ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
August 2015,
Vol. 8, No. (2):
Pgs. 103-109

Enabling New Generation Security Paradigm With Quantum Cryptography

T. VENKAT NARAYANA RAO[1], MAITHREYI SIMHACHALAM[2], SMITHA BANDYALA[2] and B. VASUNDARA DEVI[3]

[1]Computer Science and Engineering ,Sreenidhi Institute of Science & Technology, India.
[2]C.S.Engineering, Sreenidhi Institute of Science & Technology, India.
[3]Computer Science and Engineering ,Sreenidhi Institute of Science & Technology
Ghatkesar, T.S, India.

(Received: June 10, 2015; Accepted: August 15, 2015)

ABSTRACT

Quantum cryptography is a technology that ensures the security. Quantum cryptography ensures secure communication based on the fundamental physical laws. The quantum cryptography is based on the two elements of quantum mechanics -the Heisenberg Uncertainty principle and the principle of photon polarization. This paper focuses on the principle of quantum cryptography, mechanism how photons are encrypted and its contribution towards real-time security in all domains of application development.

Key words: Quantum cryptography, Quantum key distribution (QKD), Polarization, Heisenberg Uncertainty principle, Secure communication.

INTRODUCTION

In our modern age of telecommunications and the Internet, information has become a precious commodity. There are many features and applications to secure the data, commerce and payments to private communications and protecting passwords. The essential feature for secure communications is that of cryptography, which not only protects data from stealing or modification, but it can also be used for user authentication. The main aim of cryptography is to protect data which transferred in the presence of an enemy. A cryptographic transformation of data is a procedure in which the plaintext is encrypted resulting in a text, called cipher text. The cipher text can be decrypted by a designated recipient so that the original plaintext can be recaptured. The techniques of cryptography are usually categorized as traditional or modern. Traditional techniques use operations of coding using alternative words or phrases, substitution using alteration of plaintext characters. Whereas the modern techniques uses computers and depends upon extremely long keys, complicated algorithms, and intractable problems to assure the security. [1] [4][5]

The main areas of modern cryptographic Methods are Public key encryption and Secret key Encryption. Within public-key encryption, the message is encrypted with a recipient's public-key and the message can be decrypted only by the one who possesses the matching private key. A secret key is an encryption key known only to the authenticated parties (who exchanges secret messages). The risk in the secret key encryption is that if either party loses the key or it is stolen, then the system is broken.

Classical Cryptography and Key Distribution problem

Classical Cryptography is based on encrypting the plain text to be send by the source using some mathematical formula and sending it over a insecure channel to the sink where it is decrypted by reverse mathematical operation. The algorithm used for encryption is called Cipher and hence the data send over the network is called cipher text. Classic cryptographic systems are mainly based on NP-hardness of mathematical problems, called trapdoor functions as it is easy to compute the function in a way but not so easy to compute the reverse. The two main categories of cryptography are asymmetric and symmetric cryptography. Symmetric cryptography uses a single key for both encrypting and decrypting the data, whereas the asymmetric cryptography uses both a public and private key where either of them can be used for encryption and decryption.[2]

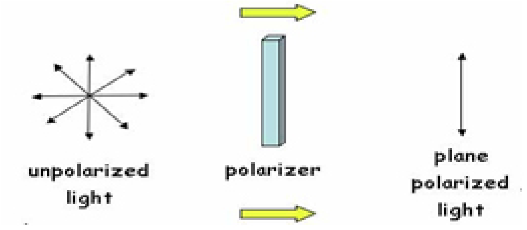

Fig. 1.1: Polarization of Light

Key Distribution Problem

Classical Cryptography suffers from Key Distribution problem i.e. how to secure the key between the parties. Earlier the only possibility way to solve the key distribution problem was to send by some physical means – a disk for containing the key. Later, this requirement is clearly unpractical and also it is so easy to check whether the medium was intercepted and its content copied – or not. As a solution to this the Public key cryptography came into existence, but they are too slow and cannot encrypt the large amount of data. Therefore to overcome the key distribution problem Quantum Cryptography is used which solves this by theory of Quantum Physics.

Quantum Cryptography

The field of cryptography has been raised from non classical atomic theory, Quantum Physics. This field is called Quantum cryptography. The classic cryptography of public and private key ciphers analyzes the strength of a cipher by means

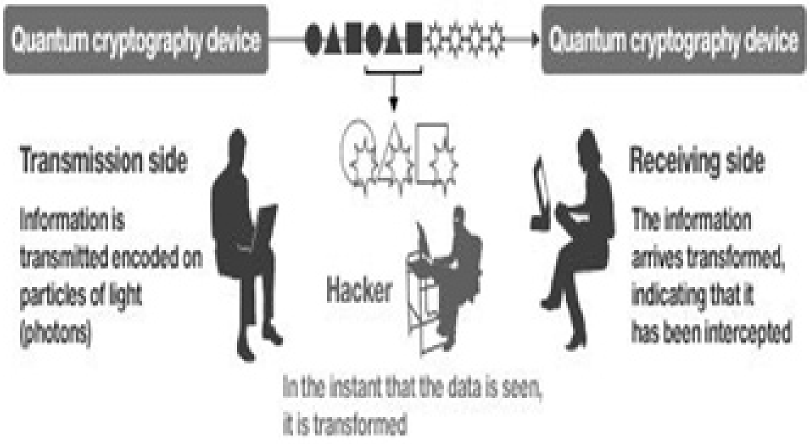
Quantum cryptography device
Quantum cryptography device
Transmission side
Information is transmitted encoded on particles of light (photons)
Hacker
In the instant that the data is seen, it is transformed
Receiving side
The information arrives transformed, indicating that it has been intercepted

Fig. 3.1: Mechanics of Quantum Cryptography

of mathematical attacks and formulas, whereas the quantum cryptography security is ensured by law of Quantum Physics.

Heisenberg Uncertainty Principle

According to Heisenberg Uncertainty Principle, the two properties which are interrelated cannot be measured individually without disturbing the remaining system. The principle tells that the photons cannot be partitioned into halves, measuring the state of photons will affect it significance. If someone attempts to detect the photon state being sent to the receiver, the error can be detected. [3][8]

Elements of Quantum Theory

Light waves are made up of millions of discrete quanta known as Photons which are mass less and have energy, momentum and angular momentum called spin. These photons are indivisible similar to Atoms, since they are units of lights. Spin carries the polarization. Photons can polarize from 0æ% to 360æ% and the position of intermediate spin (45æ% or 90æ%) inclined to certain directions can be detected using filters.

In fig 1.1, the light rays from a bulb passes through a polarization filter called polarizer (inclined to 90æ%) so as to get a vertical ray of light, if another filter is used then the inclination of the light ray will be different, as rays rotate again. If the rays are at the orthogonal angle to the filter then there will be no output. Quantum Cryptography uses LEDs (light emitting diodes) to create a photon. The source of unpolarized light LEDs are efficient to create one photon at a time. By using the polarization filters, the photon can be change from one state to another or polarize it. A vertical polarizing filter situated, can polarize the photons that emerge, which are not absorbed will emerge a vertical spin (|) on the other side. The advantage is that once the light passes through second filter (after first filter) then the orientation of the light rays can't be determined so that the channel privacy is maintained.

Table. 1: Typical Polarization state pairs

Basis	Representation	Bit 0	Bit 1
Rectilinear	+	↑	→
Diagonal	×	↗	↘

Quantum Communication

In telecommunication networks, light is used to exchange information. Each bit of information emits a pulse which sent through an optical fiber (which is used to carry light signals) to the receiver side, where it is recorded and transformed back into an electronic signal. Each pulse usually contains millions of photons. In quantum cryptography, same approach can be followed with the difference is that the pulses contain only a single photon, represents a minute amount of light. In Quantum cryptography photons are used for key transmission. Once the key is transmitted, encoding and decoding is done using the normal secret-key method.

The photons are converted to key using the binary code. Each photon's spin type represents a piece of information, usually 1 or 0. The code uses the string of 1s and 0s to create a consistent message. For instance, 111010010 could correspond with h-e-l-0. So that binary code can be allocated to each photon. Quantum cryptography resolves the key distribution problem by letting the cryptographic key exchange between the remote parties with absolute security. Quantum Communication is based on following features of Quantum mechanisms and photons:

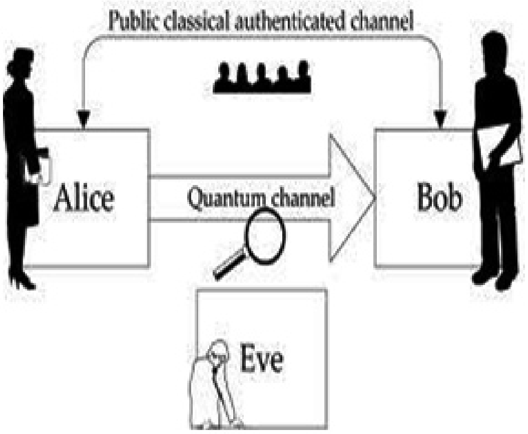

Fig. 4.1: Quantum key distribution comprises a quantum channel and a public classical authenticated channel.

- Heisenberg principle
- An entangled based protocol that means two entities can be defined such that their properties are interrelated i.e. altering one will affect the significance of other. If an entangled object (key) is shared between the parties then it maintains integrity of the keys.

Literature review

Quantum cryptography was first recommended by Stephen Weisner, in early 1970s and the plan was issued in 1983 in Sigact News, at the same time two scientists Bennet and Brassard, 1984, delivered the first quantum cryptography protocol called the “BB84.” The protocol is provably secure, depending on the quantum. The first experimental prototype was made in 1991, functioned over a distance of 32 centimeters. Shortly in June 2004, the first secured communication with quantum cryptography in computer network is settled up and running in Cambridge, Massachusetts. The quantum engineering team leader at BBN Technologies in Cambridge, Chip Elliott, transmitted the first packets of data across the Quantum Net. In April 2004, the first money transfer occurred between two Austrian banks, was encrypted by quantum key. The was buildings were 500 meters always from each other, yet fiber optics was fed throughout 1.5 kilometers of sewage system to connect them.[1][7]

Mechanics of Quantum Cryptography

The quantum cryptography depends on the quantum mechanics components – the Heisenberg Uncertainty principle and the principle of photon polarization as shown in figure 3.1. The Heisenberg Uncertainty principle states that, it is not possible to determine the quantum state of any system without disturbing the system. The theory of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem.

In general physics, the no-cloning theorem states that it is not possible to create an identical copy of a random unidentified quantum state. In 1982 Wootters and Zurekand Dieks articulated this theorem of quantum mechanics and have great implications in quantum computing.

Depending on the theory of physics, quantum cryptography does not make it possible to eavesdrop on transmitted information. Quantum cryptographic transmission encrypts the 0s and 1s of digital signal on individual particles of light known as photons. The modern optical transmission states that the digital signal (0’s and 1’s)represents strength and weakness of light as they are made up of tens of thousands of photons in which each express the same information. Even if the signal is eavesdropped (i.e., several photons are stolen) during transmission, it is not detected. On the other hand, if any third party detects the signal, then the information on the photons is suddenly transformed, meaning that it is immediately noticeable that Eve has appeared and the third party is not able to decrypt the information.

Consider, Alice sends the photons to Bob using an LED by polarizing them randomly through either the X or the + filters thus each polarized photon has one of the following possible states: **(l), (—), (/)** or **( )**. On the other hand Bob, who has no idea about what filter(s) to use, receives these photons and decides whether to calculate each with either his + or X filter, bob will deduce filters for each one. Alice and Bob will have a non-encrypted discussion after entire transmission has occured. The conversation can be public. Bob calls Alice and tells the filter he used for each photon, and Alice tells him whether it was the correct or incorrect filter to use. The conversation may be little like this[8]:

- Bob: Plus Alice: Correct
- Bob: Plus Alice: Incorrect
- Bob: X Alice: Correct

Since Bob saying only the type of filters used but not the measurements, if a third party listens their conversation, can’t determine the real string of photon. For an instance, Alice sent one photon as a (/) to Bob. Through a public (may be telephonic) conversation, Bob says he used a + filter to measure it. Alice will say “incorrect” to Bob. But if Bob says he used an X filter to measure the exact photon, Alice will say “correct.” A person or an eve listening to this conversation will only know that the particular photon could be either a (/) or a ( ), but not exact. Bob will know that the measurements are correct, because a (—) photon travelling through a + filter will remain polarized as a (—) photon.

After their conversation, Alice and Bob will delete the Bob's incorrect guess which results in identical strings of polarized photons. It may be like meaningless string of photons (like: — / | | / — — | |//—|| and so on). But once the binary code is decoded, the photons turn into a message. Alice and Bob can agree on binary assignments, 1 for photons polarized as ( ) or (—) and 0 for photons polarized like (/) or (|). Now, the string of photons may look like: 111000001111000101, which can in turn be translated into English, prime numbers or to anything that the Bob and Alice use as codes for the keys used in their encryption. Eve (E) can **passively intercept the** encrypted text and tries to decode it without letting Bob and Alice to know. Eve does this in different ways, such as by wiretapping Bob's or Alice's phone or by reading their e-mails. Quantum cryptology is the first and foremost technique that safeguards against passive interception. Since the photos can't be estimated without affecting its behavior. When Eve makes her own eavesdrop measurement, Heisenberg's Uncertainty Principle is emerged.

For instance, consider Alice sends a series of polarized photons to Bob, and Eve will set up a filter of her own to intercept the photons, in the same boat as Bob who has no idea what the polarizations of the photons Alice sent are. Like Bob, Eve can only guess the filter orientation (X filter or a + filter) used to measure the photons but not exact one. After Eve has measured the photons by randomly selecting filters to determine the spin, and pass them down the line to Bob using a LED with a filter set to the alignment, chose to measure the unique photon. Eve does this to pretend her absence and to hide her activities. But implementing the Heisenberg Uncertainty Principle, Eve's presence can be detected.

Say Alice sent one photon polarized to a (—) spin to Bob, and Eve interrupts the photon. But Eve has mistakenly chosen to use an X filter to measure the photon. If Bob randomly (and correctly) chooses a + filter to measure the original photon and finds it's polarize in either a (/) or ( ) position. Bob will ensure the filters only after communicating with Alice, till then he believes that he has chosen an incorrect filter. After acknowledging all the photons, Bob will communicate with Alice about the filters used to resolve the polarizations. If Eve intercepts the message then it results in inconsistency. In the example of the (—) photon that Alice sent, Bob will inform that he used a + filter. Alice will let him know that it is correct, but Bob will recognize that the photon he received did not match to original ((—) or (|)). Due to this difference, Bob and Alice will know that their photon has been changed by Eve, who involuntarily changed it. The polarization state pairs are shown in table I.

Alice and Bob can guard their transmission by discussing some of the correct results after they've thrown out the incorrect or wrong measurements. This is called a parity check. The message is said to be secure if the Bob's measurements are all correct (i.e., the pairs of Alice's transmitted photons and Bob's acknowledged photons all match up).
Bob and Alice can then delete the unwanted measurements and can use the left over secret measurements as the required key. If discrepancies are found, should arise in 50% of the parity checks. Bob and Alice can reduce the possibility that Eve has the remaining correct information down to a one-in-a-million chance by conducting 20 parity checks.

Advantages of Quantum Cryptography

In order to ensure that no unauthorized party misuses the content, classified message needs encryption. Long-term security is provided by Quantum cryptography and thus matches to the requirements of a number of modern legal regulations for protecting information. Quantum cryptographic technologies provide information to secure keys for encryption. The fundamental approach includes sending flow of specially organized photons, their measurement by the rightful parties and its following post-processing of the measurement data and results the cryptographic key consisting of identical random bit strings. An eavesdropper cannot gain any information on the key irrespective of the resources. Because of fundamental laws of quantum physics this property, has no traditional counterpart which makes sure that any measurement leaves ineradicable traces after. These trace evident themselves in an error-rate that can be identified by the genuine user.

Application of quantum cryptography

The most well-known and developed application of quantum cryptography is quantum key distribution (QKD) as shown in figure 4.1 . Quantum key distribution is a method used in the framework of quantum cryptography in order to generate a perfectly random key which will be shared by a sender and while receiver ensures that nobody else has a chance to gain knowledge of the key. The best known and popular method of quantum key distribution is based on the Bennet–Brassard protocol (i.e. BB84), which was invented in 1984. It depends on the no-cloning theorem, for non-orthogonal quantum states. In brief, the Bennet–Brassard protocol works as follows [3]:

- The Alice (sender) sends out a sequence of single photons. For each photon, it arbitrarily selects one of two possible base states, one having the likely polarization directions up/down and left/right, and the other one polarization directions which are angled by 45°. In every case, the definite polarization direction is also arbitrarily selected.
- The Bob (receiver) detects the polarizations of the arriving photons and also arbitrarily selects the base states. This means that on an average half of the photons will be determined with the “wrong” base states.
- Later, Alice and Bob discuss about the states used for each photon through a public channel and then all the photons with wrong origin will be rejected.

Some examples of current and near-future applications of quantum cryptography:

Ultra secure voting

With political disorder and charges of voter fraud raging in developed and developing countries alike, it was clear that building much secure voting process is inevitability. Switzerland has started using quantum cryptography from 2007 to conduct secure online voting in national and local elections. In Geneva, votes are encrypted at a central vote-counting station. Following results are transmitted to a remote data storage space facility over a dedicated optical fiber line. Results are secured through quantum cryptography, and the most vulnerable part of the data transaction is uninterruptible. This technology will soon spread worldwide since many other countries face the same specter of fraudulent elections.

Secure communication with Space

Secure interactions with satellites and astronauts is a growing concern, and a company called Quintessence Labs is working on a project for NASA will ensure secure communication with satellites and astronauts from Earth. The objective of the project is to accomplish a procedure which guarantees the safety of communications despite of the intellect or technology to which an opponent has right of access. It as well includes a permission to secure both the information “at rest” and in transit. This would eventually add to the safety of astronauts in space and perfectly preclude the needs improvement in the future beyond negligible speed increases.

Smart Power Grid

There were many rumors that the American power grid is one of the weakest targets for a virtual attack. Some major U.S. utilities are under constant attack by cyber enemies. QKarD (A small encryption device) was developed to put an end to those cyber attacks. Using the QKarD, workers were able to send absolutely secure signals using public data networks to manage smart electricity grids. Smart grids are vital for balancing supply and demand meant for efficiency. Additionally, they are considerably more secure than conventional grids, with proper protection in place [2].

Quantum Internet

With the grace of present internet technology, every transaction is made within seconds, but its security is insignificant compared to quantum-encrypted transmissions. If the quantum encryption is made available to everyone then it will result in slowing down the internet. However, in future it’s possible that one could switch seamlessly between “regular” and “quantum encrypted” internet, with the intention that the most susceptible transmissions would be passed along in a very-secure manner.

With the ascend of Facebook and other social groups, the earlier decade has been one of uncontrolled and unchecked sharing. In the coming years it may possible to see a much greater focus on concerns related to security, privacy and individual protection e.g. accessing using fingerprints, biological identification and biometrics.

CONCLUSION

We presented a review on working of quantum cryptography and quantum key distribution technology. This technology basically depends upon the polarization of photons, which cannot be regulated over long distances and in multi-channel networks. Quantum cryptography could be the first consideration of quantum mechanics at single quanta level. As a substitute for current state of mathematical algorithms which used in computing technology for provided security, quantum cryptography promises to give secure communication channel based on the laws of physics. Hence, for implementing this devices are to be developed and much more advancement is foreseen with low cost implementation with performance.

REFERENCES

1. Miss. Payal P.Kilor, Mr.Pravin. D.Soni, “Cryptography: Realizing next generation information security”, *IJAIEM,* **3**(2): (2014).
2. Quantum Cryptography using Quantum Key Distribution and its Applications, N.Sasirekha, M.Hemalatha, *International Journal of Engineering and Advanced Technology (IJEAT),* ISSN: 2249 –8958, **3**(4) (2014).
3. https://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf.
4. A Survey of the Prominent Quantum Key Distribution Protocols, Mart Haitjema, http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#security.
5. http://cdn.intechopen.com/pdfs-wm/43793.pdf
6. Quantum Cryptography: A New Approach to Information Security, *International Journal of Power System Operation and Energy Management (IJPSOEM),* **1**(1): (2011).
7. Brief History of Quantum Cryptography: A Personal Perspective Gilles Brassard University de Montreal Department information C.P. 6128H3C 3J7 Canada http://www.iro.umontreal.ca/~brassard 17 October 2005.
8. How quantum cryptology works http://science.howstuffworks.com/science-vs-myth/everyday-myths/quantum-cryptology4.htm