International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7015
***Article Received:** 06 April 2023 **Revised:** 24 May 2023 **Accepted:** 06 June 2023*

Enhanced Quantum Key Distribution Algorithm for Underwater Optical Wireless Sensor Network

Pooja Ashok Shelar[1], Parikshit Narendra Mahalle[2], Gitanjali Rahul Shinde[3] and Namrata N. Wasatkar[4].
[1]Smt. Kashibai Navale College of Engineering, Wadgaon, pujashelar7@gmail.com, Pune-46
[2]Vishwakarma Institute of Information Technology, aalborg.pnm@gmail.com, Kondhwa, Pune-48.
[3]Vishwakarma Institute of Information Technology, gr83gita@gmail.com, Kondhwa, Pune-48.
[4]Vishwakarma Institute of Information Technology, namratakharate1@gmail.com, Kondhwa, Pune-48.

Abstract: The research aims to develop an attack-free underwater optical communication channel at a distance of 50 meters. In this work, we have emphasized the importance of Quantum Key Distribution (QKD) in Naval and many other applications. An in-detail study of the Benette Brassard QKD protocol proposed in 1984 [BB84] is done with its implementation. Then as the next step, we analyzed the drawbacks of BB84 and the necessity of QKD in Underwater Optical Wireless Sensor Networks [UO-WSN]. As a solution, to identified problems, we have proposed the Enhanced BB84 protocol (EBB84) with considerations of its usage in the UO-WSN. The results showed that the EBB84 algorithm is best suitable algorithm for the underwater environment.

Keywords: Quantum Key Distribution, Underwater Optical Wireless Sensor Network, BB84, EBB84.

I. Introduction

On Earth, water is more than land. But this proportion becomes exactly reversed when we speak about the technological usage of land and water. On land, we have Terrestrial Wireless Sensor Networks (TWSN), the Internet of Things (IoT), Global Positioning Systems (GPS), robotics, and many more. When we think of technology with water bodies, then we can only name a few. For example, Underwater Acoustic Wireless Sensor Networks (UA-WSN) [1], Underwater Optical Wireless Sensor Networks (UO-WSN) [2], Underwater Autonomous Vehicles and most importantly laying down optical fiber cables on sea beds to connect the entire world to high-speed internet. The UO-WSN was minimally used as compared to UA-WSN. The reasons are costly optical sensors, less propagation distance of optical waves than acoustic waves, and the scattering phenomena. Now, things have started changing due to more advantageous features of UO-WSN over UA-WSN. The optical sensor network is proven to be more efficient in terms of maximum bandwidth, minimum propagation delays, minimum data loss at short distances, and guaranteed data security over an optical channel. The UA-WSN or UO-WSNs are used for the development of various underwater applications like tsunami monitoring, water quality monitoring, oil spill leakage detection, and marine-life research.

There are various data-link layer protocols and network-layer protocols developed for both submarine communications and surveillance of water territories. types of underwater wireless sensor networks. As such, there is no standard model available for underwater network communications as the OSI model of TWSN. There are some prototype underwater network models available for acoustic communications like JANUS [3]The research and experimentation are widely growing to explore and develop every aspect of underwater wireless sensor networks. In state-of-art, it was observed that the concept of underwater data security is comparatively less explored [4]. Among these data security for Underwater Optical communication channels is the least focused. Therefore, working on this issue, our research aims to develop an underwater quantum cryptography protocol for UO-WSN. Quantum Cryptography is one of the fastest-developing research areas in information theory by using pillars of quantum physics. On regular basis, quantum researchers design innovative protocol theories, with constantly improvising security proofs. The experiments of quantum cryptography on quantum sensors are also gradually shifting from lab to real-time implementation. In the further paper, section I will showcase the purpose behind the research, Section II gives a detailed explanation of the basics of Quantum Cryptography, whereas Section III looks at the past research work done in improvising the field of quantum cryptography. Section IV is the solution based, as its an in-detail discussion of the proposed methodology. Last is the concluding Section V.

1.1. Motivation

In 1994, according to the “Law of the Sea”, 75% of the water surface on Earth is being divided into each country in the world[5]. This division is done on the basis of distance measurement from an imaginary continuous straight line drawn on maps throughout the sea coast. This imaginary line is called a baseline. The oceans are measured using the “nautical mile”, where 1 nautical is equal to 1.852 km. Therefore, each country is assigned an area of 200 nautical miles Nm from its baseline. The Oceans are divided into five parts. First is the Internal Sea, it’s the area behind the baseline. Second is the “Territorial Sea”, which is a 12 Nm area from the baseline. Territorial Sea is private property belonging to a particular country, with complete dominance over other countries ships. Special permission is required to enter into the territorial sea of any country, The third is the “Contiguous Zone”, it’s a 24 Nm area from the baseline. In a contiguous zone, the ships are allowed to enter without any permission but are bounded to pay custom duty to that particular country. The fourth is the “Exclusive Economic Zone [EEZ]”, which is open to any surveillance or trade ships that are allowed to enter without any permission and they neither have to pay any taxes. But all the exclusive right for fishing, oil and petroleum extraction, mining, survey, conservation, and management of mineral resources and any new island if found belongs to only that concerned coastal country. Now the fifth area after 200 Nm is called the “High Sea”. The “High Sea” is an international boundary and it belongs to International Sea Bed Authority [ISA]. All the countries have equal rights to navigation, aviation, fishing, and laying down submarine cables. Hence, the most important part among all the parts is the Exclusive Economic Zone. As it’s a source of concerned countries income. Therefore, surveillance of these EEZ through all aspects is very crucial. For example, Oceanic wars or robbery of oil and petroleum, and illegal fishing. One real-time example is, the Chinese ship doing illegal fishing in Pakistan’s EEZ. The question now arises, how to secure this economic zone of the county. The current way is to guard the territory by surveillance ships. But this is not a cost-efficient and secure solution. The advancements in oceanic technology led to the development of the Underwater Wireless Optical Sensor which is not only cost-efficient but also easy to maintain and guarantees the security of confidential data with the law of physics. In the next section, we have briefly discussed how quantum physics is used to develop a quantum cryptographic algorithm for securing underwater optical communication channels.

1.2 Fundamentals of Quantum Cryptography

An underwater network implementation has many aspects like routing protocols, MAC protocols, and many more but this research focuses on the security of underwater wireless networks. The development of secure optical communication links among the underwater optical sensors and underwater vehicles is among one the most difficult challenges present in front of nations’ naval forces and also by industries working in the exclusive economic zone of the concerned country. For addressing the above issue, the best possible solution is underwater quantum cryptography. Because maths may not provide the security you need but physics can. The key aspect of Quantum cryptography is its theory based on the physics of quantum mechanics. The real-time application of quantum mechanics is in Underwater Quantum Key Distribution (QKD), which is a secure method to exchange keys in the underwater environment.

Optical Communication channels send data in individual particles of light or “photons”. The fundamental unit to represent photons is “qubits”. The spinning of the electron and photon polarization are two examples corresponding to the physical system of a qubit [6]. The qubit is a probabilistic mixture of 0 and 1, exactly in contrast to classical bits. The qubits are non-deterministic and ambiguous. The qubit state is represented by four different combinations of two complex numbers, i.e., {0, 0}, {0,1}, {1,0}, {1,1}. A single qubit can also be said as a combination of two binary bits [10], stated as:

$$\text{qubit} = \{a, b\} = a \cdot 0\text{bit} + b \cdot 1\text{bit}\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Now, qubits are generally written using Diracs notation, $|\psi\rangle$, $|0\rangle$, $|1\rangle$, where $|0\rangle$, $|1\rangle$ represents two orthogonal vectors in quantum states. The qubit $|1\rangle$ (a=0, b=1) can be considered equivalent to bit 1 and similarly, qubit $|0\rangle$ (a=1,b=0) can be considered equivalent to bit 0. The other values of a and b, are called superpositions of qubits of $|0\rangle$ and $|1\rangle$. The probability of a qubit found in the ‘0’ state is $|a|^2$ whereas the probability of getting state ‘1’ is $|b|^2$. The physical process of measuring converts the qubit into its equivalent classical bit. The Diracs notations is also popularly known as bra-ket notations, where $|\psi\rangle$ is a column vector and $\langle\psi|$ is denoted as a row vector and the combination of column and row vector is denoted as inner product or bra-ket notation ‘ $\langle\psi|\psi\rangle$’ . In this notation, a single qubit state can be written as,

$$|\psi\rangle = a.\ |0\rangle + b.\ |0\rangle\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Or

$$\langle\psi| = a.\ \langle 0| + b.\ \langle 1|\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

where,

$$|a|^2 + |b|^2 = 1\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

The equations (2), (3) and (4) suggests that, if we measure qubit $|\psi\rangle$, then it will result in ‘0’ with a probability of $|a|^2$ and ‘1’ with probability $|b|^2$. Note that the classical state “0” is representing one unit vector/ Horizontal Rectilinear Bases/+45^0 Diagonal bases and "1" is representing another unit vector/ Vertical Rectilinear Bases/-45^0 Diagonal bases, they are not a zero or one vector as shown in the below basis table.

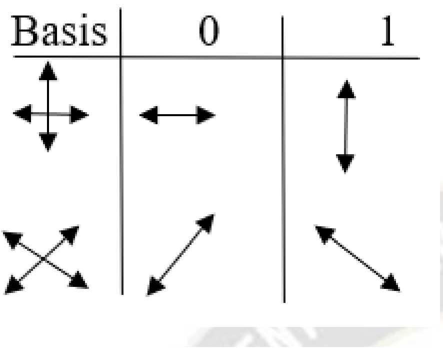


Table 1: Basis division for state '0'and '1'.

The selection of orthogonal basis vectors in two-dimensional space is completely an arbitrary process. The selected basis for the corresponding qubit is further known as a computational basis. The general selection of vectors for computational basis is as follows,

$\langle 0| = (1,0)$ $\langle 1| = (0,1)$ ………………… (5)

$| 0\rangle = (1/0)$ $| 1 \rangle = (0/1)$ …………………(6)

As $| 0\rangle$ and $| 1 \rangle$ are orthogonal vectors,

$\langle 1| 1\rangle = \langle 0| 0\rangle = 1$…………………………………(7)

$\langle 1| 0\rangle = \langle 0| 1\rangle = 0$ ………………………………… (8)

The equations (7) and (8) represent, collapsing of a superposition state to a classical state. This is due to the quantum phenomena of measuring a superposition causing the destruction of quantum bits. Note that superposition states can never be copied and also a qubit in one superposition state cannot be copied to another qubit. In case state is copied, then the original qubit state is destroyed. Therefore, quantum information can only be teleported and cannot be cloned or copied. These properties of quantum physics allow the detection of the attacker, in case he tries to copy or measure the superposition states.

1.3. Quantum Negative Rules: Quantum physics establishes a set of negative rules stating things that cannot be done. For example,

(1) Measurements cannot be taken without altering the system.

(2) Simultaneous position detection of a quantum particle is not allowed

(3) Simultaneous measurement of polarized photons on vertical/horizontal basis and diagonal basis in not allowed.

(4) Duplication of the unknown quantum state is not allowed.

The "Quantum Negative Rules", have actually become a set of positive rules for quantum cryptography. This is a recent revolution and is being used in potential cryptographic applications, due to the contrast nature of quantum physics with classical physics. Let's discuss the negative aspect of quantum physics, which gave birth to unbeatable quantum cryptography and quantum key distribution,

1. Measurements cannot be taken without altering the system:
   In a quantum system, consider a communication scenario between a sender 'Alice' and a receiver 'Bob' and an attacker 'Eve'. According to axiom (1), the positive side is that Eve has to perform measurements to extract any information from qubit. This measurement cannot be done without altering the system. Hence, any attempt of measure will reveal the presence of Eve. And therefore, he cannot get any information about the communication. In a communication scenario, imagine Alice encodes information in qubits, which she then forwards to Bob. If undisturbed qubits are received by Bob, then according to rule (1), no measurement means that the qubits received were original and are not altered by Eve. measured. But the question arises, "How to find undisturbed qubits?". The answer is Alice and Bob can self-verify, if anyone was eavesdropping. Alice and Bob randomly compare their chosen basis vector using a public communication channel.

(2) Simultaneous position detection of a quantum particle is not allowed:

According to the Heisenberg uncertainty Principle [7], it is difficult to simultaneously determine both the momentum and position of a quantum particle. The reason for this is that in quantum mechanics, particles do not have a definite position or momentum until they are measured. Instead, their properties are described by a wave function, which is a mathematical function that assigns probabilities to different outcomes of measurements. If we try to measure the position of a particle, we collapse its wave function to a single position, which means that the wave function is no longer valid for describing the particle's momentum. Similarly, when you measure the momentum of a particle, you collapse its wave function to a single momentum, which means that the wave function is no longer valid for describing the particle's position. Therefore, because the wave function cannot simultaneously describe both the position and momentum of a particle, it is impossible to determine both quantities with arbitrary precision. In quantum key distribution (QKD), the Heisenberg uncertainty principle is used to ensure the security of the communication channel. QKD is a method of securely distributing cryptographic keys using the principles of quantum mechanics. The idea behind QKD is that any attempt to eavesdrop on the quantum communication channel will inevitably disturb the quantum states being transmitted, and this disturbance can be detected by legitimate parties. In particular, the Heisenberg uncertainty principle ensures that an eavesdropper cannot measure the position and momentum of a photon (the quantum particle used in QKD) without disturbing its quantum state. This disturbance will be detectable by the legitimate parties, allowing them to detect the presence of an eavesdropper and take appropriate measures to protect the communication channel. Thus, the Heisenberg uncertainty principle plays a crucial role in the security of QKD by preventing eavesdroppers from gaining information about the transmitted quantum states without being detected

(3) Simultaneous measurement of polarized photons on vertical/horizontal basis and diagonal basis in not allowed.

The third rule is the fundamental principle of quantum mechanics. The polarization of the photon refers to the orientation of the photon’s electric field. The polarization of a photon refers to the orientation of the photon's electric field. It can be measured in different bases, such as the vertical-horizontal basis or the diagonal basis. However, Heisenberg's uncertainty principle states that the more precisely one measures the polarization of a photon on one basis, the less precisely one can measure it on another basis. For example, if one tries to measure the polarization of a photon on a vertical-horizontal basis with very high precision, the uncertainty principle tells us that the measurement on a diagonal basis will have high uncertainty. Similarly, if you measure the polarization of a photon on a diagonal basis with very high precision, the measurement on a vertical-horizontal basis will have high uncertainty. Therefore, it is not possible to simultaneously measure the polarization of a photon on the vertical-horizontal basis and the diagonal basis with high precision. This is because the act of measuring the photon's polarization in one basis affects the photon's state in a way that makes it impossible to precisely measure the polarization on the other basis. In QKD, Alice and Bob want to share a secret key that they can use to encrypt and decrypt messages. They do this by exchanging photons that are polarized in specific ways. For example, Alice might send a photon that is polarized either vertically or horizontally, and Bob will measure it using a detector that is also aligned either vertically or horizontally. If Alice and Bob both use the same polarization basis, then they can determine the polarization of the photon with perfect accuracy. However, if Alice and Bob use different polarization bases, then the Heisenberg uncertainty principle comes into play. Specifically, if Bob tries to measure a photon that was sent by Alice using a different polarization basis, then he will introduce some randomness into the measurement. In other words, Bob will not be able to determine the polarization of the photon with certainty. This property of quantum mechanics also allows Alice and Bob to detect if Eve trying to intercept their communication. If Eve tries to intercept the photons and measure them using a different polarization basis, then she will introduce some errors in the communication. Alice and Bob can detect these errors and discard the corresponding bits of the key, ensuring that their communication remains secure.

(4) Duplication of the unknown quantum state is not allowed.

The fourth rule is known as the no-cloning theorem [8]in quantum mechanics. It states that it is impossible to create an identical copy of an arbitrary unknown quantum state. This rule has significant implications for quantum information processing and cryptography because it means that it is impossible to eavesdrop on a quantum communication channel without disturbing the information being transmitted. If an eavesdropper tries to make a copy of the quantum state being transmitted, the no-cloning theorem ensures that the copy will not be identical to the original state, and the eavesdropper's presence will be detected. The no-cloning theorem is a consequence of the fundamental principles of quantum mechanics, including the superposition principle and the collapse of the wave function upon measurement.

1.4. Quantum Key Distribution [QKD]

In classical cryptography, Alice and Bob communicate secret messages without noticing eavesdropping activity. This can be done using Quantum Key Distribution. Alice sends photons the “smallest part of light” to Bob. Photons are not only particles but also waves, so they oscillate in different directions. But when they oscillate in one direction, they are called polarized. The polarizing filters[9] are used to filter photons. For example, if a photon oscillating in an up-and-down direction passes through the vertically polarized filter, then these photons are called vertically polarized. To generate a perfectly secured symmetric key Alice sends polarized photons to Bob. Then to agree on the same secret key bits, it’s mandatory that Bob holds his filter the same way as held by Alice. As shown in below figure 1, it allows the passing of light denoted by the “yellow colour”.

Article Received: *06 April 2023* ***Revised:*** *24 May 2023* ***Accepted:*** *06 June 2023*

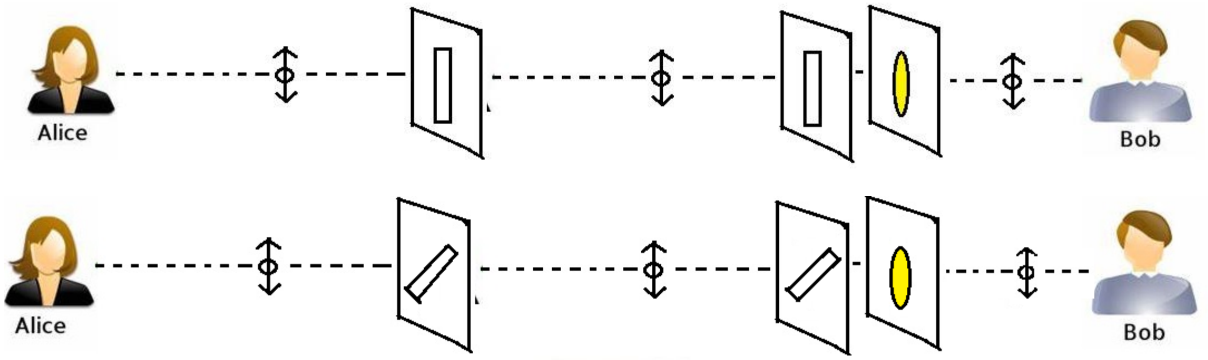


Fig1: Photons polarization using two same Polarization filters

In the case depicted in Fig. 2, if Bob holds his filter crosswise to the direction of Alice's polarization filter, then no photon passes through.

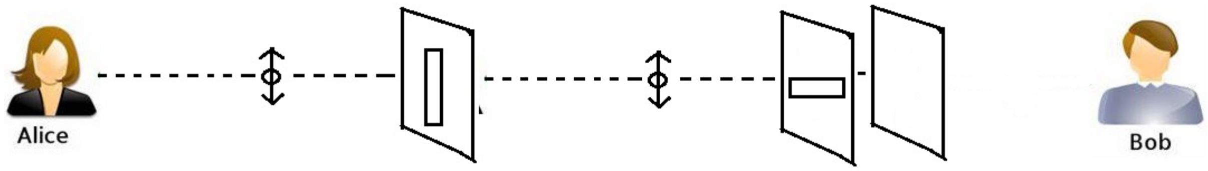


Fig.2: Photons polarization using two different polarization filters

The third case is where Bob turns his filter just a little bit to Alice's polarization direction which means if he holds it diagonally. Then there is a 50% possibility of photons passing through the diagonally held polarization filter, i.e. light may or may not pass. But if Alice polarized the photon diagonally and also bobs polarized the filter is diagonally then the photon passes

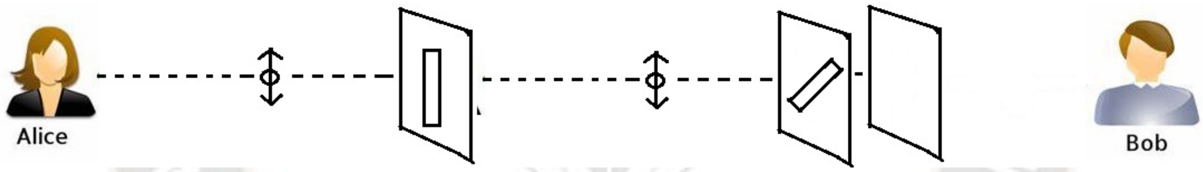


Fig.3: Photons not passing by using two different polarization filters

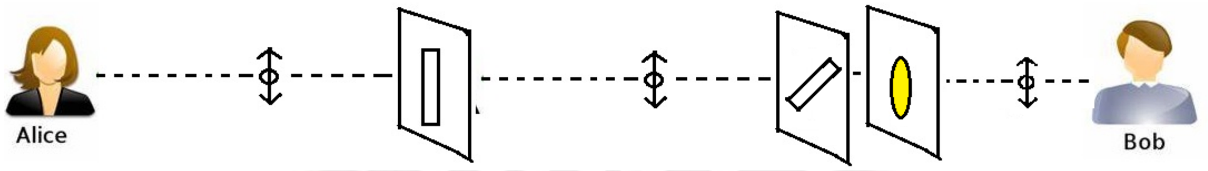


Fig.4: Photons passing by using two different polarization filters

The Quantum key is generated by keeping a record of the polarization state used. Alices makes notes of the polarization with which she sent the photons off and Bob makes a note of how he held his filter and whether light was received or not. As shown in fig. 5, Alice and Bob use two communication channels first is an optical channel to send and receive the polarized photons and the second is a public channel to talk publicly about how Alice polarized her photons and how Bob held his filter. Alice and Bob further delete the bits which are polarized using two different polarization filters, as depicted in fig.6. From the remaining ones, they build their symmetric quantum key.

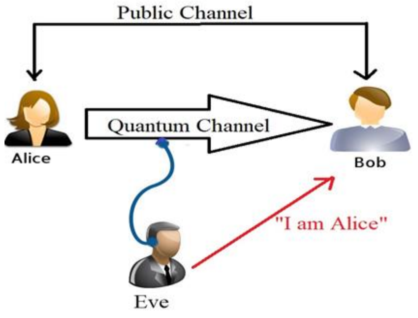


Fig. 5: Quantum key distribution System Architecture with a quantum channel and a public classical authenticated channel.

DOI: https://doi.org/10.17762/ijritcc.v11i7s.7015
***Article Received:** 06 April 2023 **Revised:** 24 May 2023 **Accepted:** 06 June 2023*

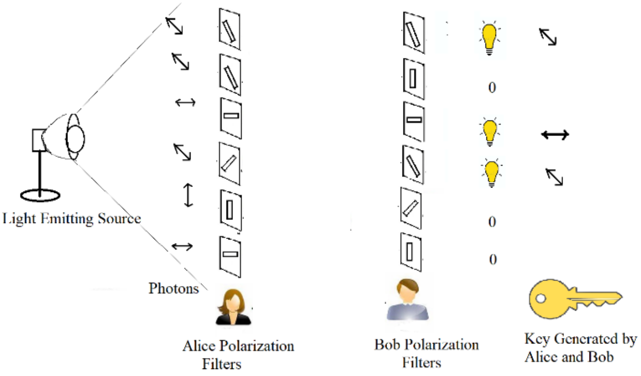


Fig 6: Process of Photon Polarization and Quantum Key Generation using the quantum and public channels.

If Eve wants to intercept the communication, then she holds her filter in between and looks if the light gets through. She has to send a new photon to Bob afterward. But she does not know if she has held the filter correctly. If Eve doesn't see any light, means she could have held her filter crosswise to Alice's filter or just slightly differently, but the photon didn't get through. If Eve does see light it could still be because a photon came through with the filter slightly rotated, so there is a possibility that she may have still held the filter incorrectly. Hence, Eve doesn't know if holding the filter diagonally was correct or not. The measurement and no-cloning property of photons restrict Eve from trying both possibilities. This leads to increased guesswork for Eve, about what to send to Bob. Alice and Bob only talk later about how they used their filters and which parts they can use for their key. Eve however has to decide beforehand whether she was correct with diagonal or non-diagonal. But without the public conversation, Eve has to guess how to proceed and thus makes often mistakes. Bob makes as many mistakes as Eve but his are deleted. Before Alice and Bob build their key, they compare individual bits. They discard the photons which are polarized using two different filters. The most special feature about QKD is that no one can eavesdrop on it without being noticed. Since QKD is based on the randomness of quantum mechanics, whether photons can pass through slightly twisted filters or not. QKD is among the most secured method for Key distribution, also because it is less prone to attacks used against traditional cryptographic methods[10].

II. Literature Survey

Quantum Key Distribution is an emerging technology that allows two parties to securely generate and share cryptographic keys using principles of quantum mechanics over a public channel without the need for any pre-shared secret. QKD has emerged as a promising solution to the security issues in wireless sensor networks, which are vulnerable to attacks due to their limited resources and exposure to the underwater environment. QKD can be implemented in the acoustic communication channels i.e UWSN and optical communication channels commonly said as Underwater Wireless Optical Communication [UWOC] [11]. Therefore, this literature survey will be divided into two parts to explore the current state of research in QKD for UWSNs and QKD for UWOC.

QKD in UWSN:

In recent years, there has been a growing interest in using QKD in underwater wireless sensor networks (UWSNs) due to their high-security requirements and unique communication characteristics. However, underwater wireless sensor networks (UWSNs) pose unique challenges for QKD due to the characteristics of the underwater environment, such as the high attenuation, multipath fading, and Doppler shift. Therefore, several research works have been conducted to explore the feasibility and performance of QKD in UWSNs. Underwater Wireless Sensor Networks (UWSNs) is a type of network that uses wireless communication between sensors deployed in the ocean to collect data. QKD can be used to secure communication in UWSNs, which are vulnerable to attacks due to the characteristics of the underwater environment. In an underwater WSN (UWSN), where communication is challenging due to harsh underwater conditions, QKD can provide secure and reliable communication. Quantum key distribution (QKD) has been proposed as a solution to this problem.

Secure Communication in UWSN using QKD [12], proposes a QKD-based scheme for secure communication in UWSNs. The authors use a single photon detector to detect the presence of eavesdroppers and ensure the security of the key distribution. The scheme is evaluated using simulations and compared to a traditional key distribution scheme. The results show that the QKD-based scheme provides better security than the traditional scheme.

QKD in Underwater Acoustic Sensor Network [13], its a QKD scheme for UWSNs that uses the time-reversal technique to overcome the challenges posed by the underwater environment. The authors use simulations to evaluate the scheme and compare it to other key distribution schemes. The results show that the QKD scheme provides better security than the other schemes and is more suitable for UWSNs. Similarly, a comprehensive review on the challenges posed by the underwater environment and the different approaches that have been proposed for QKD in UWSNs is discussed in [14].There are research works, in which presence of noise and turbulence in underwater QKD is being considered[15]. The proposed protocol uses a modified BB84 protocol and incorporates error correction and privacy amplification techniques to improve the key generation rate and security. The authors conducted simulations to demonstrate the effectiveness of the proposed protocol under different underwater conditions. In state-of-art, the researchers have also developed a hybrid QKD protocol for UWSNs [16], that combines the BB84 protocol with a complementary protocol based on coherent-state modulation. The proposed protocol can adapt to the varying underwater conditions and provides an improved key generation rate and security compared to existing protocols. The authors conducted simulations to evaluate the performance of the proposed protocol under different underwater scenarios. It's important to do a security analysis of existing QKD protocols proposed for UWSNs. As done in [17], where the authors discuss the security threats that can affect QKD in UWSNs and propose countermeasures to mitigate these threats. The paper also provides a comparative analysis of the existing QKD protocols and highlights their strengths and weaknesses. The "energy", is a precious resource in UWSN. So each algorithm developed for the underwater environment must be energy efficient. Therefore research work on QKD for UWSN proposes a QKD protocol for UWSNs with energy harvesting nodes [18]. The proposed protocol combines the BB84 protocol with a power allocation scheme that optimizes the energy usage of the nodes. The authors conducted simulations to demonstrate the effectiveness of the proposed protocol under different underwater scenarios.

QKD in UWOC: Underwater wireless optical communication (UWOC) is a communication technique that uses light/laser as a medium to transmit data in underwater environments. It is an emerging technology that provides high-speed data transfer and low latency in underwater environments. However, the security of data transmission is a critical issue at UWOC. Combining QKD with UWOC can provide a secure and efficient communication channel for underwater applications. However, UWOC faces challenges such as scattering, absorption, and turbulence that can affect the performance of QKD. QKD can be used to secure communication in UWOC, which is vulnerable to attacks due to the characteristics of the underwater environment. Therefore, there is a need to investigate the feasibility of using QKD in UWOC. In this literature review, we summarize the existing research and the current state of research on QKD in UWOC. Several studies have been conducted to investigate the performance of QKD in UWOC. There are several QKD protocols proposed for UWOC channels, along with their advantages and limitations [23]. In this literature review, we will discuss the research done on QKD in UWOC channels.

Experimental Demonstrations: There is a real-time experimental demonstration of QKD, done over an outdoor optical wireless communication channel at a distance of 1.9km [19]. The authors use a custom-built transmitter and receiver to send and receive quantum signals. The results show that QKD can be successfully implemented over long distances in an outdoor environment. Another experimental demonstration of QKD in UWOC [20] shows that QKD can be successfully implemented in UWOC, although the performance is affected by the underwater environment. The commercial QKD system and a UWOC system is establish to exchange a secure key over a distance of 50 meters [24]. The results show that QKD can be successfully implemented in UWOC channels, even in the presence of environmental noise and signal attenuation. The authors use a commercial underwater optical communication system to send and receive quantum signals. In their work, Zhu et al. (2021) [25] demonstrated an experimental implementation of QKD in UWOC. They used a free-space optical channel to simulate the underwater channel and showed that the proposed protocol can achieve a high key generation rate in the presence of turbulence and scattering. There are various secure QKD schemes for UWOC, like a work in [21] that proposes a double random-phase encoding scheme to encrypt the quantum signals and a Gaussian beam to reduce the effect of turbulence. The results show that the proposed scheme can achieve high security and a low error rate in UWOC.

QKD Performance Analysis: A performance analysis of QKD in UWOC shows that QKD can achieve high key generation rate and low error rate in UWOC under certain conditions [22].The researchers have consider various factors that affect the performance of QKD, such as channel loss, noise, transmission distance, signal attenuation, and turbulence. The results shows that QKD can provide a secure and efficient communication channel in UWOC scenarios, but the performance of different protocols varies depending on the channel conditions. Researchers have derive a model for the channel loss and analyze the error rate in QKD due to channel noise. It also shows that the performance of QKD in UWOC is significantly affected by the channel noise[26].Hence from state-of- art [27], it can be theoretically proven that performance of QKD is enormously affected by underwater environment and channel condition. In the analysis work by, Wang et al. (2021) [28] analyzed the performance of QKD in UWOC under different channel conditions. They considered the effects of scattering, attenuation, and turbulence and showed that the key generation rate decreases as the channel conditions become more severe. They also proposed a method to optimize the system parameters to maximize the key generation rate.

Focused Study on QKD Key Generation Rate: A study by Yi-Hua Zhou et al. [29] investigated the performance of QKD in a long-distance UWOC channel. The authors used a combination of polarization modulation and pulse-position modulation to increase the key generation rate in the channel. In a study by Yicheng Shi et al. [30], the authors proposed a QKD protocol that utilizes polarization entanglement in UWOC channels. The study showed that the proposed protocol can achieve a higher key generation rate compared to traditional QKD protocols in UWOC channels. Finally, a study by Qi-Hang Lu et al. [31] investigated the effect of scattering on QKD in UWOC channels. The authors proposed a QKD protocol that utilizes spatial-mode multiplexing to mitigate the effect of scattering on the key generation rate. In another study by Zhiwei Tao et al. [32], the authors proposed a protocol for QKD in turbulent UWOC channels. The proposed protocol utilizes adaptive optics and a phase-randomized reference beam to mitigate the effect of turbulence on the key generation rate. In a study by Vishal Sharma,[33], the authors investigated the effect of channel noise on QKD in UWOC. The study showed that QKD is robust to channel noise in UWOC, but the key generation rate decreases as the noise level increases. In 2008, G.S. Buller et al. [34] proposed a QKD scheme for UWOC channels that used a single-photon avalanche diode detector (SPAD) to detect the weak quantum signal. They simulated the proposed scheme and found that it was resistant to noise and could achieve a high secret key rate. In 2021, [35] Trushechkin et al. proposed a QKD scheme for UWOC channels that used a decoy-state method to prevent eavesdropping. They simulated the proposed scheme and found that it could achieve a high secret key rate with low error rate and high signal-to-noise ratio. A QKD scheme for UWOC channels that used a time-frequency coding technique to increase the signal-to-noise ratio was proposed by Zhu et al. [36]. They simulated the proposed scheme and found that it could achieve a high secret key rate with a low error rate and high signal-to-noise ratio.

Comparison with other encryption techniques: In their work, Pietro et al. (2023) [37] compared the performance of QKD with other encryption techniques in UWOC. They showed that QKD outperforms other techniques in terms of security, key generation rate, and resistance to eavesdropping. They also analysed the impact of the channel conditions on the performance of the different techniques. A review of the different QKD schemes that have been proposed for UWOC are discuss by authors in [38] with the advantages and disadvantages of each scheme. They also provide recommendations for future research in this area. The paper also includes a comparison of the different schemes based on various metrics such as security, efficiency, and scalability. This paper proposes a QKD scheme [39] for UWSNs that uses underwater wireless optical communication (UWOC) to distribute the key. The authors use simulations to evaluate the scheme and compare it to a traditional key distribution scheme. The results show that the QKD-based scheme provides better security than the traditional scheme and is suitable for UWSNs. This paper proposes a QKD scheme for UWOC [40] that uses a dual-sender setup to overcome the challenges posed by the underwater environment. The authors use simulations to evaluate the scheme and compare it to other key distribution schemes. The results show that the QKD scheme provides better security than the other schemes and is more suitable for UWOC. This paper proposes a QKD-based scheme for secure communication in UWOC [41]. The authors use a passive decoy-state method to detect the presence of eavesdroppers and ensure the security of the key distribution. The scheme is evaluated using simulations and compared to a traditional key distribution scheme. The results show that the QKD-based scheme provides better security than the traditional scheme.

QKD schemes resistance to various Attacks: In 2021, Liang et al. [42] proposed a QKD scheme for UWOC channels that used dual detectors to increase the signal-to-noise ratio. They analyzed the security of the proposed scheme and found that it was secure against various attacks. In 2021,[43] Huang et al. proposed a QKD scheme for UWOC channels that used a weak coherent pulse to transmit the quantum signal. They analyzed the security of the proposed scheme and found that it was secure against various attacks.

QKD Scheme	Description	Attacks Resisted
BB84	A protocol that uses the polarization of photons to create a shared secret key between two parties.	Intercept-and-Resend, Man-in-the-Middle
SARG04	A protocol that uses the time-bin encoding of photons to create a shared secret key between two parties.	Intercept-and-Resend, Detector Blinding

QKD Scheme	Description	Attacks Resisted
B92	A protocol that uses the polarization of photons to create a shared secret key between two parties.	PNS (Photon-Number-Splitting)
E91	A protocol that uses the entanglement of photons to create a shared secret key between two parties.	Intercept-and-Resend, Man-in-the-Middle

Table 2: Summarization table of quantum key distribution (QKD) schemes for underwater sensor networks (UWSN) and the corresponding attacks they resist

Note: UWSN stands for underwater sensor networks, and attacks such as "Intercept-and-Resend" refer to a type of eavesdropping attack where an attacker intercepts and copies transmitted quantum signals to resend them to the intended receiver while creating a copy for themselves, allowing them to access the secret key without detection. Other attacks, such as "Detector Blinding" and "Photon-Number-Splitting" refer to attacks that exploit weaknesses in QKD protocols themselves.

Generic QKD Schemes and its Comparative Study

BB84 - The BB84 [44] protocol is one of the most widely used QKD schemes. It provides high security due to the use of non-orthogonal states and random basis choices. However, it requires long key exchange times, which makes it less efficient. The scalability of BB84 is moderate, meaning that it can be used for small-scale applications but may not be suitable for larger networks.

E91 - The E91[45] protocol is another QKD scheme that provides high security. However, it is less efficient compared to other protocols since it requires multiple rounds of communication. Its scalability is low, making it unsuitable for large-scale applications.

B92 - The B92 [46] protocol provides high security and is more efficient than BB84 since it only requires two states. However, its scalability is low, which limits its use for larger networks.

SARG04 - The SARG04 [47] protocol provides high security and is more efficient than BB84 since it only requires two states. However, its scalability is also low, which limits its use for larger networks.

DPS - The DPS [48] protocol provides high security and high efficiency. It uses a photon-number resolving detector to detect photon numbers, which allows for high efficiency. Its scalability is high, making it suitable for large-scale applications.

MDI-QKD - The MDI-QKD [49] protocol provides high security and high efficiency. It uses a measurement-device-independent setup to eliminate side-channel attacks, making it more secure than other QKD schemes. Its scalability is also high, making it suitable for large-scale applications.

Twin-Field QKD - The Twin-Field QKD [50] protocol provides high security and high efficiency. It uses a single-photon detector and a homodyne detector to measure two conjugate variables, which allows for high efficiency. Its scalability is also high, making it suitable for large-scale applications.

QKD Scheme	Security	Efficiency	Scalability
BB84	High	Moderate	Moderate
E91	High	Low	Low
B92	High	High	Low
SARG04	High	High	Low
DPS	High	High	High
MDI-QKD	High	High	High
Twin-Field QKD	High	High	High

Table 3: Comparison of the different QKD schemes based on various metrics such as security, efficiency, and scalability.

The literature survey shows that there is a significant amount of research being done on QKD for UWSNs. The proposed schemes use different approaches such as time-reversal techniques, UWOC, and single photon detectors to overcome the challenges posed by the underwater environment. The simulations and comparisons show that QKD-based schemes provide better security than traditional schemes and are more suitable for UWSNs. Further research is needed to address the scalability and efficiency of QKD-based schemes for UWSNs.

The existing research has also proposed QKD protocols for UWOC and demonstrated experimental implementations, with performance analysis of QKD under different channel conditions. The proposed schemes use different approaches such as time-reversal techniques, UWOC, and single photon detectors to overcome the challenges posed by the underwater environment. The results show that QKD can achieve a high key generation rate and outperform other encryption techniques in terms of security and resistance to eavesdropping. These schemes use different techniques to improve the signal-to-noise ratio and prevent eavesdropping. The simulation results show that these schemes can achieve high secret key rates with low error rates and high security against various attacks. In state-of-art, QKD can be successfully implemented in UWOC, although the performance is affected by various factors such as channel noise, turbulence, and underwater environment. QKD has the potential to provide high-security communication in UWSNs, which are critical for a wide range of applications, including environmental monitoring, oil and gas exploration, and underwater surveillance

However, there are still open research questions in this field, such as how to optimize the QKD protocols for specific underwater environments and how to integrate QKD with other communication techniques, how to improve the performance of QKD in UWOC , high cost of QKD systems, limitations of underwater communication channels and to explore its practical applications in real-world scenarios. In context with above literature review our research focuses on developing more efficient QKD protocols for UWOC and exploring the use of QKD in other types of underwater communication systems.

III. Proposed Methodology

In information security, the key generation algorithms are generally divided into two classes symmetric (same key) and asymmetric (two different keys) cryptographic algorithms. In the recent theory of data security, keys are considered the heart of secure communication, but it’s a difficult task to ensure an attack-free symmetric key exchange. There are major challenges in symmetric key cryptography such as exhaustion of key, data attribution, key exchange, trust, and key management. Due to various problems in symmetric key cryptography, there was an increase in the importance of public key cryptography.

In our proposed work, we thought of bringing the same revolutionary story in the field of “ Quantum Cryptography”. The quantum key distribution discussed in section 1, is actually the first and most basic quantum key exchange protocol, named as BB84 proposed in 1984 by Bennett and Brassard. The key generated using the BB84 protocol is based on the Heisenberg principle and non-cloning theorem. Hence, it’s a difficult task for Eve to intercept the communication and determine the polarization state sent from Alice to Bob. This algorithm is proven by Shor and Preskill [51] to be unbreakable and secured without facilitating any need to pre-share secret information.

In spite of being unconditionally secure, the BB84 protocol suffers from a high bit error rate. This is because the total number of bits used for actual quantum key generations is only a quarter of the total number of bits exchanged. The reason is the discardation of bits whose bases selection (rectilinear or diagonal) at the sender and receiver sides does not match. As a result, shortening the key length and increasing the risk of attacks due to shorter keys.

Addressing the above issue, the proposed algorithm work towards, the reduction of the “Bit Error Rate” of the BB84 protocol. The proposed methodology aims to develop an “Enhanced BB84 [EBB84]” protocol which will also be suitable for securing the Underwater Wireless Sensor Network and Underwater Optical Communication Channel.

The proposed algorithm works on the concept of providing quantum security with zero wastage of bits processing cost and memory usage. In order to achieve the “hard security with zero waste” concept the original symmetric key cryptographic BB84 algorithm is converted into public key cryptography. The term “zero waste, is used because the discarded bits are reused and transformed into a public key. The prerequisite to finding an enhanced version of the BB84 protocol needs in-depth knowledge of the original BB84 protocol. Therefore, will first discuss the BB84 algorithmic steps and then an in-detail explanation of the proposed EBB84 algorithm.

3.1 Overview of BB84 : Even after a decade, the BB84 protocol is still considered a benchmark or ideal model for various different protocols. The fundamental explanation of the BB84 protocol is the same as explained in section 1.2,1.3 and 1.4.

BB84 Algorithm

```
1: Alice choose two random bit string ‘k’ and ‘b’, each of n-bits
   k= The bits which are to be encoded
   b=The choice of bases made to encode the bits
2: Alice Sends the encoded n-qubits to Bob
3: Bob choose one random bit string ‘b1’,
   b1= Choice of bases made to perform measurement
4: Create Table with two fields Ki (Outcome of Bob Measurement) and bi
    (corresponding basis of Alice)
5: if(bi != b1)
    {     Discard the Key bits corresponding to the b1 bases bits
    }
   else if (bi =b1)
```

DOI: https://doi.org/10.17762/ijritcc.v11i7s.7015
***Article Received:** 06 April 2023 **Revised:** 24 May 2023 **Accepted:** 06 June 2023*

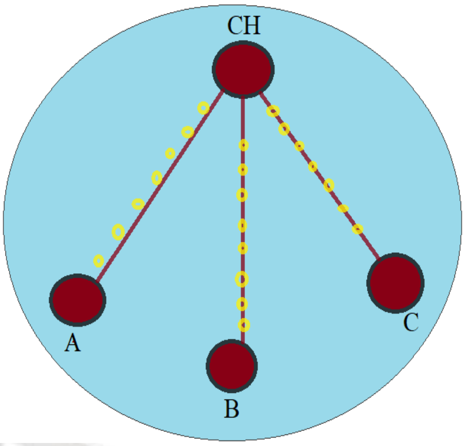
```
{
  ki = k
 }
```

Drawbacks of BB84: The point noted from the above study is that when Alice and Bob use the same polarization filters/ basis they get the exact same results. But when they both use different polarization filters/basis they get uncorrelated results. The key generation is based on a random selection of basis by Alice and Bob. Hence, if we see an average string of qubits obtained by Bob (i.e. raw key) with a 25% bit error rate. Due to such a high bit error rate, even a standard bit error correction scheme will fail. The key is also shortened because 50% of qubits are discarded in the quantum key generation process. Therefore, to overcome these issues, our research aims to propose a slightly enhanced version of the BB84 protocol.

3.2 Enhanced Benette and Brassard 84 [EBB84] QKD Protocol:

The in-detail study and implementation of the BB84 protocol suggested reducing the high bit error rate and maintaining the key size. Secondly, the main objective is also to propose a QKD algorithm suitable for Underwater Wireless Sensor Networks (UWSN)/ Underwater Optical Communication [UWOC].

EBB84 for UWSN/UWOC: The underwater sensor networks mainly use acoustic and optical waves as underwater communication mediums. The main drawback of acoustic medium is limited bandwidth, whereas the optical communication medium provides higher bandwidths for short distances. Underwater optical communication is in boom also due to unbeatable security provided by optical communication channels. The designing and developing of the QKD algorithm for UWSN is a challenging job. As the UWSNs sensor nodes are difficult to recharge and replace. Hence have limited energy in terms of computational power, and memory. Therefore, to develop a QKD algorithm suitable for UWSN, we have enhanced the BB84 protocol in terms of the number of computations and memory consumption. The EBB84 algorithm will be implemented for clustered network scenarios, the diagrammatic representation of a single cluster is as shown in the below fig.4. The cluster head is denoted as ‘CH’ whereas nodes A, B, and C are cluster members. The subsequent fig.5 denotes an attacking scenario with node E as an eavesdropper. The EBB84 algorithm will be executed between each cluster member and its corresponding cluster heads. The CH is responsible to maintain a record of all the public keys with the corresponding node ID’s.



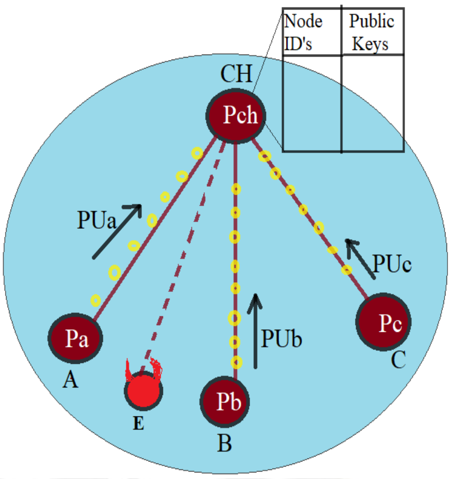


Fig 7: Architectural and Algorithmic View of Proposed Quantum Key Distribution Algorithm.

Pseudocode for EBB84

1. Alice makes a random choice of the polarization filter for qubits that she will send to Bob. For simplicity let’s use the conventions, ‘+’ for rectilinear basis and ‘x’ for diagonal basis.

2. Alice maintains a record of each qubit and the associated polarization filter with it.

3. Alice encodes each qubit, which are logical values (0/1) of a random binary string into respective basis. Alice uses above table to encode qubits. For example, if ‘0’ is encoded in rectilinear bases ‘+’ then the outcome of polarized photon is in horizontal rectilinear basis.Similarly, if 0 is encoded in X digaonal bases then output photon is in +45^0 diagonal bases. Alice then sends the polarized photons to Bob through quantum channel.

Alice Random Bit-String is:	0	1	0	1	0	0
Alice Encoding qubits into Bases:	+	+	X	+	X	+
Photons Send to Bob:	—	|	/	|	/	—

4. Bob performs measurements on the received qubits (i.e. decoding of qubits), by doing a random selection of polarization filters. A completely non-correlated random number is generated in some cases, where Bob and Alice use different polarization filters for encoding and decoding. The decoded string is also known as the raw key.

Photons Received by Bob: — | / | / —

Decoding of Photons: X + X X X +

Bobs Decoded String: 1 1 0 1 0 0

6. The selection of polarization filters by Alice and Bob is then shared over public channels. Note, that the result of the measurement is not shared as Alice and Bob know that their results are correlated in those cases where both have used the same polarization filters. The instances where bases matches are then selected to generate shared key. Further, Bob randomly reveals two bits from the shared key,

Bases shared over Public Channel: (Alice) + + X + X +

(Bob) X + X X X +

Bases Matching Ok Ok OK OK

Shared Key 1 0 0 0

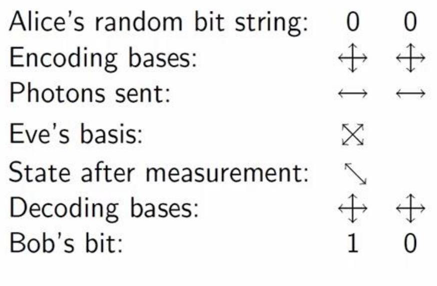
Bits revealed by Bob 0 0

Alice Conforming Bits ok ok

Resulting Secret Key 1 0

7. Alice and Bob, these steps generate two keys shifted key and a raw key. The shifted key consists of only correlated bits, which means that the bases /polarization filter selection is the same. The raw key consists of only non-correlated bits. In the BB84 protocol, this raw key is completely discarded, and the shifted key is considered the secret key. These results in a high bit error rate, wastage of processing power, and unnecessary utilization of memory space. At the same time, avoiding repetition and managing a secret key becomes a difficult job. This also makes the BB84 protocol prone to different attacking scenarios []. Hence, the EBB84 protocol reuses the bits of the raw key to generate the public key.

7) In case of no eavesdroppers, the sender and receiver will hold perfectly correlated sifted keys. But in the case of the attacking scenario, Alice and Bob can determine the presence of an eve by randomly testing elements of their sifted keys and comparing their values. They publicly agree on what bits they will use for testing, and publicly compare the values of the test bits. If the values are different, then they can assume the presence of Eve.



Alice's random bit string:	0	0
Encoding bases:	✛	✛
Photons sent:	↔	↔
Eve's basis:	✕	
State after measurement:	↘	
Decoding bases:	✛	✛
Bob's bit:	1	0

Proposed QKD-based Cryptographic Algorithm:

EBB84 Algorithm

```
1: Alice choose two random bit string ‘k’ and ‘b’, each of n-bits
   k= The bits which are to be encoded
   b= Public Key of Alice (choice of bases made to encode the bits)
2: Alice Sends the encoded n-qubits to Bob
3: Bob choose one random bit string ‘b1’,
   b1= Choice of bases made to perform measurement
4: Create Table with two fields Ki (Outcome of Bob Measurement) and bi
    (corresponding basis of Alice)
5: if(bi != b1)
     {      Discard the Key bits corresponding to the b1 bases bits
     }
   else if (bi =b1)
   {
     ki = k
     where ki is Private Key of Alice and Bob
```

IV. Results and Discussion

The verification and validation of our proposed asymmetric key-based EBB84 algorithm is done by comparing the results of EBB84 with the BB84 algorithm. The simulation is done using processor AMD Ryzen 55600U with Radeon Graphics (2.30 GHz) and installed RAM of 16.0 GB (15.3 GB usable). Operating system used is Windows 11 with system type as 64-bit operating system, x64-based processor. The programming language used is python and the development environment is NS3 UAN model and IBM Qiskit. The Qiskit is an open-source platform for working directly on IBM Quantum Computers at algorithmic and circuit levels. The results are judged by comparing both algorithms based on their execution time, key exchange time, time required for key generation, QBER (Quantum Bit Error Rate) ,and their resistance against different attacks. The graphs shows that execution time and the key generation time of BB84 algorithm is comparatively more than EBB84.Also the QBER is more for BB84 protocol as compared to EBB84.

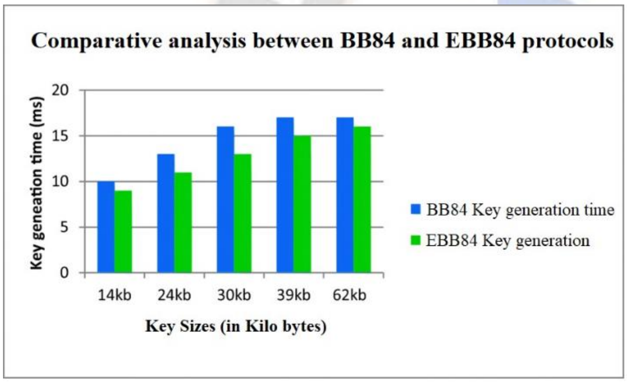


Fig 8: Comparative analysis of BB84 and EBB84 quantum cryptography protocol

Execution Time Analysis: The fig.8 shows the execution time analysis, based on the key generation time of BB84 and EBB84. The graph is plotted by using input parameters as qubits sizes/ size of basis. The resulting graph shows that for both the algorithms execution time (in milliseconds) is gradually increasing with an increase in basis size. In comparison, the proposed protocol execution time is slightly less than the BB84 protocol. For example, for the basis size of 14kb, the execution time of BB84 is 10ms whereas for EBB84 execution time is 8ms. The graph shown in fig.9 , shows the time complexity of the proposed algorithm, EBB84. The complexity changes with varying input sizes. If greater is the key size then more is the execution time required by EBB84.But the results achieves are still satisfactory if compared with time complexity analysis of BB84,shown in fig. 10.

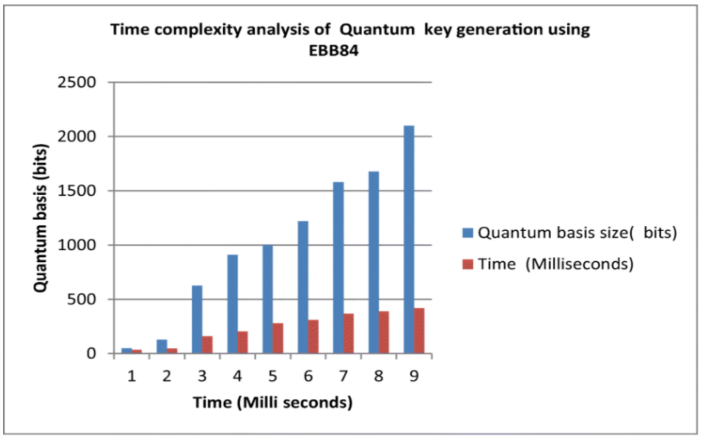


Fig 9: Time complexity analysis of quantum key generation for EBB84

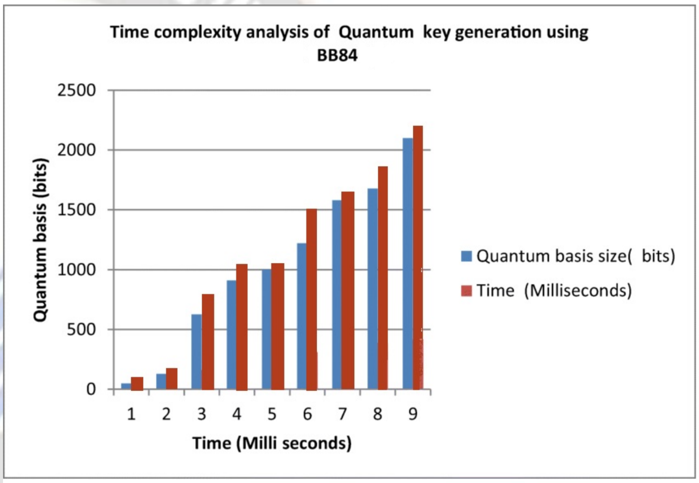


Fig. 10 : Time complexity analysis of quantum key generation for BB84

Analysis against different security attacks: The underwater optical wireless link is open for attackers to snatch the shared secret key. The underwater cryptographic algorithms and BB84 quantum key distribution algorithms have a chance to lose their secret key value. From state -of -art, it is proven experimentally and theoretically, that all known attacks like jamming attacks, spoofing attacks, DoS attacks, sinkhole attacks, wormhole attacks, blackhole attacks, and quantum attacks are possible in various underwater cryptographic schemes based on ECC, AES, DES, and quantum mechanics. But the proposed EBB84 algorithm is using quantum mechanics for asymmetric key generation and it also outstands in terms of its key generation process, space, and energy-aware computations.

Estimation of Quantum Bit Error Rate (QBER): The multiple uses of quantum repeaters, sensors, and water conditions introduce errors in transmitted qubits/photons. This affects the shifted key/shared secret key in terms of confidentiality and authenticity. Therefore, to identify number of eavesdropping/erroneous photons we use a formula for calculating Quantum Bit Error Rate [QBER]. The QBER is formulated as follows,

$$\text{QBER} = \frac{\text{Number of Erroneous Photons}}{\text{Total number of Received Photons.}}$$

The below fig.11 shows that the EBB84 QBER is comparatively lesser then BB84. At last, the calculated value of QBER is compared with a threshold value. If the value of QBER is greater than the threshold value, then algorithm instructs to stop the optical communication. The value '0' of QBER suggest 'no attack situation in quantum channel', but whereas a non-zero QBER value indicates non-ideal devices and erroneous shifted key.

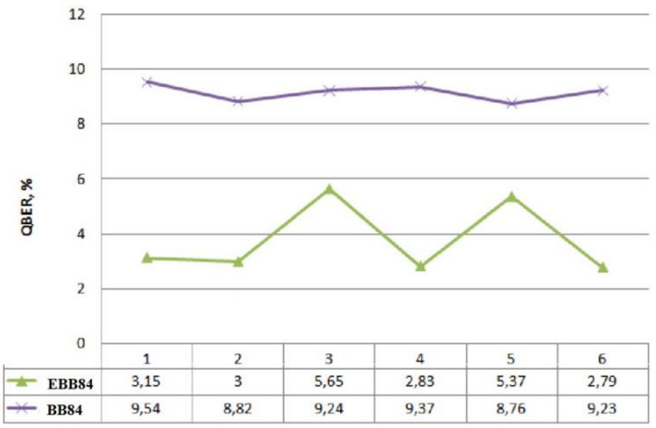


Fig.11: QBER plot for EBB84 and BB84

V. Conclusion

In this research work, we have studied and implemented a benchmark setter algorithm in Quantum Cryptography, popularly known as BB84 protocol. The outcome of BB84 was concluded to be insufficient for Underwater Wireless Optical Sensor Networks, in terms of energy and memory consumption. The BB84 protocol fails to utilize 60% of its generated key bits. This happens due to the qubit discarding process, conducted for different bases choices made by Alice and Bob. The BB84 can only exploit 40% of its secret key, that too in no attacking situation, making it unsuitable for the underwater environment. Therefore, we aimed to design an energy-efficient and highly secured quantum cryptographic algorithm for underwater optical communication channels. And as a result, we came up with the Enhanced version of the BB84 protocol named as EBB84. The proposed algorithm utilizes 100% of its generated key bits in case of no eavesdropping. This makes the secret key size of EBB84 comparatively longer than BB84, which makes it stronger and at same point also drastically reduces the wastage of the underwater node's energy and memory. Although with many advantages of the EBB84 algorithm, there is a drawback of the execution time required is slightly longer than BB84.But the time difference is very less and is ignorable for any cryptographic operations. The EBB84 also conserves the property of BB84 of being 'unconditional secure', against different types of attacks. The result analysis of EBB84 algorithm shows that the proposed algorithm is also efficient in terms of time complexity and minimum quantum bit error rate.

References

[1] Parikshit N. Mahalle, et.al., "The underwater world for digital data transmission", Springer, 2021.

[2] Meiwei Kong, et.al. ,"Underwater Optical wireless sensor network for real-time underwater environmental monitoring", Volume 1028,Next Generation Optical Communication: Components, Sub-Systems,San Francisco, California,United States,2022.

[3] John Robert Potter, "The JANUS underwater communications standard", IEEE OES UComms 14 Underwater Communications Networking Conference,2014.

[4] Irfan Ahmad, et.al. ," Underwater Wireless Communications and Networks", Hindawi,2021.

[5] https://www.imo.org/en/ourwork/legal/pages/unitednationsconventiononthelawofthesea.aspx#:~:text=The%20United%20Nations%20Convention%20on,the%20oceans%20and%20their%20resources.

[6] Ivan Djordjevic, " Quantum Mechanics Fundamentals", Quantum Information Processing and Quantum Error Correction, 2012.

[7] Mehrdad S. Sharbaf , "Quantum Cryptography: A New Generation of Information Technology Security System", IEEE, Sixth International Conference on Information Technology: New Generations,2009

[8] Jeffrey Bub , "QUANTUM INFORMATION AND COMPUTATION", Science Direct, Philosophy of Physics,2007

[9] Bharadwaj V. Srividya et.al., "An Emphasis on Quantum Cryptography and Quantum Key Distribution", IntechOpen 2020.

[10] Vimal Gaur, et al. ,"Quantum Key Distribution: Attacks and Solutions", Proceedings of the International Conference on Innovative Computing & Communications,2020.

[11] Mohamad Ali Khalighi, "Underwater wireless optical communication; recent advances and remaining challenges", IEEE, 2014.

[12] Secure Communication in Underwater Wireless Sensor Networks using Quantum Key Distribution" by J. Xu and W. Jia, published in IEEE Access in 2019.

[13] "Quantum key distribution for underwater acoustic sensor networks" by Z. Yu, H. Chen, and J. Ma, published in Optics Express in 2019.

[14] Quantum key distribution for underwater acoustic sensor networks: A review" by Y. Xu, W. Yan, and X. Hu, published in Journal of Systems Engineering and Electronics in 2018.

[15] "Underwater Quantum Key Distribution in the Presence of Noise and Turbulence" by Shijun Zheng, Jie Lin, and Shilin Xiao, published in IEEE Transactions on Communications, 2019.

[16] A Hybrid Quantum Key Distribution Protocol for Underwater Sensor Networks" by Xinxin Zhang, Huanyang Zheng, and Wenjun Sun, published in IEEE Access, 2021.

[17] Security Analysis of Quantum Key Distribution in Underwater Sensor Networks" by Tarek Gaber, Mohamed E. El-Hawary, and Hossam S. Hassanein, published in IEEE Sensors Journal, 2018.

[18] Yanfeng Wang, Qi Wu, and Zhiping Jiang," Quantum Key Distribution in Underwater Wireless Sensor Networks with Energy Harvesting Nodes", Sensors, 2021.

[19] R. F. Rice et al. ,Experimental Demonstration of Quantum Key Distribution over a 1.9 km Outdoor Optical Wireless Communication Channel", 2012

[20] Auma, G., Goldberg, R., Oliveira, A., Seo-joon, C., & Nakamura, E. Enhancing Sentiment Analysis Using Transfer Learning Techniques. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/129

[21] C. Capella et al. , Quantum Key Distribution in Underwater Wireless Optical Channels: Experimental Demonstration",2014.

[22] H. Liang et al. , "Secure Quantum Key Distribution for Underwater Wireless Optical Communication" ,2016.

[23] H. Wang et al. ,"Performance Analysis of Quantum Key Distribution over Underwater Wireless Optical Channels", 2020.

[24] X. Sun, et al., "Quantum Key Distribution in Underwater Wireless Optical Channels: An Overview" ,2019.

[25] Y. Li, et al. ,"Experimental demonstration of quantum key distribution in underwater wireless optical communication",2020.

[26] zhao feng, et al., "Experimental underwater quantum key distribution and decoy-state quantum key distribution", Optics Express , 2021.

[27] Shi-Cheng Zhao ," Performance of underwater quantum key distribution with polarization encoding", Journal of the Optical Society of America, 2019.

[28] Khalighi M. A. et al. ,"Quantum Key Distribution over Underwater Wireless Optical Channels" ,2011.

[29] Mahsa Sharifzadeh, Mahsa Ahmadirad , " Performance analysis of underwater wireless optical communication systems over a wide range of optical turbulence", Optics Communications,2018.

[30] Yi-Hua Zhou , et al., "Mode-pairing quantum key distribution based on pulse-position modulation", Optik,Elsevier,2023.

[31] Yicheng Shi , et al., "Stable Polarization Entanglement based Quantum Key Distribution over Metropolitan Fibre Network",IEEE,2020.

[32] Qi-Hang Lu, "Quantum Key Distribution Over a Channel with Scattering", American Physical Society,2022.

[33] Zhiwei Tao, et al., "Mitigating the effect of atmospheric turbulence on orbital angular momentum-based quantum key distribution using real-time adaptive optics with phase unwrapping", Optic Express,2021.

[34] Vishal Sharma, "Effect of Noise on Practical Quantum Communication Systems", Defence Science Journal,2016.

[35] G.S. Buller, et al., " Single-photon avalanche diode detectors for quantum key distribution", IET Optoelectronics, IEEE,2008.

[36] Anton Trushechkin ,et al., "Security of the decoy state method for quantum key distribution", Physics-Uspekhi,2021.

[37] Zhu Chang Hua , et al.,"A New Quantum Key Distribution Scheme Based on Frequency and Time Coding", Chinese Physics Letters,2010.

[38] Pietro Paglierani, et al. " A tutorial on Underwater Quantum Key distribution", IEEE,2023.

[39] Ansari , A. S. . (2023). Numerical Simulation and Development of Brain Tumor Segmentation and Classification of Brain Tumor Using Improved Support Vector Machine. International Journal of Intelligent Systems and Applications in Engineering, 11(2s), 35–44. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2505

[40] Silvia Tarantino, et al., "Feasibility study of Quantum Communications in Aquatic Scenarios",Optik,2020.

[41] Y. Chen, H. Fu, and L. Wang ,"Quantum key distribution for underwater optical wireless communication: a review" ,Journal of Optics in 2019.

[42] Dr. M. Varadharaj. (2019). Density Based Traffic Control System with Smart Sensing Of Emergency Vehicles. International Journal of New Practices in Management and Engineering, 8(02), 01 - 07. https://doi.org/10.17762/ijnpme.v8i02.75

[43] C. Qiao, Y. Xu, and Y. Zhang, "A Novel Quantum Key Distribution Scheme for Underwater Wireless Optical Communication" ,IEEE Transactions on Communications in 2018.

[44] J. Zhang, X. Chen, and J. Song, "Security Enhancement of Underwater Wireless Optical Communication via Quantum Key Distribution" Journal of Lightwave Technology in 2019.

[45] Liang Yang ,et al., "On the Performance of Mixed FSO-UWOC Dual-Hop Transmission Systems", IEEE Wireless Communication Letters,2021.

[46] Warren P. Grice, et al., "Quantum secret sharing using weak coherent states", U.S. Department of Energy, Office of Scientific and Technical Information,2019.

[47] Bennett CH, Brassard G , "Quantum cryptography: public key distribution and coin tossing", IEEE Conference on Computer, Systems and signal Processing, 1984.

[48] Ekert. A, Phys. Rev. Lett. 67, 661-663 ,1991.

[49] Charles H. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. 68, 3121,1992.

[50] Valerio Scarani, et al. ,"Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations", Phys. Rev. Lett. 92, 057901,2004.

[51] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto, Differential Phase Shift Quantum Key Distribution, Phys. Rev. Lett. 89, 037902 ,2002.

[52] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108, 130503 ,2012.

[53] Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. Phys. Rev. A 98, 062323,2018.

[54] Shor and Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, 85 ,2000.