Quantum Key Distribution Algorithm for Network Security

Domi Caroline S[a], and R. Arthi[b]

[a]
Department of Electronics and Communication Engineering
SRMInstitute of Science and Technology, Ramapuram Campus, Chennai.
[b]Department of Electronics and Communication Engineering
SRMInstitute of Science and Technology, Ramapuram Campus, Chennai.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Quantum computing computes using superposition principles and entanglement principles that are the part of quantum. Quantum computers are used to solve certain problems that cannot be solved using classical computers. The most widely using quantum models are quantum circuit uses qubits or quantum bits.In cryptography, Quantum cryptography provides more security than classical methods. Shor's algorithm and Grover's algorithm are mainly used methods for quantum cryptography. The encryption and decryption is done using Rectilinear bases or Diagonal bases in random manner.The Quantum key distribution QKD is a symmetric encryption key distribution method. The important feature of QKD is authentication and confidentiality. Public key protocol and a symmetric secret key is used to provide quantum safe key exchange and guarantee for long term communication in the network. In the proposed system, the Morse code is used for encryption and decryption. The Morse code used to encrypt bits as light photons that are required for quantum key distribution.

Keywords: Qubits, QKD, Quantum cryptography, Network security, Authentication and Confidentiality.

1. Introduction

Important for our day to day communication over various network need security and cryptography. The classical encryption method used for traditional networks have various types of attacks which cannot be used for quantum computers and traditional method have complex mathematical calculation. The QKD system does not have any complex computations and provide security for quantum computers. QKD is mainly used to find eavesdropper in the network. The secret key between the sender and receiver is shared over the established quantum channel. There are various types of QKD protocols which depends on modulation techniques, encryption and decryption method and the way quantum channel is established. The first QKD protocol uses discrete variable and convert it using photon polarization known as DVQKD, which is further developed into a BB84 protocol. In the BB84 protocol, single state polarization has been used to encrypt the random bits as qubits have four different representation. These qubit representations depend on the diagonal orthe rectilinear bases. In encryption and decryption, the bases are selected in a random manner that measure the photon states. All these communication are done through the physical channel. The agreement about the bases are shared between sender and receiver. The bits with different bases are deleted and the key have been generated and checked for correctness which checks for any loss in the information. The BB84 protocol is simplified as the B92 protocol which uses two states instead of four states. The eavesdropper has some prior knowledge about the way to listen to the information that is to be transmitted.

Another method to generate secret is entanglement of bits. The QKD protocol for continuous variables have been generated by using CVQKD which is more convenient that is of two types one-way and two-way systems. In one-way CVQKD approach, the transmission occurs only from the sender to the receiver but in two-way CVQKD approach the receiver also starts communication after receiving the message sender sends secret along with the received message.

The quantum key distribution QKD is used to provide a secured key two different nodes that are located in different remote locations. The QKD provides better security than classical system.

2. Related Works:

Charles Bennett and Gilles Brassard created the BB84 [1] quantum key distribution scheme in 1984. The sender generates two random strings and receiver analyses the strings. Before and after the calculation, qubits check for similarity. The quantum channel is accurate, if less than a reasonable threshold disagrees, and the shared key bits can be retrieved using the remaining bits. The author proposed a security protocol for efficient secured key management using QKG-AKA [2] mechanism. This reduce the probability of attacking by various attackers.

A security protection mode based on Power QKD [3] technology is proposed. At the same time, a new generation of QKD-based data protection transmission architecture is being developed for dispatch automation, delivery automation, electricity data collection, and video conferencing.In a multi-party environment, a primitive key establishment is required for establishing secure channels [4]. The Key establishment can only be done without quantum mechanics if some computational issue is difficult. The communication can be easily eavesdropped and can be recorded. But the confidentiality has to be maintained to avoid the damage caused by algorithmic and computational private channel secret. The AVISPA tool is developed to address the false base station attack [5] using AKA protocol for handover.

One of the major advantages of 5G network is wide access, availability and connectivity. As many devices connected to the network which leads to jamming effect. To reduce jamming effect authoradopt integration of Software Defined Networking (SDN) and Network Function Virtualization (NFV) that is known as Dual – Homed Switching Network (DSN) [6]. For all cellular communication networks, DSN provides an advanced authentication mechanism.

To improve the authentication scheme by providing Extensible Authentication protocol authentication and key agreement (EAP - AKA) [7] protocol which uses permanent name and one – way hash function to improve authentication in Mobile Edge computing (MEC) servers. The privacy [8] of the environment in SDN and NFV has to be maintained.

The Kolmogorov – Smirnov (K-S) hypothesis test [9] is introduced for efficient and quick handover authentication in physical layer. A new age called the Internet of Things IoT starts with the 5G network along with the wireless sensor network. An authenticated key management is an essential for secured communication in IoT devices. The ITEF [10] critically evaluate the security in 5G network and recommends the standards to improve the security.

The standard power system creates a network protection system to improve security by using security equipment such as firewalls, intrusion detection schemes [11]and encryption devices to ensure the secure transmission of data to a certain level. The keys are updated to improve the security but updating rate is low which reduces the data transmission security. In terms of the hidden danger of being stolen from traditional key online transmission, the system's reliability and timeliness are insufficient, and its security efficiency is further harmed. The author introduce two factor authentication and key management system [12]. The user privacy and shared authentication is used as two factors with the ability to withstand many attacks.

Due to frequent handover unnecessary latency raises in the network which is overcome by weighted secure-context information enable fast authentication scheme by using Neyman Pearson (NP) hypothesis test [13] that enhances accurate authentication and reduce time delay.In collaboration with European Training Network (ETN) committed to create a secure network coding by reducing the energy used in the small cells [14]. The mobile small cells are replaced by the use of Femtocells. The information of the users are maintained secret using lightweight security framework.The key management between the users in the network is the major issue. A shared secret key is established using an unsafe wireless medium. The secret has been ensured by using Low Density Parity Check (LDPC) codes [15]. This scheme works in the presence of the eavesdropper.

The small cells in 5G networks are upgraded with Mobile small cells with network coding (NC-MSCs) which provide high data rate device-to-device connectivity. The authorintroduce Decentralized Key management scheme [16] which distributes certificate authority function by threshold secret sharing. Every node has the master private key, which provide certificate to the node which can be used “anywhere, anytime” in the network.

The weight of the secure context information SCI is used in the network to improve the performance of the network by reducing latency and improving accuracy [17]. This is used for fast authentication in HeNet. The handover authentication schemes used in the classic network produce high latency and complexity. The author createlink signature [18] which is depend on the user location is used as authentication handover data and secure context information (SCI) remains extracted from the characteristics of wireless channel used for communication between the user and access point.The competence centered privacy security handover validation mechanism achieved authentication that is shared and UE and BS have reached a key agreement[19] that reduces handover cost.

The network's protection is a vital feature that must be maintained.The evolved packet system authentication and Key agreement (EPS-AKA) frameworks are essential security frameworks in the LTE platform [20]. The EPS-AKA algorithm is considered as important and permanent solution to provide security in LTE but it has as a drawback of using one permanent key for generating the entire future key. The EPS-AKA is the approach used to overcome authentication delay and reduce message overhead by getting authentication from foreign networks which reduces the cost of operation. In LTE communication, handover and key exchange between the users has less security. In order to provide secured handover the elliptic curve cryptography algorithm based proxy signature [21] is used which reduces the computational cost.

3. Proposed Work:

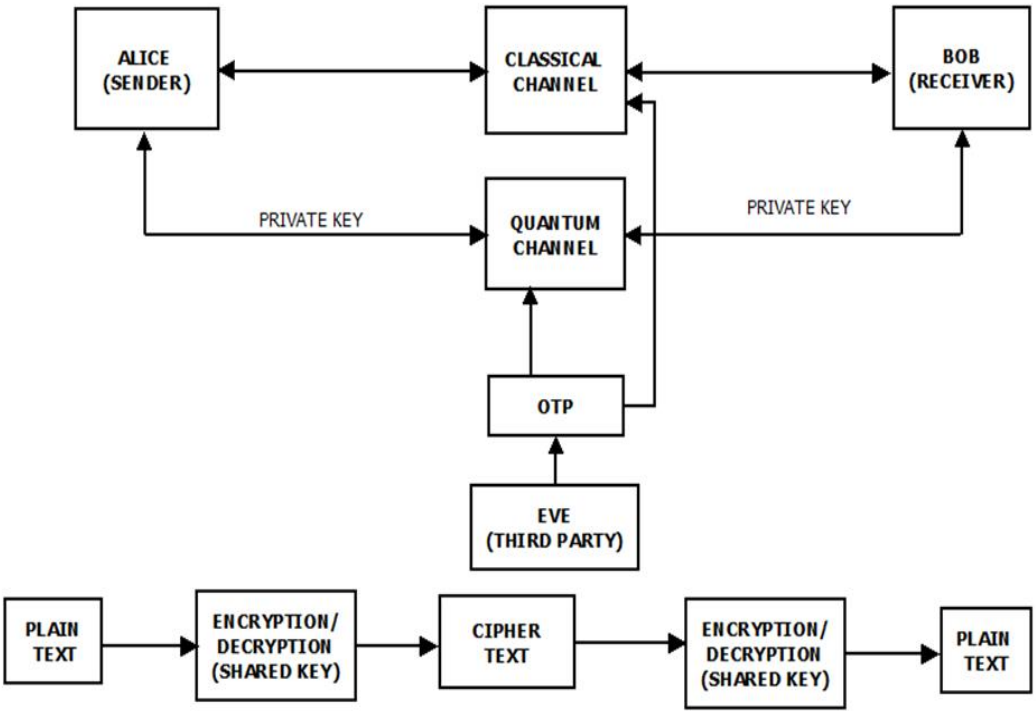

FIG 1: QKD ARCHITECTURE

The qubits are used to provide quantum channel for communication. These qubits are of two states as 1 or 0. Qubits are mentioned in two different fashion as diagonal arrows and upward/downward arrows. The information that has been transmitted are encrypted as qubits and transmitted in quantum channel. At the receiver, the qubits are decrypted in a random manner. The Quantum key Distributor have been used in between the sender and the receiver. The distributor checks for matching between the sender message and receiver message. The encrypted and decrypted message should match at least for 50%. If they are matched for 50%, then the channel is marked as quantum channel, which is used as secured channel for future communication. If the match is less than 50%, then the third party had been interrupted the communication and the information have been changed so the channel as to be changed for further communication[22]

From fig 1, The Sender and Receiver communication consists of two components that are a server and a client. Clients submit requests to the server, and the server responds to the client's requests.Typically, both the client and server interact through a computer network that they can reside in the same system or different system.

1. The Python function socket.gethostname() returns the current system's host name, which is used to run the Python interpreter. This Python function can be used in combination with socket.gethostbyname() to obtain the local host's IP address.
2. The bind () method on a server binds it to a particular ip address and port address, allowing it to listen for incoming requests on that ip address and port address..
3. Listen () is a method on a server that places it in listen mode. This enables the server to track and respond to incoming connections.
4. Accept () is a server method that returns an open connection between the server and the client, as well as the client's address.
5. When communication with a client is finished, the connection needs to be cleaned up using close()

Creating Sender:

We need to build an instance of the Socket class in order to create a server application.Here, for communication between the client and the server, we use the 5000 port number.Any other port number can be selected as well. The accept() mechanism is waiting for the client. When clients connect to the required port number, the Socket instance is returned.

Creating receiver:

We need to create an instance of the Socket class to create a client application. Here, we need to enter the server's IP address or hostname, and a port number. We use "localhost" here, since our server operates on the same device as ours.

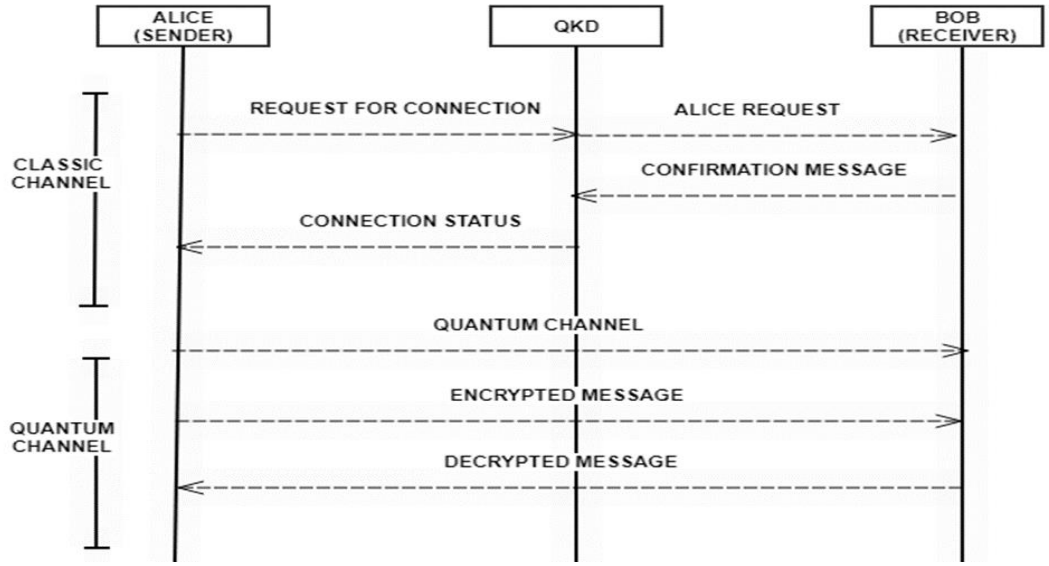

FIG 2: FLOW DIAGRAM

From fig. 2, Alice sends request for connection through the channel to the Bob. The response for the Alice's request is send back from the Bob which also checks the connection status to connect for communication. These process occurs in classic channel. The quantum channel is been established if connection is been successfully done without any loss to the data. The quantum channel is used for secured communication. The Alice and Bob share a secret key which is used as the private key for further communication.

Message encryption

The authentic message encoded as bit string. To encode letters, Sender used Morse code. However, as Sender could only send zeros and ones, sender encoded as follows

1. One is short mark, dot(.) or "dit" and other is long mark, dash(-) or "dah".
2. After every dit or dah, there is a one dot duration or one unit log gap.
3. Between every letter, there is a short gap.
4. Between every word, there is a medium gap.
5. When encoding is changed to binary, the short mark(dot) is denoted by 1 and the long mark(dash) is denoted by 111.
6. The intra character gap between letters is represented by 0.
7. The short gap is represented by 00 and the medium gap by 000.

BB84 protocol:

The steps of the BB84 protocolthe first step, the sender choose the message as bit, k and choose one random bit string, b. The sender encodes the qubit in the standard basis. When representing each basis with two perpendicular arrows, where the two distinct bases are rotated by 45, this becomes more illustrative. The encoding of each qubit would therefore look like the following: D-basis: Diagonal basis and R-basis: Rectilinear basis. After encoding the 'n' qubits, Sender sends the qubits to receiver. The receiver also generates a random bit string bi consisting of 'n' bits that determines in which bases going to perform measurements. The receiver stores the outcomes of the measurements ki together with the corresponding basis bits bi in a table. Next, Sender and receiver compare their basis bits b and bi. Whenever bi is not equal to b, the receiver measured in a different basis than sender's qubit was encoded with probability 1/2. Sender and Receiver therefore discard all key bits corresponding to these basis bits. If b is equal to bi, the qubit is prepared and calculated on the same basis, so the receiver will get the key bit encoded by the sender, k = ki writing the hidden key (unless someone eavesdropped)

Message decryption

In a first step, the encrypted bits are converted to actual bits. Then the bits are converted to Morse code. Finally translated to authentic message.

4. Results:

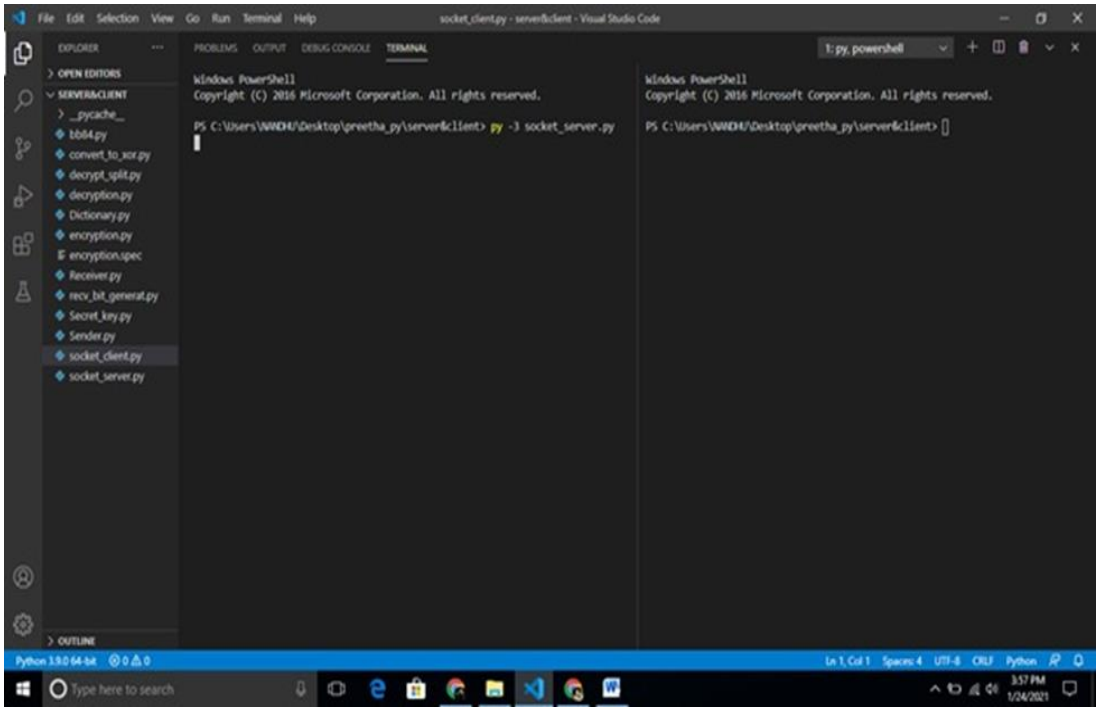

FIG 3: REQUEST TO THE SERVER FOR CONNECTION

In fig. 3, the server tries to establish a connection with the client as per request from the client.

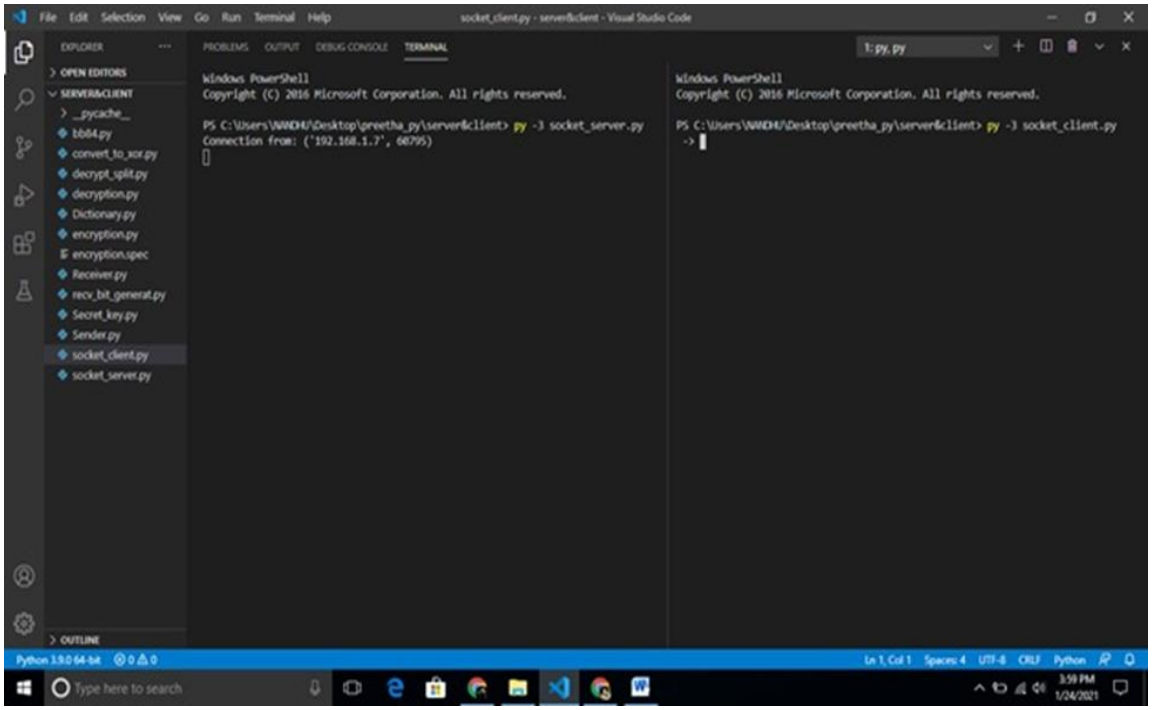

FIG 4: THE ESTABLISHMENT OF CONNECTION

In fig. 4, if the server accepts the request the connection is been established.

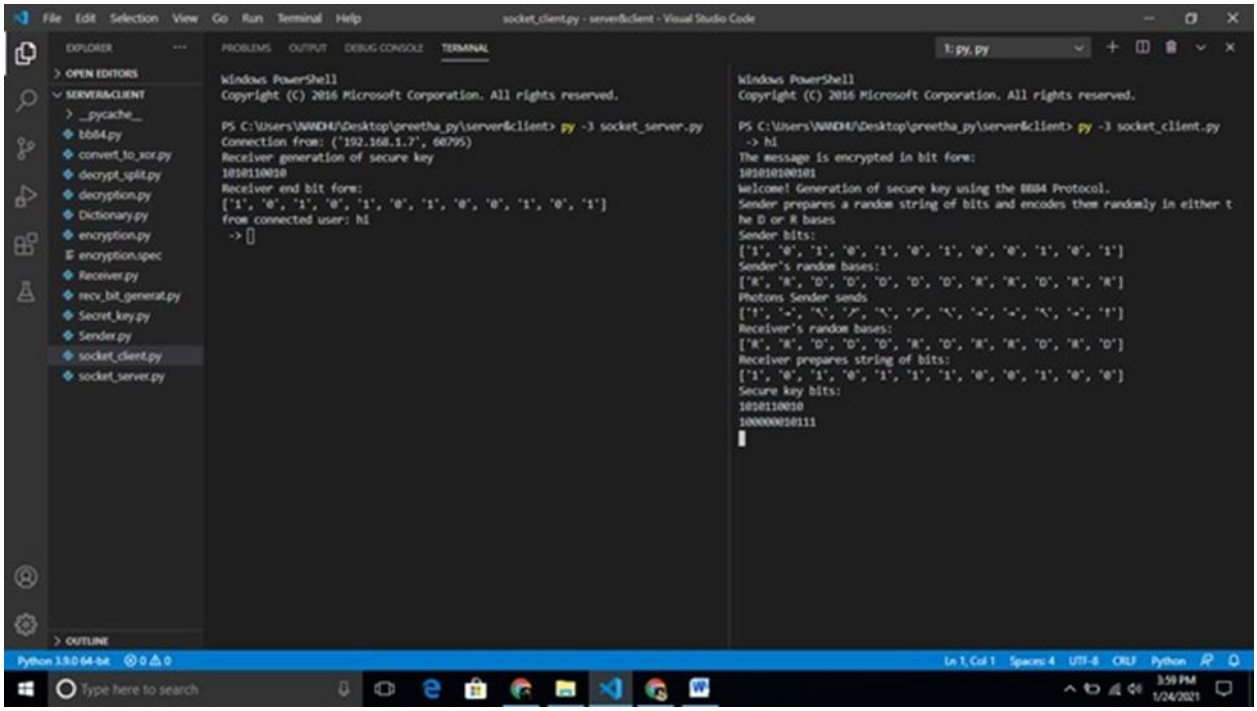

FIG 5: COMMUNICATION FROM CLIENT TO SERVER

In fig. 5, after the connection is established the communication begins. The message from the client to the server is sent as the encrypted message which is transmitted as photons in random rectilinear or diagonal bases which are converted as secured key bits. The server receives thesecure key bits which is further decrypted in similar random rectilinear or diagonal bases and the original message is retrieved.

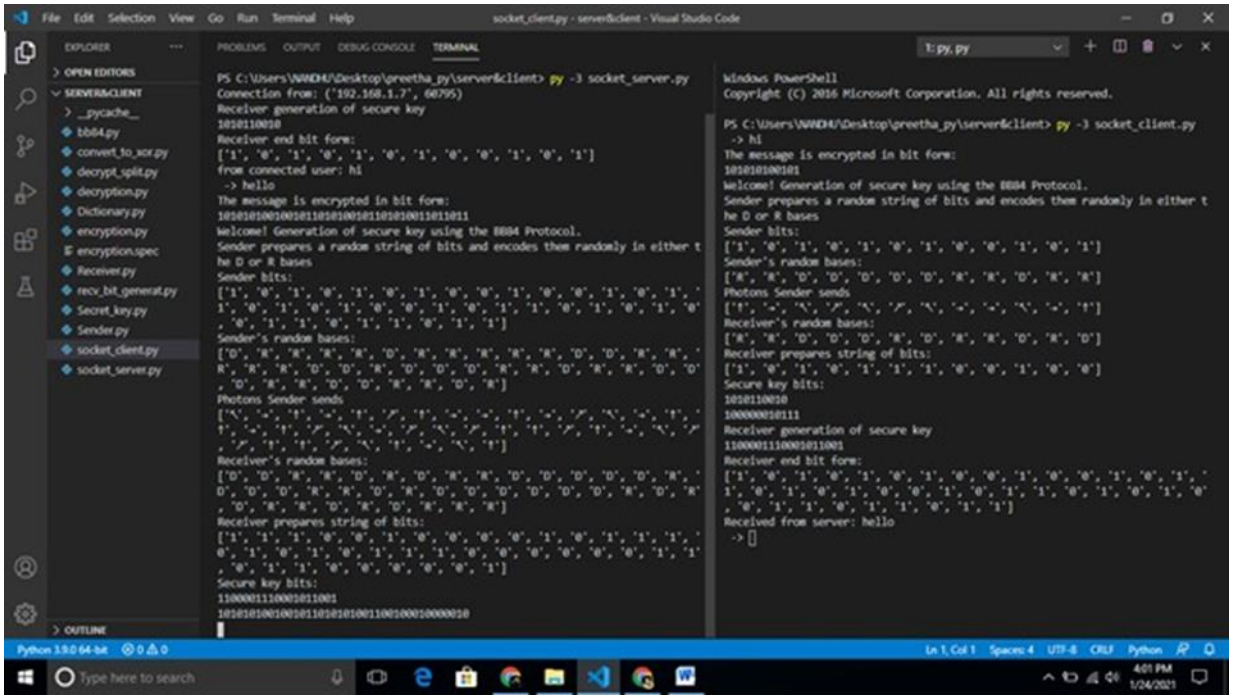

FIG 6: RESPONSE FROM SERVER TO CLIENT

In fig.6, the sender sends some secret message back to the client which is also encrypted and decrypted at the receiver end in same random rectilinear or diagonal basesand the original message isretrieved.

Conclusion:

The QKD algorithm is used to improve security in the communication system. The QKD generates light photons for encryption and decryption in the random rectilinear and diagonal bases. The approach improves the security of quantum computers than the security in the classical computers. The Morse code used for the encryption and decryption is more effective to change bits into light photons in the wireless system. The

communication between the server and the server and the client is been established and data can be transmitted. Further, the algorithm can be applied to the network of any types.

References:

1. Peng Yan, and Nengkun Yu, "The QQUIC Transport Protocol: Quantum assisted UDP Internet Connections"arXiv preprint arXiv:2006.00653 in June 2020.
2. Laszlo Gyongyosi, Laszlo Bacsardi and Sandor Imre, "A Survey on Quantum Key Distribution"in Infocommunications Journal, volume XI in June 2019.
3. Alharith A. Abdullah, Rifaat Z. Khalaf and Hamza B. Habib, "Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol"in 2nd Scientific Conference of Computer Sciences (SCCS), IEEE, 2019.
4. Aditya Sharma, Ila Sharma and Aaditya Jain "A Construction of Security Enhanced and Efficient Handover AKA Protocol in 5G Communication Network" in 10th ICCCNT 2019, IIT - Kanpur, Kanpur, India.
5. M AwaisJaved and Sohaib khan Niazi"5G Security Artifacts (DoS / DDoS and Authentication)" in 2019 International Conference on Communication Technologies (ComTech 2019).
6. Kaihong Han, Maode Ma, Xiaohong Li, Zhiyong Feng, JianyeHao"An Efficient Handover Authentication Mechanism for 5G Wireless Network" in 2019 IEEE Wireless Communications and Networking Conference (WCNC).
7. MadhusankaLiyanage, JukkaSalo, An Braeken, Tanesh Kumar, SurangaSeneviratne, Mika Ylianttila"5G Privacy: Scenarios and Solutions" in 2018 IEEE.
8. Jing Yang, Xinsheng Ji, Kaizhi Huang, Yajun Chen, Xiaoming Xu, Ming Yi "Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet" in IET Commun., 2019, Vol. 13 Iss. 2, pp. 144-152.
9. Ijaz Ahmad, Tanesh Kumar, MadhusankaLiyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov "Overview of 5G Security Challenges and Solutions" in IEEE Communications Standards Magazine March 2018 pp. 2471 – 2825.
10. ShaileshPramodBendaleand Jayashree Rajesh Prasad "Security Threats and Challenges in Future Mobile Wireless Networks" in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN).
11. SooyeonShin, andTaekyoung Kwon "Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks" in IEEE Transactions VOLUME 6, 2018.
12. Ting Ma, Feng Hu and Maode Ma "Fast and Efficient Physical Layer Authentication for 5G HetNet Handover" in 2017 27th International Telecommunication Networks and Applications Conference.
13. Jonathan Rodriguez, Ayman Radwan, Claudia Barbosa "SECRET - Secure Network Coding for Reduced Energy Next Generation Mobile Small cells" in IEEE A European Training Network in Wireless Communications and Networking for 5G.
14. AsimMazin, Kemal Davaslioglu and Richard D. Gitlin"Secure Key Management for 5G Physical Layer Security" in IEEE Transactions 2017.
15. Marcus de Ree, Georgios Mantas, Jonathan Rodriguez and Ifiok E. Otung "Distributed Trusted Authority-based Key Management for Beyond 5G Network Coding-enabled Mobile Small Cells" in IEEE Transactions 2016.
16. S. KanagaSubaRaja, S. UshaKiruthika, "An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV",in International Journal of Wireless Personal Communications, 2015
17. XiaoyuDuan and Xianbin Wang "Authentication Handover and Privacy Protection in 5G HetNets Using Software-Defined Networking" in IEEE Communications Magazine 2015.

18. Jin Cao, Maode Ma, Yulong Fu, Hui Li and Yinghui Zhang "CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets" in Journal of latex class files, vol. 14, no. 8, august 2015.
19. RajakumarArul ,Gunasekaran Raja , AlaaOmranAlmagrabi, Mohammed Saeed Alkatheiri , Sajjad Hussain Chauhdary , and Ali Kashif Bashir "A Quantum-Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario" in IEEE transactions on industrial informatics, vol. 16, no. 1, pp. 681-690, January 2020.
20. B.F. Degefa, D. Lee, J.Kim, Y. Choi and D. Won "Performance and security – enhanced authentication and key agreement protocol for SAE/LTE network" in computer network vol.94, pp. 145-163, 2016.
21. Y. Qiu, M. Ma and X. Wang, "A proxy signature – based handover authentication scheme for LTE wireless networks" in Network computation application journal vol.83, pp. 63-71, 2017.
22. Rahim, Robbi, S. Murugan, Reham R. Mostafa, Anil Kumar Dubey, R. Regin, Vikram Kulkarni, and K. S. Dhanalakshmi. "Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords." Webology 17, no. 2 (2020).