A Survey on Different Visions with Contrasting Quantum and Traditional Cryptography

S.C. Jain, PhD
Professor
Deptt. Of CSE
University College of Engineering, Kota
Rajasthan, India

Nitesh Chouhan
Assistant Professor
Deptt. Of IT
M. L. V. Govt. Textile & Engineering College, Bhilwara
Rajasthan, India

Hemant Kumar Saini
Adjunct Asst. Professor
Deptt. Of IT
M. L. V. Govt. Textile & Engineering College, Bhilwara
Rajasthan, India

ABSTRACT
Quantum cryptography is a knowledge that guarantees ultimate safety. Associated to present cryptography that might be overcome by the expansion of an ultra-high-speed computer, quantum cryptography safeguards secure message since it is founded on the important bodily laws. It is an emergent technology in which two parties may concurrently produce shared, secret cryptographic key substantial using the broadcast of quantum conditions of light. Quantum cryptography is a novel way for secret communications present the final security pledge of the holiness of a Law of Nature. The quantum cryptography conviction on two innermost rudiments of quantum technicalities-the Heisenberg Uncertainty attitude and the standard of photon partition[19]. This research paper distillates on the trust of quantum cryptography, and in what method this knowledge contribute to the system security. This paper tactics the real world demand procedure of this know-how and the future itinerary in which quantum cryptography hasten.

Keywords
Quantum cryptography; Classical cryptography; Polarization states.

1. INTRODUCTION
In the contemporary age of communications and the Internet, data has become a valuable product. Occasionally it must so be remain risk-free from stealing - in this casing, defeat of personal information to an eavesdropper. As much skin texture to security and several submissions, series from protected business and expenditure to private connections and defensive passwords. One important eye for protected transportations is that of cryptography [1] that not only shields data from larceny or modification, but can also be used for operator verification. The main goal of cryptography is to defend data moved in the probable attendance of an opponent's. A cryptographic modification of information is a progression by plaintext data is encrypted, succeeding in an tailored text, called cipher text, which do not portray the inventive input[19]. The cipher text can be dissimilar-misrepresented by a elected beneficiary so that the inventive plaintext can be summon up. The practices of cryptography are usually catalogs as established or contemporary. Outdated techniques use process of coding i.e. use of other words or phrases, reversal i.e. rearrangement of plaintext, and replacement i.e. Modification of plaintext characters). While, modern methods use computers, and be contingent upon tremendously long keys, intricate algorithms, and inflexible harms to reach assurance of security. There are two foremost turf of contemporary cryptographic means: Public key encryption [2] and Secret key encryption [1],[2]. A public-key encryption, where a communiqué is encrypted with a recipient public key. The announcement cannot be decrypted by anybody who does not possess the matching private key[19], who is thus supposed to be the proprietor of that key and the person related through the public key. A covert key is an encryption key identified only to the assembly or revelry that dialogue clandestine message. The danger in this system is that if moreover party loses the important or it is stolen, the scheme is wrecked. The growth of quantum cryptography was fortified by the inadequacies of traditional cryptographic methods, which can be alienated as whichever "public-key" or "secret-key" advances. Quantum cryptography is a method to a cryptography founded on the rules of quantum physics.

2. HISTORICAL TIMELINE
In 1917, Gilbert S Vernam, created a engine that brands a non-repeating, almost arbitrary arrangement of characters called as one-time pad. Using an encryption key the similar distance as the communication and not ever by means of that key over is the only established technique of firmly interactive. In the 1940s, Claude Shannon delivered the information-theoretic secrecy; the amount of indecision encoded message to encode it. Later on 1970s, numerous investigators, including Whitfield Diffie, Martin Hellman, Ralph Merkle, Ron Rivest, Adi Shamir, Leonard Adleman, James Ellis, Clifford Cocks, and Malcolm Williamson, invented cryptographic methods grounded on computational difficulty. Quantum cryptography was first proposed in 1984 by Brennet[3] and Brassard based on the No-Cloning theorem. It trusts on datum that itshould base security on known physical laws not on accurate difficulties.

2.1 Classical Cryptography
Classical cryptography use of some mathematical methods to bound spectators after expressive the contents of prearranged messages. The utmost general between them that are putative globally have been labeled below. Over the paper, the propagator is scheduled as 'Alice', the receiver as 'Bob', and an eavesdropper as 'Eve'[18].

2.1.1 Data Encryption Standard (DES)
The data encryption algorithm developed by IBM was founded by Lucifer, and it became Data Encryption Standard, though 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 openly proclaimed; the safety of the cypher be contingent completely on the clandestineness of the key and the key consist of arbitrarily chosen, adequately long thread of minutes. This procedure spreading the result of one plaintext bit to other bits in the cipher text[18]. Once the key

is recognized between the sender and the receiver, following announcement comprises transport cryptograms over a public channel which is defenseless to total submissive snooping. Yet the drive of founding the important between two users, that part undisclosed information originally, must at a sure phase of message use a reliable over secure channel. A chance key must first be direct through a secret channel beforehand the transmission of real message. The major disadvantage of DES is that like other traditional cryptographic apparatus it also cannot pledge eventual security of a message channel.

2.1.2 Public Key Cryptographic (PKC)

Systems with a traditional symmetric key method, every couple of users' requirements a separate key. As the amount of buyer create, the quantity of keys increase very rapidly. An n-user scheme requires n * (n - 1)/2 keys, and each client have to trail and bring to mind a key for every extra client with that it wants to join[5]. It can decrease the crisis of key proliferation by using a public key advance. In a public key or asymmetric encryption arrangement, every user has two keys: a public key and a private key. The consumer may bring out the public key freely since every key do only semi of the encryption and decryption method. The disadvantage of classical cryptosystem is that it delivers no technique for perceiving snooping. Also, with the structuring of viable quantum computer Shor's algorithm could effortlessly break RSA in polynomial time[6].

3. QUANTUM CRYPTOGRAPHY

Quantum channel structure needs a pair of separating sieves at both sender and receiver ends. So, that at sender can selected polarization and at receiver end to measure the polarization of photons. There are two types of polarization filters rectilinear and diagonal; in rectilinear sieve horizontal and vertical site of photons while in slanting it have 45 and 135 degree of location of photons. The two directives can be noticed by vertically concerned with calcite crystal and two sensors like photomultiplier. If the photon is straight polarized it will be absorbed to higher filter and to perpendicular sensor if it is vertically separated. If alike apparatus is alternated at 45 it will record slanting directions. Thus the alternated gadget is unusable for rectilinear track and vertical gadget for diagonal directive .henceforward cannot amount both concurrently thus confirming Heisenberg uncertainty principle[8]. 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 wipe out information about the features before dimension .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[13]. In Quantum Key Distribution arrangement of processes are - First, Alice generates and onward Bob a order of photons with divisions that are selected arbitrarily (0, 45, 90 or 135 degrees). Bob obtains the photons and selects arbitrarily so as to amount its straight-lined or slanting polarization for each photon. Following Bob broadcasts measurement it has made (either rectilinear or diagonal) .Alice tells him amenably, whether it correctly build. If none has snooped on the quantum network, the missing over divergences shared as privileged data between both. Alice and Bob next test for eavesdropping, for example, by openly evaluating and discarding a randomly selected subset of their polarization data. If she makes the incorrect measurement, then she resends Bob a photon dependable with the consequence of her dimension, she will have incessantly randomized the polarization first sent by Alice for a precise photon, which grounds errors in one quarter of the bits in Bob's data that have been exposed to outbreak subsequently one has no information of Alice's clandestine choice, 50% of the time (probability 1/2) one will guesstimate exactly and 50% of the time (probability 1/2) one will approximation incorrectly. If one approximations exactly, then Alice's conveyed bit is established with chance 1. On the other hand, if one approximations incorrectly, then Alice's conveyed bit is received properly with chance 1/2. Overall Alice's transmitted bit is P=1.1/2+1/2.1/2=3/4 The BB84 scheme was modified to crop a employed kit of quantum cryptography at IBM. The changes were done to knob with everyday problems. Another problem is that obtainable sensors for an instant produce an answer even once no photon has been indoors which foundations faults even type of measurement for apiece photon. Alice and Bob formerly reject all cases in which Bob has ended the inappropriate extent or in which his sensors partake disastrous to record a photon after there has been no snooping. A supplementary breakable end is key storage. It also cannot be used almost due to the practical infeasibility of keeping up photons for additional than a tiny helping of a second [8]..

3.1 Quantum Computing

Quantum calculating uses a important information component, the significant bit or 'qubit,'[1] diverse from classical processors, which use the 'bit', a reasonable unit grounded on whether an electrical signal is off or on done a pathway. Distinct classical adding, wherever each bit covers only one of two possible values [7], each qubit is in a incessant variety between '1' or '0' and a scheme of qubits grip *each* set of standards in apiece qubit. Figure 1 demonstrations a contrast between the standards in a bit and a qubit.

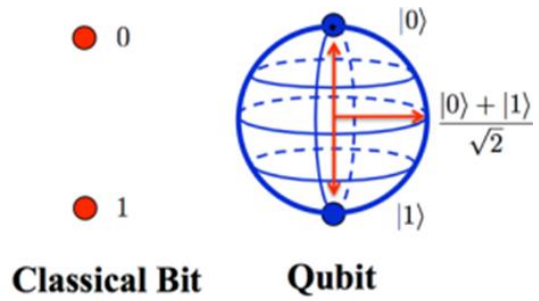

Fig 1. Comparison of classical and quantum bits

3.2 Quantum Key Distribution

Individually photon transmits one "qubit" of info. Division can be used to signify a 0 or 1. A handler can propose a key by distribution a stream of arbitrarily polarized photons. This arrangement can be transformed to a binary key. If the key was interrupted it could be rejected and a new watercourse of aimlessly polarized photons sent[9]. This procedure, recognized as BB84 after its discoverers and year of journal, was initially labeled using photon divergence conditions to convey the data. Now the stages as shown in Fig.2 whose procedure are as follows.

1 Alice connects with Bob via a quantum network sending him photons.
2 Then they deliberate consequences using a public network.

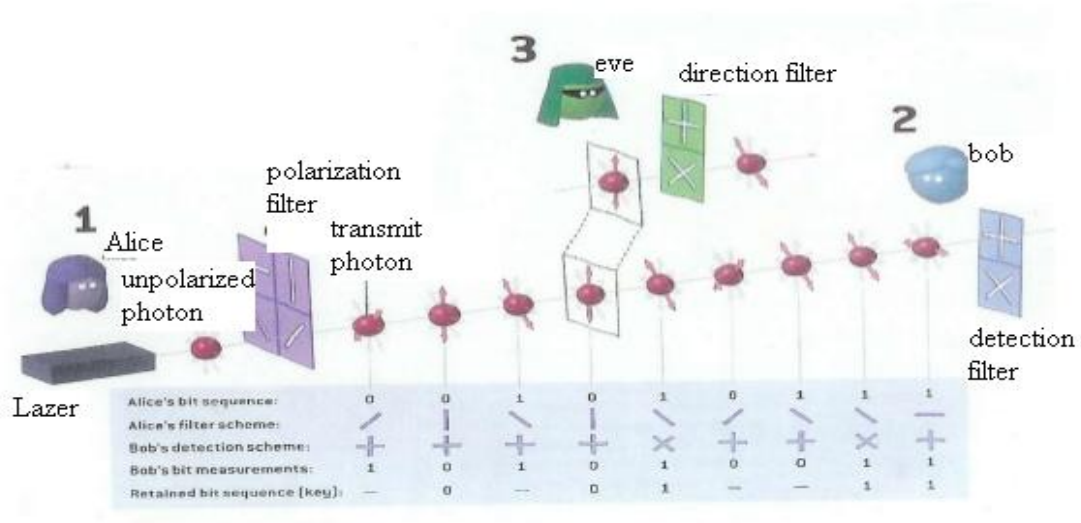

Fig.2 Quantum Communication

3 After getting an encryption key Bob can encrypt his messages and send them by any public channel.
4 One with the 0-90 degree basis and one with 45-135 degree basis.
5 Alice uses her polarizer's to send randomly photons to Bob in one of the four possible polarizations 0, 45, 90,135 degree.
6 Bob uses his polarizer's to measure each polarization of photons he receives.
7 He can use the basis or but not both simultaneously.

The quantum cryptography will put to applied use on numerous seats like ATN, video conferencing, finance and life science, which required progressive information security [10]

3.3 Mechanics of Quantum Cryptography

The quantum cryptography varies on two vital mechanisms of quantum workings-the Heisenberg doubt standard and the standard of photon division [3]. The Heisenberg doubt main beliefs state that, it is not possible to decide the quantum situation of any scheme without distributes so as to scheme. The hypothesis of photon polarization states that, an eavesdropper not copy unidentified qubits i.e. indefinite quantum state, due to no-clone theorem which was first introduced by Wootters and Zurek in 1982. Varying on the hypothesis of physics [4], quantum cryptography do not create it likely to eavesdrop on transmit in order. It is attract substantial notice as a stand-in for other current cryptographic method, that are base on computational safety. Quantum cryptographic broadcast coded the 0s and 1s of a digitized on entity of beam called photons. By difference, current optical communication expresses the 0s and 1s of the digitized since the power and flaw of light correspondingly.

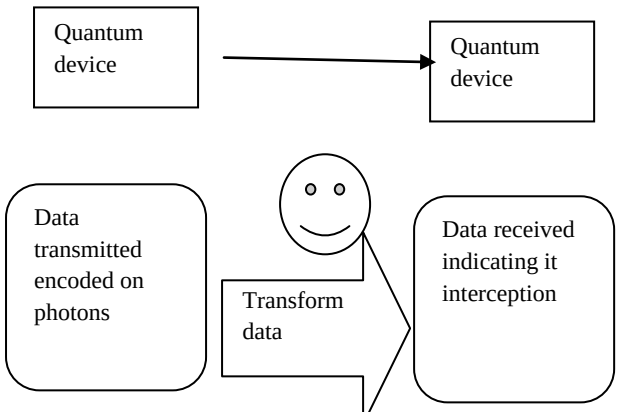

Fig.3 Quantum Cryptography

For the reason that the physically powerful and weak light are complete up of thousands of photons that every communicate the same in order, if more than a few photons are stolen (i.e., the signal is eavesdropped on) during transmission, it is not detect. Alternatively, in the container of quantum cryptography, if an unknown user notices (eavesdrop on) the signal, the in turn on the photons is unexpectedly as overhear something has appear and the third revelry is not talented to decrypt the in turn.

Indestructible scenery of Quantum Cryptography use the current acquaintance of physics to expand a cryptosystem that is must not be beaten - namely single that is wholly protected next to being compromise devoid of information of the correspondent or the recipient of the communication. Quantum communiqué occupy programming in sequence in quantum state, or qubits, in distinction to conventional communications utilize of bits. Frequently, photons are hand-me-down for this quantum state. Quantum key division is only used to construct and allocate a key, not to convey a few communication facts. This solution can afterward be worn with any preferred encryption algorithm to encrypt (and decrypt) a message, that can followed by be transmit more a normal message channel. Quantum cryptography obtain its basic security from the fact that each qubit of information is carried by a single photon, and that each photon will be altered as soon as it is read once. Any attempt to intercept message bits can be easily detected as shown in Fig.3.

4. BB84 PROTOCOL

This protocol was proposed by Bennett and Brassard in 1984 [5] and hence named as BB84. This was the first protocol planned to use photons for secure data transmission over the network. As per this protocol any two conjugate state pairs can be used by two parties for information exchange using photons on optical communication channel. This protocol uses

two main steps the quantum state transmission step and the classical post processing step as discussed in [14].

A comparison of various protocols proposed in quantum cryptography, in tabular form is shown in table-1.

Table 1: History of QC protocols

Year	Principles	Applications	Name of protocol
1984	Heisenberg Uncertainty Principles	Photon Polarization state is defined in it.	BB84
1991	Quantum Intertwined	Intertwined photons were used in place of polarization.	E91
1992	Heisenberg Uncertainty Principles	only two states compulsory instead of four polarization states.	BB92
1999	Heisenberg Uncertainty Principles	It has 6 states: ±x, ±y, ±z on the Poincare sphere, as there were only four in BB84.	SSP
2003	Quantum Entanglemen	It is simple in configuration, has efficient time domain use and it shows robustness against Photon Number Splitting attack.	DPS
2004	Heisenberg Uncertainty Principles	It becomes more robust if attenuated laser pulses are used instead of single photon sources. It provide more security than BB84 against of Photon Number Splitting attack.	SARG04
2004	Quantum Entanglemen	Able to work when there are high bit rates of weak coherent pulses. This can reduce PNS attack	COW
2009	Heisenberg Uncertainty Principles	In this two parties used two bases: one for encoding „0 and the other for encoding „1‟ instead of using two direction of one single base	KMB09
2012	Public private key cryptography	Hard to implement as there are many exchange cycles of qubits among users. It can distribute keys among n number of systems and one key message distribution centre. As no classical channel are used do it is secure fro Man-In-The-Middle attacks	S09
2013	Heisenberg Uncertainty Principles	Uses random seed. it has zero information loss. Differs only in the classical procedure, as compared to BB84.No need of hardware upgrade for implementation.	S13

5. CLASSICAL VS QUAMTUM CRYPTOGRAPHY

Both quantum cryptography and classical cryptography can be compared as depicted in Table 2 on following dimensions:

5.1 Fundamental Dimension

In theory, any traditional private channel can be effortlessly checked inertly, deprived of the information to sender or receiver that the snooping has been done. On the other hand,, security in quantum cryptography is based on the basic principles of quantum mechanics, so the potentials of chief changes necessities for future are virtually insignificant

5.2 Commercial Dimension

Commercial solutions for QC that previously exist; they are only appropriate for point-to-point connections. But this is main issue in case of important cryptography reduction to such an equal necessitate too much progress

5.3 Applicative Dimension

Table 2: Comparison of Quantum vs 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
Cost	1Mbit/s avg.[10]	Depend on Computing power
Register storage (n bit) at any moment	Crypto chip €100,000[11]	Almost zero
Communication Range	one n-bit string	2n n-bit strings
Requirements	10 miles max.[9]	Million of miles
Life expectancy	Devoted h/w & communication. lines	S/w and portable
Medium	Dependent	Independent

The digital signatures disclose the genuineness of the numerical data to the receiver. A digital signature promises receiver that the communication was shaped by a known sender, and it was not different in transit. The three main procedures are key generation, validation, and key confirmation. But it know that algorithms cannot be realized in QC very easily. Therefore QC lacks many critical features like digital signature, certified mail etc[16].

5.4 Technological Dimension

Quantum cryptography is based on combination of ideas from quantum physics and information theory. The safety normal in QC is based on propositions in traditional information theory and on the Heisenberg's indecision principle [17].

Tests have confirmed that answers can be replaced over reserves of a few heaps at low bit rate. Its amalgamation with conventional top-secret key cryptographic algorithms licenses growing the privacy of data broadcasts to a strange high level.so, it's obvious that quantum cryptography (QC) is having more benefit than Classical Cryptography (CC) however few issues are yet to be resolved.

6. CONCLUSION

Quantum cryptography is based on combination of ideas from quantum physics and information theory. The safety normal in QC is based on propositions in traditional information theory and on the Heisenberg's indecision principle. Tests have confirmed that answers can be replaced over reserves of a few heaps at low bit rate. Its amalgamation with conventional top-secret key cryptographic algorithms licenses growing the privacy of data broadcasts to a strange high level.so, it's obvious that quantum cryptography (QC) is having more benefit than Classical Cryptography (CC) however few issues are yet to be resolved.

7. FUTUE DIRECTION & CHALLENGES

In the future, improving the presentation of applied QKD systems and additional developments, both in key frequency and secure spread space, are compulsory for some applications. Another vital point is that, in real life, that is, quantum gestures part the channel with steady traditional signals. The concluding area is to attain a client genial QKD system that can be naturally comprised in the Internet. To attain a higher QKD key rate, one can reflect other QKD protocols. Incessant variable QKD is predictable to get a higher key rate in the minor and average broadcast distance. Still, the scalability is a big quiz, as none distinguishes how to shape a great gauge quantum computer, which is stimulating subject to be functioned out

8. 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.

[5] 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.

[6] Tan, Xiaoqing. "Introduction to quantum cryptography." Theory and Practice of Cryptography and Network Security Protocols and Technologies, ISBN (2013): 978-953.

[7] Wheeler, John Archibald, and Wojciech Hubert Zurek, eds. Quantum theory and measurement. Princeton University Press, 2014.

[8] Chung, Yu Fang, Zhen Yu Wu, and Tzer Shyong Chen. "Unconditionally secure cryptosystems based on quantum cryptography." Information Sciences 178.8 (2008): 2044-2058.

[9] Singh, Hitesh, et al. "Quantum Key Distribution Protocols: A Review." Journal of Computational Information Systems 8.7 (2012): 2839-2849

[10] Zhao, Yi, et al. "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems." Physical Review A 78.4 (2008): 042333

[11] Wiechers, Carlos, et al. "After-gate attack on a quantum cryptosystem." New Journal of Physics 13.1 (2011): 013043.

[12] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt Ch, Makarov V and Leuchs G, 2011, Aftergate attack on quantum cryptosystem, New Journal of Physics 13, 013043.

[13] NIST: Hark! Group Demonstrates First Heralded Single Photon Source Made from Silicon http://www.nist.gov/cnst/herald-062712.cfm.

[14] Hwang, Won-Young. "Quantum key distribution with high loss: Toward global secure communication." Physical Review Letters 91.5 (2003): 057901.

[15] Johny, Shiji, and Anil Antony. "A Review on BB84 Protocol in Quantum Cryptography.

[16] Rubya, T., N. Prema Latha, and B. Sangeetha. "A survey on recent security trends using quantum cryptography." IJCSE 2.9 (2010): 3038-3042

[17] Lo, Hoi-Kwong, and Yi Zhao. "Quantum cryptography." Encyclopedia of Complexity and Systems Science (2009): 7265-7289.

[18] Teja, V.; Banerjee, P.; Sharma, N.N.; Mittal, R.K., "Quantum cryptography: State-of-art, challenges and future perspectives," in Nanotechnology, 2007. IEEE-NANO 2007. 7th IEEE Conference on , vol., no., pp.1296-1301, 2-5 Aug. 2007. doi: 10.1109/NANO.2007.4601420

[19] Miss. Payal P. Kilor, Mr.Pravin.D.Soni," Quantum Cryptography: Realizing next generation information security", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014 .ISSN 2319 – 4847.