# Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper

**Aakash Goyal[1], Sapna Aggarwal[2] and Aanchal Jain[3]**

*[1]M.Tech. Student (CSE) JIET-Jind, India*
*[2]Assistant Professor, CSE Department, JIET-Jind, India*
*[3]M.Tech. Student (ECE), BMIET-Sonipat, India*
*E-mail: aakash.goyal99@gmail.com[1], sapna.ruby@gmail.com[2], aanchal.always@gmail.com[3]*

**Abstract**
Cryptography long had been a valuable, essential tool for defensive computer security. A technique whether classical or modern must be well-built and also must be practically viable. With the application of quantum mechanics principles to cryptography, a new dimension to secure communication can be given; such system so developed can detect eavesdropping and assure that it should not occur at all. Work presents the brief review of the existing state of quantum cryptography science. Core principles of the quantum cryptography are demonstrated by giving the example of BB84 protocol. Work principally presents quantum cryptography's comparison with classical cryptography.

**Keywords:** BB84 protocol;, Quantum cryptography; Classical cryptography; Polarization states;

## Introduction

Cryptography is the science in which the use of mathematics occurs to encrypt and decrypt data .Cryptography enables user to store sensitive information or transmit it across Insecure networks (like the Internet) so that it cannot be read by anyone other than the intended receiver. To attain secure transmission, an algorithm is used which unite the message with additional information to produce a cryptogram. The algorithm is called as cipher and the additional information is known as the key. This technique is termed as encryption.

Whereas cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Quantum cryptographic devices in general make use of individual photons of light and take benefit of Heisenberg's uncertainty principle, according to which attempt to compute a quantum system disturbs it and yields partial information about its state before the measurement. Eavesdropping on a quantum communications channel thus causes an unavoidable disturbance, alerting the legal users. Quantum techniques also support the achievement of cryptographic objectives such as enabling two mutually suspicious parties to make combined decisions based on private information, while compromising its confidentiality as little as possible. Physical devices with these specialized cryptographic protocols can invoke up streams of random bits whose values will remain unknown to third parties. When we use these bits as key material for Vernam ciphers, we can get Shannon's ideal of perfect secrecy—cheaply and easily.

The development of quantum cryptography was inspired by the short comings of classical cryptography methods. In classical cryptography communicating parties need to share a secret sequence of random numbers, the key, that is exchanged by physical means and thus open to security loopholes. The classical cryptography does not detect eavesdropping like quantum cryptography, also with increase in computing power and new computational techniques are developed, the numerical keys will no longer be able to provide satisfactory levels of secure communications. These flaws led to the development of quantum cryptography, whose security basis is quantum mechanics [2]. This paper presents the comparison of quantum and classical cryptography on several backgrounds.

### *Historical Timeline*

In 1917, Gilbert S Vernam, an AT&T employee, created a machine that makes a non-repeating, virtually random sequence of characters called as one-time pad. Using an encryption key the same length as the message and never using that key again is the only proven method of securely communicating. In the 1940s, Claude Shannon provided the information-theoretic basis for secrecy; the amount of uncertainty that can be commenced into an encoded message can't be greater than that of the cryptographic key used to encode it. In the early 1970s, or possibly earlier, numerous researchers, including Whitfield Diffie, Martin Hellman, Ralph Merkle, Ron Rivest, Adi Shamir, Leonard Adleman, James Ellis, Clifford Cocks, and Malcolm Williamson, invented cryptographic techniques based on computational complexity. Quantum cryptography was first proposed in 1984 by Brennet and Brassard [1] based on the No-Cloning theorem. It relies on fact that we should base security on known physical laws not on mathematical complexities.

## Classical Cryptography

Classical cryptography makes use of several mathematical techniques to restrict eavesdroppers from knowing the contents of encrypted messages. The most popular among them that are adopted globally have been described below.

Throughout the paper, the transmitter is referred as 'Alice', the receiver as 'Bob', and an eavesdropper as 'Eve'.

***Data Encryption Standard (DES)***

The data encryption algorithm developed by IBM for NBS was based on Lucifer, and it became known as the Data Encryption Standard, although its proper name is DEA (Data Encryption Algorithm) in the United States and DEA1 (Data Encryption Algorithm-1) in other countries. In DES [4] the encrypting and decrypting algorithms are publicly announced; the security of the cryptogram depends entirely on the secrecy of the key and the key consist of randomly chosen, sufficiently long string of bits. This algorithm ensures that the output bits have no apparent relationship to the input bits and spreading the effect of one plaintext bit to other bits in the cipher text. Once the key is established between the sender and the receiver, subsequent communication involves sending cryptograms over a public channel which is vulnerable to total passive eavesdropping. However with the purpose of establishing the key between two users, who share no secret information initially, must at a certain stage of communication use a reliable and a very secure channel. A random key must first be send through a secret channel before the transfer of actual message. The major drawback of DES is that like other classical cryptographic mechanism it also cannot guarantee ultimate security of a communication channel.

***Public Key Cryptographic (PKC) Systems***

With a conventional symmetric key system, each pair of users needs a separate key. As the number of users grows, the number of keys increases very rapidly. An n-user system requires n * (n - 1)/2 keys, and each user must track and remember a key for each other user with which he or she wants to communicate. We can reduce the problem of key proliferation by using a public key approach. In a public key or asymmetric encryption system, each user has two keys: a public key and a private key. The user may publish the public key freely because each key does only half of the encryption and decryption process [3]. The keys would be inverse functions. If 'Alice' wants to send a secret message to 'Bob', he would encrypt his message with Bob's public key and send it via an insecure channel. 'Bob' receiving the message would then decode it using his private key. This methodology ensures that the sender can't decode his own message once encrypted. These systems make use of the fact that certain mathematical operations are simple to do in one direction than the other. For example, multiplication of two large prime numbers is easy but factoring the result would be infeasible if the number is large and computational assets are poor. RSA (Rivest-Shamir-Adleman encryption Algorithm), the first PKC cryptosystem [5] obtains its security from the straightforward fact that factoring of large numbers is extremely tough. The disadvantage of classical cryptosystem is that it provides no method for detecting eavesdropping. Also, with the building of feasible quantum computer Shor's algorithm could easily break RSA in polynomial time.

***One-time pad (OTP) Cryptosystem***

The one-time pad cryptosystem [6] created by Gilbert Vernam in 1917 is very simple and yet, very effective. The system ensures perfect secrecy. A one-time pad is sometimes considered as ideal cipher. The system is named after encryption method in which a large, non repeating set of keys is written on sheets of paper, attached together into a pad. For the encryption to work, the receiver needs a pad identical to that of the sender. The major disadvantage with one-time pad is even though its security it is very impractical. For every message encoded with the system, the participants have to to exchange a secret key that has at least the same length. The one-time pad method needs absolute synchronization between sender and receiver and no key should be used twice.

**Quantum Cryptography**

Quantum channel construction requires a pair of polarizing filters at both sender and receiver ends. So, that at sender end we can send photos of selected polarization and at receiver end to measure the polarization of photons. There are two types of polarization filters rectilinear and diagonal; in rectilinear filter we have horizontal and vertical orientation of photons whereas in diagonal we have 45 and 135 degree of orientation of photons. The two directions can be detected by vertically oriented calcite crystal and two detectors like photomultiplier. If the photon is horizontally polarized it will be directed to upper filter and to vertical detector if it is vertically polarized. If similar apparatus is rotated at 45 it will record diagonal directions. Thus the rotated apparatus is useless for rectilinear direction and vertical apparatus for diagonal direction .hence we cant measure both simultaneously thus verifying Heisenberg uncertainty principle.BB84 Protocol was developed by Charles H, Bennett of the IBM Thomas J. Watson Research Centre and Gilles Brassard of the University of Montreal, quantum cryptography is based on the fact that measuring a quantum system such as a photon irreversibly changes its state and wipes out information about the aspects before measurement [1]. It uses two channels-quantum by which Alice and bob send polarized photons second is classical public channel by which they send ordinary messages such as comparing and conferring the signals sent through quantum channel. In Quantum Key Distribution sequence of operations are as follow:-

First, Alice generates and forwards Bob a sequence of photons with polarizations that are chosen randomly (0, 45, 90 or 135 degrees). Bob receives the photons and chooses randomly whether to measure its rectilinear or diagonal polarization for each photon. Next Bob publicizes which kind of measurement he has made (either rectilinear or diagonal) but not the measurement result for each photon. Alice tells him openly, whether he has made the correct type of measurement for each photon. Alice and Bob then discard all cases in which Bob has made the incorrect measurement or in which his detectors have failed to record a photon.

| Bit sequence | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Alice logic sequence | 0 | 0 | 1 | 1 | 1 | 1 |
| After passing a polarizing filter | ↑ | ↖ | → | → | ↗ | ↗ |
| Bob's polarization states | ↑ | ↖ | ↖ | → | ↑ | ↗ |
| Bob's correct states tested by Alice | V | V | | V | | V |
| Quantum key | ↑ | ↖ | | → | | ↗ |

**Figure 1:** Sequence of operations

If none has eavesdropped on the quantum channel, the left over polarizations should be shared as secret information between Alice and Bob. Alice and Bob next test for eavesdropping, for example, by openly evaluating and discarding a randomly selected subset of their polarization data. If the evaluation shows proof of eavesdropping, Alice and Bob abandon all their data and start again with a fresh lot of photons. Otherwise they adopt the left over polarizations as shared secret bits, reading 0 or 45-degree photons as binary 0's and 90 or 135-degree photons as binary 1's. If she makes the incorrect measurement, then she resends Bob a photon reliable with the result of her measurement, she will have forever randomized the polarization originally sent by Alice for a particular photon, which causes errors in one fourth of the bits in Bob's data that have been subjected to attack since one has no information of Alice's secret choice, 50% of the time (probability 1/2) one will estimate exactly and 50% of the time (probability 1/2) one will estimate incorrectly. If one estimates exactly, then Alice's transmitted bit is received with probability 1. On the other hand, if one estimates wrongly, then Alice's transmitted bit is received correctly with probability 1/2[7]. Overall the probability of accurately receiving Alice's transmitted bit is

P=1.1/2+1/2.1/2=3/4

The BB84 scheme was customized to produce a working kit of quantum cryptography at IBM. The modifications were done to handle with practical problems like noise in the detectors. In BB84 scheme encoding is done as single polarized photon for each bit but this kit encodes each bit in a dim flash of light. This initiates a fresh eavesdropping danger to the system, if Eve taps into the beam; splitting each flash into two flashes of lesser intensity can be done, evaluating one for her while letting the other move to Bob. If Eve diverts only a meek fraction of the beam, Bob may not see the abating signal, or may take it as expected losses in the channel. This attack can be successfully let down by reducing data transmission rate, by sending very dim flashes of an intensity less than one photon per flash on average. Another problem is that available detectors for a moment produce a reaction even when no photon has been arrived which sources errors even when there has been no eavesdropping. An added fragile end is key storage. Once Alice and Bob have recognized the key, they must store it until it is required. But the longer they keep the key in, the more they are vulnerable to unauthorized check. It is possible to build a cryptosystem based on the well-known Einstein-Podolsky-Rosen (EPR) effect. Employing the EPR effect, Ekert recently developed a cryptosystem that gave assurance of security of both key storage and key distribution. It also cannot be used practically due to the technical infeasibility of stocking up photons for more than a tiny portion of a second [8].

**Classical V/S Quantum Cryptography**

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

***Fundamental dimension***

In theory, any classical private channel can be easily monitored inertly, without the knowledge to sender or receiver that the eavesdropping has been done. Classical physics is the theory of macroscopic bodies and phenomena such as radio signals that allows a physical property of an object to be measured without disturbing other properties. Cryptographic key like information is encoded in computable physical properties of some object or signal. Thus there is open possibility of passive eavesdropping in classical cryptography. Quantum theory which is basis of quantum cryptography is believed to direct all objects, but its consequences are mainly noticeable in individual atoms or subatomic particles like microscopic systems. As far as classical cryptography is concerned there is frequent requirement of using longer keys as computational power doubles in every 18 months and cost of computation is reducing rapidly with time [moors law]. Thus an algorithm using k bit key which is secure may not be secure in future, i.e. it needs regular updating. On the other hand,, security in quantum cryptography is based on the basic principles of quantum mechanics, so the possibilities of major changes requirements for future are almost negligible.

***Commercial dimensions***

Commercial solutions for QC that already exist; they are only suitable for point-to-point connections. On the other hand, crypto chip made by the siemens and Graz technical university [11] makes possible the creation of networks with many participants, and cost of €100,000 per unit, 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. Also, cryptographic system based on classical cryptography can be implemented on small hardware component like smart card , but this is major issue in case of quantum cryptography shrinkage to such a level require too much development.

***Application dimensions***

The digital signatures reveal the authenticity of the digital data to the receiver. A digital signature assures recipient that the message was formed by a known sender, and it was not changed in transit. The three main algorithms are key generation, signing, and key verification. But we know that

algorithms cannot be implemented in QC very easily. Therefore QC lacks many critical features like digital signature, certified mail etc.

***Technological dimensions***

Chinese scientists accomplished the worlds most long-distance of quantum communication transmission (teleportation), or as "instant matter transmission technology" technology. From the China University of Technology and researchers at Tsinghua University, Hefei National Laboratory in their free-space quantum communication experiments, and effectively enlarges the communication distance to 10 miles [9]. But classical cryptography can be used to communication distance of several million miles. According to the latest research, Toshiba achieve new record bit rate for quantum key distribution, that is, 1 Mbit/s on average [10]. On the other hand the bit rate of classical cryptography depends on the computational power largely.

***Other dimensions***

Communication medium is not an issue in classical cryptography because its security depends only on the computational complexity. Thus, this removes the need for excessively secure channels. On the other hand communication of quantum cryptography require a quantum channel like optical fiber or through air (wireless), also, there is constantly a likelihood of 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. Whereas an n-qubit quantum register can store at any moment a superposition of all $2^n$ n-bit strings.

**Comparison of Quantum and Classical Cryptography**

| **Features** | **Quantum cryptography** | **Classical cryptography** |
|---|---|---|
| Basis | Quantum mechanics | Mathematical computation |
| Development | Infantile & not tested fully | Deployed and tested |
| Existing Infrastructure | Sophisticated | Widely used |
| Digital Signature | Not present | Present |
| Bit rate | 1Mbit/s avg.[10] | Depend on Computing power |
| Cost | Crypto chip €100,000[11] | Almost zero |
| Register storage (n bit) at any moment | one n-bit string | $2^n$ n-bit strings |
| Communication Range | 10 miles max.[9] | Million of miles |
| Requirements | Devoted h/w & communication. lines | S/w and portable |
| Life expectancy | No change as based on physics laws | Require changes as computing power increases |
| Medium | Dependent | Independent |

**Conclusion**

Quantum cryptography is based on mixture of concepts from quantum physics and information theory. The security standard in QC is based on theorems in classical information theory and on the Heisenberg's uncertainty principle. Experiments have demonstrated that keys can be exchanged over distances of a few miles at low bit rate. Its combination with classical secret key cryptographic algorithms permits increasing the confidentiality of data transmissions to an extraordinary high level. From comparison, it's obvious that quantum cryptography (QC) is having more advantage than Classical Cryptography (CC) though some issues are yet to be solved. This is mainly due to the implementation problems but in future there exist possibilities that most of the problems in quantum cryptography will get resolved.

**Challenges & Future Direction**

In the future, enhancing the performance of practical QKD systems and further improvements, both in key rate and secure transmission distance, are necessary for some applications. Another vital point is that, in real life, that is, quantum signals may share the channel with regular classical signals. The final goal is to achieve a client affable QKD system that can be effortlessly included in the Internet. To achieve a higher QKD key rate, one can consider other QKD protocols. Continuous variable QKD is projected to get a higher key rate in the small and medium transmission distance. Still, the scalability is a big challenge, as no one knows how to build a large scale quantum computer, which is interesting subject to be worked out.

**References**


[1] C. Bennett and G. Brassard, in Proceedings of IEEE, International Conference on Computers, Systems.

[2] Hughes, Richard J., D.M. Alde, P. Dyer, G.G. Luther, G.L. Morgan, and M. Schauer, Quantum cryptography, Contemporary Physics, Vol. 36, No. 3 (1995).

[3] Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C (cloth) Author(s): Bruce Schneier.

[4] FIPS. 46-3, '"Data Encryption Standard," Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, US. Department of Commerce, Washington D.C., October 25, 1999.

[5] R.L. Rivest, "Dr. Ron Rivest on the Difficulty of Factoring," Cipher text: The RSA Newsletter, v. 1, n. 1, fall 1993, pp. 6-8.

[6] G. R. Blakley, "One Time Pads Are Key Safeguarding Schemes, Not Cryptosystems Fast Key Safeguarding Schemes (Threshold Schemes) Exist." , Proceedings of the 1980 IEEE Symposium on Security and Privacy, 1980, pp. 108-113.

**[7]** Charles H. Bennett, Gilles Brassard, and Artur K. Ekert "Quantum Cryptography", Scientific American 267:4, (October 1992).

**[8]** Einstein, A., B. Podolsky, N. Rosen, Can quantum,

mechanical description of physical reality be considered complete?, Phys. Rev. 47, 777 (1935).

**[9]** Quantum communication transmission experiments http://www.waybeta.com/news/10441/quotquantum-communication-transmissionquot-experiments-in-china-_-the-success-of-huawei-wireless-network-card-news/

[10] **Cambridge Lab of Toshiba** http://www.physorg.com/news191010509.html

**[11]** Affordable Quantum Cryptography http://www.siemens.com/innovation/apps/pof_microsite/_pof-spring-2009/_html_en/interview-christian-monyk.html