ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, No 5, May 2013

STUDY OF QUANTUM CRYPTOGRAPHY

Swapnika*
SES, BPSMV
Khanpur kalan, Sonepat

Rajani bala
SES,BPSMV
Khanpur kalan , Sonepat

Kavita
SES,BPSMV
khanpur kalan,sonepat

Abstract-The concept of quantum cryptography involves the quantum physics by which two parties can establish a secure key exchange. The security in such system is defined by the laws of quantum physics. Quantum cryptography holds its root from Steven weisner's conjugate coding. The basics of quantum cryptography is based on two principles of mechanics namely, Heisenberg's uncertainty principle and photo polarization law. The uncertainty law says that the quantum of any state cannot be determined by without disturbing the particular system whereas the law of photo polarization says that the unknown qubits can never be guessed by traffic analysis or another kind of passive attack. This paper presents the current scenario of quantum cryptography, its implementation and its future use.

Keywords – Cryptography, photon, quantum, Heisenberg uncertainty principle, polarization of light

I. INTRODUCTION

Cryptography [1] is a technique of encrypting and decrypting the message so as to maintain the confidentiality of the data. The usage of cryptography is not new in the digital world. The cryptography is in use since historical times. Julius Caesar used Cryptography and gave the world "Caesar Cipher ".For effective, we chop – off the message into small chunks and then encrypt the messages by an encrypting algorithm and are sent via a communication medium to the receiver's side. Further, he receiver side decrypts the message by using the counterpart of the encryption algorithm and receives the message. But at times the messages get hacked by an intruder during the communication phase or by an attacker challenging the encryption algorithm. Based on attacks, the algorithms and techniques are always changed and a new and more secure and sophisticated cryptographic algorithm are sought-after. It has been observed that most of the time either the adversary ruptures the connection to get message or attacks the algorithm. For secret key communication, the two users who wish to establish communication should meet to exchange key or either use a secure courier service, both of which is absolutely impractical.

Hence, in quantum cryptographic we present a more reliable and secure communication which has amalgamation of quantum physics and cryptography. Hence a more complex and sophisticated approach to encryption and decryption. The quantum cryptography defines a light as a beam of neglible weight charged particles known as photons.
The photons differ from each there in terms of orientation. The entangled pairs [8] can be defined as the pairs of photons which are generated by particular reactions. The entanglement of the photons lays an effect on their randomness. For example- consider 2 beam of lights B1 and B2. When B1 is measured with a polarization filter only one half of the photons pass the filter. Whether a particular photon will pasta filter or not is completely based on its randomness. But when B2 is measured with the polarization filter consisting of entangled companions of B1 and also the filter oriented at an angle of 90 degrees so that when B1 will pass the filter then B2 will also do it and also if B1 will not pass so shall not B2. this figure shows a polarized light.

The whole concept of quantum cryptography lies in uncertainty principle states that there are certain pairs of a special physical properties which are related in a way that while estimating one property simultaneously another property cannot be observed whereas in polarization of photons direction of measurement lays an important effect on further measurements. In quantum key distribution we use quantum mechanics for secure communication. In this scenario, both the users generate a common bit string which is used as the key for encryption and decryption. Also, in quantum cryptography, the presence of an adversary can also be detected very easily

Quantum cryptography imparts a secure key distribution and is not meant for transmission of any messages. The quantum cryptography's security model uses physics rather than mathematics; hence it is quite secure from other cryptographic techniques. Because of its reliable and strong cryptographic mechanism, mow-a-days, it has been used in business communities and for international secret groups. It was first experimented in the year 1989 over a distance of 32 cm but today it is securely transmitted over miles with the help of optical fibers.
He QC works as follows:-

a) Firstly. A set of photons swath different and random orientations are sent to the receiver as possible key for encryption and decryption process.
b) This stream of photons is then converted to generate a stream of bits.
c) If any, intruder receives this key, then it is of no use to him as it this only a stream off random bits.
d) On receiving the key, the process of encryption and decryption can be started.
e) After encrypting the message with such key, the message can be sent over telephone electronic mail or even a regular mail.

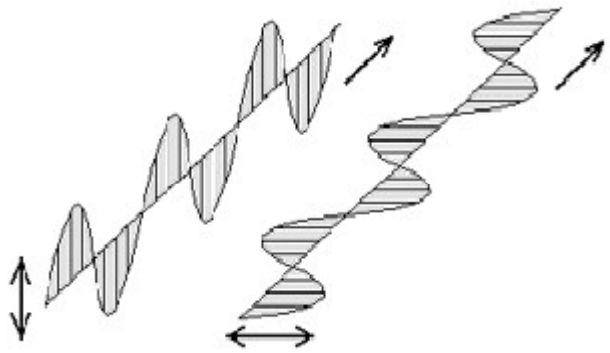

Figure 1: showing vertically and horizontally polarized light

II. CONVENTIONAL WORK IN QC

A. BB84 ENCODING SCHEME

BB84 scheme uses the two pairs of state in which both the photons are orthogonal to each other and the two pairs should be conjugate to each other. Such types of pairs can be

- Rectilinear basis of vertical and horizontal of 0 and 90 degrees.
- Diagonal basis of 45 and 135 degrees.
- Circular basis of left and right handed.

Since all these pairs are also conjugate to each other hence any two of them can be used... hence in this the quantum information can be stored in non orthogonal states.

B. B92 ENCODING SCHEME

It holds its roots from BB84 encoding scheme. It uses two states of BB84, i.e., 0 and 45 are used and represented by 0 and 1. Then these non orthogonal bits are encoded by the sender in such a manner that not even a single bit can be determined with absolute certaininty.
It was developed in the year 1992 by Charles Bennett.

C. EKERT ENCODING SCHEME

Developed in the year 1992by Arthur ekert, which takes advantage of the entanglement of photons. In this a photon is divided into two by laser and then one half of the photon is kept with the sender while the other half is sent as key to receiver from sender.

III. QUANTUM CRYPTOGRAPHY TECHNOLOGIES

Quantum technologies secure key distribution by two phenomenons- the device for creation of photons and then their detection. A photon gun is considered as the most ideal source for the creation single photon, but its practical implementation is not yet possible. Certain attempts have been done by researchers to produce the photons either by a light emitting p-n junction or with the help of a carbon atom. In light emitting p-n junction they try to produce single photons as per the demand but in carbon they replace it by nitrogen which then creates a hole and then further an excitation by the laser a photon is developed . But none of these technologies can be used for quantum cryptography as they are not much secure. A most common way is to decrease the intensity of the laser beam so that there should be only one emission allowed per pulse but these beams presents more than one photons and further these photons proves out to be hazardous as they extra photon can be used by the adversary. Just like the creation, detection of a single photon is also difficult.

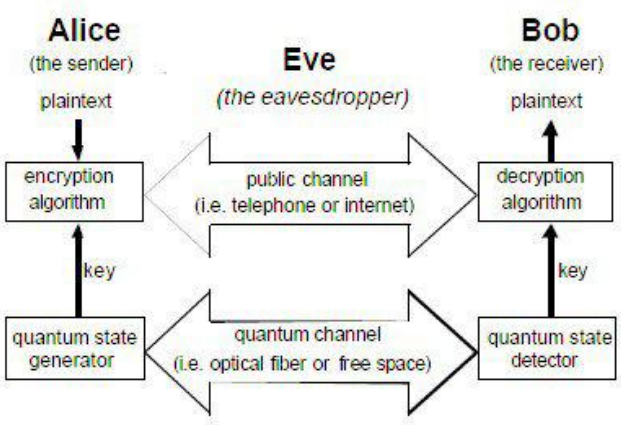

Figure 2 Quantum Cryptography

The common practice is to use avalanche photodiodes. Such devices operate in Geiger mode. In this mode the voltage is higher than the breakdown voltage of the diode and hence a photon absorbs the energy, gets excited and then causes the avalanche (electrical). Now to detect another photon, the device should stabiles the current and then device should be set in reset mode which is on other hand is very time consuming. Also silicon's wavelength detection is best at 800 nanometers and hence, lays no impact or is totally immune to the rays of wavelength 1100 nanometers and above. In telecommunication, Germanium (Ge) or indium-gallium-arsenide (InGaAs) is used as detectors but these are less efficient to be use with quantum cryptography.

IV PROPOSED METHODOLGY

Cryptography is a technique which can not only be installed for correct ans secure communication but also for safe key distribution. In this paper we presented a technique for such a safe key distribution techniques

V PROPOSED OUTCOME

Quantum cryptography secures the communication system by the implementation of laws of physics and not much of mathematical computation is required. The parameters and the devices used in this technique are not fictions and hence can be implemented in the real world.

VI CONCLUSIONS

Cryptography has always been an area of research and refinement. More and more tasks and more and more techniques always improve this field. The inclusion of physics in this field has given a new definition to the cryptography. In this paper we explained that how can a key be safely exchanged or distributed to both the entities of the communications.

VII REFRENCES

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance Of two quantum key- distribution Protocols," Phys. Rev. A vol. 73, 2006.
[2] C. Elliott, D. Pearson, and G. Troxel, "Quantum Cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, Technologies, architectures, and protocols for computer Communications 2003...
[3] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," Journal of
[4] Homer, Iliad 6.213, transl. Ian Johnston (in English), Malaspina University-College, Nanaimo, BC, Canada (2000).
[5] Charles Anthon, The first six books of Homer's Iliad with English notes, critical & Explanatory, a metrical index, & Homeric Glossary, Harper & Brothers, New York, p. 396 (1875).
[6]Old Spartan Factsat http://www.geocities.com/Athens/Aegean/7849/spfacts.html.
[7] D.R. Stinson, Cryptography, Theory and Practice, CRC Press, Inc., Boca Raton, p. 4 (1995).
[8] T.P. Leary, Cryptology in the 15th and 16th Century, Cryptologia 20, No. 3, pp. 223-242 (July 1996).
[9] E.A. Poe, the Gold Bug, in Tales of Mystery And Imagination, Wordsworth Editions Ltd., Ware, pp. 1-46 (1993).
[10] A.C. Doyle, the Adventure of the Dancing Men, in The Annotated Sherlock Holmes, Vol. 2, ed. W.S. Baring-Gould, Wings Books, New Jersey, pp. 527-545 (1992).
[11] G.S. Vernam, Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications, J. AIEE 45, pp. 109-115 (1926). cryptology vol. 18, pp. 133 - 165 200
[12] 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.
[13] D. Mayers,"Unconditional security in quantum cryptography", Journal of the ACM, Vol. 48, No. 3, pp.351-406, May 2001.
[14] P. Shor, J. Priskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.
[15] P. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms". Proc. of the 35th Annual Symposium on Foundations of Computer Science (FOCS), IEEE Computer Society Press, 124-134,Nov. 1994.