ISSN:0975-9646



# Current Refuge Trends using Classical and Quantum Cryptography

**Rohit Kumar**
*Department of Computer Science*
*Sharda University*
*Greater Noida, India*

**Ritika Chugh**
*Assistant Professor*
*Department of Computer Science*
*Sharda University*
*Greater Noida, India*

**Samudra Gupt Maurya**
*Department of Computer Science*
*Sharda University*
*Greater Noida, India*

**P.V. Manoj**
*Department of Computer Science*
*Sharda University*
*Greater Noida, India*

**Abstract: Cryptography is the knowledge of keeping private information from unofficial access of ensuring data integrity and endorsement, and it is the strongest tool for scheming against much category of security threats. Role of cryptography appears in several secured area like government agencies, large banks, telecommunications companies and additional corporations who handle sensitive or military data. Quantum cryptography is a capable technology in which two revelries may simultaneously generate mutual, secret cryptographic key material expending the transmission of quantum states of light. This paper consists of the foremost aspects of quantum cryptography and it considers the information about where and all quantum cryptography proceeds place.**

*Keywords: Classical cryptography, Quantum cryptography, Quantum protocols, BB84, B92, Quantum key distribution, QKD*

## I. INTRODUCTION

The behavior of quantum cryptography opens a entrance to tremendously intriguing possibilities for cryptography, the art and science of communicating in the occurrence of adversaries [1,2]. Interesting appearances of quantum mechanics include the existence of inseparable quanta and of entangled systems, both of which lie at the basis of quantum cryptography (QC). QC is one of the few salable applications of quantum physics at the single quantum equal.

Other requests of quantum mechanics to cryptography, which tend to originate in three flavors:

- Quantum mechanics can be castoff to break classical cryptographic protocols (as with quantum factoring).
- Quantum states can make probable new or improved cryptographic protocols keeping classical information (as with quantum key distribution or unalienable encryption).
- Cryptographic methods can be practical to protect quantum information as a substitute of classical information. Examples would include quantum underground sharing schemes and quantum substantiation protocols.

We investigate the alterations between classical cryptographic techniques and quantum cryptography, as well probable advantages and applications of each. In section 2, we present attributes of classical cryptography and its transformation with quantum cryptography and Section 3 summarizes Quantum Key distribution and Quantum Entanglement. Section 4 describes the quantum cryptographic protocols, eavesdropping, and we achieve with a discussion on the recent progress and quantum crypto network debuts.

## 2. CLASSICAL CRYPTOGRAPHY

Cryptography is the art of transcription a message unintelligible to any unconstitutional party. Although confidentiality is the outdated application of cryptography, it is used nowadays to accomplish broader objectives, such as substantiation, digital signatures [10].

To accomplish this goal, an algorithm (also termed as cryptosystem or cipher) is used to combine a message with some added information (known as the key) and yield a cryptogram. The primary submission of cryptography is to send surreptitious messages.

Many cryptographic systems are centered on computational assumptions. Decrypting is comparable to solving some computationally problematic problem, one that cannot be rejoined in polynomial time in some refuge parameters. The central difficult in cryptography is the key distribution problem, for which there are fundamentally two solutions: one based on mathematics, classical cryptography, and one constructed on Physics (quantum cryptography). While conventional cryptography relies on the computational effort of factoring large integers, quantum cryptography relies on what we consider to be the universal laws of quantum mechanics.

These classical cryptosystems originated in two flavors: symmetric systems, and asymmetric systems [6]. The security of public key cryptosystems is constructed on computational complexity. The indication is to use mathematical objects called one-way functions. So far, no one has showed the existence of any one-way purpose with a trapdoor; so, the existence of secure irregular cryptosystems is not proven. This positions a serious threat to these cryptosystems. For instance, an instantaneous breakthrough in mathematics could make electronic money suddenly worthless. To limit such economic and social

risks, there is no unusual but to turn to symmetrical cryptosystems. QC has a role to play in such substitute systems.

*Secret key cryptography*

- Requires confident channel for key distribution
- In opinion every classical channel can be monitored passively
- Security is mostly based on difficult non proven algorithms

*Public key cryptography*

- Security is based on non-demonstrated mathematical assumptions (e. g. in RSA cipher, effort of factoring large numbers)
- Break through renders messages apprehensive retro actively

## 3 QUANTUM KEY DISTRIBUTION PROTOCOL - BB84 PROTOCOL

While Wiesner's idea was unique, it would be difficult to contrivance. Others would later adjust the use of non-orthogonal states to speak the problem of key establishment, spawning the study of quantum key distribution (QKD). For all of the protocols defined below, we use the same setup. Alice and Bob portion an insecure, possibly noisy, quantum channel and a public, but authenticated, classical channel. Eve can cooperate freely with the quantum channel, removing or shifting the qubits at will.

While access to the information on the classical channel, she cannot change these messages or send messages impersonating Alice or Bob. The quantum protocols are said to have absolute security. The term can be misleading since there are "conditions" such as the authenticated classical channel. Furthermore, QKD protocols are definite with high probability. Thus, with some probability, still exponentially small, Eve will be able to learn information. Nonetheless, the term unqualified is used in literature and will be used here. A common criticism of QKD is the necessity of an authenticated classical channel. Authentication, certifying that people are who they claim to be, is a non-trivial issue [7].Yet, without it, QKD protocols are defenseless to man-in-the-middle attacks.

In these attacks, Eve could impersonate Alice and Bob to each other, allowing her to decipher their communication. It is worth noting that classical key establishment schemes are vulnerable to the same attack. A well-known authentication scheme using hash functions was developed by Mark Wegman and Larry Carter in 1981 [8]. Quantum Cryptography Background 23tication key and fails with a probability that is exponentially small in the size of the key. Unfortunately, as with the one-time pad, it raises the issue of how the parties establish the key. Wegman-Carter authentication schemes work well in conjunction with QKD because newly generated key bits can be used for authentication, which subsequently allows for the generation of more key bits2. To start the protocol, we might assume that Alice and Bob share a small authentication key. In this sense, QKD is sometimes thought of as quantum key expansion (QKE).

Each photon carries one "qubit" of information. Polarization can be used to characterize a 0 or 1. A user can applaud a key by sending a stream of randomly polarized photons. This classification can be converted to a binary key. If the key was interrupted it could be discarded and a new stream of erratically polarized photons sent. This protocol, known as BB84 after its inventors and year of periodical, was originally described using photon polarization states to diffuse the information. However, any two pairs of conjugate states can be used for the protocol, and many optical fibre based implementations defined as BB84 use phase encoded states

Now the steps of the protocol are as follows.

- ✓ Alice communicates with Bob via a quantum channel conveyance him photons.
- ✓ Then they converse results using a public channel.
- ✓ After receiving an encryption key Bob can encrypt his messages and conduct them by any public channel.
- ✓ One with the 0-90 degree basis and one with 45¬135 degree basis.
- ✓ Alice uses her polarizer's to send randomly photons to Bob in one of the four possible polarizations 0, 45, 90,135 degree.
- ✓ Bob uses his polarizer's to measure each polarization of photons he receives.
- ✓ He can use the basis or but not both instantaneously.

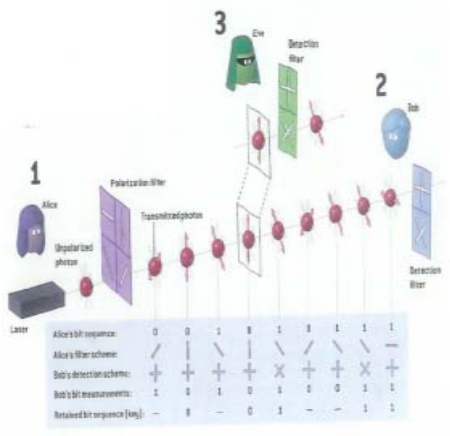


Fig Quantum Communication

The quantum cryptography will put to concrete use on many places like ATN, video conferencing, economics and life science, which required advanced information security [12].

## 4. QUANTUM CRYPTOGRAPHIC PROTOCOLS

Recent interest in quantum cryptography has been motivated by the fact that quantum algorithms, such as Shor's algorithms for integer factorization and detached logarithm [9], threaten the security of classical cryptosystems. A range of quantum cryptographic protocols for key distribution, bit assurance, oblivious transfer and other problems [10] have been extensively studied. Furthermore, the enactment of quantum cryptographic protocols has turned out to be expressively easier than the implementation of quantum algorithms.

Quantum cryptographic protocols are considered with the intention that their security is definite by the laws of quantum physics. Naturally it is necessary to prove, for any certain protocol that this is indeed the case. The most notable result in this area is Mayer's proof [3] of the absolute security of the quantum key distribution protocol "BB84" [12]

This proof guarantees the security of BB84 in the occurrence of an attacker who can perform any procedure allowed by quantum physics; hence the refuge of the protocol will not be compromised by imminent developments in quantum computing. Mayer's results, and others of the same kind [4,3], are enormously important contributions to the study of quantum cryptography.

However, a mathematical proof of the security of a protocol does not in itself assurance the security of an effected system which relies on the protocol. Experience of classical cryptography has shown that, through the progression from a faultless protocol to an implementation, many security dimness can arise. For example: the system might not correctly instrument the desired protocol; there strength be security flaws which only perform at the implementation level and which are not detectable at the level of generalization used in proofs; problems can also ascend at boundaries amongst systems and between components which have dissimilar execution models or data representations.

Quantum cryptographic systems must be evaluated at a level of detail that is closer to a practical implementation. Computer scientists have established a range of techniques and tools for the analysis and authentication of communication systems and protocols. Those mostly relevant to security analysis are measured by Ryan et al. [7]. This approach has two key features. The first is the use of formal languages to indeed specify the behavior of the system and the properties which it is unescapable to satisfy. The second is the use of automated software tools to either verify that a system satisfies a description or to discover flaws.

There are classical solutions to anxious communication all rely on making some sort of hypothesis, 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 influence allow us to weaken or remove these assumptions. For illustration, it is possible to make a quantum digital mark, which is secure against all attacks allowed by quantum mechanics.

Many classical cryptographic protocols work by erection up the protocol from simpler protocols. Two particularly suitable simple protocols are Authentication of quantum messages [8] and the other called bit commitment. Standard classical cryptographic protocols for bit commitment rely on Bob having limited computational power. For a while, it was thought quantum bit obligations protocols existed which were unconditionally secure. However, it turns out that if Alice and Bob have quantum computers, any protocol for which Bob cannot regulate the value of Alice's bit allows Alice to safely change the bit without Bob finding out. This was a great frustration, and later results proved that many other quantum cryptographic protocols were also difficult. However, there are still a number of possible protocols that have not been ruled out, including some of considerable interest. Quantum computation may allow us to accomplish some of these operations more safely than any classical protocol.

## 5 CONCLUSIONS

Hence quantum cryptography is a new technology; it is unpredictably easy to integrate. The last three years have seen studied advances in experimental quantum cryptography systems and several companies have established quantum cryptography prototypes because it is uncompromisingly secure key distribution, faster key refresh rate (than customary approaches), truly random key generation, unreserved eavesdropping protection, proactive interference detection, lower total cost of ownership, future proof security, speedy set-up, with virtually zero conservation. Thus Quantum cryptography promises to modernize secure communication by providing security based on the essential laws of physics, instead of the current state of mathematical algorithms or computing technology.

## REFERENCES


[1] Gabor Erde Lyi, Tim Meyer, Tobias Riege, And Jo Rg Rothe Quantum Cryptography: A Survey Dagmar Bruss, ACM Computing Surveys, Vol. 39, No.2, Article 6, Publication date: June 2007

[2] ICAO, "Manual of technical provisions for the aeronautical telecommunications network (atn) - standard and recommended practices (sarps)," Mars 2001.

[3] B. Witulski, "Key management," in Presentation at DLK Users Forum, Brussels, Belgium, June 1995.

[4] J.McMath,"Aeronautical telecommunication network(atn): Security, key management and distribution security, key management and distribution,"in AEEC Data Link Users Forum and ESC/GAD, Titan Corporation, Public Release: 03-0052 edition, Hanscom, MA, USA, February 2003.

[5] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp.175-179.

[6] C. Bennett, F. Bessettee, G. Brassard, L. Salvail, and J. Smolin,"Experimental quantum cryptography," September 1991.

[7] N. Gisin and al, "Quantum cryptography," Reviews Modern Physics,vol. 74, pp. 145-195, January 2002.

[8] C. Elliott, "Building the quantum network," BBN Technologies (USA), June 2002.

[9] M. D. Dang and M. Riguldel, "Usage of secure networks built usingquantum technology," 2004.

[10] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptographycriterion," Submitted to Electronics Letters, 2004.

[11] W. T. Buttler and al, "Practical free-space quantum key distribution over 1km," Phys. Rev. Lett., vol. 81, pp. 3283-3286, 1998

[12] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night,"New Journal of Physics, vol. 4, pp. 43.1-43.14, 2002.

[13] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity,and H. Weinfurter, "Long distance free-space quantum cryptography,"In New Journal of Physics, vol. 4, pp. 43.1-43.14, 2002.

[14] Elliott, Chip. "Quantum Cryptography", IEEE Security & Privacy, 2004

[15] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," September 2002.

[16] D. Mayers, "Unconditional security in quantum cryptography," JACM, vol. 48, no. 3, pp. 351-406, May 2001.
[17] H. Inamori, N. L'utkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," July 2001.
[18] Quoc-Cuong Le, Patrick Bellot "Enhancement of AGT Telecommunication Security using Quantum Cryptography" published in IEEE Research, Innovation and Vision for the Future International Conference. pp .7 - 16, Feb 2006.
[19] H.-K. Lo, "Communication complexity and security of quantum key distribution," April 2004.
[20] H.-K. Lo and H. Chau, "Unconditional security of quantum key distribution over abitrarily long distance," Science, pp. 2050-2056, 1999.
[21] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," April 2004.
[22] C. Guenther, "The relevance of quantum cryptography in modern cryptographic systems," December 2003.
[23] P. Bellot, M. D. Dang, and H. Q. Nguyen, "A new authentication scheme for quantum key distribution," 2004.