International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

QUANTUM KEY DISTRIBUTION

Roshini Murali Krishnan[1], Suganthi. S [2], Vaishali. R[3], Vidhya Prakash. R[4]

[1,2,3,4]*Department of Computer Science and Engineering, R.M.K Engineering College, Tamil Nadu, India*

Abstract - *Protection power of key distribution of most traditional cryptography relies on mathematical complexity and the irrational time needed to break the algorithm. However it will be ineffective if the secret key distribution technique is susceptible. Quantum key distribution is an innovative technique for dependable communication in ever-evolving and more and more vulnerable surroundings. In quantum key distribution, the secret key is generated by means of using single particles of light (photon) and their intrinsic quantum states to create an unbreakable cryptosystem as an alternative of the use of numerical keys. This key can be used with any public key encryption algorithm to encrypt and decrypt a message which can be sent over a well-known communication channel.*

Keywords: **Quantum Key Distribution, Middle-in-the-man-attack, BB84 protocol, Advanced Encryption Standards, Substitution Permutation Network**

1. INTRODUCTION

Quantum Key Distribution is the technique of producing a private key shared among two entities by using a quantum channel and an authenticated classical channel (e.g., a cellphone line). The private key can then be used to encrypt a message which is sent over an classical channel (along with internet connection). Contrast to conventional cryptography where the security is typically based totally on the fact that an opponent is not able to resolve a particular mathematical problem, QKD achieves safety via the laws of quantum physics. An eavesdropper trying to intervene the quantum key exchange, will be detected as he will leave some traces. In this case, the QKD protocol ends the key generation.

1.1.1 UNCERTAINITY

In quantum mechanics, measurement is a major part, not only an external method as in physics. It is far viable to encode data into a few quantum properties of a photon so that any attempt to track them always disturbs them in some detectable way. The impact arises due to the fact in quantum communication, certain physical properties of photons are complementary within the sense that trying to measure the properties of a particular photon always disturbs the other photons. This is called Heisenberg uncertainty principle. The two properties which might be regularly utilized in quantum cryptography are two photon polarization; rectilinear polarization (horizontal and vertical) and diagonal polarization (45° and 135°).

1.1.2 MIDDLE-IN-THE- MAN-ATTACK

Man-in-the-middle attacks in quantum cryptography are not possible due to Heisenberg's Uncertainty Principle. If an intruder tries to intercept the photons, he will change them if he uses the wrong detector. He cannot emit the photons to Bob correctly again because it will introduce unacceptable errors into the communication channel. If entangled photons are used by Alice and Bob, then it is not possible to attack these because emitting three entangled photons would reduce the strength of each photon to such a degree that it can be easily detected. Intruder cannot use a man-in-the-middle attack, since he would have to measure an entangled photon disrupting the other photons and he would have to emit both photons again. This is not possible to be done by the laws of quantum physics. Other attacks might occur due to which fibre optic line is required between the two points linked by quantum cryptography. If it is possible to tamper with the equipment used in quantum cryptography, it is possible to generate keys that are not secure using a random number generator attacks.

1.2 EXISTING SYSTEM

Modern key distribution techniques are practical and can be done for any distance. Public key ciphers such as Diffie-Hellman, RSA and ECC are used for exchanging symmetric keys. Public-key cryptography or asymmetric cryptography is an encryption scheme that makes use of two mathematically related, but no longer equal keys - a private key and a public key. Unlike symmetric key algorithms that rely upon one key to each encrypt and decrypt, every key performs a unique function .For encryption these keys can be used, for instance with AES. This key distribution technique offers a couple of challenges. Its security is threatened by using random number generators, new attack strategies, advances to CPU power and the emergence of quantum computers. Quantum computer systems will ultimately render a lot of modern-day encryption dangers. A specific challenge is that information encrypted today can be intercepted and stored for decryption via quantum computer systems. The primary quantum cryptography protocol defined a way to use photon polarization states to transmit the secret key through a quantum communication channel. This protocol is the BB84 protocol and classified as prepare-and-measure-based QKD protocol. BB84 protocol uses single photon to transmit and distribute random bits to generate the secret key.

1.3. PROPOSED SYSTEM

In proposed system we use the QKD protocol and other variant protocols which can be the recognized as secure protocols. The QKD protocol includes four phases. The first phase is the transmission of the randomly encoded single photon circulation over the quantum channel from Alice (the sender) to Bob (the receiver) to establish a primary key. Alice continues a transient database of the state of every photon sent. The second phase is shifting where Bob sends the photons detected and their bases to Alice over the classical channel. Bases refer to how the photons have been measured. Photons may be encoded in certainly one of bases (e.g., horizontal/vertical or diagonal polarizations).If there is most effectively one photon then only, one base can be implemented. If the photon base is not measured properly, the value will be wrong. If it is far measured within the incorrect base by the photon detector, the generated value may be random. Alice keeps in its database best of those entries obtained by Bob in the proper base and sends this revised list again to Bob over the classical channel. Bob retains those entries in his revised listing. Alice and Bob now have an identical shared key. These keys are of the same length however may additionally have a few errors. That is referred to as quantum bit error rate and it is due to eavesdropping. The third phase is reconciliation to correct these errors. After errors are removed the sender can send the information to the receiver using the key.

2. SYSTEM DESIGN AND IMPLEMENTATION

2.1. QUANTUM KEY STATE TRANSMISSION

Essentially there are two types of QKD protocol schemes, the first scheme is prepare-and-measure-based QKD protocol and the second scheme is entanglement based QKD protocol. The Alice has to put together the information as polarized photon with the usage of photon detectors and then the Bob ought to measure that photons dispatched. Prepare-and-measure-based QKD protocol using Heisenberg's uncertainty principle in which it is not possible to measure the quantum states without changing its unique quantum state.

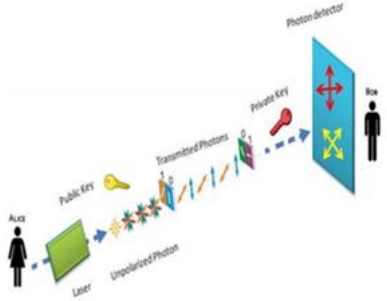

FIGURE 2.1 PHOTON TRANSMISSIONS

2.2. GENERATION OF RANDOM KEY

A Photon emitter is used to supply photons which are polarized in four directions- horizontal, vertical, diagonal left and diagonal right in which each photon can convert one bit of information like vertical polarization for "0" and horizontal polarization for "1" or right diagonal polarization for "1" and left diagonal polarization for "1".There are two detectors A for horizontal, vertical and another detector B for diagonally polarized photons. The photons randomly go through one of the detectors and the photons are transformed to bits .If the photon become detected via the incorrect detector the bit generated via the photon is removed. All the last bits which were shaped with the aid of the photons accomplishing correct detectors shape the quantum key.

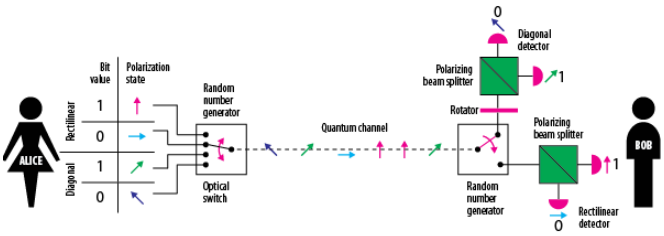

Figure 2.2. Generation of random key

2.3. ERROR CORRECTION

According no-cloning theorem, the quantum bit (qubit) cannot be copied or amplified without changing them. This mechanism allows the QKD system to detect the presence of eavesdropper via the usage of the error parameter during the transmission process of photons from Alice to Bob. In the meantime, in entanglement-based QKD protocol, Alice and Bob use entanglement photons principle to distribute secret key.

Entanglement is the state of photons with correlated physical properties. The entangled photons cannot be defined by specifying the states of each particle and will contain information such that it is not possible to obtain information from a single particle. It is crucial for long distance communication.

2.4. ENCRYPTION

Using the shared secret Key Alice can encrypt the message using AES Encryption algorithm and transmit it to Bob. It consists of three block ciphers: AES-128, AES-192 and AES-256. The ciphers encrypt and decrypt information in blocks of 128 bits by using cryptographic keys of 128-bits, 192-bits and 256-bits respectively. The Rijndael cipher accepts extra block sizes and key lengths but it is not followed in AES. Symmetric ciphers use the secret key for encrypting and decrypting, so the sender and the receiver should both recognize and use the identical secret key. There are 10 rounds for 128-bit keys, 12 rounds for 192-

bit keys and 14 rounds for 256-bit keys there are many processing steps that consist of substitution, transposition and combining of the enter plaintext and reworking it till the very last output of cipher text. The AES encryption defines some changes to be carried out on data in the form of an array. Step one is to put the data into an array after which the cipher alterations are repeated over some encryption rounds. The number of rounds is determined by the length of key-10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. The first transformation in the AES encryption cipher is substitution of information using a substitution table; the second one transformation shifts records rows, the third is mixing of columns. The final transformation is XOR operation executed on every column using a distinctive part of the encryption key. Longer keys need extra rounds to finish.

2.5. DECRYPTION

Using shared secret key Bob decrypts the message. The usage of AES decryption rules helps to view the plain text. AES decryption involves transforming data Rijndael block decipher algorithm to make it readable to those owning unique knowledge, commonly referred to as a key. The Encrypted records can only be deciphered if one has the key . The decryption set of rules is a fixed of well described steps to convert data from an unreadable format to a decoded format. The end result of the process is decrypted records, referred to as decipher text. AES decryption set of regulations is an iterated block decipher set of rules with a tough and speedy block length of 128 and a variable key duration. The AES operates on 128 bits of data and generates 128 bits of output. The period of the important thing used to decrypt this enter records may be 128, 192 or 256 bits. AES has been designed as a SPN(Substitution-Permutation Network) and decryption manner uses 10, 12 and 14 decryption rounds for key length of 128, 192 and 256 bits respectively.

CONCLUSION

Compared to the classical cryptography, probabilities of data being intercepted and modified are extremely low in quantum cryptography. QKD helps in generating secret keys which is based on the rules of quantum physics. Key sharing need a communication channel between the entities which is costly. Quantum principles do not permit to send keys to two or more different locations due to which it requires separate channels between source and many destinations. This is major disadvantage of quantum communication through optical channel.

FUTURE WORK

Protection of QKD encryption system appears powerful however it is still experimental and its first users outside the research community are likely to be the ones for whom safety is of greater importance than cost. QKD can be used in network routes and offer Ethernet connections for high-security communications. It can also be adopted in government and industries for encrypting important data.

REFERENCES

[1] Aakash Goyal, Sapna Aggarwal and Aanchal Jain,"**Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper",** 5th IEEE International Conference on Advanced Computing & Communication Technologies [ICACCT-2011] ISBN 81-87885-03-3

[2] *Marcin Niemiec and Andrzej R. Pach, AGH University of Science and Technology,* **"Management of Security in Quantum Cryptography",** published in IEEE Communications Magazine August 2013

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

[4] Dr. PhysicsA, Quantum Mechanics Concepts: 1 Dirac Notation and Photon Polarization, Published on Aug 20, 2013,Available:https://www.youtube.com/watch?v=pBh7Xqbh5JQ

[5] Dr. PhysicsA, Quantum Mechanics Concepts: 2 Photon Polarization, Published on Aug 27, 2013,Part2 of a series: continues photon polarization , Available :https: //www.youtube. com /watch?v=zNMzUf5GZsQ

[6] V. Padmavathi, B. Vishnu Vardhan, A. V. N. Krishna," **Quantum Cryptography and Quantum Key Distribution Protocols: A Survey"**, 2016 IEEE 6th International Conference on Advanced Computing Conference

[7] Stamatios V. Kartalopoulos, Williams Professor in Telecommunications Networking,The University of Oklahoma," **Chaotic Quantum Cryptography",** The Fourth International Conference on Information Assurance and Security

[8] W. K. Wootters and W. H. Zurek, "**A Single Quantum Cannot be Cloned**", Nature 299, 802-803, 1982.