A Secure Communication through "Quantum Cryptography"

Deepak Kumar Verma
Department of Computer Science & Information Technology
Babasaheb Bhimrao Ambedkar University, Satellite Campus, Amethi, India

Abstract— today the information security has become the most critical and challenging task not only in defense but also in every environment, weather it may be a government organization or it may be the information of a common people. At present several techniques are available that provides the information security using various algorithmic mechanism like encryption - decryption and many more. Each of these classical techniques provides the more powerful locks to secure the information from eavesdroppers. But the possibility of the lock to be broken or the leakage of information always exists in every mechanism. Each security mechanism available today is lagging in terms of reliability either in one or more parameters i.e. we are not assure that this particular method will provide the security throughout the data transmission. So once again information security has become the most challenging task because no method available today is as reliable that it can provide the hundred percent assurance of information security and we can depend upon. Here we have described a new technique towards the information security through Quantum Cryptography that provides a new way of protecting data when it travels in the network. This method introduces the concept of quantum mechanics or light waves to protect the data from being hacked since according to the property of light we can't measure the two interrelated properties individually without affecting the other. Here in this paper we have described that how we can use the quantum mechanics in the area of information security to provide a more reliable technique that will raise the alarm at the very arrival of burglar.

Key words: Cryptography, Quantum Cryptography, Photons, Light Wave

I. INTRODUCTION

Cryptography is the science of keeping private information from unauthorized access of ensuring data integrity and authentication, and it is the strongest tool for controlling against much kind of security threats. Quantum cryptography is an emerging technology in which two parties can secure network Communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics [1]. Quantum Cryptography or Quantum Key Distribution (QKD) solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of quantum physics. The quantum cryptography relies on two important elements of quantum mechanics-the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning Theorem which was first presented by wootters and zurek in 1982 [1,2]. Extensive studies have been undertaken on QKD since it was noted that quantum computers could break public key cryptosystems based on number theory. Some research is in progress for the integration of QKD with the protocols in different layers of OSI model. The examples of such research effort are the integration of QKD in point-to-point protocol (PPP) OSI layer 2 and the integration of QKD with IPSEC at OSI layer-3. All these works are moving towards the utilization of QKD technology for enhancing the security of modern computing applications on the internet [3].

Quantum mechanics is a completely different science where in as Niels Bohr once said, "If you say that you understand quantum mechanics, then you don't understand it", or as John Wheeler said, "If you are not confused by quantum mechanics then you don't understand it".

The major difference [2] between other sciences and quantum mechanics is that:

- Uncertainty exists in all measurements of quantum mechanics and is a fundamental aspect of the quantum mechanical universe. In Newtonian physics one can find both position and speed of a car at the same time, but not in quantum mechanics where in the more accurately you measure one property, the less accurate becomes the value of the other related property.
- Observation impacts the outcome of the experiment. This is called the collapsing of the wave function. Unlike in the classical physics where no matter one observes an experiment or not, the result of the experiment remains the same. But in quantum mechanics there are no observers, all observers are participants here, and that is because mere observation of an experiment can lead to a completely different result.

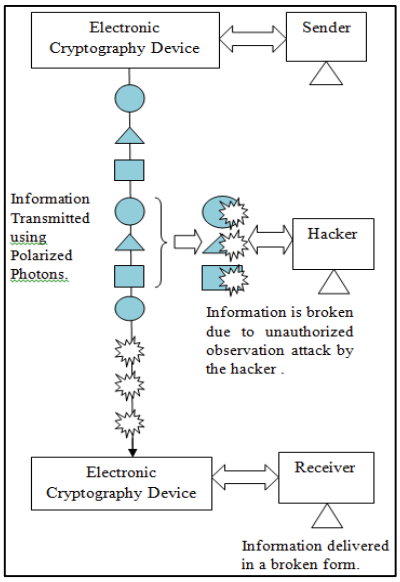

Fig. 1: Transmission of information using Polarized Photons.

The second aspect above is what will be used in Quantum Security. Mere observation of the data in transmission by a hacker will alter the data which can then be recognized by the recipient as a hacking attempt and the recipient can decide to abort the data transaction by informing the sender. The following fig.1 illustrates a network in which the sender is sending the information which is send to the receiver through the network using polarized photons. And this information is altered by the hacker due to observation attack of polarized photons. Hence the receiver will get the broken information and can discard the information or can stop the entire transmission.

Quantum Entanglement is the key here. This is a quantum mechanical feature where in if you have two entangled particles (say like very close twins), and if you observe one particle no matter how far it is from its entangled twin, the property of the observed particle will change due to observation and this would cause the entangled twin to change its property correspondingly. And this happens instantaneously, no matter how far the two particles are.

II. POLARIZATION OF PHOTONS

In quantum communication data is send through photons. Light waves are made up of millions of discrete quanta called Photons. They are mass less and have energy, momentum and angular momentum called spin. Spin carries the polarization. These photons are indivisible much like Atoms it just that they are units of lights. Photons can be polarized from 0^o to 360^o and intermediate spin positions like 45^o or 90^o can be detected using filters inclined to certain directions [4]. Photons can have a rectangular or a circular polarization. A physical device can observe rectangular or circular polarization but not both. Rectangular polarization can be horizontal noted "↔" or vertical noted "↕". Circular polarization can be left noted "↺" or right noted "↻". Moreover, if a physical device tries to measure circular polarization on a photon that is rectangular polarized, then it gets random results: either left or right, each with a probability of 50%. And the act of measurement changes the state of the photon. The situation is symmetric if a physical device measures rectangular polarization of a photon that is circularly polarized. Session keys are made of bits, 0 or 1. We agree that: bit 0 can be encoded either by an horizontal "↔" or a left "↺" polarization of a photon and bit 1 can be encoded either by a vertical "↕" or a right "↻" polarization of a photon. Such an encoded bit is called a quantum bit or qubit. Transmitting a key becomes transmitting a sequence of polarized photons. The system uses lasers to generate individual photons polarized in one of two modes: vertical / horizontal or diagonally 45^0 [6].

III. ELEMENTS OF QUANTUM THEORY

In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber – a thin fiber of glass used to carry light signals – to the receiver, where it is registered and transformed back into an electronic signal. These pulses typically contain millions of photons. In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. A single photon represents a very tiny amount of light [5]. Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms.

IV. QUANTUM COMMUNICATION

In this paper we have illustrated the aspects of quantum security through which the observation of the data in transmission by a hacker will be recognized by the recipient as a hacking attempt and the recipient can decide to abort or cancel the data transmission by informing the sender. In fig. 2 we have described the quantum communication concept that how the sender and receiver will communicate each other to ensure that the key is secure. In quantum communication first the sender will generate a random secret key and send it to the recipient over the public internet using entangled polarized photons. Any observation in between by an eaves dropper will alter the key value in transition and the value received by the recipient will not match with the value which the sender originally sent. This is because any observation causes the photons to get polarized in the state they were measured in and the original information is lost. So when the recipient sends back the secret key based on the received photons, the sender would observe that it is different from what it had actually sent to the recipient and so in this case the entire transaction would be aborted, and a new secret key will be generated by the sender and sent once again. Once the key received back by the sender matches the original value which the sender had sent to the recipient, the key is said to have been securely transmitted to the recipient and is then used to transmit the remaining data.

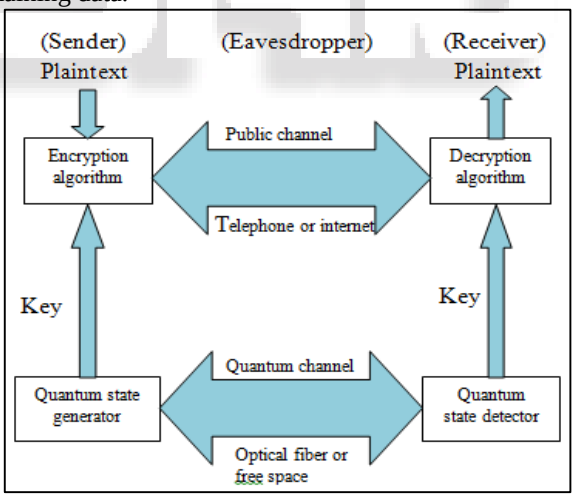

Fig. 2: Transmission of Secret key using Quantum cryptography.

So it is actually a two-step communication between the sender and the receiver:

1) Sender sends the encrypted key in the form of entangled polarized photons.
2) Recipients received the photons and measure the key value by measuring the polarization.
3) Recipient sends back the measured key value i.e. the polarization values.
4) Sender sends the basis on which each photon was polarized in.
5) Recipient sends the basis on which each photon's polarization was measured in.

6) Sender compares the values of only those photons for which both the sender and receiver used the same basis to create and measure the polarization. Any discrepancy in these values means there is a possible eaves dropping by a third party and in that case the transaction is aborted and is started afresh. Internet security today relies on the inability of today's computing machines to calculate and break the encryption key trying out all possible combinations. Where as in quantum security the principle used is that of detecting any attempt to read the security key being transferred and aborting all future data transfer in such case. Hence using quantum communication the secure key can be transmitted safely.

V. LIMITATIONS OF QUANTUM CRYPTOGRAPHY

In quantum cryptography data travels in the form of photons through optical channel or wireless channel, there is always a possibility of change in polarization in photon. In quantum cryptography optical channel is used to transmit the qbits (single photons). Exchanging information using single photon needs a dedicated channel of high quality in order to achieve high speed communication. It is impossible to send keys to two or more different locations using a quantum channel as multiplexing is against quantum's principles. Therefore it demands separate channels linking the source with the many destinations, which implies high cost [6,7]. This is a major disadvantage faced by quantum communication especially through optical channel.

VI. CONCLUSION

In this paper we find that quantum cryptography is a new technique of information security that provides a more reliable solution of the key distribution problem. The quantum cryptography is better solution of information security as compared to other traditional mathematical encryption decryption method due to secure key distribution, faster key refresh rate (than traditional approaches), truly random key generation, unconditional eavesdropping protection, proactive intrusion detection, lower total cost of ownership, future proof security, speedy set-up, with virtually zero maintenance. Thus Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. So by using quantum cryptography we can reduce the problems of secure key distribution (SKD) at a maximum possible extent.

REFERENCES

[1] Rishi Dutt Sharma "Quantum Cryptography: A New Approach to Information Security" International Journal of Power System Operation and Energy Management (IJPSOEM) Volume-1, Issue-1, 2011.
[2] P. M. Mathews and K. Venkatesan "A Text Book of Quantum Mechanics", Tata McGraw-Hill Publication, 37th Reprint 2007.
[3] Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi "Improving TLS Security by Quantum Cryptography" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010.
[4] T. Rubya, N. Prema Latha and B. Sangeetha "A Survey on Recent Security Trends using Quantum Cryptography" International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010.
[5] Alan Mink, Sheila Frankel and Ray Perlner "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration" International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009.
[6] Vibha Ojha, Anand Sharma, Vishal Goar and Prakriti Trivedi "Limitations of Practical Quantum Cryptography" International Journal of Computer Trends and Technology- March to April Issue 2011.
[7] D. Mayers, "Unconditional Security in Quantum Cryptography", Journal of the ACM, Vol. 48, No. 3, pp.351-406, May 2001.
[8] P. Shor, J. Priskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.
[9] http://en.wikipedia.org/wiki/Quantum cryptography
[10] http://ec.europa.eu/research/fp6/index_en. cfm? p=0

