The Next Level of Information Security: Impact of Quantum Cryptography

Abhishek Agnihotri

M.Tech Scholer

Dr. A.P.J. Abdul Kalam Technical University, U.P, India.

abhiagni1991@gmail.com

***Abstract*- By the development of ultra high-speed computers, existing modern cryptography could be failed whereas Quantum cryptography guarantees the secure communication whose security based on the legality of quantum mechanics. This research paper concentrates on the strong basics of quantum cryptography and how it guarantees the secure communication over the network. There are two ways to conduct Quantum Cryptography which uses Heisenberg uncertainty principle and differ in the way information is passed between the users, one uses polarized photons and one uses entangled photons. Keys are generated by using the quantum properties of light. Further this paper concentrates on the research directions in which quantum cryptography speeds up and also outlines that how quantum cryptography can be used to implement real world application.**

Index terms- Quantum cryptography, Communication, Information Security.

I. INTRODUCTION

In the era of informational technology, information has become a valuable commodity. Large amount of confidential data like commercial, personal, military, government policies are transmitted over the network. It is important to develop the technique which guarantees the secure and authentic communication over the network. The technique to keep our information safe from the eavesdroppers is called cryptography in which we encrypt our original data at the sender side before sending it over the network and the data is decrypted at the receiver side to recover original data. The main aim of cryptography is to transfer the data securely over the network in the presence of potential eavesdropper. Modern cryptography is mostly relies on mathematical theories and computer science practices whereas Quantum cryptography relies on the universal laws of quantum mechanics. The interesting properties of Quantum mechanics i.e. Heisenberg Uncertainty Principle and Entanglement are main ideas behind the Quantum Cryptography. Measurement is destructive in quantum mechanics which makes quantum cryptography able to detect an eavesdropping i.e. Quantum cryptography is the technique where eavesdropping is detected and detection of eavesdropping makes this technique perfectly secure for information sharing over the network. Basic goal of authentic, secure communication threatens by Quantum computing because it is able to do certain type of computations which conventional computers can't, eavesdropper can easily listen into private network and pretend to be whom they are not by broking the cryptographic keys easily using quantum computers, in spite of this, some algorithms used today are also safe in Quantum computing because Quantum computer can not able to brake all cryptographic keys [2]. The idea of Quantum cryptography will play a important role for information security when Quantum Computers exist in the world.

II. HOW QUANTUM CRYPTOGRAPHY WORKS

Quantum cryptography can be conducted in two ways which rely on Heisenberg uncertainty principle. These techniques are differ in the way information is passed between the user.

Communication has a one-way quantum channel i.e. used for sending information from Alice to Bob and two-way public channel that could be the internet. Polarized photons are used to communicate over Quantum Channel. There are generally three types of polarization used in the Quantum cryptography- Rectilinear, Diagonal and Circular. Bits are sent over the Quantum Channel by choosing one of the polarization schemes. When bits are sent, Bob can't sense the arbitrary polarization of the photon, he simply make decision to interpret because of Heisenberg uncertainty principle which states that certain pairs of physical properties can not measured simultaneously. There is no way by which bob can determine and Alice couldn't tell him over the public channel- that would ruin what we are trying to achieve [3]. The idea is that Alice sends random bits using random polarization and Bob also uses random polarization when photons are received. Then Alice tells to Bob over the public channel that what polarizations she used without telling him the bit values. Bob compares his polarization list with the polarization list which Alice sent and the union of these lists is

used to generate the secret keys. Bob tell to Alice about their correct guesses of polarizations over the public channel and these bits are used for the communication over the public channel.

III. POTENTIAL WEAKNESSES IN TODAY'S KEYS

There is no guarantee that the strongest keys used today in the commerce and government based on factoring large numbers will secure forever. 2048-bit keys are thought to be very safe because it take millions of years using most advanced computers to break them. A key using RSA's Security RC5-64 algorithm has broken recently. A student at Notre Dame University, using 10,000 computers working around the clock for 549 days, broke a 109-bit key (Reuters, Notre Dame) [4]. Manindra Agrawal, a computer scientist at Indian institute of technology has solved a bigger problem for mathematicians over a years- that how to tell that a number is prime without performing factoring [4]. This doesn't mean that today's encryption schemes can be broken and a large number can easily factorized but finally it opens a door for mathematicians that how to find that a number is prime without factoring a number. This shows that the keys used today can be broken by enough computing power, not today but in the future these keys will broke. Then what happens? Answer is - Quantum Computers and Quantum cryptography will use for secure information sharing over the network.

IV. IDEA BEHIND THE SECURITY OF QUANTUM CRYPTOGRAPHY

There are three main reasons behind the security of Quantum Cryptography. First, no-cloning algorithm [6],[7], messages could not be copied and sent on because they would be in an unknown quantum states. Second, an eavesdropping in the communication can disturb the system and the messages are useless and garbled for the recipient. Third, An eavesdropper can not put back the message to it's original state i.e. eavesdropper can not make fool to the users. If the system is intercepted, the system seems to be broken. No efforts can alter the fact that observing the system can not reversible. If a lucky eavesdropper correctly measure the each bit of message, he has the secret key and he can intercept the message. But here quantum cryptography do not fail, intercepting the message would broke the system and users aware of it, then they would generate another secret key.

V. DETECTION FOR EAVESDROPPING

Eve can intercept the channel and tries to measure them. As Bob is not able to sense what polarization Alice used, Eve would also not able to sense it. As Bob, Eve will also try to measure them. The chance to measure the correct polarization is totally depend on the schemes used for polarization. If two polarizations i.e. horizontal and vertical, are used, then there is a possibility of 1/2 for each bit polarization and if four polarizations are used i.e. horizontal, vertical, left diagonal, right diagonal, are used, then there is a possibility of 1/4 for each bit polarization. Measurement is destructive in Quantum mechanics. The particle takes the result of the measurement as a state [1]. In case of two polarization scheme, eve has a probability of 1/2 to measure in right manner, if he measures correctly, he will unnoticed and does not disturb the state but when he makes a wrong measurement, he caught. Half of the time, he got irrelevant results. He wants not to send the states for the wrong measurement, but it's not possible for him as he don't know that which polarization scheme is used. Bob and eve have the same difficulty as they both don't know that what polarization scheme is used. But this symmetry is not for always because the classical authenticated channel is used for all the communications for sifting, which allows Alice to be sure that she is communicating to the Bob not to Eve, and Alice and Bob can share key elements which are correctly measured.

VI. RESEARCH DIRECTIONS

Classical cryptography is still very secure because it depends on the algorithms that can't be broken even in less than the lifetime of universe by the computers used today. Quantum cryptography is not much demanded in the theory yet so we can't say surely that when this technology comes into play and protect our information. When quantum computers come into play, the computational speed will increase considerably so the complexity of algorithms will less to brake. No doubt that Quantum cryptography is true invention in the field and in the developing state. In spite of some defectiveness, it is above all that is come into play before it. In spite of some implementations, this technique is far away to come into play and secure our information.

VII. REAL WORLD APPLICATION IMPLEMENTATIONS

The most infamous and developed application of quantum cryptography is Quantum key distribution. Quantum Key Distribution [5] is an approach for producing the perfectly random key which is shared by sender and receiver with the surety that nobody has a chance to sense about key. Bennett and Brassard was invented the protocol in 1984 for key distribution using quantum mechanism [6]. Other applications of Quantum mechanics to cryptography fall into the categories-

- Quantum mechanics can be used to break classical algorithms.
- Quantum states can be used to make new and securely improved protocols to protect classical information.

VIII. CONCLUSION

Cryptography is a very important issue for today's world and Quantum cryptography makes it independent of mathematical

formulas and protects algorithms created being cracked by the intruder. Quantum cryptography is a quantum jump in the field of information security. Quantum cryptography is still far away but it is the top most secure technique developed yet to protect our information. Quantum cryptography will come into play when quantum computers exist.

REFERENCES

[1] Quantum cryptography and secret key distillation- Cambridge University Press, Gilles Van Assche.
[2] Quantum safe cryptography and security- An Introduction, benefits, enablers and challenges, june 2015, ISBN No. 979-10-92620-03-0, European Telecommunications standards institute.
[3] The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography – Simon Singh.
[4] Quantum encryption- A means to perfect security? - SANS institute infosec reading room, Bruce R. Aubum, GSEC V.1.4b.
[5] Mehrdad S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System".2009, pp. 1644-1648.
[6] 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, Bangalore, India, pp. 175-179, December 1984. (Bennett–Brassard protocol).
[7] W. K. Wooters and W. H. Zurek, "A single quantum cannot be cloned", Nature 299, 802 (1982) (no-cloningtheorem).