International Journal of Current Engineering and Technology
©2020 **INPRESSCO**®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

A Survey on Quantum cryptography versus classical Cryptography

Praveer Dubey[#]* and Ompal Yadav^

[#]Computer science, GGSIPU university, India
^Scientist-D, MEIT Gov. of India

Received 21 Sept 2020, Accepted 24 Nov 2020, Available online 26 Nov 2020, **Vol.10, No.6 (Nov/Dec 2020)**

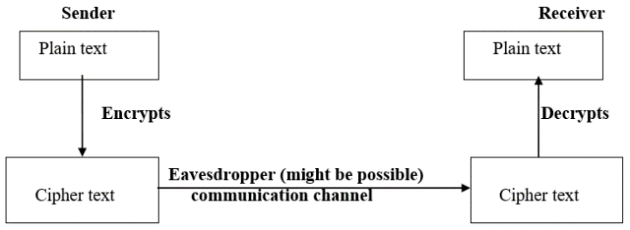
Abstract

Quantum Cryptography is an approach to securing communications by applying the phenomena of quantum physics. Unlike traditional classical cryptography, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography is focused on the physics of information. The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either public-key or secret-key Methods. There are classical solutions to insecure communication all rely on making some or assumption, about the computational power of a cheater, about the number of cheaters, or something of this kind. Based on quantum key distribution, one might hope that a quantum computer might allow us to weaken or remove these assumptions.

Keywords: *Single-photon source; Photon statistics; Quantum dots; Quantum key distribution (QKD)*

1. Introduction

Cryptography is the art of rendering a message unintelligible to any unauthorized party .Basically cryptography means the hidden/secret way of communication between two parties and this all will possible when the communicative data will be hidden between the channel through which the data travels to reach from sender to receiver, and the process of hiding the data which has to communicate with appropriate receiver at sender side is called as Encryption and the encrypted data is known as cipher text, while the process of converting cipher text into plain text is known as decryption/deciphering. Thus, there are three agents will be there i.e. one who sends data(sender), one who will receive data(receiver) and one to whom data should be protected from eavesdrop (eavesdropper) i.e. diagrammatical description:



In cryptography, there are mainly four backbones which we have to take into our consideration:

1) Secrecy of key 2) Message authentication 3) Intrusion detection 4) Message repudiation There are two threats of eavesdropper i.e.
1) Unauthorized access 2) Modification of received data and forwarding of modified data to intended receiver.

Two types of crypto system possible on the basis of key used for encryption and decryption: Symmetric cryptosystem and Asymmetric cryptosystem. In symmetric cryptosystem both the encryption and decryption are processed by using same key (public key), while in asymmetric cryptosystem the encryption is performed by using public key while decryption achieved by secret key. [While symmetric cryptosystem is faster than asymmetric cryptosystem.] Some examples of these symmetric and asymmetric cryptosystem are:

Symmetric – OTP (one time pad), DES (data encryption standard), AES (advanced encryption standard) etc.
Asymmetric - RSA, DH etc. The main drawback of conventional cryptosystem is that the robustness of the system completely depends on the complexity of used algorithm i.e. logical part and there is no dependency on communication channel (classical) that is, we cannot declare the channel (classical) security and cannot detect the eavesdropper presence in it.

The implementation of quantum mechanics in cryptosystem brings the concept of quantum cryptography. Quantum Cryptography was first proposed in 1984. Since then there has been significant

*Corresponding author's ORCID ID: 0000-0002-5589-2312
DOI: https://doi.org/10.14741/ijcet/v.10.6.3

development in it and recently scientists have succeeded in transmitting data through a reasonable distance of 250 Km in free space but at a fruitless transmission speed of 16-bits per second. Although confidentiality is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures and non-repudiation. Quantum systems are exponentially power full. i.e. system of 500 particle has 2^500 computing problem. Classically: either increase speed or parallelism 2^500 >> #particle in the universe 2^500 >> age of universe in femto-seconds.

Classical	**Quantum**
Classical bits(binary bits used)	Qubits
Classical channel(unsecure channel)	Quantum channel(secure channel)
Eavesdrop detection not possible	Eavesdrop detection possible

Q-bits

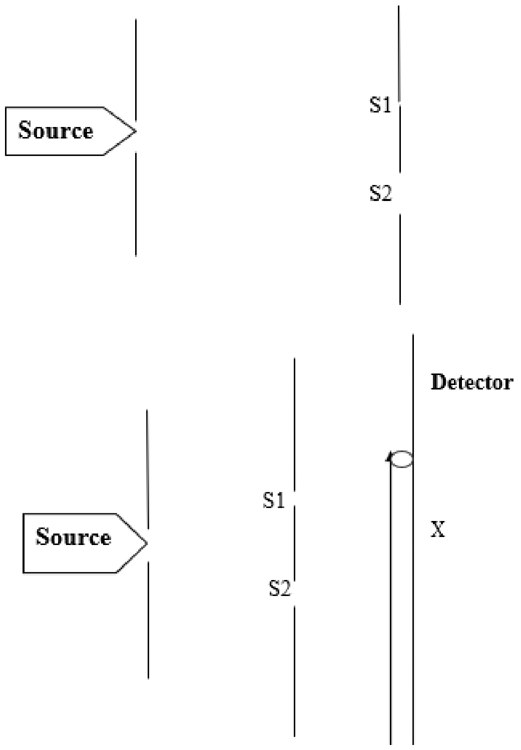
A q-bit (or quantum bit) is similar in concept to a standard „bit‟-it is a memory element. It can hold not only the states „0‟ and „1‟ but a linear superposition of both, α|0> + β|1>. The quantum bit, or q-bit, is the simplest unit of quantum information .In physicists terms we denote the states |0> and |1> respectively. Either classical or quantum, are the simplest possible units of information. They are oracle-like objects that, when asked a question (i.e., when *measured*), can respond in one of only two ways. Measuring a bit, either classical or quantum, will result in one of two possible outcomes. At first glance, this makes it sound like there is no difference between bits and q-bits. In fact, the difference is not in the possible *answers*, but in the possible *questions*. For normal bits, only a single measurement is permitted, meaning that only a single question can be asked: Is this bit a zero or a one?

In contrast, a q-bit is a Bit, either classical or quantum, are the simplest possible units of information. They are oracle-like objects that, when asked a question (i.e., when *measured*), can respond in one of only two ways. Measuring a bit, either classical or quantum, will result in one of two possible outcomes. At first glance, this makes it sound like there is no difference between bits and q-bits. In fact, the difference is not in the possible *answers*, but in the possible *questions*. For normal bits, only a single measurement is permitted, meaning that only a single question can be asked: Is this bit a zero or a one? In Examples of q-bits as follows:

- Atomic Orbit (The electrons within an atom exist in quantized energy levels)
- Photon Polarization (a photon may be described as a travelling electromagnetic wave. an electromagnetic Wave has a polarization which describes the orientation of the electric field oscillations.
- Spins (Like photon polarization, the spin of a (spin-1/2) particle is a two-state system, and can be described by a q-bit.)Contrast, a q-bit is a system which can be asked many, many different questions, but to each question, only one of two answers can be given. Double-slit Experiment

Double-slit Experiment

There is lots of theory about quantum particles, like-Quantum objects travels either in form of Waves‟ or particles‟. i.e. Wave-Particle duality nature of objects. For showing this strange and uncertain behavior of Quantum particles, there is an experiment given by Young called Young’s Double-Slit experiment, this is as following:



Bullets	**Water waves**	**Photons/Electrons**
Discrete Probability of arrival No interference	Continuous Intensity interference	Discrete Probability of arrival interference
N12=N1+N2	I12 ≠ I1+I2 H12=H1+H2 |I|= H^2	I12 ≠ I1+I2 a12=a1+a2 |I|= |a|^2

Thus in above experiment, we are experimenting with three different object i.e. with bullets, water and photon/electrons (light). And as described in above comparative table, It is clear that is when we are injecting bullets from any source and these bullets passes from two different slits and at a particular time and in position when it strikes then found that discrete behavior observed and by nature of particles measured in probability of arrival of these particles in fixed time duration.

And found that when this experiment performed by opening only one slit and observed at same point as before then again from other single slit, the number of total strokes of particle from two slit at that point is equal to sum of two single slit strokes at same point in fixed amount of time and no interference possible because of discrete behavior of the particles. While, when the same experiment performing with water flow then by observing intensity of flow we are observing the nature of water waves and found that the intensity at a point in double slit experiment is not equal to sum of two single slit experiment at same point and interference also possible. Similarly, after observing the particle and wave behavior when we observed the same experiment with light particles we found that light behaves in both way that is like particles and waves both. That is, when light particles strikes in the detector screen at a particular point they showed their discrete behavior like particles while the illumination of light depends on the intensity of light particle which is same as wave behavior i.e. intensity of light particles at particular point in the detector screen in double slit experiment is not equal to two single slit experiment intensity at the same point. This is the main problem in implementation of quantum theory in real aspect because of Quantum particles duality nature (wave-particle dual nature.

Polarization principle

- Light emanating from some source, sun, or a light bulb, vibrates in all direction at right angle to the direction of propagation and is un-polarized. i.e. A light wave that is vibrating in more than one plane is referred to as un- polarized light.
- It is possible to transform un-polarized light into polarized light. Polarized light waves are light waves in which the vibration occurs in a single plane.

The process of transforming un-polarized light into polarized light is known as Polarization. In optical mineralogy we need to produce light which vibrates in a single direction and we need to know the vibration direction of the light ray. These two requirements can be easily met but polarizing the light coming from the light source, by means of a polarizing filter.

The quantum cryptography relies on two important elements of quantum mechanics:

1) Heisenberg uncertainty principle
2) Principle of photon polarization

Heisenberg uncertainty principle states that it is not possible to measure the quantum state of any system without disturbing that system. The principle of photon polarization states that an eavesdropper cannot copy unknown Q-bits i.e. unknown states, due to no-cloning theorem (by Wootters and Zurek)

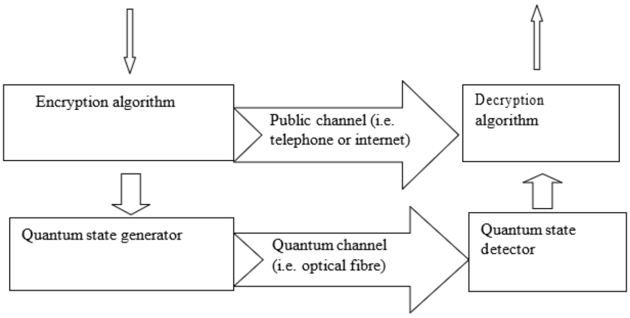
- Key distribution relies on two things:

1) Physically secure channel (trusted couriers)
2) Conditional security of difficult mathematical problem

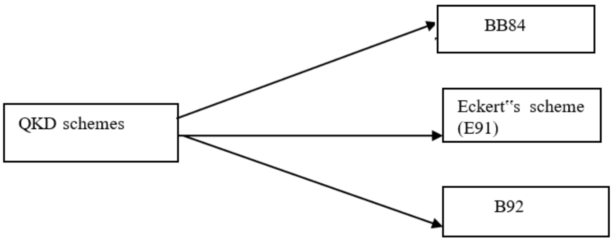
- Secure key distribution becomes possible with quantum communications. In this procedure the key is distributed over the quantum channel and not the encrypted message.

This is why we need two channels between A and B.

1) One public channel for encrypted message
2) Other for key distribution (quantum channel)



There are some key distribution techniques have been proposed over past time, in which three main techniques has been implemented in small level which are as following:



BB84 (Bennett and Brassard)

BB84 allows two parties, sender and receiver, to establish a secret, common key sequence using polarized photons-qbits. The BB84 scheme uses single photons transmission from Alice to Bob, which are prepared at random in four partly orthogonal polarization states: 0, 45, 90 and 135 degree. BB84 uses two polarizations

1) Rectilinear polarization (0 and 90 degree) 2) Diagonal polarization (45 and 135 degree)

Table 1 Rectilinear and diagonal polarized signal representations

Bases	Rectilinear	Diagonal	Rectilinear	Diagonal
State	0 degree	45 degree	90 degree	135 degree
Q-bit	→	↗	↑	↖
Bit	0	0	1	1

Steps of the BB84 scheme:

1) Sender generates a random binary sequences s.
2) Sender chooses which type of photon to use (rectilinear polarized R or diagonally polarized D) in order to represent each bit in s. let b denote the sequence of each polarization base.
3) Sender uses specialized equipment, including a light source and a set of polarization, to create a sequence p of polarized photons Q-bits whose polarization directions represent the bits in s.
4) Sender sends the Q-bits p to receiver over an optical fiber.
5) For each Q-bit received, receiver makes a guess of which base is polarized: rectilinearly or diagonally, and sets up his measurement device accordingly.
6) Receiver measures each Q-bit with respect to the basis chosen in step5, producing a new sequence of bits.
7) Sender and receiver communicate over a classical, possibly public channel. Specifically, s sender tells to receiver the choice of basis for each bit, and receiver tells to sender whether he made the same choice. The bits for which sender and receiver have used different bases are discarded from s and s‟.

The key point in this scheme is the polarization state of photons and the variable polarization filter, and because the polarization of single photons is not readable without altering it and because it is not reproducible, E the eavesdropper cannot read the polarization of single photons, reproduce it and send it to B.

2. Attacks

PNS attack

Because true single photon sources are currently impractical to implement in QKD experiments. Such experiments typically make of highly attenuated light so that the photon rate is low. Attenuated light in this way will not produce anti-bunched photons, so some photons are produced in multi- photon bunches. In this case, it is possible for an eavesdropper to split off and store a single photon while the other photons are received by legitimate parties without any effect on their polarization. The eavesdropper could then monitor the public announcement of bases and make measurement using the correct bases, leading to an undetected information leak. This sort of attack is referred to as photon number splitting (PNS) attack.

Man in the middle attack – Eve can be the 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. This is only possible if there is lack of authentication when Alice and Bob talk to each other. By ensuring that proper authentication procedures are used, this kind of attack can be avoided.

Conclusion

Hence quantum cryptography is a new technology. QKD indeed possesses the potential to bring a revolution in the field of network security. Traditional key exchange algorithms cannot provide any indication of eavesdropping or guarantee of key security. In contrast, when using QKD, one can determine if an adversary is eavesdropping on the link because it will induce errors in the key exchange process. Over the last 28 years, research in the QKD area has matured the technology and resulted in commercial QKD implementations. Quantum key distribution offers greater potential for secure communications than any previous cryptographic protocol. Thus, QKD protocols give unconditional security based on the laws of physics alone.

References

A talk on Quantum Cryptography or How Alice outwits Eve (Samuel J. Lomonaco)

Limitations of Practical Quantum Cryptography (Vibha Ojha, Anand Sharma, Vishal Guar, Prakrit Trivedi)

Advantages of classical cryptography over Quantum Cryptography(Vibha Ojha, Anand sharma, S.K. Lenka, S.R. Biradar)

Modified One time Pad Security Scheme: Random Key Generation Approach (Sharad patil, Manoj devare, Ajay Kumar)

Quantum Cryptography: How to beat the code breakers using quantum mechanics (Pheonix, Simon J., and Paul D. Townsend)

Detection of Eavesdropping in Quantum Key Distribution using Bell‟s Theorem and Error Rate Calculation (David Gaharia and Joel Wibron; july6,2011)

An Approach to Secure Authentication Protocol with Group Signature based Quantum Cryptography (V. Padmavathi, M. Madhavi and N. Nagalakshmi January, 2013)

Identifying vulnerabilities of quantum cryptography in secure optical data transport (Kartalopoulos, S.V. milcom 2005, vol 5, pp. 2788-2796)

The Transport Layer Security (TLS) Protocol Version 1.1(Dierks, T. and E. Rescorla, RFC 4346, April 2006)

Limitations on practical quantum cryptography, (G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders,Phys. Rev. Lett., vol. 85, pp.1330–1333, 2000)

Quantum Resistant Public Key Cryptography: A Survey (R. Perlner and D. Cooper,Proc of IDtrust 2009, Gaithersburg, MD, Apr. 14-19)