 595 bps, with QBER lower than 2.5% through a 30 m long artificial quantum channel in Jerlov Coastal water, between water Type 1 and 3. The water was experimentally characterized by using laser beams at two wavelengths, 450 nm and 520 nm. By extrapolation, the authors claim that the system can operate at a distance of 345 m in Jerlov Type I water. The authors implemented a software tool in MATLAB for real-time postprocessing, including sifting, error estimation, error correction, and privacy amplification.

In [111], the authors presented a UQKD system operating over a 10.4 m channel Jerlov Type II seawater channel; the system is an evolution of the project presented in [109], and uses a blue laser (450 nm) transmitting pulses at 20 MHz. By using BB84, the decoy-state protocol and polarization encoding, this system could achieve a SKGR of 1.82 kbps, with QBER of 1.55%. By extrapolation, the authors showed that the system could be used up to 300 m in Jerlov Type I water, with SKGR of 27.4 bps. One significant step forward with respect to [109] was the integration of some fundamental ancillary functions, which are necessary for the application of UQKD in real-life scenarios. Specifically, a classical optical channel was integrated in the system, so that the two UQKD end nodes could autonomously communicate, without any interaction through a laboratory local network. Besides providing a public channel as required by BB84, this integrated optical link could be used for end-node synchronization, and to support pointing and tracking capabilities, as required when operating in a real-life scenario. Also, a further step towards space and power minimization consumption is achieved through the use of field programmable gate array- (FPGA-) based boards. The FPGA boards were responsible for sifting the keys and then sent the sifted keys to two personal computers at each end. The software tool on the computers handled the correction of errors, checking for errors, and privacy amplification. With this UQKD system, real-time secret keys could be generated.

In [112, 113], Kebapci et al. demonstrated a practical implementation of an UQKD system that uses the BB84 protocol enabling to run in real time. It was constructed using a combination of an FPGA and an on-board computer (OBC) connected to optical components. The FPGA was utilized to perform real-time photon counting. Both the transmitting and receiving units were powered by an external uninterruptible power supply and could be monitored from a connected computer. Additionally, the system included a visible laser and an alignment indicator to aid in manual alignment verification. The public channel was implemented using a dedicated Ethernet cable. Experimental results that validated the system at a distance of 7 m in clear water were reported.

4.4. Continuous Variable UQKD. The currently available UQKD systems are mostly based on discrete variable protocols, which exploit the properties of single photons to convey information. The use of single photons, which are highly vulnerable to path loss in their transmission through seawater, is the main origin of most of the weaknesses and performance limitations of this approach [8]. A possible alternative, widely investigated in terrestrial networks, is the use of continuous variable protocols (CVPs). CVPs rely on the measurement of quadrature components of light, performed by optical homodyne detection [8]. CVP-based systems can offer various advantages because they transmit light beams composed of many photons rather than single photons. In particular, they are compatible with the highly capable and relatively inexpensive off-the-shelf devices used in commercial optical communication equipment, which now makes CVP-based QKD a hot topic in the terrestrial telecommunication realm. However, few papers aimed at analyzing the application of CVP to UCs are available in the literature. Moreover, they are mostly based on computer simulations rather than experimental work [114, 115].

5. Challenges and Future Prospects

In this section, we delve into two crucial aspects of QKD networks. Firstly, we assess the TRL of UQKD, comparing its current status to established QKD applications. Secondly, we explore the challenging issue of authenticating the UQKD public channel, highlighting the unique considerations and limitations in underwater communication networks.

5.1. Technology Readiness Level of UQKD. From the survey carried out in the previous section, we can infer that the TRL of UQKD is significantly lower than the TRL of QKD applications in fiber/satellite links, which is assumed close to 7 ("system prototyping demonstration in an operational environment") [116]. Nevertheless, some evolution trends in the path towards the practical adoption of UQKD can be identified. Presently, all reported activities on UQKD are based on proof-of-concept systems operating in lab environments [48, 110–112, 114]. With the development and validation of the equipment discussed in subsection 4.3, the TRL of UQKD systems has evolved from 1–3 ("Basic Research, Concept Stage") to 4 ("Laboratory research, Validation"). Also, experimental setups are evolving: from the

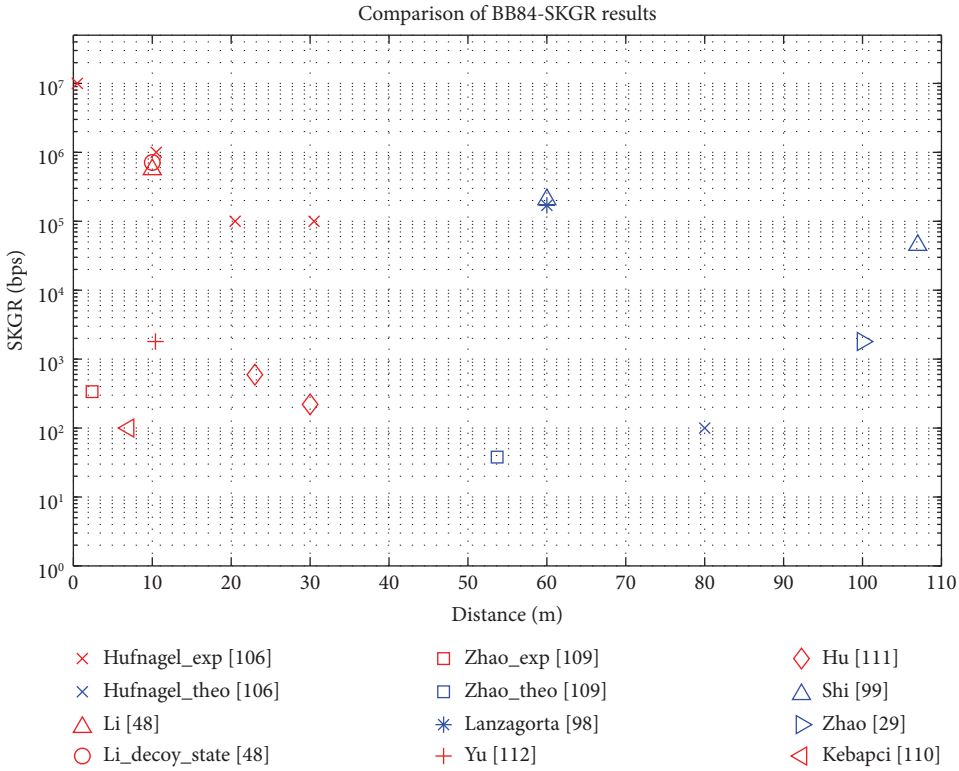

FIGURE 10: Experimental and theoretical values of underwater SKGR (vertical axis: logarithmic scale) as a function of distance (horizontal axis), obtained with the BB84 protocol. The values are from the following papers: the Hufnagel_exp and Hufnagel_theo series from [106]; the Li and Li_decoy_state series from [48]; the Zao_exp and Zao_theo from [109]; the Lanzagorta series from [98]; the Yu series from [111]; the Hu series from [110]; the Shi series from [100]; the Zhao series from [29]; the Kebapci series from [113]. Red symbols indicate experimental results, and blue symbols indicate theoretical results, or extrapolated results from experimental data. The Hufnagel_exp, Hufnagel_theo, and Li_decoy_state series have been obtained with the support of the decoy-state protocol.

first lab tests carried out through pipes, the most recent experiments are being carried out in open pools, in some cases with controlled level of turbulence, on platforms built in a river [104, 105] or in a large-scale marine test platform [110].

The UQKD systems described in subsection 4.3 can only operate in a lab or in a highly controlled environment. One reason is that dimension, weight, and power consumption of such systems make them hardly usable in a real-life scenario, for instance, integrated in an underwater autonomous vehicle. Nonetheless, there is a clear trend towards space and power consumption reductions through the adoption of small size and low-power devices such as field programmable gate arrays [111, 112]. Furthermore, some fundamental ancillary functionalities are needed to apply UQKD in real-life environments, such as the classic QKD public channel, time synchronization between UQKD nodes, and the pointing, acquisition, and tracking technology needed to establish a stable and low noise quantum channel in free space [117]. Some UQKD implementations aimed at integrating these mandatory functional blocks are ongoing. The problem of aligning transmitter and receiver is an active research field in underwater optical communications [118]. However, studies about the development of such ancillary functions specifically designed for UQKD systems are not available yet, at least in the open literature, and a complete solution is still missing [111].

A debated aspect of UQKD is the range (i.e., the maximum distance between Alice and Bob) at which a UQKD system can operate. The plot in Figure 10 shows some selected experimental and theoretical BB84-SKGR values available in the literature, expressed as a function of the distance between Alice and Bob. One can observe some significant performance gaps among the obtained SKGR results. Such gaps can be explained by relevant differences both in the adopted experimental setups and in the performance of the used hardware components. For instance, the authors in [48, 106, 109] operate the laser photon source at different frequencies, i.e., 1 GHz, 20 MHz, and 1 MHz, respectively, thus originating a greatly different number of photons per time unit; the authors in [48, 109] perform experiments with different water attenuation coefficients: $0.08\,\mathrm{m}^{-1}$ in [48], versus values in the range 0.11 to $0.68\,\mathrm{m}^{-1}$ in [109]. Nevertheless, the available experimental results clearly confirm the feasibility of UQKD. Moreover, it can be reasonably assumed that current UQKD systems can successfully operate at distances of about 30 m in lab tests. Finally, both extrapolation of experimental results and values provided by theoretical studies agree on the fact that it should be possible, in a near future, to extend the quantum

channel length up to 80–100 m, with a SKGR in the range 100 to 1000 bps. In this case, UQKD can become a useful technique to implement key distribution in a number of real-life UC scenarios.

5.2. Authentication of the UQKD Public Channel. QKD systems require authentication in the classical public channel because they are vulnerable to the man-in-the-middle type of attacks [8, 119]. In a man-in-the-middle attack to a system with two legitimate parties, Eve impersonates one legitimate party to the other. For instance, in a public key cryptosystem, Eve could send her public key to Alice, pretending she is Bob. She could then impersonate Alice towards Bob, thus creating an encrypted communication channel between Alice and Bob under her complete control [8, 24]. Similarly, in a QKD scenario, Eve could create a quantum channel between Alice and herself, pretending to be Bob, and a second independent quantum channel between herself and Bob, pretending to be Alice. Finally, she could share two different symmetric secret keys, one with Alice and one with Bob, and copy and decrypt all the encrypted data exchanged by Alice and Bob.

In terrestrial classical networks, public key infrastructures typically rely on a hierarchical system based on certificates released by certification authorities (CAs) to guarantee that a certain public key really belongs to a given entity [8, 24]. As an example, web browsers usually have built-in CA public keys. This way, they can verify certificates of other keys and establish secure connections with any website with certified public keys [8]. However, the use of hierarchical systems based on certificates and CA still is very hard to implement in underwater networks due to bandwidth restrictions [4].

In the literature, the authentication problem for underwater acoustic networks (UANs) has been specifically addressed [4, 5, 120]. In the underwater domain, symmetric key-based authentication is usually employed. In the case of secret key shared by multiple nodes, the typical assumption is that, having a legitimate key, the network nodes are trusted and none of them is misbehaving by impersonating other identities [4, 6]. Conversely, if entity authentication is required, a dedicated secret key must be used for each point-to-point connection. However, the use of a symmetric key scheme for authentication would reintroduce the KDP, as discussed in the Introduction. Public key-based authentication can overcome such a drawback, providing a much higher degree of flexibility. The use of public key cryptography in UANs has been proven, based on elliptic curve cryptography techniques and the adoption of implicit certificates. Implicit certificates can implement and securely validate the association between a node identity and its public key without using an explicit signature mechanism [5]. Moreover, they can use data structures of smaller size with respect to the X.509 certificates, usually adopted in terrestrial networks, which can have a size of hundreds of bytes, and are therefore unusable in restricted resource environments such as UANs [5]. Unfortunately, the public key-based authentication schemes currently available for UANS (such as those given in [5, 120]), being based on elliptic curve cryptography techniques, are quantum vulnerable [8]. The problem of applying quantum-safe authentication schemes to the QKD public channel is an ongoing research activity for terrestrial networks [119, 121] and for the IoT [122]. Experimental efforts are also currently being spent to implement (terrestrial) quantum networks that can offer confidentiality, integrity, authentication, and nonrepudiation relying on quantum digital signatures [123]. However, to the best of the authors' knowledge, the UQKD public channel authentication problem has not been addressed yet, at least in the open literature.

6. Conclusions

In 1984, Bennet and Brassard presented BB84, the first QKD protocol. Since then, QKD has become a fast-growing technology in fiber cable and satellite communications and is rapidly moving towards in-field testing and technological prototypes. Conversely, the application of QKD to the underwater domain is at a very early stage, still confined to lab experiments and proof-of-concept prototypes. Nonetheless, theoretical studies and extrapolations of experimental results indicate that UQKD can successfully achieve distances of tens to hundreds of meters depending on the turbidity of the environment. With such knowledge at hand, one may envision future UQKD systems operating in various undersea applications. Yet, to reach the required level of technical maturity, it is essential we transition from focused laboratory research to underwater field experiments; only such a transition will accurately characterize system performance. In addition, such field testing will provide insight about issues often hidden in laboratory setups, such as the operational system size, power consumption, and cost and overall robustness in diverse conditions.

Disclosure

Preprints of this paper have previously been published [124–126].

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This review is supported by the NATO Allied Command Transformation, Norfolk, USA.

References

[1] C. Lal, R. Petroccia, K. Pelekanakis, M. Conti, and J. Alves, "Toward the development of secure underwater acoustic networks," *IEEE Journal of Oceanic Engineering*, vol. 42, no. 4, pp. 1075–1087, 2017.

[2] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 54–60, 2015.

[3] D. Mary, E. Ko, S.-G. Kim, S.-H. Yum, S.-Y. Shin, and S.-H. Park, "A systematic review on recent trends, challenges,

privacy and security issues of underwater internet of things," *Sensors*, vol. 21, no. 24, p. 8262, 2021.

[4] S. Jiang, "On securing underwater acoustic networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 729–752, 2019.

[5] A. T. Capossele, C. Petrioli, G. Saturni, D. Spaccini, and D. Venturi, "Securing underwater communications: key agreement based on fully hashed MQV," in *Proceedings of the International Conference on Underwater Networks & Systems*, Boston, MA, USA, November, 2017.

[6] G. Ateniese, A. Capossele, P. Gianci, C. Petrioli, and D. Spaccini, "SecFun: security frameworkfor underwater acoustic sensor networks," in *Proceedings of the MTS/IEEE Oceans 2015*, pp. 1–9, Genova, Italy, May, 2015.

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK, 2010.

[8] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation*, Cambridge University Pres, Cambridge, UK, 2006.

[9] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the Annual Symposium on Foundations of Computer Science*, pp. 124–134, Santa Fe, NM, USA, November, 1994.

[10] National Cyber Security Center, "Preparing for quantum-safe cryptography," 2020, https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

[11] National Institute of Standards and Technology, "Post-quantum cryptography," 2020, http://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[12] H. Becker, "ARM whitepaper: post-quantum cryptography," 2020, https://community.arm.com/arm-research/m/resources/1002.

[13] E. T. S. Institute, "Quantum-safe cryptography (QSC); limits to quantum computing applied to symmetric key sizes," ETSI GR QSC 006 v1.1.1, 2017.

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996, https://arxiv.org/abs/quant-ph/9605043.

[15] G. Alagic, D. Cooper, Q. Dang et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," 2022, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458.

[16] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH," in *Advances in Cryptology - EUROCRYPT 2023*, Springer, Cham, Switzerland, 2023.

[17] W. Beullens, *Breaking Rainbow Takes a Weekend on a Laptop*, vol. 10, Springer, Berlin, Germany, 2022.

[18] S. Pirandola, U. L. Andersen, L. Banchi et al., "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[19] J. Roth, E. Karatsiolis, and J. Krämer, "Classic McEliece implementation with low memory footprint," in *Smart Card Research and Advanced Applications*, Springer, Berlin, Germany, 2021.

[20] National Institute of Standards and Technology, "Lightweight cryptography," 2002, http://csrc.nist.gov/projects/lighweight-cryptography.

[21] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[22] K. Pelekanakis, S. A. Yıldırım, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: feature extraction and quantization," in *Proceedings of the Underwater Communications and Networking Conference*, pp. 1–5, Guangdong, China, November, 2021.

[23] G. Sklivanitis, K. Pelekanakis, S. A. Yıldırım, R. Petroccia, J. Alves, and D. A. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: reconciliation and privacy amplification," in *Proceedings of the Underwater Communications and Networking Conference*, pp. 1–5, Guangdong, China, November, 2021.

[24] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, USA, 1996.

[25] C. H. Bennet and G. Brassard, "Public-key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, December, 1984.

[26] National Security Agency/Central Security Service, "Quantum key distribution (QKD) and quantum cryptography (QC)," 2018, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[27] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, "Secure quantum communication technologies and systems: from labs to markets," *Quantum Reports*, vol. 2, no. 1, pp. 80–106, 2020.

[28] L. Ji, J. Gao, A. L. Yang et al., "Towards quantum communications in free-space seawater," *Optics Express*, vol. 25, no. 17, pp. 19 795–819 806, 2017.

[29] S.-C. Zhao, X.-H. Han, Y. Xiao, Y. Shen, Y.-J. Gu, and W.-D. Li, "Performance of underwater quantum key distribution with polarization encoding," *Journal of the Optical Society of America A*, vol. 36, no. 5, p. 883, 2019.

[30] A. H. F. Raouf, "Performance analysis of quantum key distribution in underwater channels," M.Sc. thesis, Özyeğin University, Istanbul, Türkiye, 2021.

[31] S. Ecker, J. Pseiner, J. Piris, and M. Bohmann, "Advances in entanglement-based QKD for space applications," 2022, https://arxiv.org/abs/2210.02229.

[32] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[33] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[34] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, pp. 3018–3021, 1998.

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

[36] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, no. 5, Article ID 057901, 2004.

[37] A. K. Ekert, "Quantum cryptography and Bell's theorem," in *Quantum Measurements in Optics*, pp. 413–418, Springer, Berlin, Germany, 1992.

[38] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, no. 5, pp. 557–559, 1992.

[39] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, Article ID 130503, 2012.

[40] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[41] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, no. 3, Article ID 031043, 2018.

[42] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[43] A. H. Fahim Raouf and M. Uysal, "On the optimization of underwater quantum key distribution systems with time-gated SPADs," *Journal of the Optical Society of America B*, vol. 39, no. 8, pp. 2013–2019, 2022.

[44] L. Zhang, Y. Wang, Z. Yin et al., "Real-time compensation of phase drift for phase-encoded quantum key distribution systems," *Chinese Science Bulletin*, vol. 56, no. 22, pp. 2305–2311, 2011.

[45] V. Scarani, H. Bechmann-Pasquinucci, J. Cerf, M. Dušek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

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

[47] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, Article ID 230504, 2005.

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

[49] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Physical Review Letters*, vol. 90, no. 16, Article ID 167904, 2003.

[50] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," *Physical Review A*, vol. 69, no. 3, Article ID 032316, 2004.

[51] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," *Physical Review Letters*, vol. 93, no. 12, Article ID 120501, 2004.

[52] S. Kuppam, "Modelling of quantum key distribution protocols in communicating quantum processes language with verification and analysis in PRISM," in *Proceedings of the International Conference on Simulation and Modeling Methodologies, Technologies and Applications*, pp. 75–82, Porto, Portugal, July, 2018.

[53] M. Koashi, "Security of quantum key distribution with discrete rotational symmetry," 2005, https://arxiv.org/abs/quant-ph/0507154.

[54] H. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," *Quantum Information and Computation*, vol. 1, no. 2, pp. 81–94, 2001.

[55] E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," *Physical Review A*, vol. 65, no. 5, Article ID 052310, 2002.

[56] N. Ilic, "The Ekert protocol," *Journal of Physics*, vol. 334, p. 22, 2007.

[57] A. Acin, S. Massar, and S. Pironio, "Efficient quantum key distribution secure against no-signalling eavesdroppers," *New Journal of Physics*, vol. 8, no. 8, p. 126, 2006.

[58] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, no. 1, Article ID 15043, 2017.

[59] J. Gu, X.-Y. Cao, Y. Fu et al., "Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources," *Science Bulletin*, vol. 67, no. 21, pp. 2167–2175, 2022.

[60] H.-T. Zhu, Y. Huang, H. Liu et al., "Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking," *Physical Review Letters*, vol. 130, no. 3, Article ID 030801, 2023.

[61] L. Zhou, J. Lin, Y.-M. Xie et al., "Experimental quantum communication overcomes the rate-loss limit without global phase tracking," *Physical Review Letters*, vol. 130, no. 25, Article ID 250801, 2023.

[62] Y.-M. Xie, J.-L. Bai, Y.-S. Lu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, "Advantages of asynchronous measurement-device-independent quantum key distribution in intercity networks," *Physical Review Applied*, vol. 19, no. 5, Article ID 054070, 2023.

[63] Y.-M. Xie, Y.-S. Lu, C.-X. Weng et al., "Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference," *PRX Quantum*, vol. 3, no. 2, Article ID 020315, 2022.

[64] P. Zeng, H. Zhou, W. Wu, and X. Ma, "Mode-pairing quantum key distribution," *Nature Communications*, vol. 13, no. 1, p. 3903, 2022.

[65] T. C. Ralph, "Security of continuous-variable quantum cryptography," *Physical Review A*, vol. 62, no. 6, Article ID 062306, 2000.

[66] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, no. 2, Article ID 022309, 2000.

[67] A. Leverrier and P. Grangier, "Continuous-variable quantum key distribution protocols with a discrete modulation," 2010, https://arxiv.org/abs/1002.4083.

[68] K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Physical Review A*, vol. 97, no. 2, Article ID 022310, 2018.

[69] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," *Physical Review A*, vol. 79, no. 1, Article ID 012307, 2009.

[70] Y. Guo, R. Li, Q. Liao, J. Zhou, and D. Huang, "Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier," *Physics Letters A*, vol. 382, no. 6, pp. 372–381, 2018.

[71] P. Papanastasiou and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: composable security under collective Gaussian attacks," *Physical Review Research*, vol. 3, no. 1, Article ID 013047, 2021.

[72] W.-B. Liu, C.-L. Li, Y.-M. Xie et al., "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance," *PRX Quantum*, vol. 2, no. 4, Article ID 040334, 2021.

[73] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," *New Journal of Physics*, vol. 8, no. 5, p. 75, 2006.

[74] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan et al., "High-dimensional quantum cryptography with twisted

light," *New Journal of Physics*, vol. 17, no. 3, Article ID 033033, 2015.
[75] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Npj Quantum Information*, vol. 2, no. 1, pp. 16025–16112, 2016.
[76] C. Kollmitzer and M. Pivk, *Applied Quantum Cryptography*, vol. 797, Springer, Berlin, Germany, 2010.
[77] J. H. Shapiro, "Near-field turbulence effects on quantum-key distribution," *Physical Review A*, vol. 67, no. 2, Article ID 022309, 2003.
[78] M. Safari and M. Uysal, "Relay-assisted quantum-key distribution over long atmospheric channels," *Journal of Lightwave Technology*, vol. 27, no. 20, pp. 4508–4515, 2009.
[79] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 1879–1883, Los Angeles, CA, USA, June, 2009.
[80] J. Martinez Mateo, D. Elkouss, and V. Martin, "Blind reconciliation," *Quantum Information and Computation*, vol. 12, no. 9&10, pp. 791–812, 2012.
[81] A. H. Fahim Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *Journal of the Optical Society of America B*, vol. 37, no. 2, pp. 564–573, 2020.
[82] A. H. Fahim Raouf, M. Safari, and M. Uysal, "Multi-hop quantum key distribution with passive relays over underwater turbulence channels," *Journal of the Optical Society of America B*, vol. 37, no. 12, pp. 3614–3621, 2020.
[83] J. W. Goodman, *Introduction to Fourier Optics*, Roberts and Company publishers, Greenwood Village, CO, USA, 2005.
[84] D. A. B. Miller, "Waves, modes, communications, and optics: a tutorial," *Advances in Optics and Photonics*, vol. 11, no. 3, pp. 679–825, 2019.
[85] L. C. Andrews and R. L. M. Phillips, *Laser Beam Propagation through Random Media*, SPIE Press, Bellingham, WA, USA, second edition, 2005.
[86] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of decoy state quantum key distribution over underwater turbulence channels," *Journal of the Optical Society of America B*, vol. 39, no. 6, pp. 1470–1478, 2022.
[87] N. G. Jerlov, *Marine Optics*, Elsevier Oceanograpghy Series, New York, NY, USA, 1976.
[88] D. Mobley, *Light and Water: Radiative Transfer in Natural Waters*, Academic Press, Cambridge, MA, USA, 1994.
[89] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 543–552, 2019.
[90] M. G. Solonenko and C. D. Mobley, "Inherent optical properties of Jerlov water types," *Applied Optics*, vol. 54, no. 17, pp. 5392–5401, 2015.
[91] E. Aas, N. K. Højerslev, J. Høkedal, and K. Sørensen, "Optical water types of the Nordic seas and adjacent areas," *Oceanologia*, vol. 55, no. 2, pp. 471–482, 2013.
[92] B. M. Cochenour, L. J. Mullen, and A. E. Laux, "Characterization of the beam-spread function for underwater wireless optical communications links," *IEEE Journal of Oceanic Engineering*, vol. 33, no. 4, pp. 513–521, 2008.
[93] C. Gabriel, M.-A. Khalighi, S. Bourennane, P. Leon, and V. Rigaud, "Monte-carlo-based channel characterization for underwater optical communication systems," *Journal of Optical Communications and Networking*, vol. 5, no. 1, pp. 1–12, 2013.
[94] F. Hanson and S. Radic, "High bandwidth underwater optical communication," *Applied Optics*, vol. 47, no. 2, pp. 277–283, 2008.
[95] M. Lanzagorta, *Underwater Communications*, Morgan & Claypool, San rafael, CA, USA, 2012.
[96] C. Mobley, E. Boss, and C. Roesler, *Ocean Optics Web Book*, University of Oslo, Oslo, Norway, 2010.
[97] D. Slepian, "Analytic solution of two apodization problems," *Journal of the Optical Society of America*, vol. 55, no. 9, pp. 1110–1115, 1965.
[98] M. Lanzagorta and J. Uhlmann, "Assessing feasibility of secure quantum communications involving underwater assets," *IEEE Journal of Oceanic Engineering*, vol. 45, no. 3, pp. 1138–1147, 2020.
[99] D. Rogers, J. C. Bienfang, A. Mink et al., "Free-space quantum cryptography in the H-alpha Fraunhofer window," *Free-Space Laser Communications VI*, vol. 6304, pp. 296–305, 2006.
[100] P. Shi, S. C. Zhao, Y. J. Gu, and W. D. Li, "Channel analysis for single photon underwater free space quantum key distribution," *Journal of the Optical Society of America*, vol. 32, no. 3, pp. 349–356, 2015.
[101] Y. Zhou and X. Zhou, "Performance analysis of quantum key distribution based on air-water channel," *Optoelectronics Letters*, vol. 11, pp. 149–152, 2015.
[102] M. Lopes and N. Sarwade, "Optimized decoy state QKD for underwater free space communication," *International Journal of Quantum Information*, vol. 16, Article ID 1850019, 2018.
[103] J. A. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Optics Express*, vol. 27, no. 3, pp. 3055–3064, 2019.
[104] F. Bouchard, A. Sit, F. Hufnagel et al., "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express*, vol. 26, no. 17, pp. 22 563–622 573, 2018.
[105] F. Hufnagel, A. Sit, F. Grenapin et al., "Characterization of an underwater channel for quantum communications in the Ottawa River," *Optics Express*, vol. 27, no. 19, pp. 26 346–426 354, 2019.
[106] F. Hufnagel, A. Sit, F. Bouchard et al., "Investigation of underwater quantum channels in a 30 meter flume tank using structured photons," *New Journal of Physics*, vol. 22, no. 9, Article ID 093074, 2020.
[107] C.-Q. Hu, Z.-Q. Yan, J. Gao et al., "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," *Photonics Research*, vol. 7, no. 8, pp. A40–A44, 2019.
[108] Y. Chen, W.-G. Shen, Z. Li et al., "Underwater transmission of high-dimensional twisted photons over 55 meters," *PhotoniX*, vol. 1, pp. 5–11, 2020.
[109] S.-C. Zhao, W.-D. Li, Y. Shen et al., "Experimental investigation of quantum key distribution over a water channel," *Applied Optics*, vol. 58, pp. 3902–3907, 2019.
[110] C.-Q. Hu, Z.-Q. Yan, J. Gao et al., "Decoy-state quantum key distribution over a long-distance high-loss air-water channel," *Physical Review Applied*, vol. 15, no. 2, 2021.
[111] Y. Yu, W.-D. Li, Y. Wei et al., "Experimental demonstration of underwater decoy-state quantum key distribution with all-optical transmission," *Optics Express*, vol. 29, no. 19, pp. 30 506–530 519, 2021.
[112] B. Kebapci, G. Mutlu, I. Baglica et al., "Real-time implementation of an underwater quantum key distribution system," in *Proceedings of the Underwater Communications*

and Networking Conference, pp. 1–5, Guangdong, China, November, 2022.

[113] B. Kebapci, V. E. Levent, S. Ergin et al., "Fpga-based implementation of an underwater quantum key distribution system with bb84 protocol," *IEEE Photonics Journal*, vol. 15, no. 4, pp. 1–10, 2023.

[114] Y. Mao, X. Wu, W. Huang et al., "Monte Carlo-based performance analysis for underwater continuous-variable quantum key distribution," *Applied Sciences*, vol. 10, no. 17, p. 5744, 2020.

[115] Y. Wang, S. Zou, Y. Mao, and Y. Guo, "Improving underwater continuous variable measurement-device-independent quantum key distribution via zero-photon catalysis," *Entropy*, vol. 22, no. 5, p. 571, 2020.

[116] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technology*, vol. 8, no. 1, pp. 24–53, 2021.

[117] S. Liao, W. Cai, W. Liu et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[118] Y. Weng, J. Pajarinen, R. Akrour, T. Matsuda, J. Peters, and T. Maki, "Reinforcement learning based underwater wireless optical communication alignment for autonomous underwater vehicles," *IEEE Journal of Oceanic Engineering*, vol. 47, no. 4, pp. 1231–1245, 2022.

[119] L.-J. Wang, K. Zhang, J.-Y. Wang et al., "Experimental authentication of quantum key distribution with post-quantum cryptography," *Npj Quantum Information*, vol. 7, p. 67, 2021.

[120] E. Souza, H. C. Wong, Í. S. Cunha, A. A. F. Loureiro, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proceedings of the IEEE Symposium on Computers and Communications (ISCC)*, pp. 299–304, Split, Croatia, July, 2013.

[121] L.-J. Wang, Y. Zhou, J. Yin, and Q. Chen, "Authentication of quantum key distribution with post-quantum cryptography and replay attacks," 2022, https://arxiv.org/abs/2206.01164.

[122] K. S. Roy and H. K. Kalita, "A quantum safe user authentication protocol for the internet of things," *International Journal of Next-Generation Computing*, vol. 10, 2019.

[123] H.-L. Yin, Y. Fu, C.-L. Li et al., "Experimental quantum secure network with digital signatures and encryption," *National Science Review*, vol. 10, no. 4, p. nwac228, 2023.

[124] P. Paglierani, A. H. Fahim Raouf, K. Pelekanakis, R. Petroccia, J. Alves, and M. Uysal, "A tutorial on underwater quantum key distribution," *TechRxiv*, 2023.

[125] P. Paglierani, A. H. Fahim Raouf, K. Pelekanakis, R. Petroccia, J. Alves, and M. Uysal, "A primer to underwater quantum key distribution," *TechRxiv*, 2023.

[126] P. Paglierani, A. H. Fahim Raouf, K. Pelekanakis, R. Petroccia, J. Alves, and M. Uysal, "A primer on underwater quantum key distribution," *TechRxiv*, 2023.