IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

# A Preliminary Study about an emerging approach in Cryptography: Quantum Cryptography

Poornachander V
Research Scholar, Department of Computer Science
Osmania University, Hyderabad

***Abstract* - The word cryptography is the artwork of mystery writing. Generally, humans consider cryptography because the art of mangling data into obvious unintelligibility in a way permitting a secret technique of untangling. The fundamental provider supplied by cryptography is the potential to send data among members in a manner that others can't read in a right format. Here we will give attention to the sort of cryptography this is based on representing information as numbers and mathematically manipulating those numbers. And we have various encryption techniques to send data in a cryptographic manner. Here we have an emerging technology for this new era called Quantum cryptography. The first-rate and famous instance of quantum cryptography is the quantum key distribution which gives an information-theoretically comfy method to the important thing change trouble. Presently used famous public-key encryption and signature schemes may be damaged by using quantum adversaries. The benefit of quantum cryptography lies in the truth that it permits the completion of diverse cryptographic responsibilities which can be established or conjectured to be not possible the usage of simplest classical (i.e. non-quantum) verbal exchange. This paper deals with the detailed technology about Quantum Cryptography.**

**Index Terms: Cryptography, Encryption, Decryption, Quantum Cryptography.**

## 1. INTRODUCTION

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data.
Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in non-repudiation. This means that neither the creator nor the receiver of the information may claim they did not create or receive it.

Cryptography is also known as cryptology. Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include:

- Secret Key Cryptography (SKC) - Here only one key is used for both encryption and decryption. This type of encryption is also referred to as symmetric encryption.
- Public Key Cryptography (PKC): Here two keys are used. This type of encryption is also called asymmetric encryption. One key is the public key and anyone can have access to it. The other key is the private key, and only the owner can access it. The sender encrypts the information using the receiver's public key. The receiver decrypts the message using his/her private key. For non-repudiation, the sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows who sent it.
- Hash Functions: These are different from SKC and PKC. They have no key at all and are also called one-way encryption. Hash functions are mainly used to ensure that a file has remained unchanged.

***Applications:*** To Protect Privacy, Confidentiality, Insuring data Integrity (Detecting and Preventing Unauthorized data manipulations), Authentication (The means by which two parties can positively identify each other), Non- Repudiation (To hold people responsible for their actions).

***Steps involved in Cryptography Process:***

1. Plain text- The Original message.
2. Cipher Text- The disguised message
3. Key - A set of Parameters supplied to encryption and decryption algorithm.
4. Encryption – Using a key to change plain text in to cipher text
5. Decryption – Using a key to change cipher text back into something readable.

And the most straightforward example is to be found using the simple mono-alphabetic substitution cipher method, in which each letter in the alphabet is shifted by an integer value. The key supplied to this algorithm would be that integer value. One of the most common modes of modern encryption uses a protocol commonly known as PGP. This stands for "Pretty Good Privacy", and uses a system of two keys, therefore bypassing the key distribution problem. The public key is a one-way algorithm for encrypting data. Each user has a public key and a private key.

Once information has been converted to cipher text and delivered, the recipient can decrypt the data using their private key. Public key encryption algorithms exploit the fact that some mathematical operations are easier to do in one direction. Unfortunately, when computing technology and modern mathematics render current algorithms (which often depend on the difficulty of factoring large integers) obsolete, the system of two keys will no longer be secure.

Quantum Cryptography is very much applicable for the following mentioned reasons that Quantum Computing and mathematical advances may soon render current algorithms obsolete and Classical cryptography techniques allow the key transmission to be passively monitored without alerting the legitimate issues.

Quantum cryptography is that the most advanced technology within the space of quantum info. The primary basic quantum conception is within the method of creating the transition from strictly research to Associate in Nursing industrial application. Thus, it's fascinating to create the systems a lot of stable and easier for the employment of some potential end-users curious about secure communication, instead of in quantum physics.

The provided info solely scratches the surface of a continued developing topic.

Even ancient civilisations complete the importance of human action firmly to avoid that precious secrets comprise the incorrect hands. There are two classical cryptograms area unit introduced that area unit supported 2 differing kinds of key. On the one hand, there's the asymmetrical cryptosystem is commonly named as public-key cryptosystem. This technique still dominates the markets, though the safety depends on unverified mathematical assumptions. On the opposite hand, there's the symmetrical cryptosystem, conjointly referred to as secret-key cryptosystem, it provides excellent security.

Basic Operations:

1. "Alice" prepares a series of photons with random polarizations – either 45, 90, 135, or 180 degrees. She sends these photons to "Bob" over a quantum channel.
2. Bob measures the photons. He randomly chooses a filter by which to measure the incoming photons, and records which filter he uses. If he measures 45 or 90 degrees, a 0 bit is recorded; if he measures 135 or 180 degrees, a 1 bit is recorded.
3. Using a normal, unsecured channel, Alice and Bob communicate to find which bits Bob used the correct filter for. These values are now become a secret key between Alice and Bob.
4. Error correction processes performed by Alice and Bob can be performed to determine if "Eve" was eavesdropping on the transmission.

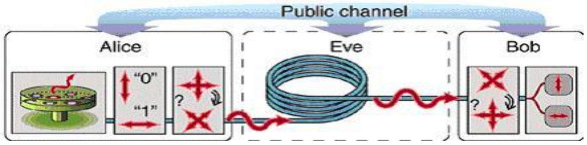

***Fig 1. Basic Operations in Quantum Cryptography***

IFERP connecting engineers... developing research

### *Detecting an Eaves Dropper:*

Heisenberg’s uncertainty principle states that there are certain conjugate variables on which limits are placed on the simultaneous knowledge of both. Measuring one variable will necessarily affect the other. Polarization properties of light fall into this category, therefore, an interloper who is trying to intercept and measure the optical signal will invariably affect the system in a such a way that their interference will be noticed.

### *Evolution of Quantum Cryptography:*

- In 1970, Stephen J. Weisner designed a theoretical bank note that would be impossible to duplicate, using the laws of quantum mechanics. He proposed using similar principles for cryptography.
- In the 1980’s, Charles Bennett and Gilles Brassard used Weisner's ideas to develop the first quantum mechanics based cryptosystem. They were able to transmit, through open air, a distance of about 30 cm by 1989.
- In June of 2003 British Researchers led by Dr. Andrew Shields transmitted a usable key over 100 km of fiber optic cable.
- Nov. 3, 2003 – MagiQ systems announces general availability of world’s first commercially available quantum cryptography system, supporting key exchanges at distances up to 120 km.

### *Using EPR Entangled Pairs for Quantum Cryptography:*

- Uses conjugate pairs for information exchange
- Sender retains one particle
- Receiver obtains “matching” particle
- Anything that happens to one particle happens also to its matched particle
- Attempt in intercepting the sent particle results in disturbance of both the sent and retained particle
- Sender is alerted that the message has been compromised
- Inability to store entangled pairs for more than a fraction of a second makes this theory unrealistic to implement

Weaknesses and Disadvantages:

1. Only works along unbroken and relatively short fiber optic cables. Record as of March 2004, 120 Km.
2. Does not solve authentication Problem.
3. Relatively High Cost.
4. Does not address some of the weakest links in data security such as human corruptibility and key storage.

## CONCLUSION:

Quantum cryptography developments promise to address some of the problems that plague classical encryption techniques such as the key distribution problem and the predicted breakdown of the public/private key system. Quantum cryptography operates on the Heisenberg uncertainty principle and random polarization of light. Another purely theoretical basis involves EPR entangled pairs. Due to the high cost of implementation and the adequacy of current crypto logical methods, it is unlikely that quantum cryptography will be in widespread use for several years.

## REFERENCES:

1.Bennett, C. H., G. Brassard and A. K. Ekert. “Quantum Cryptography”, Scientific American. October 1992: pp. 752 – 753.

2.Hammond, Andrew. MagiQ. [Online] Available at: http://www.magiqtech.com/press/Magiq_Navajo_Launch.pdf, May 11, 2004.

3.Kahn, David. “The Codebreakers”. Macmillan, 1967. Nickels, Ian. Informal in-person interviews conducted in May 2004 at SRJC.

4.The European Information Society Group. “Briefing 16 Anne. 1: What is Cryptography?”