Intl J Engg Sci Adv Research 2016 March; 2(1):49-50 ISSN NO: 2395-0730

An Apical Approach towards Key Distribution System Based on Quantum Mechanism in Cryptology

Neeraj Dwivedi
M.Tech Scholer
Dr. A.P.J. Abdul Kalam Technical University, U.P, India.
dwivedineeraj13@gmail.com

***Abstract*- By using the methods of quantum computing, a computer could able to factor large prime numbers easily. Although it is true that existing strongest encryption keys has not broken yet but there is no guarantee that these keys will be secure forever. In this paper, we will concentrate on the solution of key distribution problem i.e. Quantum key Distribution, which distributes the secret keys very securely. QKD enables the sender and receiver to create secure secret keys in the presence of potential intruder. The fundamental laws of Quantum mechanics and Quantum information theory are the ideas behind this key distribution system. Further this paper concentrates on how the security of QKD is achievable and also analyzes the security of this system against many different attacks.**

Index Terms- Quantum Key Distribution, Secret-key Distillation, Cryptography.

I. INTRODUCTION

Sending information securely over the network has been and still remains a challenge for a computer scientist as well as physicist. As long as more information is sent over the network, there is need for even more security. Cryptography is the science of converting data into unreadable format and need of cryptography remains as long as eavesdropper exists. Therefore, cryptography handles the security of information among the many potential eavesdroppers. Modern cryptography relies on mathematical theories and computer science practices which is capable to secure our data but it would not remain secure always. As ultra high speed computers come into play, this cryptographic algorithm could be fail. Recently, some practical shows that modern cryptography can break with some or more efforts. A student at Notre Dame University has broken 109-bit key using 10,000 computers working around the clock for 549 days [2]. This practical show that breaking today's powerful keys is not far away. Classical security systems are extremely weak in comparison with Quantum computing. If Quantum computing became tangible and useable, conventional cryptography would easy to break.

II. CLASSICAL CRYPTOGRAPHY

The Classical cryptosystem is of two types- symmetric systems and asymmetric systems. In secret key cryptography, a single key is used for both encryption and decryption. It requires secure channel for key distribution and security is based on non proven, complicated algorithms whereas security in public key cryptography is based on non prove assumptions. The problem in the cryptography which is the main concern of all researchers from decades is to secretly transport the key to the authentic user. Simply we can say that key distribution is the major problem. The solutions to this problem are categorized in two sub areas of cryptography- Classical cryptography and Quantum cryptography.

III. QUANTUM CRYPTOGRAPHY

Quantum cryptography comes into play when Quantum computers will exist. Quantum cryptography gives us perfectly secure data transfer over the network in the presence of potential eves. The first practical of Quantum cryptography could transfer the secret key the data over 30 centimeters using polarized photons, calcite crystals and elect optical device.

IV. QUANTUM KEY DISTRIBUTION(QKD)

Quantum Key distribution permits sender (Alice) and receiver (Bob) to communicate over the quantum channel to detect any form of eavesdropping that may or may not interrupt the channel. Encrypting data is not the main purpose of QKD, it guarantees the secrecy of distributed keys [1]. In turn, legitimate parties use this key for encryption. Two links ensure the confidentiality of data: encryption algorithm and quantum-distributed keys. Strength of these links should not compromise because if one of these links broken, whole chain is compromised. Confidentiality of the key is ensured by the laws of Quantum mechanics. If the eavesdropper tries to interrupt the channel, she will be detected. Keys will discard while no confidential data is transmitted yet. Encryption algorithm has also strong properties. If encryption keys are as long as the message and not used for subsequent messages, confidentiality of message is also guaranteed.

V. HOW QKD WORKS

Two channels are required for quantum communication: Quantum channel and public channel. Quantum carriers travel over the Quantum channel. Any particles which obey the laws of Quantum mechanics can be used. Photons, elementary particles of light are usually used and the channel may be an optical fiber or open air. Open air is used for satellite communication while optical fiber is used for telecommunication. Alice encodes random pieces of information in quantum carriers that form a key. During the transmission eve can listen to the Alice and Bob, but this not the problem because eavesdropping is detectable and Secret-key Distillation provides the way by which Alice and Bob recover from such errors and form a key out of the bits unknown to the eve. Alice and bob requires a public classical authenticated channel to compare a fraction of key to check for any errors caused by eavesdropping [3]. Authentication and publicness are the important characteristics of public channel.

VI. SECRET- KEY DISTILLATION

Secret- key distillation is the process of forming the new key out of the bits unknown to eve. Alice and Bob may decide to abort the protocol as in the case errors may cause by the eavesdropper are detected. Numbers of errors counted by Alice and Bob and divide this number by n to obtain the expected fraction e of the transmission errors in the whole set of keys elements, where e is called bit error rate. Secret-key distillation usually comprises with the steps called reconciliation and privacy amplification [4]. Reconciliation is the process of correcting the transmission errors and privacy amplification is the process which wipes out Eve’s information at the cost of a reduced key. Finally Alice and Bob can used the secret key obtained by power amplification. They can use it to encrypt message by creating secure channel. Public authenticated classical channel is used for communications in secret-key distillation process.

VII. CONCLUSION

From above discussion we can say that the key distribution process closes the door for eavesdropping. The feature of detecting eavesdropping makes this cryptographic field so powerful. Some work has done in this field and efforts are continue worldwide to make it in use fully.

REFERENCES

[1] Quantum cryptography and secret key distillation- Cambridge University Press, Gilles Van Assche.

[2] Quantum encryption- A means to perfect security? - SANS institute infosec reading room, Bruce R. Aubum, GSEC V.1.4b.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol,"