National College of Ireland

Secure sharing of secret key on insecure channel using Quantum key distribution

MSc Internship
Msc in Cyber Security

Shirish Kumar Shrikant Jagdale
Student ID: X18146023

School of Computing
National College of Ireland

Supervisor: Mr Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Mr Shirish Kumar Shrikant Jagdale
Student ID:	x18146023
Programme:	Msc Cyber Security **Year:** 2019-2020
Module:	Academic Internship
Supervisor:	Mr Imran Khan
Submission Due Date:	12th December 2019
Project Title:	Secure sharing of secret key on insecure channel using Quantum key distribution

Word Count:4986 **Page Count 16**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Secure sharing of secret key on insecure channel using Quantum key distribution

Shirish Kumar Shrikant Jagdale
X18146023

Abstract

In today's era of internet and network application, need for security has become of vital importance. Most of our important data is stored in computer and recently on cloud, also whenever we need to send data to some other person, we make use of internet thus, need of data security becomes increasingly important. Protecting important sensitive data against any unauthorized access is a major concern. Cryptography is one of the methods to safeguard all our important data from being stolen or intercepted by unwanted person. We can rely on classical cryptography for securing our data however, with the advancement of computation they are being phased out. Therefore, Quantum Key Distribution promises a secure key agreement by using law of quantum mechanics thus, QKD becomes a significant trend of new cryptographic revolution. This paper explains how QKD is used for secure sharing of key between two entities i.e. Alice and Bob and further using this shared key for encryption and decryption of text data. In addition to this, paper also discuss about implementation of QKD-BB84 protocol and test result indicates that QKD is secure against man-in-the-middle attack. However, physically implementing QKD is a greatest challenge due to need of Quantum computers and cost of setup.

Keywords: - QKD, Quantum Cryptography, BB84, encryption and decryption, Quantum physics, qubits, uncertainty principle, classical cryptography.

1 Introduction

To conduct secure and reliable communication over a network there are various number of methods available. One of the such most secure and reliable method is cryptography. Cryptography has become crucial for providing security to large number of applications. It has numerous uses from securing defence operations to security automations and DRM (digital right management) protection of IP's. The challenge over here is to provide better security for growing demands in field of computation which is drastically increasing. But, one of the major problems that we face when cryptography is used for securing the data is key management. Key management includes all policies from generation, establishment, distribution, and revocation of keys. Security of any cryptographic data depends upon use of strong and efficient key distribution and management mechanism.

A numerous amount of key management protocols has been proposed over the years such as Rivets–Shamir–Adleman (RSA) [1] cryptosystem whose security totally depend upon complexity of mathematical equations used for generation of cryptographic key, but this could suffer from advancement of computational power for example quantum computers or quantum computing. Other than public key cryptography, symmetric key cryptography such

as AES [Advance encryption Standard] and OTP [One Time Pad] was also proposed but all these algorithm or key management protocols fails to provide one major security concern and that is securing a key on insecure channel i.e. internet. Because, if attacker eavesdrop on network, he/she will get easy access to cryptographic key which is used to encrypt a message.

Quantum Key Distribution holds the capability of distributing symmetric key with the Information Theoretic Security (ITS) the security which is based upon Heisenberg uncertainty principle and quantum no cloning theorem [2]. In QKD a binary digit bit is encoded into quantum state of light which is known as quantum bits or qubits which is physically impossible to get compromised by an eavesdropping this is how quantum key distribution secure a key distribution.

In this paper, we have proposed a method to securely share secret key with the help of Quantum Key Distribution (QKD), so that no third party can have access to it. In this method sender in our case Alice generate random bits from four bases i.e. horizontal, vertical, diagonal and anti- diagonal which are called as qubits and send it to receiver Bob via public quantum channel. At receiver end Bob measures the received qubits from random basis he chooses and send the corresponding results and choice of his basis to Alice, in return Alice also send her choice of basis to Bob this phase is called quantum phase. Then, both sender and receiver send their corresponding matched bits and compare with their own bits thus, both comes to common point and key is shared between them.

Research Statement: Does Quantum key distribution gives security to shared secret key from eavesdropper?

The rest of the paper is structured as follows section II We have Related Work, which focuses on understanding the previous work done in key management. The next section is Methodology, where we have discussed the architectural aspects of research, explaining different components that we used in research and how the process will execute through proposed framework. Section IV is Design Specification; section V is Implementation part where we have implemented QKD BB84 protocol using java program. Section VI is evaluation where test case is run, and results of corresponding test was discussed. in Section VII we have given conclusion along with scope for future work.

2 Related Work

The Literature Review over here represents the recent studies done on cryptographic key management such as generation, establishment, distribution and securing the key. The first sub section 2.1 gives background about different cryptographic algorithm and their comparison. Sub section 2.2, 2.3, and 2.4 give brief about different work done on key management solutions such as generation, distribution, and its security. However, the main security of any cryptographic algorithm relies on how secure the key is when it is transported on insecure channel. Thus, in later part of sub section 2.4 we have discussed about the related work done in field of Quantum Key distribution (QKD) for secure transmission of data.

2.1 Different Cryptographic algorithms

In network security and cryptography, there are two types of encryption which are known as symmetric key encryption and asymmetric key encryption. In symmetric key same key is used for encryption and decryption, thus encryption key is calculated from decryption key and vice versa. However, in asymmetric key encryption also known as public key cryptography a pair of keys, public and private key is used for encryption and decryption process. So, in public key cryptography each public key is published, and its corresponding private key is kept secret. [3]
The classification of cryptographic algorithm is shown below.

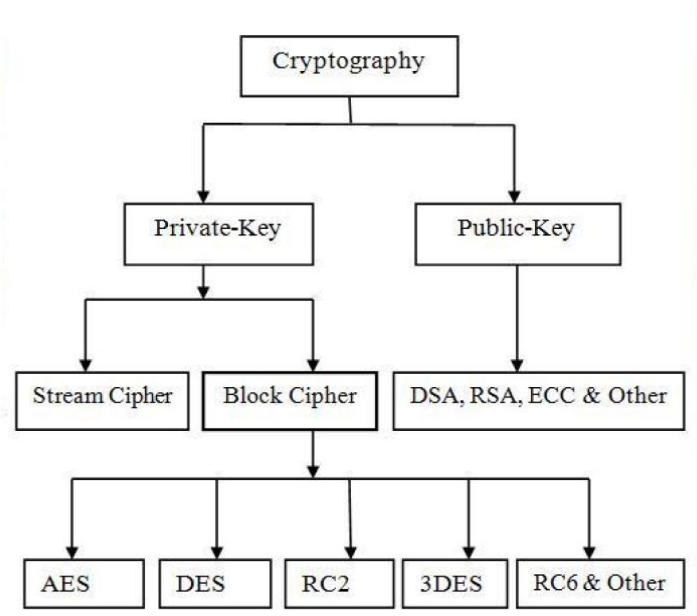

Fig -1 Classification of cryptographic algorithm [4]

As there are several cryptographic algorithms present the strength and efficiency of any algorithm depends on its architecture and security. Thus, researcher Vishal Choudhary in [4] done comparative analysis of different cryptographic algorithm, key generation algorithm and discussed about elliptical curve cryptography and concluded that even though RSA and AES cryptographic models are extensively used in providing security over the internet, but they lack in terms of providing security to key distribution system. Author also expected that the elliptic curve cryptography may play crucial role in future in implementing several cryptographic algorithms due to its small key size and faster encryption and decryption operations but currently it fails to provide security solutions to resource limited system solutions like sensor networks, smart cards and mobile devices.
In another research done by researchers Sonam Beniwal, Ekta and Savita [5] presented a paper in which analysis of random key cryptography and RSA is done. The comparison of these two algorithms was done on the base of how time efficient these algorithms are. However, the security of these algorithms totally depends upon there complexity i.e. key size and number of data blocks, with increase in computational power these algorithms can be breached in future.

Algorithm	No of keys	Algorithm used	Output size (bits)	Speed of algorithm	Effect of key compromise	Complexity	Key management and sharing	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) against collision attacks	First Published
MD2	0	MD	128	fast	NA	Medium	NA	128 (3 X32)	512	64	And, Xor, Rot, Add (mod 232), Or	≤18	1992
SHA-0	0	SHA	160	fast	NA	Medium	NA	160 (5 × 32	512	80	And, Xor, Rot, Add (mod 232), Or	<34	1993
SHA-1	0	SHA	160	fast	NA	Medium	NA	160 (5 × 32	512	80	And, Xor, Rot, Add (mod 232), Or	<63	1995
SHA-224 SHA-256	0	SHA	224 256	fast	NA	Medium	NA	256 (8 × 32)	512	64	And, Xor, Rot, Add (mod 232), Or, Shr	112 128	2004 2001
SHA-384 SHA-512	0	SHA	384 512	fast	NA	Medium	NA	512 (8 × 64)	1024	80	And, Xor, Rot, Add (mod 264), Or, Shr	192 256	2001
SHA-512/224 SHA-512/256	0	SHA	224 256	fast	NA	Medium	NA	512 (8 × 64)	1024	80	And, Xor, Rot, Add (mod 264), Or, Shr	112 128	2012
SHA3-224 SHA3-256 SHA3-384 SHA3-512	0	SHA	224 256 384 512	fast	NA	Medium	NA	1600 (5 × 5 × 64)	1152 1088 832 576	24	And, Xor, Rot, Not	112 128 192 256	2015
Symmetric key algorithm	1	AES	128	fast	Loss of both sender and receiver	Medium	complex	512 (8 × 64)	128	10	XOR,ROTL,SHL	128	2001
Asymmetric key algorithm	2	RSA	2048	Relatively slow	Only loss for owner of Asymmetric key	High	Easy and secure	512 (8 × 64)	128	10	XOR,NOT	128	1977

Fig -2 Comparative analysis of different cryptographic algorithm [4]

In [6] authors have done analysis of different cryptographic approaches such as 3DES, DES, AES and Blowfish integrated with BB84 quantum cryptography protocol and deployed them on cloud and local environment. Then measured their performances on basis of computational time and found that the performance of these cryptographic algorithms was much better in cloud than the local environment. Therefore, looking at above comparative analysis we found that AES algorithm is most promising in terms of security and efficiency thus in our project we use AES protocol for encryption and decryption of data.

2.2 Key Generation

According to Auguste Kerckhoff's principle for any cryptographic system the key should be kept secret rather than its algorithm [7]. Thus, key plays a vital role in field of cryptography. In paper [8] author gave a brief about generation of symmetric key by modifying Diffie-Hellman using ABC conjecture. ABC Conjecture usually have three positive integers A, B, C and are relatively prime such that they satisfy the condition A+B=C. The selection of C is done in a way that A and B will be large composite number. To decide the position of value coefficient value A Diffie- Hellmen protocol has been used which is done in three stages. The paper concluded that modified algorithm was able to produce required robustness and prevent

from known vulnerabilities of Diffie-Hellman algorithm. However, the proposed algorithm cannot be used in real time because of its competitive time and complexity.

In another experiment [9] author proposed a method of generating cryptographic key using biometric features. In this paper a biometric key has been generated from selecting bits of chaotic bispectral transform to user's 3D face images. Due to fuzzy nature of biometric, bio key contains some errors. Thus, error correction method was also introduced in this paper and the performance of implementation was judged upon false acceptation and rejection of statics. In conclusion the paper states that there are other some biometric based key generation techniques which show better results and can be used for generating keys of longer size.

In similar kind of research [10] biometric key is generated using cancellable fingerprint templates, in which a cancellable template from original fingerprint template of both sender and receiver is generated. Then both the parties share their cancellable templates with each other in encrypted form. Both parties receive these templates and merge their own cancellable templates with templates received to form one master template from which the secret key is generated which is used for encryption and decryption of message. As only cancellable templates are shared on channel which is in encrypted form the attacker is not able to get access to these templates. However, to extract the features from these algorithm needs lot of sensors and complex computations or mathematics and another major issue generates from these implementations are that they need to be stored in secured place or the attacker should not get access to them. Thus, in next section we will discuss about research done in securely storing the cryptographic key.

2.3 Key Protection

Even if key with appropriate key size are strong against any known vulnerabilities, they still suffer from weakness due to key protection. They are often written down or stored in insecure location. The example of an attack happening on stored keys are cold boot attack, in which the key is been find when system is shut down another such attack is finding the key in RAM as during execution an unencrypted key is stored on RAM. In paper [11] author proposed a method of securing a key using key wrap technique in which the initial value of key A0 is set to as A6 thus while unwrapping the key, the algorithm should return A6, if not so the error message should be given. However, in conclusion author states one of the major disadvantages is that AES involves several invocations with presumption. Another researcher in [12] proposed a method in which a cryptographic key is stored on virtual RAM i.e. on cloud. In this technique the cryptographic key is stored on virtual RAM in scattered form at randomly generated location. Thus, during encryption and decryption process the crypto processor will hold minimum portion of round key, the scattered key is never gathered at time of encryption or decryption thus stopping attackers to gain an access to whole key even if the virtual memory is been compromised. In conclusion this technique effectively protects cryptographic key in virtual environment against Brute force attack and any other memory extraction related attack. However, with increase in security the efficiency is affected as it consumes more space while storing the key in memory. Even though, a key is stored at secure place the issue still exists to secure the key in transit.

2.4 Key Distribution

[13] describes the use of session key for secure transmission of data between sender and receiver. In session key there are two variant of key establishment protocol one is key transportation, and another is key generation. In first phase the key is generated by one entity and then it is securely shared to another one. In second phase key is constructed individually by entities through a pre-determined agreement. These key generated are then used as session key for all the cryptographic operations. For this proposed research a trusted server has been used for communication between sender and receiver before the key generation. During the key establishment both the communicating parties authenticate each other. The research was studied and tested on SPAN and Avispa-1.6 and the outcome of the test shows that generation and use of session key for secure transmission of data is safe.

In other research, [14] author proposed a computation method for shared private key between communicating entities. In this the users performs strong computation based on exponential method to generate the secret value. Algorithm takes identification parameters such as identification ID's from users as input and output generated is common secret key computed using Diffie-Hellmen key exchange protocol. The research has been tested on Scyther tool to test provability and security and the results concluded that if not mistake happen at the time of authentication it is safe against all the know attacks. However, if any mistake happens at the time of authentication this method is prone to man in the middle attack.

[15] author proposed a method to securely transit a key on channel using mobile agent key distribution model on wireless network. This technique employs the model of public key cryptography in which every node will have the public key of every other node associated to it. The model consists of three different type of nodes which are BS base station node, CH cluster head node and MN sensor node which stores the public key. When the size of network increases the number of shared keys stored in these nodes also increase. Similar kind of work is also proposed by [16]in which a large pool of keys is generated for each node and stored in their memory. Each node tries to find their adjacent node with whom it shares the common key. These techniques are highly efficient and shows throughput however, the security of the system and key totally depend on how secure the node is? If anyone node on network gets compromised the adjacent node connected to it will also get compromised and thus whole system will fail.

Hence to overcome all these drawbacks [17] proposed a method to use quantum key distribution for secure transmission of key on current WDM network. In this technique QKD transmitter generates a single photon and encodes a stream of bits on single photon which is called as qubits. The polarization of qubit is randomly selected among four different states in which horizontal or diagonal -45-degree states 0 bit while vertical or diagonal +45-degree states 1 bit. Then QKD transmitter sends these qubits to QKD receiver where it randomly selects one of two bases rectilinear or diagonal to measure each incoming qubit and record selected base and incoming qubits. For error correction and estimation QKD receiver and transmitter shares and compares sample of qubits. If there is any attempt to eavesdrop on the network the qubits change its state thus, receiver gets to know that there was an attempt of an attack. In Concluding the author states that this method is more secure than other traditional key distribution techniques however the cost to establish the quantum channel is expensive, but this can be reduced in future by using different approaches of QKD.

In [18] Author discussed about different protocols such as BB84, B92 and SARG4 used in quantum key distribution to carry out a task of key exchange with a great security. In concluding author states that each protocol uses unique law of physics for security of secret key and each have their own pros and cons. In another research [19] researcher done analysis of two cryptographic protocols BB84 and B92 on basis of their QBER value which gives information about presence of eavesdropper on network. The results of analysis show that even though B92 is easy to implement but BB84 protocol ensures high secure communication over a channel loss in comparison to B92. Thus, in our research we choose BB84 QKD protocol to ensure the security of our system.

3 Research Methodology

[20] describes how a MITM attack exploits the shortcomings in the arrangement of the correspondence convention and convinces the victim to move through the attacker instead of the ordinary switch. [Alexandra Research papers pdf downloaded] shows how attack can be performed on a system using backdoor entry SAT which is also called as guess and determine attack thus, any password stored on system can easily be accessed and according to principle of modern cryptography in any case cryptographic key should be kept secured for the security of any cryptographic algorithm. Hence key should be protected in any circumstances and thus [21] proposed a method of key distribution using quantum cryptography. So, in our research Quantum Key Distribution is used to securely transmit a key between sender and receiver. Also, in [22] shows how AES algorithm is more superior than any other algorithm in terms of efficiency while encrypting and decrypting the data. Hence AES algorithm is used for encryption process and QKD will be used to securely exchange of the key. The following section will briefly discuss about Quantum Key Distribution and AES algorithm.

3.1 Quantum Key Distribution

Quantum Key Distribution was invented by Charles Bennett and Gilles Brassard in 1984 thus protocol used in QKD is called as BB84. QKD was initially based upon the idea of S. Wiesner who proposed the concept of quantum money. In contrast to public key cryptography it has been proven to be unconditionally secure i.e. secure against any attack even in future, irrespective of the computing power or any other resources. The security of Quantum Key Distribution relies on the law of quantum mechanics and Heisenberg uncertainty principle. This property is used to establish random keys between two communicating parties and guarantees that it is perfectly secret from any other user eavesdropping on line.

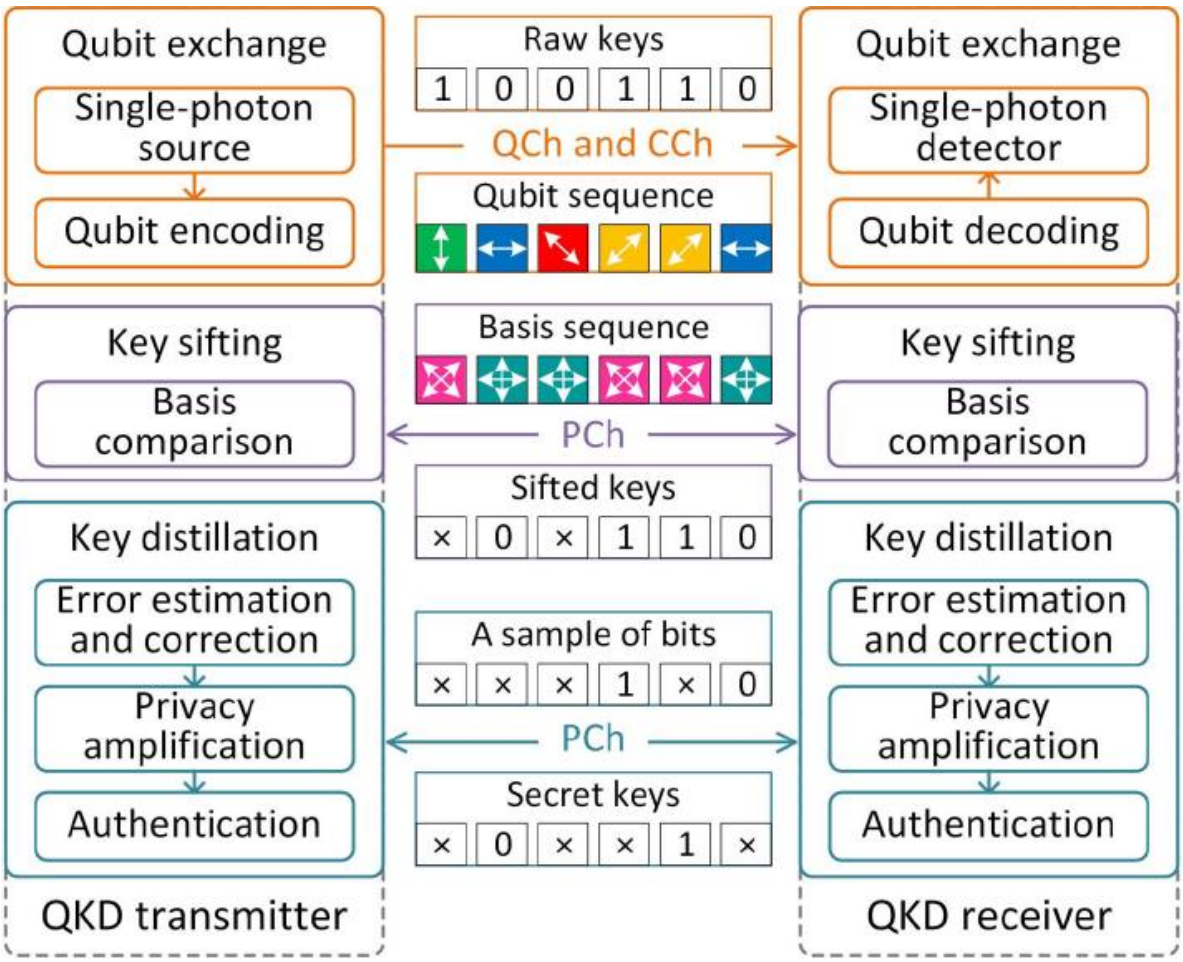

Fig 3 Quantum Key Distribution protocol [17]

In quantum key distribution sender encodes some information into a quantum state which is called as qubits and send It to receiver. Receiver measures the received qubits with its own bases and send response back to sender. Both sender and receiver used classical communication (fiber) for generation of secret key. Sender sends some fraction of random signals to receiver and announces them in response receiver send is measurements and outcome obtain from measuring the random signals. Depending upon the amount of error from the comparison, both sender and receiver decides whether they have to generate key or not. Thus, if an attacker tries to eavesdrop on network both sender and receiver will get high rate of error and key will be not generated because any tampering to quantum bits (qubits) will make it change. Hence it is highly resistant against any Man-in-the-middle attack. Quantum Key Distribution has some following features. [23]

- Detection of measurement
  Detection of measurement means the attacker cannot eavesdrop on network without introducing disturbance to it. So, whenever someone tries to access the Quantum bits, they change their states and thus both the communicating parties get to know about presence of eavesdroppers on network.

- Uncertainty principle
  This principle states that the simultaneous values of non-commuting observables cannot be evaluated on a single copy of the quantum state and hence the quantum states remain undistributed

- No- cloning theorem
  In quantum mechanics, it is impossible to make a perfect copy of an unknown state with perfect fidelity. This prevents an eavesdropper from simply intercepting the communication channel and making copies (so as to make measurements on them later) of the transmitted quantum states.

- Non- orthogonality principle
  The principle states that suppose we have quantum states that are not orthogonal, then it can be proven that there is no quantum measurement that is capable of separating states.

Due to above features QKD become most promising candidate to be used in our research. Since the key is random and unknow to attacker, it is unable to get any information by just intercepting the encrypted text. This phenomenon is beyond the ability of classical information processing.

3.2 AES encryption

AES or Advanced Encryption Standard algorithm is one of the block cipher encryption algorithms that was published by National Institute of Standard and Technology in year 2000. The AES was mainly developed to replace DES after finding some vulnerabilities in it. The main aim of the AES was to improve security issues found in DES algorithm. AES has the best ability to protect sensitive data from attackers and is not allowed them to break the encrypt data as compared to other proposed algorithm.

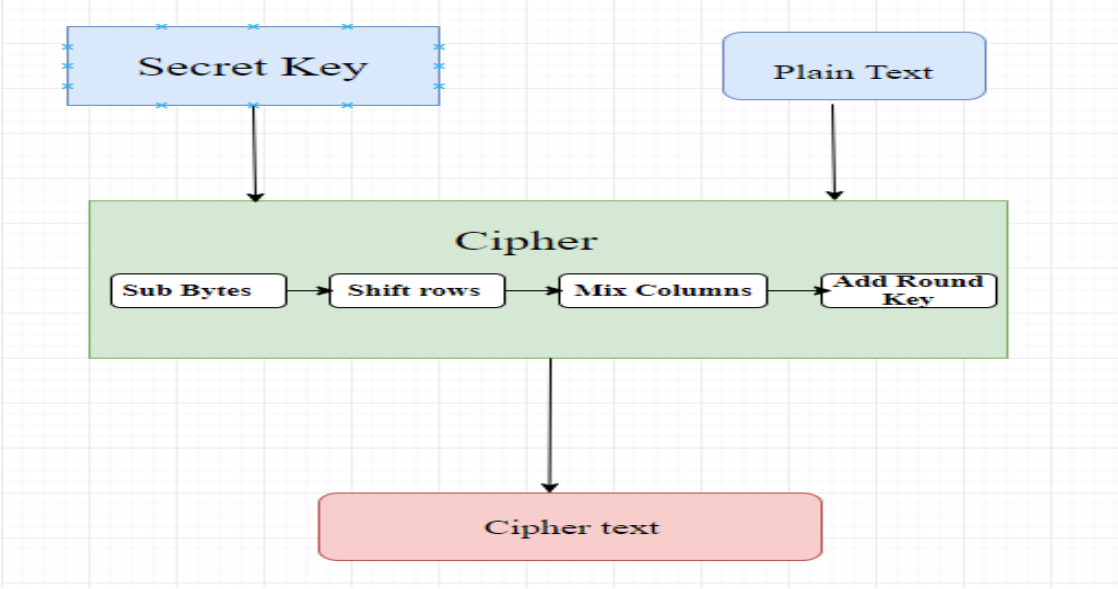

Fig 4 Architecture of AES algorithm

AES uses iterative cipher instead of Feistel cipher. To encrypt and decrypt data it uses a technique called as substitution and permutation network (SPN). SPN is a mathematical operation that are performed on block cipher. Advance Encryption Standard mainly deals with 128 bits (16 byte) fixed plaintext block size, it mainly operates on matrix of bytes.

Another feature of AES is number of rounds depends upon the size of key. There are three different key size in AES algorithm 128 bits, 192 bits, 256 bits. The length of keys decides how many rounds the algorithm is going to use, 10 rounds for 128 bits, 12 rounds for 192 bits and 14 rounds for 256 bits key [24]. In proposed system AES algorithm is used for encryption and decryption because it is fast and secure. In next section we describe how the above techniques are implemented in the research and flow of this.

4 Design Specification

This paper proposes a method in which Quantum Key Distribution is used with BB84 protocol for secure sharing of cryptographic key and AES algorithm for encryption and decryption. The proposed model to use QKD for secure sharing of key is divided into two phases Quantum phase and Classical phase.

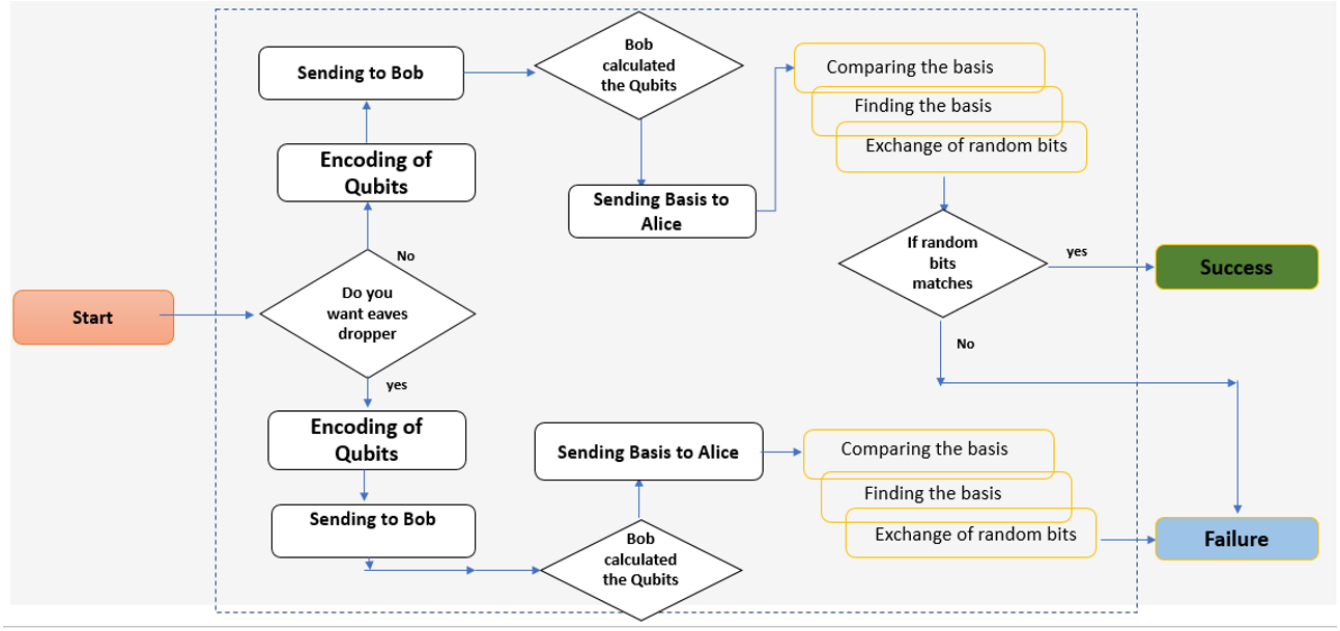

Fig 5 Flow diagram of proposed system

4.1 Quantum Phase

In quantum phase, two communicating parties in our case Alice and Bob use a quantum channel to communicate. Both Alice and Both use quantum signals called as qubits and perform measurement

- Alice generate a random sequence of strings drawn from four signal state i.e. horizontal, vertical, diagonal and anti-diagonal.
- The generated random quantum signal (Qubits) are send to Bob.
- Bob performs quantum measurement on received qubits and decode bit value
- Alice keeps record of signals selected.

- Bob records of his bases choice and result of measurement.

4.2 Classical Phase

In Classical phase both Alice and Bob use a classical channel (fiber) in order to get a secret key from there correlated data.

- Alice choses some random qubits and announces it to Bob.
- Bob in response tell Alice which basis he has use to read the qubits.
- Bob has portion of the key that has been recorded correctly and send it to Alice over classical public channel.
- Both Alice and Bob compare their part of key.
- If eve is present the bit recorded by Bob will differ from the bits sent by Alice.
- Depending on amount of error obtain during comparison, Alice and Bob decide whether to use key or not.

4.3 Error Propagation

Out of bits received to Bob, 50% of bits were discarded due to choice of wrong basis. If an attacker intercepts the network there is 25% probability that an incorrect value was transferred to Bob. Therefore, choice of wrong basis (50%) and wrong qubits recorded (50%)

$$1/2 * 1/2 = 1/4 = 25\%$$

Hence, probability of Bob finding an eavesdropper on network is 25%. This is elaborated further.

1) In our research, 1024-bit key was used, out of which only half key is been used with the assumption that 50% of key got discarded due to selection of wrong basis. Therefore,

$$1/2 * 1024 = 512 \text{ bits remaining}$$

2) Out of remaining key 50% is used to find presence of an eavesdropper

$$1/2 * 512 = 256 \text{ bits}$$

Therefore only 256-bit key is used as a final key for encryption message.

3) There are around 25% chance that bob will identify the eavesdropper and 75% probability of not. Thus, for entire 256- bit key there is 256 ^ ¾ times eavesdropper will not get detected

$$256^{\wedge} ¾ = 1.0367724e^{\wedge}-32$$

Hence, for 256-bit size key there are one in nonillion chances of attacker will not be get identified.

5 Implementation

For this experiment java programming language is used and the program is run on eclipse IDE. The purpose of this experiment is to secure a secret cryptographic key from attacker when it is transmitted over a network channel.

5.1 Quantum Phase

In this phase Alice first generates the random bits using random number generator, for every generated bits Alice chooses one of bases from vertical, horizonal, diagonal and anti-diagonal. Then send the generated qubit (quantum signals) from the chosen base to Bob using quantum channel.

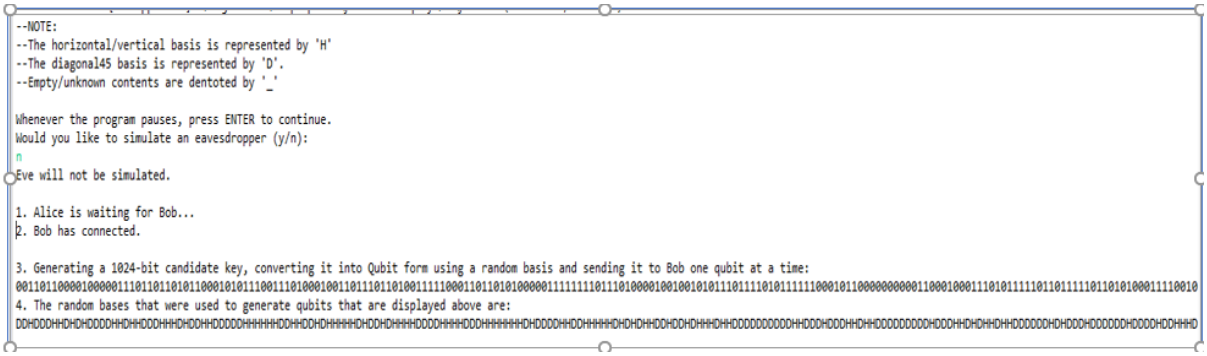

Fig -5 random qubits generation

Bob measure the received qubits with randomly chosen basis. Then in response Bob send basis which he has choose for measurement of qubits to Alice.

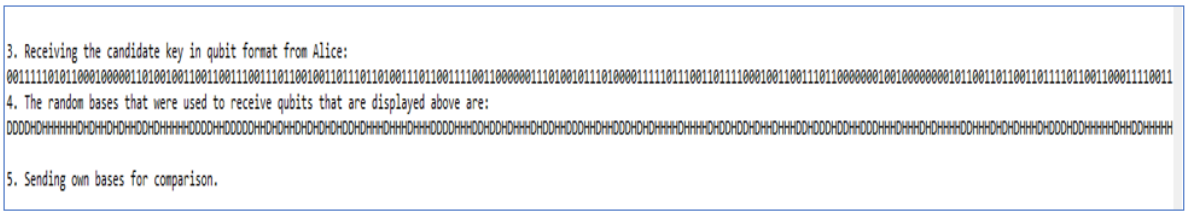

Fig -6 Receiving qubits from Alice

Alice receive the basis used by Bob and then in response send her own choice of basis for the comparison.

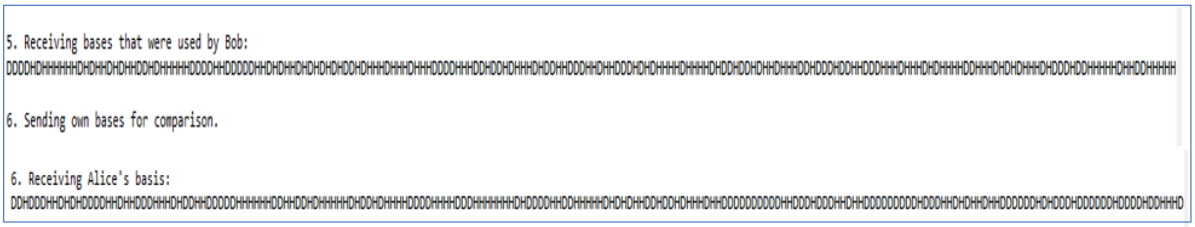

Fig -7 Exchanging Basis with each other

After both Alice and Bob swap there corresponding bases. Then, they use classical communication channel for further process.

5.2 Classical Phase

After exchanging the bases both Alice and Bob match common bases and sends random bits to test the presence of eavesdropper on network

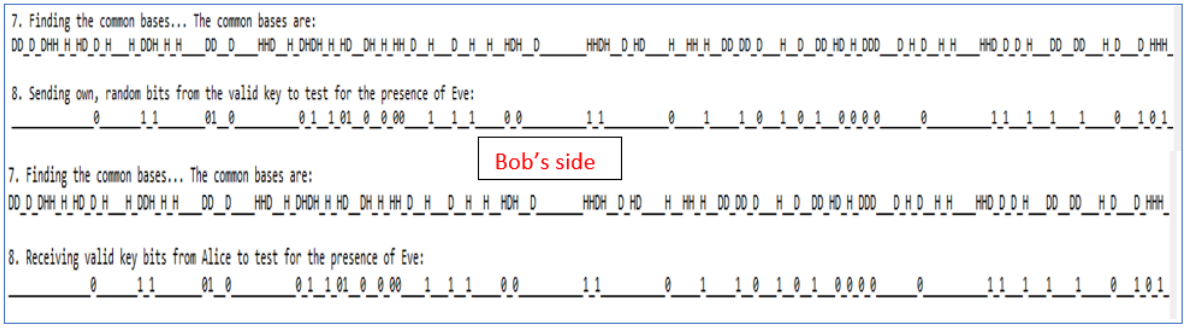

Fig -8 Exchanging common bases

Then after receiving valid key bits both Alice and Bob compare the received bit and secret key is generated and shared.
A 256-bit common secret key is shared between Alice and Bob and this key is further used for encryption and decryption on information.

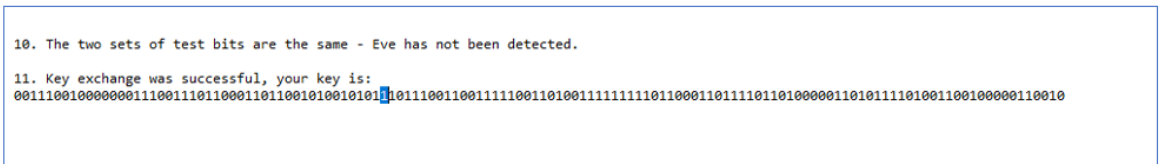

Fig -9 Secret Key generated

The key we got from Quantum Key Distribution is used for encryption of plain text. When we use same key for decrypt the cipher text, we get same plain text which was encrypted this is because we have use 256-bit AES block cipher algorithm. AES is a symmetric key cryptography thus same key can be used for encryption and decryption of message.

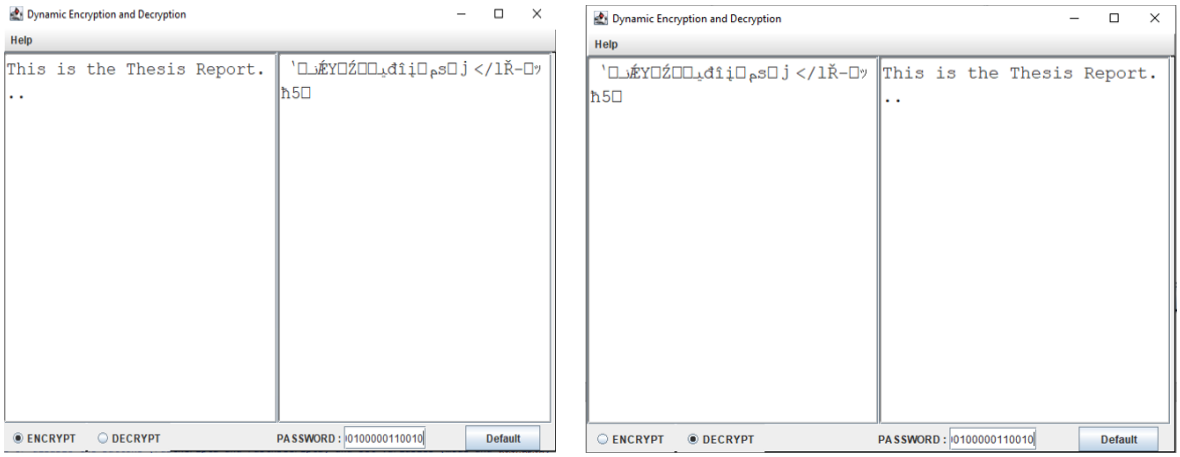

Fig -10 Encryption and Decryption process

6 Evaluation

This section shows how are proposed system is secured against a cryptographic attack (Man-in-the-middle) and measurement of its performance.

6.1 Man in the middle attack manual / Case Study 1

The eavesdropper is introduced on a quantum network to listen the communication between two parties. In normal condition when an attacker eavesdrop on network, the channel is prone to MITM attack. But, in our proposed system the attacker fails to perform man in the middle attack.

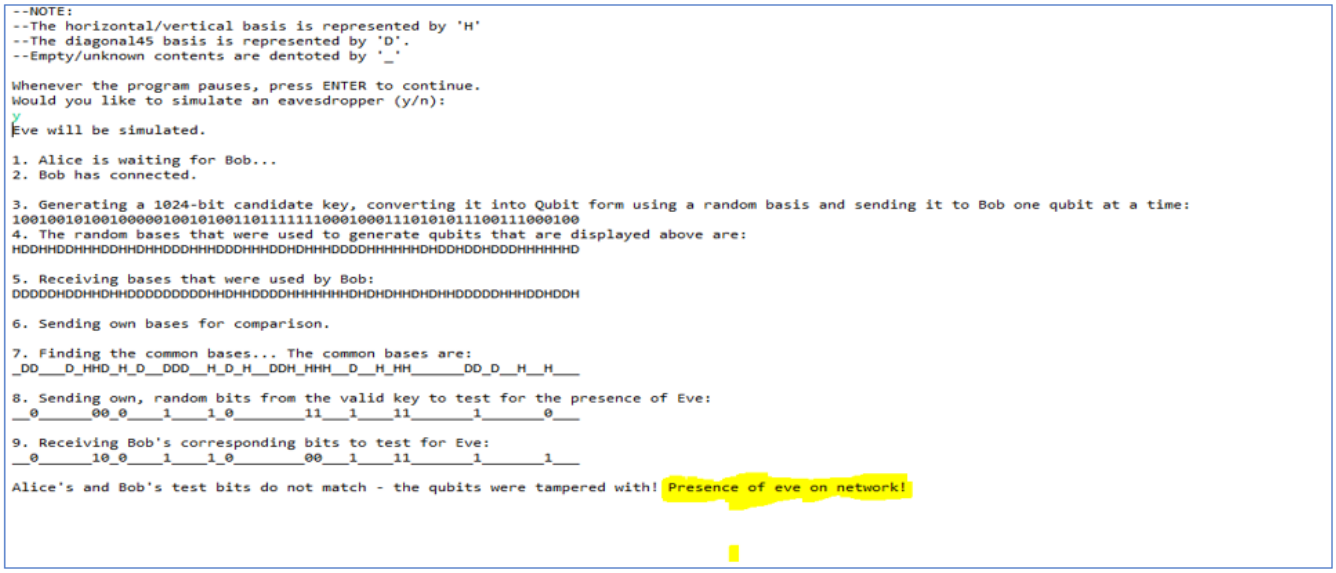

Fig -11 Illustration of Man in the middle attack

The reason for failure of MITM attack is whenever there is tampering with qubits on communication channel, they change their states and thus receiver gets wrong qubit and both communicating parties get to know about presence of eavesdropper.

6.2 Discussion

The main aim of the research was to secure a key from an attacker when it is in transit. For this we have performed a test in which an eavesdropper was introduced on the network and the result we got from the test is that attacker got no success in accessing the private secret key.

A similar approach was proposed [14] in which two communicating parties computes a common secret key using Diffie-Hellman key exchange protocol. When comparing the results of this approached with our proposed method it was found that the approached described in [14] was vulnerable to man in the middle attack if something went wrong during authentication phase.

Even if, our proposed system looks theoretically secured, their exists some challenges in providing proof of security in practical, due to this we were able to present only one test case

as to perform further test there was physical dependency. Some of the examples of physical attacks are side channel attacks, Photon number splitting attack and large pulse attack. However, these challenges can be overcome by making changes in physical system and can be protected from these attacks.

Thus, from the results of test and studies our proposed system can be used for securing the secret key from cryptographic attack.

7 Conclusion and Future Work

This paper illustrates the method of secure sharing of secret key using Quantum Key Distribution. This method helps to protect against a cryptographic attack such as man in the middle attack as the attacker is not able to read the communication happening between the two parties. This due to security of QKD system is based upon quantum physics and Heisenberg uncertainty principle, which gives QKD added advantage over any other cryptographic algorithm. However, the physical implementation and cost for the setup are the major problems face while working on the QKD as it requires quantum computers and electronic components. Thus, in future concept of quantum key distribution can be employed on our current network as at the end the final goal is to achieve a QKD system that can be used by client on internet and this can be interesting topic to worked out.

8 Acknowledgment

I would like to pay my special regards to mentor Mr. Imran Khan for continuously supporting me throughout the academic research internship process. Also, I would like to thank all my fellow colleagues who all supported me with their technical expertise whenever I have faced any obstacles during implementation of research. I wish to thank Mr. Kiran Kadapatti whose assistance was a milestone in the completion of this project. In addition, I want to thank National College of Ireland to provide me with the opportunity and resources to work on my research.

References

[1] A. Shamir, R. L. Rivest and L. Adleman, "A Method for Obtaining Digital," National Science Foundation, Masschusetts, 1978.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus and M. Peev, "The Security of practical quantum key distribution," *Reviews of Modern Physics,* vol. 81, p. 1345, 2009.

[3] RedHat, "Introduction to Public-Key Cryptography," in *Planning How to Deploy Red Hat Certificate System*, RedHat.

[4] V. Choudary , S. Taruna and L. B. Purbey, "A Comparative Analysis of Cryptographic Keys and," in *IEEE*, Jaipur, 2018.

[5] S. Beniwal, E. and S. , "An Effective Efficiency Analysis of Random Key," in *IEEE*, Delhi, 2015.

[6] G. Murali and S. R. Prasad, "Comparison of Cryptographic Algorithms in Cloud and," in *IEEE*, Banglore, 2017.

[7] "Kerckhoffs enumerated six principles for field ciphers," in *La Cryptographie militare*, 1883.

[8] A. K. Mishra and S. S. Ghosh , "Generation of Symmetric Sharing Key," in *IEEE*, Sikkim, 2017.

[9] V. Chandran and B. Chen, "Biometric Based Cryptographic Key Generation from Faces," in *IEEE*, Glenelg, Australia, 2008.

[10] A. Sarkar and B. K. Singh, "Cryptographic Key Generation From Cancelable," in *IEEE*, Jamshedpur, 2018.

[11] R. Sridevi and N. Rajitha, "Cryptographic Key Protection in a cryptoprocessor," in *International Conference on Information Security and Privacy*, Nagpur, 2015.

[12] M. Fatma, A. Bushra, S. Khaled, Y. Y. Chan and D. Ernesto , "A Scattering Technique for Protecting," in *IEEE*, Abu Dhabi, 2017.

[13] S. Arora and M. Hussain, "Secure Session Key Sharing Using Symmetric Key," in *IEEE*, Ajmer, 2017.

[14] N. Bruce and J. L. Hoon , "An Efficient and Provable Secret Shared Key Computation for Cryptographic Protocol across," in *IEEE*, Busan, 2015.

[15] R. kuchipudi , A. A. M. Qyser and V. Balaram, "An Efficient Hybrid Dynamic Key Distribution in Wireless Sensor Networks with reduced memory," in *IEEE*, Hyderabad, 2016.

[16] H. Y. Dae and J. L. Pil , "Exact Formulae for Resilience in Random Key Predistribution Schemes," *TRANSACTIONS ON WIRELESS COMMUNICATIONS,* vol. 11, 2012.

[17] Y. Z. J. W. X. Y. Z. M. J. Z. Yuan Cao, "Cost-Efficient Quantum Key Distribution over WDM Network," in *IEEE*, 2019.

[18] M. A. A. A. Mohamed Elboukhari, "Quantum Key Distribution Protocols: A Survey," *International journal of Universal Computer Science,* vol. 1, p. 67, 2010.

[19] F. M. A. H. W. R Etengu, "Performance Comparison of BB84 and B92 Satellite-Based Free Space Quantum Optical Communication Systems in the Presence of Channel Effects," *Journal of Optical Communications,* vol. 1, p. 47, 2011.

[20] A. A. M. M. Z. S. J.-C. T. Avijit Mallika, "Man-in-the-middle-attack: Understanding in simple words," *International Journal of Data and Network Science ,* vol. 3, 2019.

[21] S. Wijesekera, X. Huang and D. Sharma, "Quantum cryptography based Key Distribution in IEEE 802.11 networks - analysis on reconciliation phase," in *IEEE*, Istanbu, 2011.

[22] D. P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," *Global Journal of Computer Science and Technology,* vol. 13, no. 15, 2013.

[23] H. M. M. Senekane, Security of Quantum Key Distribution Protocols, intochpen, 2018.

[24] A. M. Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," in *Research gate*, 2017.