International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Analysis of Cryptography: Classical verses Quantum Cryptography

Pooja Anil Patil[1], Renuka Boda[2]

[1,2] *Student, Dept. Of MCA, Bharati Vidyapeeth's Institute of Management and Information Technology, India*

Abstract - *Now a day's security is important aspects to secure the data during the transmission of data from sender to receiver over a network. This transmission can be done through the different tools. Now a day's, our sensitive and personal data or information stored in computers, on cloud or on some private storage. So that it's need to be protect these data from unauthorized user or from malicious attack. Therefore here we focused on the cryptography concept which helps to protect our information from being stolen or intercepted by third parties. For securing data unconditionally during communication, Quantum cryptography can be used. This is important concept for practical purpose to secure sensitive data which is under development. Currently classical cryptography used which relies on the solely on the hardness of mathematical equations. Thus this paper compares classical cryptography to quantum cryptography and its major problems, its limitations of quantum and classical cryptography.*

Key Words: **QC, CC, Photon, Communication, polarization, BB84, BB92.**

1. INTRODUCTION

Cryptography is techniques for securing communication in the presence of third parties, unauthorized user or some malicious attack. Generally, it is about constructing and analysing protocols that overcome the pressure of attackers and they are related to various aspects of information data security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography bisects the disciplines of computer science, and electrical engineering, mathematics. Modern cryptography techniques classified into two techniques as public key encryption and secret key encryption.

In Public Key Cryptography, messages are transmitted or exchanged using the encryption techniques. So convoluted that even full acknowledgment of the climbing operation provides no useful information for how it can be undone. Each user has two type of key as public key and private key; the former is used by others to encrypt messages, and the latter is used by the receiver to decrypt them.

Modern cryptosystem is a Quantum Cryptography which helps to makes the key unconditionally secure with quantum. Quantum Cryptography is composed of two words as Quantum and Cryptography. Quantum is the smallest discrete quantity part of some physical property that a system can possess and then Cryptography enables to store sensitive information or exchanged it across insecure networks so that it cannot be read by anyone like attackers, intruders etc. except the intended recipient.

For cryptographic task, Quantum Cryptography uses the quantum. Quantum Cryptography is based upon conventional cryptographic methods which extends these through the use of quantum effects. In Quantum Cryptography, Quantum Key Distribution (QKD) is used for generating a secret key shared between two parties using two channels as a quantum channel and an authenticated classical channel. The private keys obtained and then encrypt messages that are sent over an insecure classical channel using that obtained private key.

2. LITERATURE REVIEW

There are different research papers which were developed for quantum cryptography, classical cryptography or comparison of both.

In this chapter, a broad description of literature is presented. Starting with the paper [6] presented that how advantages of classical cryptography which protect our data against hackers.

Then come to the paper of [1]. They presented different protocols of quantum cryptography which helps to overcome the limitation of classical cryptography.

Then come to next paper as [3] by N.Sasirekha, M.Hemalatha. They represented that how to generate key using quantum cryptography which is more secure and where they implemented. They represent quantum cryptography in south region telecommunication and how to overcome the future predicted cyber crimes.

3. METHODOLOGY

Mainly Cryptography can be classified as Quantum Cryptography (QC) and Classical Cryptography (CC). These are given below.

3.1 CLASSICAL CRYPTOGRAPHY AND THEIR TECHNIQUES

Classical Cryptography is the process of transforming message as a plain text or original information into a cipher text (encrypted format) which are not easily readable and understandable. So that it may be travel over unsafe channels or communications. The message transformation process is controlled by a data string (key). So that anyone getting cipher text while it is on unsafe channel would need to have appropriate key which is set during transformation process. Using this key, receiver will be able to get the original information and the authorized receiver is assumed to have that key. Classical Cryptography comes with two main techniques:

A) Asymmetric Cryptography:

Asymmetric cryptography uses key pair to secure the data. The existing problem of key distribution is solved using asymmetric cryptography. It uses a pair of keys for encryption as public key to encrypt the data and corresponding private key decrypt the data. Your public key published to the world and keep private key as secret.

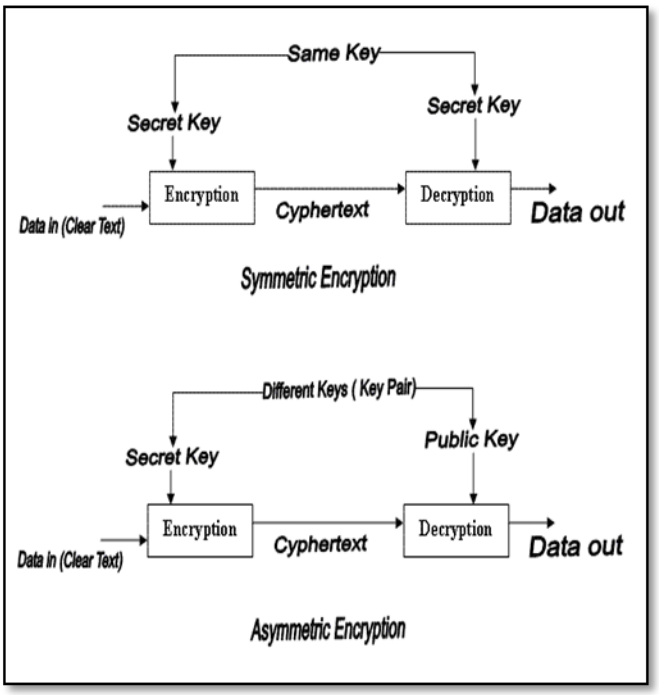

Fig -1: Symmetric and Asymmetric Cryptography

B) Symmetric Cryptography:

In symmetric cryptography, encryption and decryption process can be performed using only one single key. In symmetric cryptography, plain text is encrypted and decrypted using same key which is private key. The main limitation of symmetric cryptography has private key distribution among sender and receiver. Classical cryptography techniques are subject to a number of disadvantages so that quantum cryptography is done.

3.2 QUANTUM CRYPTOGRAPHY AND THEIR PROTOCOLS

Quantum Cryptography is a cryptography which allows storing sensitive data or transmitting it across insecure network channels so that it cannot be read by anyone except the particular or targeted recipient. So, Quantum is used for doing cryptographic tasks. Quantum Cryptography is almost based on classical cryptographic methods and extends these using quantum effects. Quantum Key Distribution (QKD) is used for generating a secret (private) key shared between sender and receiver using both channel .The private key obtained and then these key is used to encrypt messages that are sent over an insecure classical channel

Using this principle, QC provides unconditional security to protect our data. A unit of quantum information is also called as qubit or quantum bit. A qubit can have values 0 or 1 which can retain superposition state of these two bits. Using Quantum cryptography, secret key is obtained, and then it can be used with classical cryptographic techniques as the one- time-pad to allow the parties to interact. In Quantum Key Distribution, we consider two peoples as Alice and bob which obtains some quantum states and measures them.

A QKD system contains two channels such as a quantum channel which is only used to transmit single photon transparent optical path and a classical channel which is channel can be a conventional IP channel. The key can be generated by communicating through quantum channels and then they communicate through classical channels to determine their measurements results leads to secret key bit. QKD systems continually generate new private keys that share automatically on both sides.

The private key may be changed for every second continuously. Thus a compromised key in system can only decrypted a smallest amount of encoded information. Creating a secret-key from stream of single photon, each photon is encoded with a bit value of 0 or 1,and by a photon in some superposition state, such as polarization and then these photons are emitted by a conventional laser as pulses of light so that most pulses do not emit a photon. Using this way, communication has the ability to create true random secret key, which suitable keys can be generated using conventional cryptographic methods.

A classical Cryptography that makes use of these keys. Then these key can be used for communication. A classical cryptography used once then the keys have

been exchanged. This means that possibility of unbreakable Cryptography.

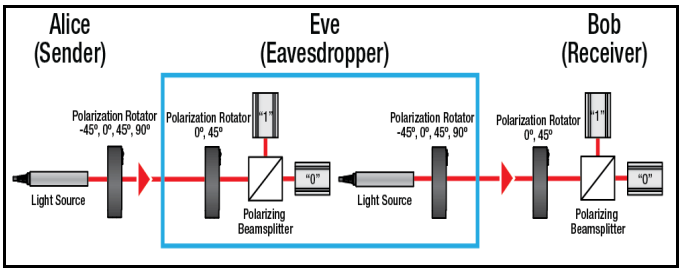

Fig -2: Quantum Cryptography Principle Process

A quantum (cryptographic) protocol could be a data communications procedure that use quantum development is designed to make sure secure communications. Quantum protocols like BB84 were originally developed for the exchange of cryptographic keys solely. There are 3 main quantum cryptography protocols projected thus they are as follows:

A) BB84 Protocol:

BB84 is a first quantum cryptography protocol. The protocol is possibly secure, building on the quantum property that information gain is barely potential at the expense of troubling the signal once the two states, we tend to try to tell apart don't seem to be orthogonal . It's expressed as a technique of firmly human activity a non-public key from one user to a different to be used in one-time pad coding.

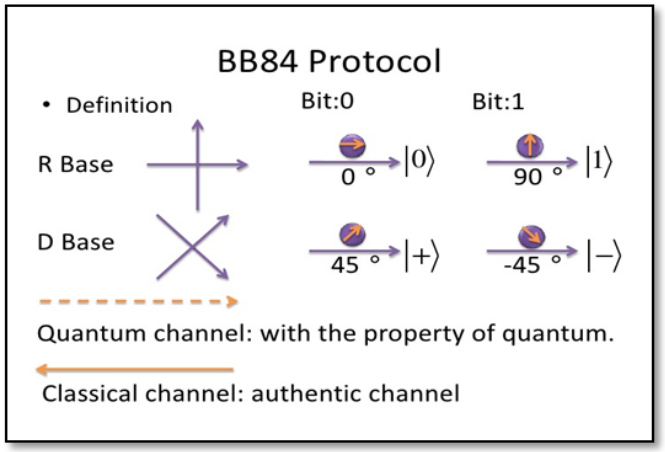

Fig -3: BB84 Protocol

B) BB92 Protocol:

After BB84 protocol was revealed, it seems those single non orthogonal bases are often used instead, while without affecting the security of the protocol against eavesdropping. This idea is employed within the BB92 protocol, which is otherwise similar to BB84. The key change in B92 is that only two states are necessary instead of the attainable four polarization states in BB84.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Fig -3: Quantum Transmission and process

Fig -4: Quantum Bases

Above figure 3 and figure 4 shows, zero will be encoded as zero degrees within the rectilinearly basis and one will be encoded by 45 degrees in the diagonal bases. Alice transmits to Bob a string of photons encoded with randomly chosen bits however this time the bits Alice chooses dictates which bases she should be use. Bob still randomly chooses a basis by which count if he chooses the incorrect basis, he can measure nothing; a condition in quantum machines that is referred to as erasure. Bob will merely tell Alice when every bit she sends whether or not measured it properly.

4. COMPARISON OF CLASSICAL AND QUANTUM CRYPTOGRAPHY

Classical Cryptography has many points of strength: it's independent of the transmission medium. Since the transmission distance does not admit the rule, the Classical Cryptography is ready to administer secure communication over variant kilometers. Additionally, Classical Cryptography is easy in the sense that the algorithms may be implemented in software, hardware or a hybrid of both. Most significantly, Classical Cryptography doesn't need special specifications concerning the courier; thus Classical Cryptography isn't thought-about pricey. On the other hand, the most three important drawbacks of the Classical Cryptography exist. First, the existence of some loopholes within the algorithm: these may also exploited by the hackers to interrupt the system's security. The algorithmic rule short anticipation is additionally a serious downside in Classical Cryptography. Therefore, it's necessary to extend the key size so as to increase the life time. Finally, Classical Cryptography algorithms require higher quantity of computation to be effective.

On the opposite hand, Quantum Cryptography suffers from several points of weaknesses. When transmitting the data,

the photon might change its polarization. This may happen as results of non-homologous transmission media or the intentional interruption of a hacker. Algorithms don't seem to be simply implemented in Quantum Cryptography. Sensational style necessities of the photons emitter too sensitive to be met. Quantum Cryptography isn't appropriate for long distances. The technique is at risk of hacking by time-shift attack. The possibility to generate excellent copies of an unknown quantum state by victimization stirred emission or bunching properties of light. It is much unsuitable to multiplex in a quantum channel; thus, every single photon required a dedicated channel of high quality that makes it terribly costly.

First, the optical devices that take care of photons are expensive. Second, the quality of mistreatment the system since the user ought to have a background regarding physics. Third, the dearth of security standards for the equipment; users ought to be assured that it's been enforced in a secure QKD by sellers. Finally, QKD is sensible just for short transmission distances: this can be truly main obstacle against spreading this technology wide. In short, there are several problems referring to Quantum Cryptography that the laws of physics cannot beware of. Therefore, there's still a protracted manner off before excluding the CC and looking forward to Quantum Cryptography within the world of knowledge security.

Both quantum cryptography and classical cryptography can be compared on following dimensions:

1. Technological dimensions:

Quantum communication transmission effectively enlarges the communication distance to 10 miles. But classical cryptography can be used to communication distance of several million miles. The new record is bit rate for quantum key distribution, that is, 1 Mbit/s on average and bit rate of classical cryptography depends on the computational power largely.

2. Economic dimensions:

Quantum Cryptography is only suitable for point-to-point connections. The system is very expensive and requires a lot of work. On other hand classical cryptography can be implemented in software and its cost for consumer is almost zero. But this is major issue in case of quantum cryptography shrinkage to such a level requires too much development.

3. Application dimensions:

The digital signatures reveal the authenticity of the digital data to the receiver. A digital signature assures recipient and it was not changed in transit. The three main algorithms are key generation, signing, and key verification. But in Quantum Cryptography, algorithms cannot be implemented very easily.

4. Fundamental dimension:

In theory, any classical private channels can be easily, monitored inertly without the knowledge to sender or receiver that the eavesdropping has been done.

5. Other dimensions:

Communication medium is not an issue in classical cryptography and communication of quantum cryptography require a quantum channel like optical fiber or through air. Also, there is constantly a modification in polarization of photon due to Birefringence effect or rough paths that cause change in refractive index due to damage sometimes. Also, an n bit classical register can store at any moment exactly one n- bit string.

Quantum Cryptography Real life Application:

The first Quantum Key Distribution (QKD) system in a real world application –vote counting in Geneva federal elections in 2007 was deployed by ID Quantique Company. There are 3 business units of ID Quantique: quantum safe security, random number generators, and scientific instrumentation.

3. RESULT

This research paper gives the idea about, if sender sends data to the receiver through single one by one photons to receiver. But during transmission of data, some attackers are trying to hack information. If only single photon changes during the hacking, on that time receiver comes to know about eavesdropper through the modified photon. This process is shown in below Fig 5.

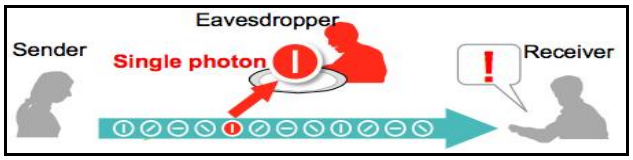

Fig -5: Loss of photon during QC

So during this paper study, we tend to found some contras points within the literature. We tend to list these encountered conflicts. One of the most points of strength of QC is that the no-clone theory, which implies the impossibility of repeating the polarization states. However, it's potential to repeat photons using amplified single-photon inputs. They consequently update the 4-way shake protocol into what they referred to as Quantum shake protocol.

On the opposite hand, we've to spotlight that in theory speaking, QC is taken into account associate completely secure method of communication. However, the employment of imperfect devices could produce security loopholes. Therefore, this could be taken into thought once planning a secure communication. Obviously, Quantum Cryptography may be a worthy technique. From our purpose of read, it'd be a lot of helpful if we tend to thought of a mixture of each

approaches: Classical Cryptography and Quantum Cryptography.

6. CONCLUSIONS

In this research paper we concluded that transmission of sensitive data from one or more senders/receivers, some stronger technique is needed. So it is our opinion that its fix that quantum cryptography and their methods are better than the classical cryptography for secure data transmission. Quantum cryptography is a powerful tool to secure information in future in which we can feel more secure.

So that we say that best technique for securing information is Quantum cryptography. But if we use both Quantum Cryptography and Classical Cryptography combine then it gives more secure result during protecting the data. But there is some limitation of the quantum cryptography which needs to be overcome in future. Based on our study and findings so far, it is our opinion that quantum cryptography is one of the best techniques to secure sensitive information but if we use quantum cryptography with classical cryptography then its gives more effective result which helps to protect the sensitive information.

REFERENCES

[1] Key Distillation Process on Quantum Cryptography Protocols in Network Security M. Indra Sena Reddy, K.Subba Reddy, M. Purushotham Reddy, P.J. Bhat, Volume 2, Issue 6, June 2012 ISSN: 2277 128X

[2] A SURVEY OF QUANTUM AND CLASSICAL CRYPTOGRAPHY Derrick Chait, Texas A&M University-Corpus Christi Faculty Advisor: Ahmed Mahdy, Texas A&M University-Corpus Christi

[3] Quantum Cryptography using Quantum Key Distribution and its Applications N.Sasirekha, M.Hemalatha (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014

[4] P Article M Agic : Need For Quantum Cryptography Research in the south Asian Region Dhishan Dhammearatchi Vol. 6, No. 5, September 2015

[5] Quantum Cryptography and Its Applications over the Internet Chi-Yuan Chen, Guo-Jyun Zeng, Fang-Jhu Lin, Yao-Hsin Chou, and Han-Chieh Chao

[6] Advantages of Classical Cryptography Over the Quantum Cryptography Vibha Ojha Anand Sharma S. K. Lenka S. R. Biradar Vol (2), Issue (5), May 2012. 25