*International Journal of Latest Trends in Engineering and Technology*
*Special Issue SACAIM 2017, pp. 514-518*
*e-ISSN:2278-621X*

# ANALYSIS OF ENCRYPTION AND DECRYPTION USING QUANTUM CRYPTOGRAPHY

Deekshith K N[1], Karthik[2], Linson Lorance[3] & Mrs Annapoorna Shetty[4]

**Abstract–In the recent timesecurity became an important research area for many researchers in the field of digital data security in data transmission where a little research has done. In this paper a security approach for digital objects such as digital photos, digital bits, information and documents are proposed. This new security method contains advance and high-tech method of security which helps to protect important private data from threats.This paper is to explain Quantum Cryptography, how can it be achieved by using the principles of quantum mechanics and also explains disadvantages of traditional cryptography techniques and how it be overcome by using this advance quantum cryptography methods. This quantum cryptography can increase the security level to 100 step forward than whatever we are using now. By using this we can transmit information and data without any fear of threats and hacking,**
**Keywords – Quantum Cryptography, QU-BITS,Uncertainty principle, No clone theorem.**

## 1. INTRODUCTION

In daily life exchanging of information is very important as well asnecessary. The information may be very important or may not, but the person who sends and receives it has concern of secured transmission of information. Now security is achieved by classical methods such as using passwords, digital signature, key distribution and encryption methods like RSA, Cipher algorithm.But how much secure are these methods? According to ITRC (Identity Theft Resource Center)in year 2015, 40% of Businesssector, 35.5% of the health/medical sector, 9.1% of Banking/Credit/Financial, 8.1% of Government/military sector, and 7.4% of education sector were hacked. And percentage of hacking is increasing year by year. So we need that one type of protection of data/information which should be very protective from all threats. Is this possible? Yes possible.This can be achieved by using quantum cryptography technics.

The Quantum cryptography was first proposed by STEPHEN WIESNER in the year of 1970, at the Columbia University. He introduced the concept of quantum conjugate coding. His seminar paper titled "conjugate coding" was rejected by IEEE information theory society, but was published by SIGACT news in 1983. In his paper he showed how to store and transmit two messages by encoding them in to two "conjugate observables", by using linear and circular polarization of light, which can be received and decoded. He illustrated his idea with the design of bank notes. In 1984 Charles H, Bennett (IBM's Thomas J. Watson Research Center), and Gilles Brassard (University de Montreal), proposed a Wiesner's"conjugate observables", now called as BB84 (quantum key distribution). In the year 1991 Arthur Ekert developed a different approach to quantum key distribution based on quantum correlation known as Quantum entanglement. Random rotations of polarization by both sender and receiverhave been proposed in Kak'sthree-stage quantum cryptography protocol. This principle can be used for continuous, unbreakable encryption of data if single photon is used. Here each single photon represents single bit of statistical data which is called as QU-bits.

## 2. DISADVANTAGES OF CLASSICAL ENCRIPTION

It is very difficult broke the strongest encryption keys used in commerce and government, but not impossible. That these keys, based on factoring large numbers, will be secure forever. Currently, very long keys such as 2048bit keys are thought to be very safe, as it would take millions of years using the most advanced computers to break them. Recently A student at Notre Dame University, using 10,000 computers working around 549 days, broke a 109-bit key. This demonstrates both the difficulty of breaking keys and the fact that they can be broken given enough computer power. Someone may discover a mathematical shortcut that allows high speed factoring of large numbers. A computer scientist at the Indian Institute of Technology, Manindra Agrawal, recently solved a problem that, how to tell if a number is prime without performing any factoring. Which

[1]Department of MCA. St. Aloysius Institute of Management & Information Technology (AIMIT), Mangaluru, Karnataka, India
[2]Department of MCA. St. Aloysius Institute of Management & Information Technology (AIMIT), Mangaluru, Karnataka, India
[3]Department of MCA. St. Aloysius Institute of Management & Information Technology (AIMIT), Mangaluru, Karnataka, India
[4]Asst. professor Department of MCA. St. Aloysius Institute of Management & Information Technology (AIMIT), Mangaluru, Karnataka, India

does not mean that large key can break easily but shows a mathematician can find the shortest method to factoring. Now we also working towards quantum computation. It has been shown that a computer utilizing quantum computing methods could quickly factor large numbers. In 1994, Peter Shor of AT&T Laboratories invented a quantum algorithm to quickly factor large numbers. Using such an algorithm on a quantum computer would reduce time to find the factor of large number. Here is the reason that shows disadvantages of classical cryptography.

1. Possibility of breaking code/key.
2. Hacking is easy.
3. Information may encrypted but coping is possible.
4. To be secure a large bits number is used.
5. Sometime sender and receiver not even got to know that information were hacked or not during transmission.
6. All secret information depends on single key.
7. It does not guard against the vulnerabilities or threats.

## 3. WHY QUANTUM CRIPTOGRAPHY IS BETTER THAN CLSSICLE?

Quantumcryptography is secure for four main reasons.

1. The quantum no-cloning theorem.
2. Uncertainty principle.
3. Measurement of quantum state will disturb the system
4. The effects that produced by measuring a quantum property are irreversible.

## 4. QUANTUM MECHANICS

*4.1 Defination of quantum mechanics–*

The branch of physics that deals with the mathematical description of the motion and interaction of subatomic particles, incorporating the concepts of quantization of energy, wave–particle duality, the uncertainty principle, and the correspondence principle.

*4.2 Defination of quantum computation/information–*

The study of computer/computation by using quantum mechanics properties is known as quantum computing and the information which used in the quantum state are known as quantum information. This method is used when physical basis for a computer is an explicitly quantum system, which cannot be explained by classical theories physics.

## 5. EQUATIONS

*5.1 Scrodinger equation –*

A1. Time dependent Schrodinger equation –

$$i\hbar\frac{\partial\psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m}\nabla^2\psi(x,t) + V(x)\psi(x,t)$$

A2. Time independent Schrodinger equation –

$$i\hbar\frac{\partial\psi(x)}{\partial t} = -\frac{\hbar^2}{2m}\nabla^2\psi(x) + V(x)\psi(x)$$

Where x denots position of the particle. t denots time.

A. Hiesenberg uncertainty principle –

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

X=change in position

P=change in momentum

## 6.THEORIES RELATED TO QUANTUM CRYPTOGRAPHY

*6.1 A brief note on quantum state/duality of light –*

In 1905 Max Planck and Albert Einstein explained the photoelectric effect by assuming that light is actually a stream of little particles, or packets of energy known as photons or quanta. In which they proposed the existence of discrete energy packets during the transmission of light. The particle theory of light is explained by Black Body Radiation as well as photoelectric

effect, but when same light is projected to the Double slit experiment light behave like wave, which then made the conclusion that light acts as both particle and wave know as wave-particle duality of light.

*6.2 Uncertainty principle–*

Uncertainty principle which is also known as Heisenberg's uncertainty principle. It says that at a given instant if the position of particle is accurately known then the momentum cannot be accurate. That is measuring of position and momentum both of the particle is not possible, there must be error of ħ/2 (where ħ is reduced plank constant i.e. ħ=h/2π) hence to measure the position of quanta we would affect it. Which implies we cannot measure quantum system character without changing it.

*6.3 Quantum entanglement (No clone theorm)–*

This quantum mechanical theory explains that the characteristics of a particle in quantum state such as position, momentum, spin, polarization performed on an entangled particle are found to be appropriately correlated. EPR paradox also comes under it. Because of all these properties of quantum particle it is impossible to clone the original particle if we try to clone it will destroys the original particle. Which can see by using controlled not gate system the most important component in quantum computation and can be used to entangle and disentangle the EPR state.

*6.4 Quantum bits(Qu-bits)–*

We are all familiar with bits, in practice we use diff erent two-state systems to represent a bit. We usually denote the outcomes of a measurement on a two-state system as "0" and "1". In fact, any two clearly distinguishable states may physically represent a bit. One of the states would denote "0" and the other one would represent "1". For example, we can use our hands to physically represent a bit. To visualize it assume that you are at one end of a big hall and I am at the other end. You can see me and we have pre-decided that I'll send you some information by raising up or lowering down my right hand. Say our chosen convention is such that if my right hand is up for 2 seconds then you note "1" and if it is down for 2 seconds then you note "0". Now if my right hand is up for 4 seconds, down for 6 seconds and again up for 2 seconds, then you receive 110001. The idea is that two distinguishable states of my hand (up and down) can be used to represent a bit. This is how the information transmitted using classical bits.

When the information processing task is done with the help of quantum mechanical systems, then in comparison to classical computation and classical information processing we obtain quantum computation and quantum information processing. The comparison continues and there exists a building block of quantum information, which is the quantum analogue of a bit. Such an analogue is called a quantum bit or a QU-bit. The diff erence between a bit and a QU-bit lies in the fact that a bit is either in the state 0 or in 1, but the QU-bit can be in a superposition state, i.e., a QU-bit is allowed to exist simultaneously in the states 0 and 1. The below figure A, where we show a two-level atom with an electron. The electron is shown by an electron cloud that depicts that the electron can simultaneously exist in both the energy states (say 0 and 1).Another example of a QU-bit is a single photon which encounters a beam splitter, as shown in Fig. B. A beam splitter transmits part of the incident light and reflects the rest. Now when the single photon encounters the beam splitter then it emerges in a superposition of the reflected path and the transmitted path. If we consider one path as 0, and the other as 1, then the photon is simultaneously in both the states and thus we have a QU-bit. If we add two detectors along the two paths shown in Fig. B, then only one detector will be clicked at a time (remember that our input state is a single photon). Similarly, if we observe the state of the electron in the atom shown in Fig. A then we will observe it either in the ground state (0) or in the excited state (1). Thus measurement destroys the superposition, and after measurement a quantum state collapses to one of the possible states. This is an important postulate of quantum mechanics.

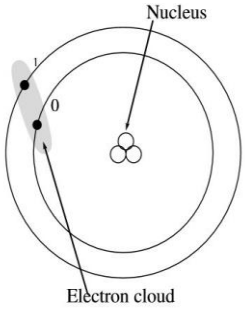



Fig A

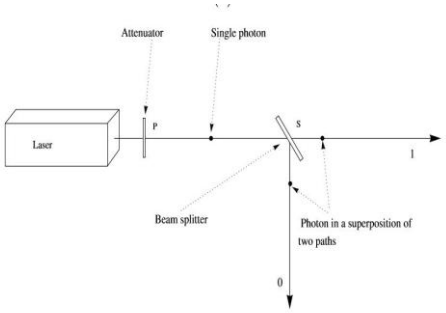



Fig B

We can also think of using a photon as a QU-bit in a diff erent manner. As it can have only two polarization states, it is an ideal two-level quantum system and we may use it as a QU-bit. Specifically, we may use the orthogonal polarization states of a photon to define 0 and 1. For example, if we choose to describe the state of a QU-bit as superposition of the linear polarization states in the horizontal and vertical directions, then we can set ↕⇒ 0, ↔⇒ 1. Similarly, we can also choose circular polarization

states to describe the state of a QU-bit as superposition of the left circularly polarization state and right circularly polarization state. To be precise, we can set ⇒ 0 ⇒ 1. Similarly, spin states of electron or nucleus may be used as a QU-bit. Spin states of the electrons are used as QU-bits in ion traps and spin states of the nucleus are used as QU-bits in NMR. In both cases it is a convention to use spin up state as 0 and spin down state as 1. Now if we consider two QU-bits, we find that together they can simultaneously represent 4 alternative states (say binary numbers 00, 01, 10 and 11). The idea can easily be extended to n-QU-bit system where we can simultaneously store $2^n$ alternatives. The most important point is that a system of QU-bits can exist in a superposition of large number of possible alternative states. Superposition states allow many computations to be performed simultaneously, and that gives rise to what is known as quantum parallelism. The superposition can be viewed as the essential resource behind the advantages of the quantum computer.

*6.5 Super position theorm–*

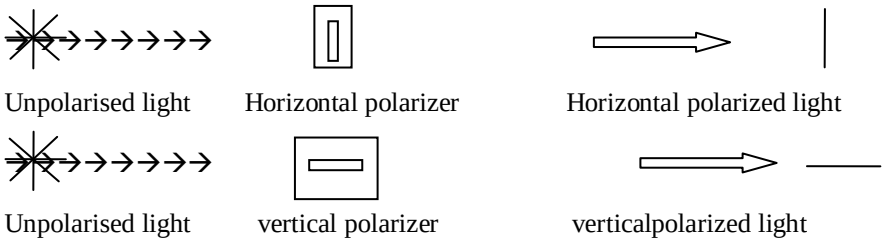
Quantum superposition is a fundamental principle of quantum mechanics. It states that every quantum state can be represented as a sum of two or more other distinct states. Mathematically, it refers to a property of solutions to the Schrodingerequation, since the Schrödinger equation is linear, any linear combination of solutions will also be a solution. One of the example for superposition is interference peaks from an electron wave in a double-slit experiment. Another example is a quantum logical QU-bit state, as used in quantum information processing, which is a linear superposition of the "basis states" |0> and |1>. Here |0>is the Dirac notation for the quantum state that will always give the result 0 when converted to classical logic by a measurement. Likewise |1>is the state that will always convert to 1.

*6.6 Polarization–*

The process of converting unpolarized light into polarized light is known as polarization. This can be achieved by using Polaroids. There are several different types of polarization methods they are

1) Linear polarization
2) Circular polarization
3) Elliptical polarization

Example:



Unpolarised light Horizontal polarizer Horizontal polarized light

Unpolarised light vertical polarizer verticalpolarized light

**7. ENCRYPTION METHODS**

*7.1 Quantum key distribution-*

Quantum key distribution is nothing but sharing of similar key between two parties. Similar key can be shared by using polarization concept. Key is generated with random rotation of polarizer (Polaroid). Which is synced at sender and receiver ends. Usually we explain this concept by using the conversation between Alice and Bob.

Let me consider one part that is sender is Linson and the other one is Lawrence who receives the sent bits. The concept used in here is simple of creating a QU-bit and in quantum key distribution we use polarization concept and vibration of photon as I am mentioned above on QU-bit.Let me consider horizontal polarization light is to represent 0 and vertical polarization is to represent 1. Here is the table that explains how this scheme works.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Linc:scheme | + | + | + | + | × | × | × | + |
| Linc:bits | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| Lins:QU-bit | ↕ | ↕ | ↔ | ↕ | / | / | \ | ↕ |
| Law:scheme | + | × | × | + | + | × | × | + |
| Law:QU-bit | ↕ | \ | \ | ↕ | ↔ | / | \ | ↕ |
| Law:Bit | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| Key select | S | | | S | | S | S | S |

Here S represents selected keys. This is how the key is distributed between two parties. If in between some third person enters and tries to check the distributed key the distribution of key fails because of quantum mechanics principles. This distribution of key method also protected against quantum computing methods. This method is successfully demonstrated on IBM laboratory by transmitting photon around 60 kilo meters.

*7.2 Position(location) based quantum encription–*

By using geographical location position based quantum cryptography can be achieved. It is very simple concept, the receiver (Lawrence) must be at particular location then only he can read and receive the information sent by Linson. In this type of cryptography Linson have to request Lawrence to be in particular location. This cryptography cannot achieved by using classical protocols because of occurrence of lot of colluding adversaries. This method first tried 2002 named as QUANTUM TAGGING, finally scientist got result on year 2010. The problem arrived in the method is EPR paradox (Einstein–Podolsky–Rosen) sometime particles interacts in such a way that finding of both position and momentum is possibleit is involved with quantum entanglement. Whichafter it was bounded with noisy-quantum storage model.

*7.3 Quantum coin-flipping cryptography–*

Quantum coin flipping cryptography can be used in between two parties who not trust each other. In this cryptography Linson sends a sequence of QU-bits through the communicational channel. Lawrence gasses on what basis Linson send the information. Linson determines whether Lawrence own or not then only he sends all his information to Lawrence. Advantage of quantum coin flipping is easy to detect third party entry to the communication channel because of a single photon can read only once in a system. This approach of theory is very secure but it is very difficult achieve in practically.

*7.4 List of some other approch of quantum cryptography*

1) Quantum commitment
2) Bounded quantum storage model (BQSM)
3) Devise independent quantum cryptography
4) Post-Quantum cryptography

## 8. ADVATAGES OF QUANTUM CRYPTOGRAPHY

1. Un-breakable
2. Simple to use and privacy is more
3. Maintenance is easy
4. Provides un breakable security
5. It detects entering of threats to the system
6. It detects eve's dropping
7. Most important point is it provides lots of support to the concept of Quantum computation.

## 9. CONCLUSSION

In this paper, an approach for quantum cryptography of digital information transmission is proposed. This approach provides ultimate security to transmission of data. This approach is very different and advanced to compare any other earlier cryptographic technique. It is based on physics quantum mechanics theory. There are lots of types of quantum cryptography which is already experimented and succeeded. Some of them are theoretically proved which can be implemented in future. This method removes all type of security issues and threats. That is no one can crack others information.

## 10. REFERENCES

[1] Narasihma S A,Professor physics department, Govt. First Grade College Koppa, 577126.
[2] Siri Krishnamoorthi M, Msc physics, Kuvempu university.
[3] "An intruduction to Quantum Computer science", by N. David Mermin.
[4] "Quantum computation and quantum information", by Michael Nielsen and Isaac L. Chaung.
[5] Paper titled "An introduction to Quantum mechamics".
[6] http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html
[7] https://users.soe.ucsc.edu/~yanli/res/quantum_cryptography_intro.pdf
[8] "Quantum resistance public key cryptograpy: a survey", by R. Perlner and D. cooper.
[9] https://www.intechopen.com/books/theory-and-practice-of-cryptography-and-network-security-protocols-and-technologies/introduction-to-quantum-cryptography