# Quantum Mechanics and Cryptography

**Shiv Kumar[1], Shrawan Kumar[2], Bimlendu Verma[3]**

[1, 2, 3] Mewar University, Chittorgargh, Department of Computer Science of Engineering
NH-79, Gangrar-312901, India

**Abstract:** ***Cryptography is the way of making data or messages more secure and private. It is the oldest techniques to secure data. This technique is based on algorithms and mathematical calculation. The main problem of this technique is key distribution or storing key or key generation. Anyone can hack key on net if he/she know the algorithm used in key generation process easily. It may take a day to years. But if we distribute key using light and quantum mechanics it will be much more secure. It will take million of years to hack it because it is not based on mathematical computation that can be guess easily. So, our data becomes more secure and private which is much more precious now a day.***

**Keywords:** Cryptography, quantum, encryption, decryption, key distribution, photon**.**

## 1. Introduction

The process of converting from plaintext to cipher text is known as enciphering or encryption; restoring the plaintext from the cipher text is deciphering or decryption. The many schemes used for encryption constitute the area of study known as cryptography [1]

Cryptography means keeping communications private. It is a practical art of converting messages or data into a different form, such that no one read them without having access to the 'key'. The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or 'cipher' (in which case the message as a whole is converted, rather than individual characters). It deals with encryption, decryption and authentication.

### 1.1 Basis of Cryptography

Any data (suppose "nice") can be changed into unreadable format using encryption and unreadable format data can be changed into readable format using decryption that is original data ( "nice" ). Its decryption can be seen in fig1.1

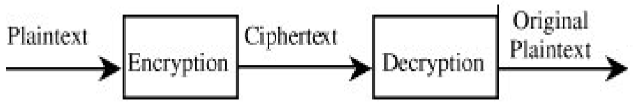

**Figure 1.1:** Encryption and Decryption Process

### 1.2 Terminology of Cryptography

- **Encryption** is the process of encoding a message so that its meaning is not obvious.
- **Decryption** is the reverse process, transforming an encrypted message back into its normal, original form. Alternatively, the terms encode and decode or encipher and decipher are used instead of encrypt and decrypt.
- **Cryptosystem**: A system for encryption and decryption is called a cryptosystem.
- **Plain text**: The original form of a message is known as plaintext.
- **Cipher text**: the encrypted form is called cipher text.
- **Original text:** the decrypted form is called original text.

### 1.3 Types of Cryptography

There are three types of cryptography and they are following:

1) Based on public key: Also known as asymmetric cryptography [3].Where two keys are used. The public key is used to encrypt a message. The private key is used to decrypt a message. Encryption and decryption are two mathematical functions that are inverses of each other.
2) Based on Secret key: Also known as conventional cryptography or symmetric cryptography. It uses only single key called private key which is secret[4] and same key is used in both process encryption and decryption.
3) Based on Hash function: Also known as message digest or one way transformation. Hash function is a mathematical transformation that takes a message of arbitrary length (transformed into a string of bits) and computes from it a fixed-length (short) number.

## 2. Data Transferring Using Quantum Mechanics

Entanglement is one of the products of quantum mechanics, the area of physics that aims to deliver the ultra-fast quantum as shown in fig.2. It links two quantum particles, such as photons, no matter how far away from each other they are, in such a way that any changes to one can be measured in the other. Although the theory has been known for about 70 years, scientists have only been able to generate entanglement within the past five to 10 years.

**Figure 2:** Use of quantum to transfer data

### 2.1 Quantum Theory

The essence of quantum theory is the realization that elementary particles (electrons, protons, neutrons etc.).It has the ability to behave as waves. A test which neatly demonstrates this peculiar behavior, known as wave/particle duality, in light photons is the twin slit interference experiment. If light is directed at two slits in a screen the waves will radiate outwards as shown below in Fig.2.1 [6] intensities caused by light waves interference.

**Figure 2.1:** Pattern formed on screen showing differing

Photons are some pretty amazing particles. They have no mass, they're the smallest measure of light, and they can exist in all of their possible states at once, called the wave function. This means that whatever direction a photon can spin in -- say, diagonally, vertically and horizontally -- it does all at once. Light in this state is called un polarized. This is exactly the same as if you constantly moved east, west, north, south, and up-and-down at the same time.

The foundation of quantum physics is the unpredictability factor. This unpredictability is pretty much defined by Heisenberg's Uncertainty Principle. This principle says, essentially, that it's impossible to know both an object's position and velocity -- at the same time.

But when dealing with photons for encryption, Heisenberg's principle can be used to our advantage. To create a photon, quantum cryptographers use LEDs – light emitting diodes, a source of un polarized light. LEDs are capable of creating just one photon at a time, which is how a string of photons can be created, rather than a wild burst. Through the use of polarization filters, we can force the photon to take one state or another -- or polarize it. If we use a vertical polarizing filter situated beyond a LED, we can polarize the photons that emerge: The photons that aren't absorbed will emerge on the other side with a vertical spin. The thing about photons is that once they're polarized, they can't be accurately measured again, except by a filter like the one that initially produced their current spin. So if a photon with a vertical spin is measured through a diagonal filter, either the photon won't pass through the filter or the filter will affect the photon's behavior, causing it to take a diagonal spin. In this sense, the information on the photon's original polarization is lost, and so, too, is any information attached to the photon's spin.

### 2.2 Need of Quantum Cryptography

As per Shannon's rules, if the data being encrypted is either much longer than the key or if the key is used repeatedly then, with sufficient computation power, it is possible to infer the message. So to have an unbreakable code, we need a key that is as long as the data and that are not repeated. This is the Vernam code or one-time pad. The biggest practical problem of such an encryption scheme is the difficulty of distributing the key. If the key could be secretly distributed then the data itself could be distributed. The solution to the problem of key distribution was provided by C. Bennett and G. Brassard who first suggested how to use quantum mechanics for secure key distribution.

### 2.3 Working of Quantum Cryptography

Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin?[8] This is where binary code comes into play. Each type of a photon's spin represents one piece of information -- usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon. For example, a photon that has a vertical spin can be assigned a 1. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive [7].

When Alice sends Bob her photons using an LED as shown in fig.2.3a, she'll randomly polarize them through either the X or the + filters, so that each polarized photon has one of four possible states: (|), (--), (/) or ( ) [source: Vittorio]. As Bob receives these photons, he decides whether to measure each with either his + or X filter -- he can't use both filters together. Keep in mind, Bob has no idea what filter to use for each photon, he's guessing for each one. After the entire transmission, Bob and Alice have a non-encrypted discussion about the transmission.

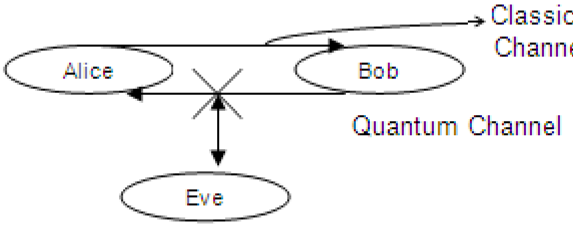

**Figure 2.3a:** Data attachment in quantum channel.

The reason this conversation can be public is because of the way it's carried out. Bob calls Alice and tells her which filter he used for each photon, and she tells him whether it was the correct or incorrect filter to use. Their conversation may sound a little like this (shown in fig2.3b):

Bob: PlusAlice: Correct
Bob: PlusAlice: Incorrect
Bob: XAlice: Correct

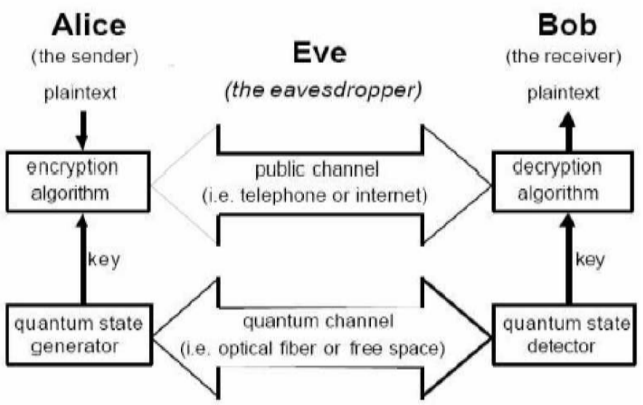

**Figure 2.3b:** Encryption and Decryption in Quantum cryptography

Since Bob isn't saying what his measurements are -- only the type of filter he used -- a third party listening in on their conversation can't determine what the actual photon sequence is. Here's an example. Say Alice sent one photon as a ( / ) and 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 that particular photon, Alice will say "correct." A person listening will only know that that particular photon could be either a ( / ) or a ( ), but not which one definitively. Bob will know that his measurements are correct, because a (--) photon traveling through a + filter will remain polarized as a (--) photon after it passes through the filter.

After their odd conversation, Alice and Bob both throw out the results from Bob's incorrect guesses. This leaves Alice and Bob with identical strings of polarized protons. It my look a little like this: -- / | | | / -- -- | | | -- / | … and so on. To Alice and Bob, this is a meaningless string of photons. But once binary code is applied, the photons become a message. Bob and Alice can agree on binary assignments, say 1 for photons polarized as ( ) and ( -- ) and 0 for photons polarized like ( / ) and ( | ).

This means that their string of photons now looks like this: 11110000011110001010. Which can in turn be translated into English, Spanish, Navajo, prime numbers or anything else the Bob and Alice use as codes for the keys used in their encryption

### 2.4 Advantages Quantum Cryptography

Basically there are number of advantages of this type of cryptography. Most important is that it is much more secure than the conventional cryptography because it does not use any physical medium or network to transfer key. But it uses photon to do this. Others are following:

- **User Identification**: We cannot identify senders and receivers easily. So, hacking cannot be done easily
- **More Life Time**: Life time of algorithm increases because Computational power increases.
- **Communication distance**: As data flow using photon. So, range increases automatically
- **Platform independent**: As it can be implemented by using both hardware and software

### 2.5 Disadvantages Quantum Cryptography

The length of quantum cryptology capability is so short is because of interference. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. This means that a 1 may come through as a 0 -- this is the probability factor at work in quantum. The length of present quantum cryptology is 150 kilometers (about 93 miles). But this is still far short of the distance requirements needed to transmit information with modern computer and telecommunication systems.

## 3. Analysis of Quantum Cryptography

We can analyze quantum cryptology for many purposes. We can analyze its problem or its performance or problems in key distribution. First we will discuss basic problems of quantum cryptography [9].

### 3.1 Problems of Quantum Cryptography

The length of present quantum cryptology is 150 to 200 kilometers. So, this is the main problem for the modern computer era. But basic problems are related to attacks on quantum crypto and length of its and they are:

- **Attack using beam splitter –** When multiple photons are produced. At that times, using a beam splitter, Eve can infer some amount of information. However the difficulty of such an approach is that there is no way for her to find out when a pulse consists of multiple photons. If a splitter is used when a single photon is passing then the photons have to choose between Eve's and Bob's scheme detectors.
- **Length limitation: –** When optical fiber is used, the pulse needs to be amplified every some distance. Thus, we cannot establish this scheme over long distance and instead will have to be done hop-by-hop. So this is the great challenges or hurdles of the quantum cryptography.
- **Man in the middle attack –** This is only possible if there is lack of authentication when Alice and Bob talk to each other when Eve works as man in the middle acting as Bob to Alice and as Alice to Bob and thus establish a complete BB84 protocol with both of them. By ensuring that proper authentication procedures are used, this kind of attack can be avoided

### 3.2 Performances quantum key distribution:

Quantum Key Distribution (QKD) allows two remote parties to share a key with absolute secrecy. QKD was born as an alternative to public key cryptography, which currently protects the vast majority of our information. [10] . In particular, the two cornerstones sustaining the security of QKD are the Heisenberg Uncertainty Principle and the No Cloning Theorem, which both protect the secrecy of the transmission of a key that will be later used for encryption. This key will be shared by two remote parties - commonly referred to as Alice and Bob - by using properties of single photons that follow an uncertainty principle such as two linearly polarized non orthogonal states. The Uncertainty Principle guarantees that tapping the quantum channel by an eavesdropper will cause a disturbance that sender and receiver can detect. On the other hand the No Cloning Theorem forbids perfect copies of an unknown quantum state, which prevents an eavesdropper from cloning the quantum states.

In any QKD protocol the so-called quantum channel is used to transmit the quantum states encoding the binary values of the cryptographic key. This channel is usually free space or optical fiber and this selection divides the two main types of QKD systems. The progress in both approximations since this technology was born 25 years ago has been outstanding, although it must be said that there are still great challenges to overcome. In free space systems the first implementation was over only 30 cm of air in 1991 and was later extended to 150m, 1km, 1.6km and finally in 2002 quantum keys were successfully exchanged between two mountains in Germany at a distance of 23 km . The world record to date is 140 km between La Palma and Tenerife in the Canary Islands in 2007 [3]. The first transmission in optical fiber was realized in 1993 and only three years later the distance was increased to 23 km through standard telecommunications fiber of the telecommunications provider Swisscom. This distance has been further enhanced to 150 km by Los Alamos National Laboratories and to 200 km, which currently holds the world record by collaboration between NTT, NIST and Stanford University.

### 3.3 Attack analysis over key distribution

On QKD number of attacks is possible, but they are based on specific properties. Some of them are Intercept/Resend attack, Beam Splitting attack, Trojan Horse and Faked State attack. But research works on these attacks are done by number of researchers and they successfully find out the solution of these types of attacks [11]. But we will focus in individual attack by using intercept and resend (I/R) and beam splitting methods. This must be done to check the tolerability of the system. So, all attacks are possible on individual once.

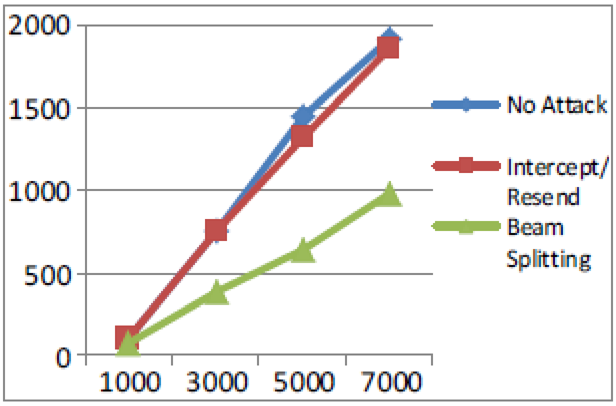

**Figure 3.3:** Initials Bits Length v/s Final Bits Length

In fig.3.3. initial bits length emitted by Alice is represented by x-axis and final bits length which is the outcome of BB84 protocol is represented by y-axis. Here, the clear strength of PNS (or Beam Splitting) attack can be seen over the Intercept/Resend attack. The length of final bit length is much lower in case of Beam Splitting attack than that of I/R attack while error rate is lower than the maximum allowable error rate. On the other hand, I/R attack seem close to the no attack line. On close examination of results, it can further be inference that Eve has 50% probability to measure the incoming bits from Alice correctly.

Considering Trojan Horse attack and Faked State attacks, these lead to the advent of new and powerful attacking strategies. The beauty of these attacks is that these are out of box attacks. I/R attack and Beam splitting attacks are used as sub strategies in these attacks. These are quite powerful attacks in themselves and their main strength is that if they are implemented perfectly then these are undetectable. The proposed countermeasures for these attacks are also not that much perfect as they themselves decrease the efficiency of BB84 protocol.

On close examination, I/R attack is proposed under ideal environment while the others have taken the practical Imperfection of the communication system under their key areas of interest and hence are quite realistic ones. But, it does not imply that I/R attack is not effective one as it is used for the extraction of information of emitted photons in the remaining Protocols.

## 4. Conclusions

In this way we can say that encryption of data using light and quantum mechanics is much more secure and private then the classical methods of cryptography because key is distributed using photons between two users. So this cryptography is called “Quantum cryptography” and this technique can be used to transmit any personal data or information, which will be more secure and private.

## 5. Acknowledgments

Foremost, I would like to express my sincere gratitude to my advisor Mr. Shrawan Kumar Sharma for the continuous support of my study, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this paper. I could not have imagined having a better advisor and mentor for my M. Tech study. Besides my advisor, I would like to thank the rest of my department professors or lecturers: Prof. R. P. Ojha and Santosh Upadhyay and others, for their encouragement, insightful comments, and hard questions. Last but not the least; I would like to thank beloved, Sneha Rani supporting me spiritually throughout my life.

## References

[1] William Stallings, ”Cryptography and Network Security Principles and Practice”, Fifth Edition, pp 32
[2] Charles P. Pfleeger,” Security in Computing”, Fourth Edition pp 2.1
[3] William Stallings, ”Cryptography and Network Security Principles and Practice”, Fifth Edition, pp 269

[4] William Stallings, “Cryptography and Network Security Principles and Practice “,Fifth Edition ,pp 60
[5] William Stallings,“ Cryptography and Network Security Principles and Practice”, Fifth Edition, pp 693
[6] John K. N. Murphy ,”Quantum Theory and Wave/Particle Duality “, http://www.hotquanta.com/wpd.html
[7] Josh Clark, HowStuffWorks "How Quantum Cryptology Works"
[8] Vibha Ojha, Anand Sharma, WAP journal, ISSN: 2222-2510, Vol (2), Issue (5), May 2012.
[9] Quantum Cryptography in Practice – Chip Elliot, Dr David Pearson, Dr Gregory Toxel @bbn.com
[10] María-José García-Martínez, Natalia Denisenko, Diego Soto, Verónica Fernández,” Analysis of Quantum Key Distribution as a Disruptive Technology”
[11] José García-Martínez, Natalia Denisenko, Diego Soto, Verónica Fernández.” Analysis of Quantum Key Disribution as a Disruptive Technology”

## Author Profile

**Shiv Kumar** received the M. Tech. degree in Computer Science and Engineering from Mewar University Chittorgargh in 2012. During 2007-2013, he stayed in Canon India Private limited Center of Excellence center and India Software Center Noida and Gurgaon of India. He knows with Mewar University, Chittorgargh, India.

**Bimlendu Prasad Verma** is an M.Tech in (Computer Science and Engineering) from FET, Mewar University and is a Member of IEEE. He is a keen contributor in forums like Code Project, Expert Exchange, and Microsoft Technet. His interest areas are Document formats, Print Rendering and Document Management Systems

**Shrawan Kumar Sharma** is currently pursuing masters degree program in Computer science and engineering in Mewar University, India.