

Original Article

# Survey on Information Security and Quantum Cryptography

Masira Kulkarni<sup>1</sup>, Prashant Dhotre<sup>2</sup>

<sup>1</sup> PhD Student, IT Department, MIT School of Computing, MITADT University, Loni Kalbhor, Pune, India

<sup>2</sup> Professor, IT Department, MIT School of Computing, MITADT University, Loni Kalbhor, Pune, India

Received Date: 05 March 2023

Revised Date: 20 March 2023

Accepted Date: 06 April 2022

**Abstract:** The number of Internet users globally peaked at 4.7 billion in early 2020, representing a startling 1,187% surge in just 20 years. In addition, our growing reliance on Internet-based technology produces enormous amounts of data (1 followed by 21 zeros!). A large portion of this data needs to be encrypted because it contains "sensitive" information. To make sure that only authorized persons in possession of encryption keys may access this data, we utilize sophisticated encryption technologies. Data may be encrypted, or made into information that can only be decoded by someone with the right "key," by converting plain text into scrambled data. Quantum cryptography, then, is the application of quantum physics to the encryption and transmission of data in an unbreakable manner. This study will address the limitations of the traditionally employed encryption algorithm, some literature reviews, and the concept of quantum cryptography along with its working structure, limitations, and applications.

**Keywords:** Cryptography methods, Quantum cryptography, Quantum key distribution (QKD), Photon polarization methods.

## I. INTRODUCTION

The science of protecting information from outside observers by converting the information to codes using certain techniques is termed as cryptography. The information, or plaintext, is altered into cipher text, or unfathomable text, through some encryption techniques. We can decode the cipher text into plaintext just by using key at the user side for which we need to share with them by using the communication channel. We can heighten our security by utilizing cryptography to make associations that are more protected and flawless. Because of enhancements in cryptography strategies, just approved clients ought to have the option to get to encrypted files, folders or network connections.

Cryptography focuses on following some principles:

1. **Confidentiality:** Confidentiality is the condition in which only the intended receiver can see the contents of message after encrypting it.
2. **Non-repudiation:** On the off chance that a message is non-renounced, the individual who sent it can't later withdraw or debate the plan behind it.
3. **Integrity:** Integrity is the assurance in which the data will not be changed during its storage and transport time.
4. **Authenticity:** Authenticity can confirm the message and intended receiver's message.

These principles help us in assuring that the information is safe and unblemished. There are three different types of cryptography:

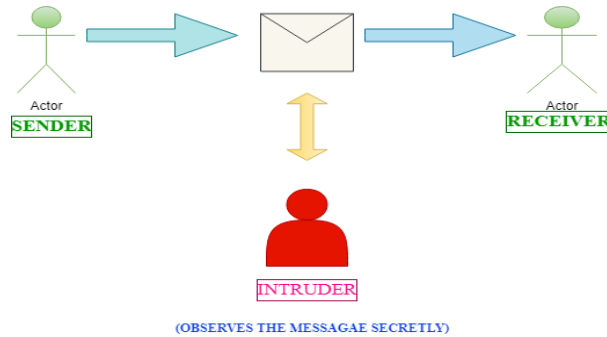
1. Symmetric-key Algorithms
2. Asymmetric-key Algorithms
3. Hash Functions

While there are tons of symmetric-key cryptographic procedures that are either accepted or known to be quantum-safe, laying out shared secret symmetric keys through a depended medium is customarily achieved with public key strategies that are known to be powerless against quantum dangers. This is the greatest imperfection of symmetric key procedures in the presence of a quantum PC. This raises the issue of how to move symmetric keys between remote gatherings without utilizing old-fashioned, perilous public key procedures securely.

QKD Quantum Key Distribution is one of the suggested fixes for the key distribution issue. Other than RSA or ECC, there are other key distribution techniques that use public key methods. However, QKD is a cryptographic starting point which delivers security that is ensured by the laws of physics, in contrast to conventional public key techniques. It has been demonstrated that QKD, a technique for secure key setup [GIS02], is information theoretically safe against any assault, including quantum attacks. This indicates that QKD is safe right now and always will be, even if an enemy possesses infinite

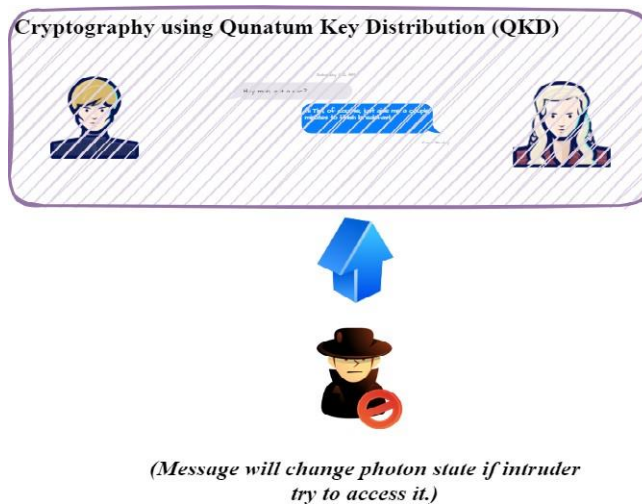
computational resources, including infinite classical and quantum computing resources.

QKD resists future developments in cryptanalysis or quantum computing by allowing verifiable security based on basic rules of quantum physics. The Advanced Encryption Standard (AES) or one-time pad encryption may both be utilized with quantum safe symmetric key algorithms, and as a result, quantum key distribution offers a way to transfer secret keys in an encrypted fashion.



**Figure 1: Attack of Intruder on Messaging Channel**

Above figure shows how the message is secretly observed by the intruder. They can change the message using certain encryption and decryption methodology. To avoid this situation we can make use of quantum key distribution (QKD) for message encryption and decryption.



**Figure 2: Basic Model of Cryptography using QKD**

Individual photons are used in quantum key distribution (QKD) to exchange cryptographic keys between the transmitter and the receiver. One bit of data is represented by each photon. The photon's states, such as polarization or spin, decide whether the bit is a 1 or a 0. Using this technique, a cryptographic key that has been photon ally encoded may be sent from one side to another. Any effort to measure or decode the message will cause the photons' state to shift due to their special qualities as quantum particles. This ambiguity makes it more likely that the communication will be destroyed or altered, making it simple for both the sender and the recipient to identify a compromised message. In order to avoid interception or decryption, QKD instead detects eavesdropping and causes the communication to self-destruct.

This paper is divided into 6 sections. In section 2 we discussed about the related works, section 3 we study working of QKD Model, section 4 we discussed a case study, section 5 we discussed application of QKD. In section 6, we will conclude our work.

## II. RELATED WORK

An expansive overview of QKD defended optic networks is handed in this study. The basics of qubits, different QKD conventions and strategies, feathers of assaults on QKD conventions, network models, and state of the art styles made to address the crucial systems administration issues in QKD. Gotten optic associations are points that have been shrouded to fabricate a appreciation of QKD got optic associations alongside this paper fragment a portion of the issues and difficulties that we want to determine in future. They do a thorough analysis of the slice- edge QKD defended optic networks, which will impact communication networks in the coming decades. They detail the crucial establishment procedure and clarify the procedures and styles employed in QKD defended optic networks [1].

The QKD network is a vital piece of foundation that ensures total security for end clients' and applications' admittance to the key distribution services. Till date, multiple nations and academic institutions have expended money on doing theoretical research and real-world field tests on QKD networks. This paper surveys and sums up the discoveries of past examination on these points and afterward this three security challenges were proposed [2]:

1. The absence of a P2M mechanism in QKD networks.
2. The multiple-path strategy's heavy resource consumption of quantum nodes.
3. The absence of a legitimate security interface between old style end clients/applications and quantum hubs.

As a new generation of cryptography in the information theory realm, QKD is presented in this work as a series of QKD protocols across time. Furthermore, the QKD protocol theoretically resolves a number of quantum cryptography-related problems, in instance, are driven by quantum theory. The non-cloning theory, which ca uses any permeation to change, is what gives quantum mechanics its power. On the other hand, this study's clarification of unclear concepts made it plain what each QKD protocol's mechanism was. This study also shows the result through secure communication, the QKD protocol offers a Secure Shared Key (SSK) between authorized parties. With a 0.0% exposure to the SSK, the secret key should be resilient against any kind of information assault. In several information exchange systems, QKD is anticipated to be the next generation of secret keys. [3].

Sensitive information must be sent between two or more places via a more powerful mechanism. In the future, the security of crucial data will surely be improved by QKD and other QC (quantum computing) methods. A powerful and encouraging step toward a time when we can feel safer about how and what we exchange is quantum encryption. The paper also discusses the exchange of QKD with the help of example and also some correction steps [4].

The study concentrated on the fundamentals of the DVQKD which is also known as Discrete Variable Quantum Key Distribution and CVQKD which means Continuous Variable Quantum Key Distribution protocols, the key characteristics of the most current implementations, and the use of QKD in both conventional and quantum communication networks. The author has explained DVQKD with its modulation, eavesdropping, measurement and key distillation and similarly CVQKD with its modulation, eavesdropping, measurement and reconciliation. Along with it some measures of QKD over optical fiber, free spaced optical QKD, QKD in the traditional internet. Attributes of recent OKD implementation had been discussed in the paper [5].

We also briefly discuss some other fields of study that are still in the theoretical research stage but are receiving a lot of attention from academics. Quantum private correlation, quantum mysterious democratic, quantum fixed bid sell off, quantum public key cryptosystem, quantum key understanding, quantum discussion, and quantum character validation are a portion of these areas. Members' characters are not confirmed in QSMC fields like QPC and QKA. This represents a significant risk to the convention's security in light of the fact that any outcast could act like an approved member and take the members' classified data or misdirect others by sending a bogus message. Therefore, it makes sense to research and develop protocols that include authentication procedures. Additionally, the issue of noise has always caused a lot of anxiety in academia [6].

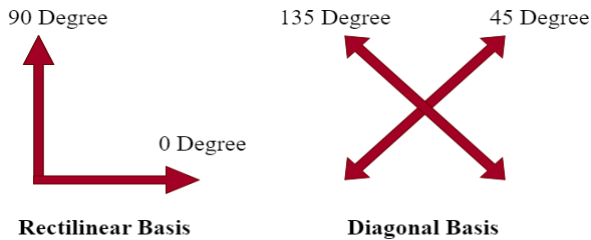
In this article, we present the discoveries of a contraption and convention planned to execute the quantum key dispersion strategy, in which two clients who don't definitely realize each other's private or public keys first trade an irregular quantum transmission comprised of exceptionally faint blazes of spellbound light [7].

## III. QKD WORKING MODEL

The issues with secret-key cryptography are resolved by quantum cryptography by giving two users who are in different places a mechanism to safely construct a secret key and to determine if eavesdropping has taken place[9]. Quantum

cryptography's security is independent of challenging mathematical puzzles. By taking advantage of the characteristics of small particles like photons, quantum cryptography is able to accomplish these astounding feats. The photons have three selected bases for polarization, and measurements made using these bases are likely to yield the following results [1]:

1. Rectilinear this can be either vertical or horizontal.
2. Circular either in left-circular or right-circular.
3. Diagonal at 45 or 135 degrees.



**Figure 3: Photo Polarization State**

Despite the fact that there are three bases, just two bases are at any point utilized in a quantum cryptography convention. However, because photons are quantum particles, their properties can only be determined through measurement. The property of the object is affected by the measurement type. This proposes that a photon's polarization not entirely set in stone after it is estimated, and that the estimation's premise will meaningfully affect the polarization.





#### **A. Process of quantum information and quantum bits**

An interdisciplinary field is that of quantum information processing or quantum information science. It is a synthesis of quantum physics, computer science, information science engineering, mathematics, and chemistry.

The fundamental unit of classical information theory is the bit, or binary digit. It is viewed as a 0 or a 1 regardless of how it is physically represented. For instance, a high voltage denotes a true value of 1, while a low voltage denotes a false value of 0. Quantum information is stored in quantum bits often known as qubits or qbts. There are two operations that take place in quantum cryptography [1].

They are polarization and conversion. To put it another way, the information is divided into bits of 0s and 1s, which are then sent using polarized photons. The sender places photons into a specific quantum state, which the receiver will then detect.

There are four possible polarizations for a photon: 90, 0, 45, and -45 degrees. Three distinct measurement bases are used to determine the size of a photon: rectilinear, circular, and diagonal. The receiver is able to discriminate between photons with polarizations of 0 and 90 degrees or -45 and 45 degrees [1].

<b>Rectilinear</b>	<b>1's</b>	<b>Vertical</b>	
	<b>0's</b>	<b>Horizontal</b>	
<b>Diagonal</b>	<b>1's</b>	<b>Vertical</b>	
	<b>0's</b>	<b>Horizontal</b>	

**Figure 4: Rectilinear State and Diagonal State**

#### **B. Heisenberg Uncertainty Principle**

Only one of a pair of conjugates in a quantum system has a property that can be confidently known, according to the most fundamental Heisenberg Uncertainty Principle (HUP). Heisenberg demonstrated how each possible measurement of a particle's location would modify its conjugate property by stating the Heisenberg Uncertainty Principle, which first applied to a

particle's position and momentum. Therefore, knowing both traits simultaneously and with confidence is not feasible. Quantum cryptography can affect this idea; however it frequently uses the conjugate property of photon polarization on other bases. For communication between transmitter and receiver, photons are perhaps the most practical quantum system since they can travel via fiber optic lines.

### C. Key Exchange method using an example

John and Nick will agree to communicate on a key which is known as shifting key. Here in this key exchange we have consider the BB843 protocol which follows under prepare and measure category. Where sender has to send the series of photonsto receiver and then need to cross check it. There are certain steps to understand the key exchange method:

#### a) Sending Phase

1. Before sending each burst of photons to Nick, John chooses the polarization. The sender and the receiver agree on a common key, and the goal is not to transfer a particular key.
2. Polarized photons are created with the aid of a laser or an LED as the light source.

#### b) Receiving and converting

A process of random way point mobility model as follow:

1. Nick creates a series of circular or rectilinear bases at random and measures the polarization of each photon.
2. Nick informs John the base order he chose, unconcerned that others might overhear this information via the classical channel.
3. John officially acknowledges in the traditional channel that the bases were properly chosen.
4. Aside from the bases they chose properly, John and Nick ignore all other observations.
5. The remaining observations are transformed to binary code, where the left circular or horizontal value is 0 and the right circular or vertical value is 1.

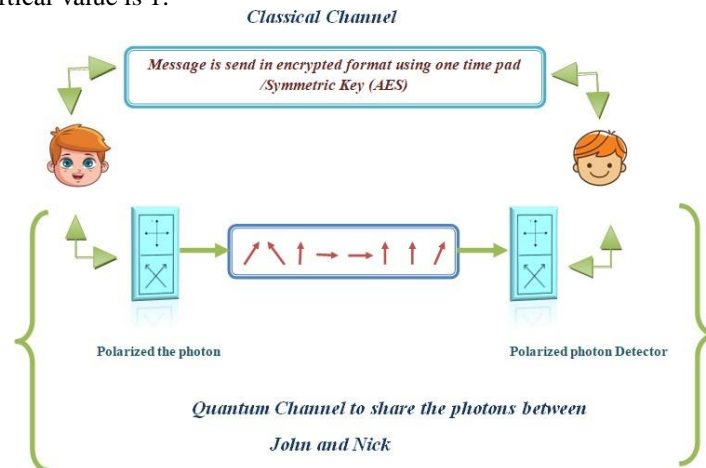


Figure 5: Block Diagram

Alice Sends Photons measuring Basis								
Bits of Photons are	1	0	1	0	0	1	0	1
Bob Detect(Raw Key)								
Bits of Photons are	1	1	1	0	1	1	0	1
Send bits of photons to Alice through classical channel	1	1	1	0	1	1	0	1
Alice confirm the key	T	F	T	T	F	T	T	T
Secret Key	1		1	0		1	0	1

Figure 6: Key Exchange Method

#### **D. Correcting error phase I**

1. John and Nick decide on random permutations of the bits in the final string in order to randomize the placements of errors. Although it is exceedingly difficult to spot two faults right next to one another, it is possible for a series of bits to be altered by an instrument error or random noise. In this scenario, randomization is helpful. To make the risk of numerous errors per block as reduced as possible, the strings are divided into blocks of size  $k$  [4].
2. RD (Random Direction Models): In this model, fundamentally every single hub picks irregular heading and an irregular speed then it moves along the edge and afterward it keeps on rehashing a similar cycle. Thus, this kind of versatility model outcomes in a uniform circulation in the situation region. John's string contains 101100 and Bounce's string contains 101111. Despite the fact that there are two blunders in the block, the equality is as yet 1, for this situation. Making  $k$  little is one of the techniques taken to diminish the probability of this happening since, particularly once the blunders are randomized, there is impressively less likelihood of two mistakes happening in a block of size 50 than there is in a block of 500 [4].
3. For each block, John and Nick compute and trade parities. To maintain security, the computed parity is made available, and the final bit of each block is then destroyed. This is done to render the knowledge useless to Eve [4].
4. Each block with a unique report is divided further. The mistake is located and fixed using binary search. Alternately, if the key's length is already long enough, those blocks might be eliminated [4].
5. Then, steps 2 through 5 are repeated with an increasing block size,  $k$ , to find additional faults. In order to detect more errors, steps 2 through 5 are then repeated with an increasing block size,  $k$  [4].

#### **E. Correcting error phase II**

6. John and Nick perform another randomized check to see if there are any new faults. They compare parities and publicly decide on a random selection of half the bit places in their string before discarding the last digit as previously described [4].
7. There is a  $1/50$  chance that the parities will disagree if the strings are different. The fault is then located and removed using a binary search, as previously mentioned [4].
8. John and Nick can come to the conclusion that their strings differ with probability  $(1/2)^r$  after  $r$  iterations of step 1 go by without any discrepancies. Of course,  $r$  can be increased to any value and still have arbitrary little discrepancies [4].

#### **F. Detecting Eavesdropping**

Quantum cryptography follows the three basic rules:

9. At any given time, particles can exist in more than one location or state.
10. A quantum property cannot be observed without changing or disturbing it.
11. Whole particle cannot be copied.

Using the above three basic principles of quantum cryptography we will come to know whether the Eve has tried to read the message. By publicly comparing a random chunk of their created sequence, John and Nick can look for errors. They can set up a separate channel if they are not happy with the mistake rate. This makes sure that even though John and Nick cannot prevent Eve from listening in, they will always be aware of her presence [4].

### **IV. CASE STUDY**

A combat drone, also known as an unmanned combat aerial vehicle (UCAV), is a device that may be used for target detection, investigation, superintendence, and identification of military activity. In areas that are difficult for drone attacks to reach, use bombs, ATGMs, or missiles. These drones often have varied degrees of control and are followed in real-time. Drone attack and combat intelligence are employed as opposed to UCAV, investigation and superintendence. This kind of drone doesn't require a pilot because it can operate on its own [8].

The drones are lightweight, compact, and GCS-enabled for remote control. The idea of combat drones was introduced by Lee De Forest, U. A. Sanabria, and the creator of radio equipment. They had a piece published in Popular Mechanics in 1940 [8].

The advance military drone was created by nuclear physicist and former director of Lawrence Livermore National Laboratory, John Stuart Foster Jr. When Foster had the idea to make weapons and drew out plans in 1971, he was a model aero plane enthusiast. By 1973, the Defense Advanced Research Projects Agency had created two instances, known as "Prairie" and "Calera." They could stay in the air up to two hours while carrying a 28-pound load thanks to a modified lawnmower motor that propelled them into the air [8].

Israel utilized unarmed US Ryan Firebee targeted drones during the Yom Kippur War in 1973 to pressure Egypt to destroy all of its anti-aircraft systems. Israeli pilots successfully completed this mission without suffering any injuries after quickly exploiting Egypt's porous defenses. Iran employed a drone with six RPG-7 rounds during the early 1990s Iran-Iraq War [8].

2,400 people were said to have died as a result of US drone attacks in January 2014. In just five years, the number of people killed by US drone assaults reached 6,000 in June 2015. To increase secure data transfer, the Internet of Military Things (IoMT) for the battlefield application may use standard security approaches or cryptographic methods. The 1G to 5G communication about their latency that is started in the drone of battlefields application conventionally. The latency for a 1G connection is 1000 ms, a 2G connection is 600–750 ms, a 3G connection is 100 ms, a 4G connection is 10 ms, and a 5G connection is 5 ms. In a combat application, even a 1 ms latency is intolerable. Therefore, in addition to the 5G network's 1 ms latency, we also need an ultra-low latency network. In the IoMT setting, the suggested technology may be applied to the battlefield [8].

Certain issues were as follows:

1. Latency and reliability
2. Security and privacy
3. Throughput
4. Integrity

#### **A. Performance Evaluation of above case study:**

The performance evaluation of the suggested quantum cryptography-based system is covered in this section. The author had conducted a thorough theoretical investigation of the elements that make up our inventive architecture. The performance analysis mainly consider the latency and throughput as well as the quantum computing concepts are included to achieve more security as that of existing security methods. The detail analysis is as below [8].

1. Latency Analysis: 5G networks take a lot less time than 4G and 5G networks do. Due to which the 5G networks gets an advantage over the competition. Rapid transmission is crucial since it helps with mission-critical jobs [8].
2. Quantum cryptography: The basic principle of quantum cryptography helps us to detect the third party [8].
3. Throughput Analysis: Throughput analysis means total time taken in network to process the data. And the observation tell us that 3G and 4G takes more time as compare to 5G. So the author selects 5G for implementation [8].

### **V. APPLICATION OF QUANTUM COMPUTING**

1. Industry and research center
2. Secure voting System
3. Military services across the nation
4. Space Communication
5. Quantum Internet

### **VI. CONCLUSION**

This paper gives a basic idea of quantum cryptography how it works with the help of example and it is clearly stated that quantum cryptography is more powerful to secure our data and it is beneficial. We also discuss the two main types of protocols P&M and entanglement based scheme. We have even discussed the limitation and application of quantum cryptography. But it is clearly stated that quantum cryptography helps us to secure the data more as compare to classical technique.

#### **Interest Conflicts**

We declare that there is no conflict of interest concerning the publishing of this paper.

#### **Funding Statement**

There is no any funding for this work.

### **VII. REFERENCES**

- [1] Sharma, P., Agrawal, A., Bhatia, V., Prakash, S., & Mishra, A. K. (2021). Quantum Key Distribution Secured Optical Networks: A Survey. IEEE Open Journal of the Communications Society, 2, 2049–2083. doi:10.1109/ojcoms.2021.3106659.
- [2] Tsai, C.-W.; Yang, C.-W.; Lin, J.; Chang, Y.-C.; Chang, R.-S. Quantum Key Distribution Networks: Challenges and Future Research

- Issues in Security. Appl. Sci. 2021, 11, 3767. <https://doi.org/10.3390/app11093767>.
- [3] Abushgra, A.A. Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review. Cryptography 2022, 6, 12 <https://doi.org/10.3390/cryptography6010012>.
- [4] N.Sasirekha, M.Hemalatha, Quantum Cryptography using Quantum Key Distribution and its Applications. International Journal of Engineering and Advanced Technology. Volume-3 Issue-4, April 2014. ISSN: 2249-8958.
- [5] Laszlo Gyongyosi, Laszlo Bacsardi, Sandor Imre. A Survey on Quantum Key Distribution. Infocommunications Journal. 08 January 2021, Volume XI, Number 2. DOI: 10.36244/ICJ.2019.2.2.
- [6] Huanguo Zhang, Zhaoxu Ji, Houzhen Wang, Wanqing Wu. Survey on Quantum Information Security. China Communications, October 2019.
- [7] J. Aditya, P. Shankar Rao, Quantum Cryptography, Proceedings of computer society of India, 2005.
- [8] Vishakha k. Ralegankar, Jagruti Bagul, Bhaumikkumar Thakkar, Rajesh Gupta, Sudeep Tanwar I, Gulshan Sharma, And Innocent E. Davidson, Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study, IEEE Access, Volume: 10, Page(s): 1475 – 1492, DOI: 10.1109/ACCESS.2021.3138753.