(IJIEST) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

LEVERAGING QUANTUM CRYPTOGRAPHY IN ENHANCING DATA TRANSMISSION SECURITY IN CONTENT DELIVERY NETWORK

Jahnvi Gupta
Student, University Institute of Engineering and Technology, Panjab University, Chandigarh, India

ABSTRACT

Security is necessary for the web and system user. In quantum cryptography, it uses material science law for key generation. It is a circumstance and application-specific cryptography method. The cryptography technique separates the main features and encrypts the data, and enhances the key generation algorithm using cryptography. The decryption key is used at the authentic side for data decryption. There are particular methodologies for the key generation that are examined in this paper. The paper moreover researched the development of the quantum key presentation for key generation and encoding.

I. INTRODUCTION

Cryptography ensures that it will generate the passage and communication level security by encoding the information. The cryptography method moreover provides secure communication. To keep the data more secure, it is mandatory to transmit the data in private. The particular key cryptography saves the data to the authentic user. As security is necessary when information goes accessible, cryptography is done to improve the safety, staunch quality, generosity, and reasonability of cryptography methodologies. The whole cryptography measure is distributed into three central stages. The cryptographic key is being shared in the primary stage. The sender side generates these keys. For both the end, there is a common key or a single key for encryption and decryption. The accompanying task is to share the key to an authentic person once the key is generated. Conspicuous sharing strategies are described for key movements. The key dispersal is either constrained by the sender, fused control or the pariah. The last stage is to use key cryptography while sharing the key and make the communication more secure.. The key build encoding is performed on the sender side, and concerning the beneficiary side, the key-based translating is performing. The actual encoding and translating measure shows up in figure 1.

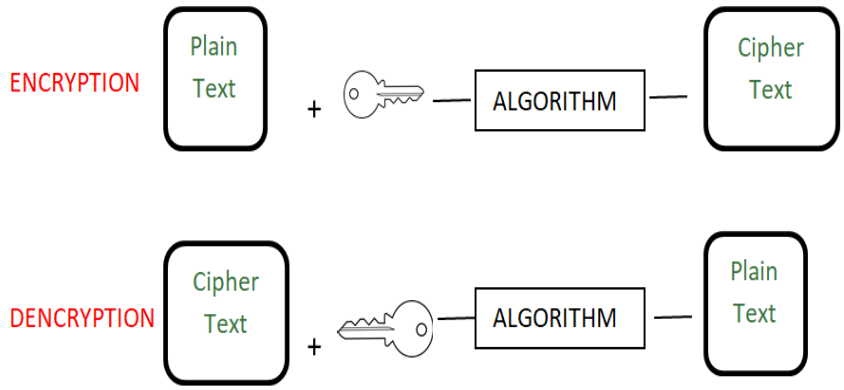

Fig 1: Encryption based on Key

Different experts give different cryptography and methodology level courses of action. A winner among the best cryptography methodologies is a quantum cryptography procedure. The detailed cryptographic system is elaborated in the below section.

II. RELATED WORK

A) Cryptography based on Quantum

The quantum channel based correspondence is performed utilizing the quantum cryptography technique. The figure illustrates that the encryption method is formed with a quantum placed together generator on the sender side on the plain substance to apply information encoding. Information is related to a quantum state finder to dispose of the hidden key on the beneficiary side. The encoded study about this key, the unwinding calculation, is identified with restricting the text back. The work shows can give certain encoded correspondence in authentic conditions. The system ensures the confirmation method with the principle messages course of action. The methodology associated with the quantum cryptography strategy against the gossip shows up in figure 2. The figure explains that the encryption structure is worked with a quantum put together generator on the sender side on the plain substance to apply information encoding. The quantum channel based correspondence is performed utilizing the quantum cryptography technique. The encoded thinking about this key, the unwinding calculation, is identified with confining the substance back. Information is related to a quantum state finder to dispose of the shrouded key on the beneficiary side. The work shows can give certain encoded correspondence in authentic conditions.

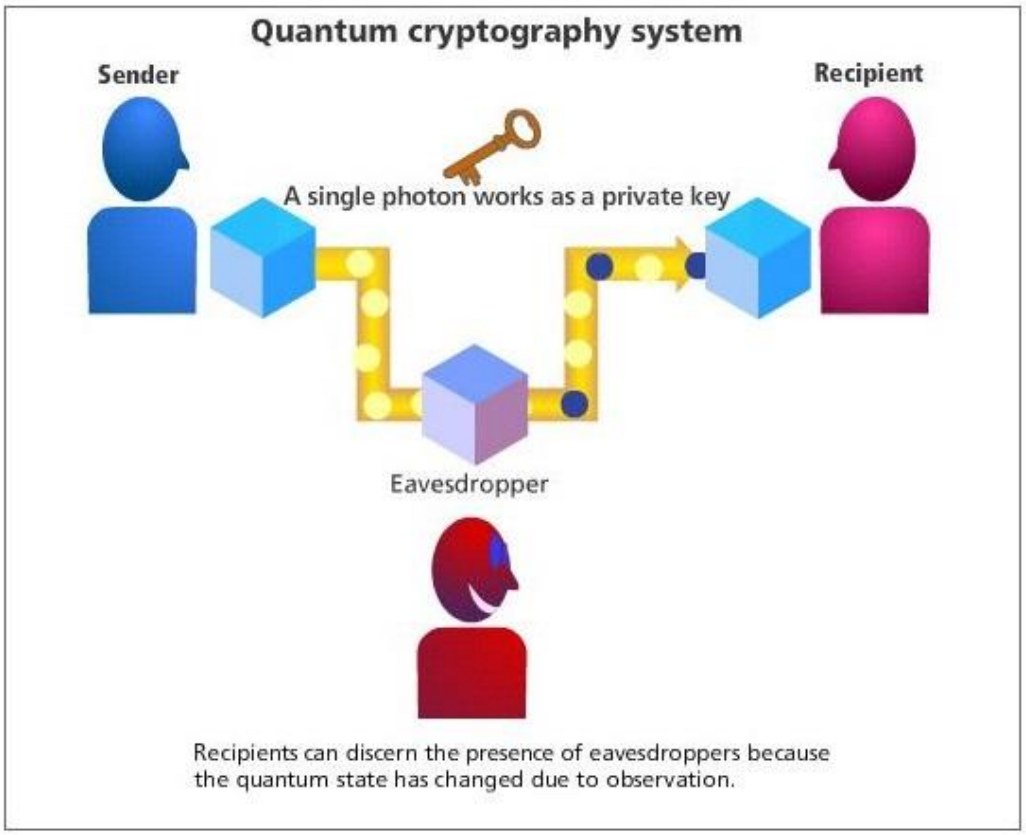

Fig 2: Quantum Cryptography

In this paper, an examination of the quantum cryptography procedures is described. The report has perceived the degree of quantum cryptography and examined certain key age and sharing procedures. Approximately, the basic cryptography methodology for secure correspondence is described. The region moreover recognized the degree of quantum cryptography. In fragment II, the work described by before investigators is discussed. In region III, the safe key age procedures are researched under quantum techniques. In portion IV, the completion of the work is described.

B) Cryptography

The Cryptography word is taken from pair of Greek words, which indicate "secret creating". Cryptography is the way toward scrambling the main element by changing and subbing the primary importance, planning it in an incomprehensible course of action for other people. Cryptography is an effective way to secure the information sent through the framework correspondence ways. cryptography and cryptanalysis is game planned by Cryptology. Cryptanalysis is the strategy for getting the introduced messages into extraordinary compositions. All around, cryptography is trading data from source to the objective by changing it through a secret code. The cryptosystems use plaintext as data and make a figure content using encryption computation, taking the private key as data.

C) Steganography

It is the technique wherein audio, text, picture, or video cover-up inside another file, message, picture, or video. The word steganography joins the Greek words steganos (στεγανός), inferring "got, masked, or guaranteed", and graphein (γράυειν) meaning "creating".

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a composition on cryptography and steganography, disguised as a book on charm. All around, the covered messages have every one of the reserves of being (or are a piece of) something different: pictures, articles, shopping records, or some other cover content. For example, the secret message may be in impalpable ink between the visible lines of a private letter. A couple of executions of steganography that don't have a typical secret are sorts of safety through the absence of transparency, while key-subordinate steganography plans adhere to Kerckhoffs' guidelines.

The advantage of steganography over cryptography alone is that the generated secret message doesn't attract care, viewing itself as a dissent of assessment. Perceptible encoded messages—paying little mind to how rugged—energize interest and may in themselves be ensnaring in countries where encryption is illicit. Subsequently, while cryptography demonstrates getting the substance of a message alone, steganography is accented over concealing how a secret message is being sent and hiding the meaning of the message.

Steganography hides the information inside PC records. Electronic exchanges may fuse stenographic coding inside a transport layer in automated steganography, for instance, a recorded archive, picture record, program or show. Media articles are ideal for steganography transmission by virtue of their gigantic size. For example, an operator may start with a harmless image dataset and adjust the gloom of each hundredth pixel to contrast with a character in the character set, a change so authentic that no one knows it without looking and analyzing in deep.

D) LSB Technique is used in Steganography

Today, while changing a simple picture over to mechanical design, we generally pick between three unique methods of addressing colors:

- 24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.
- 8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.
- 8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

(IJIEST) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

LSB inclusion adjusts the LSBs of each tone in 24-digit pictures, or the LSBs of the 8-cycle an incentive for 8-bit images.

III. EXISTING WORK

While sharing the information, security is an essential part of keeping in mind. There are already many cryptographic techniques that give affirmation under the private, public, and open keys. To transfer secure and safe messages from one person to another, there is a need for key-based message encoding, which double the data transfer security. Many experts suggested enormous assessment of key techniques, key-based encryption and key sharing. Quantum based cryptography is one of the types which utilizes the strategy level and imperativeness level boundaries.

Sharbaf et al. (Sharbaf et al., 2009) have displayed an assessment build work regarding quantum key cryptography. Maker portrayed a theory-based exhibiting to control arrange security and gave this current reality move up to the quantum cryptography show. The author gave an imperative change to quantum cryptography show for secure correspondence in the framework.

(Kartalopoulos et al., 2005) gave work on related polarization show for watchful equality using Quantum cryptography methodologies. The maker passed an examination on cryptography methodologies and perceived the key age and recognizing verification system. Maker associated work on fiber optic transmission for topological change. Researcher similarly perceived the specific issues regarding the particular system and portrayed the key transport method for quantum control in a novel methodology. Maker associated the fiber medium based correspondence exhibiting for certain post consistently conditions.

Researcher (Kurochkin et al., 2009) gave a brief stage build working considering quantum cryptography systems. Maker described the work to apply the game plan under polarization system and delivered the amazing correspondence line for feasible correspondence control continuously method. (Sharbaf et al., 2011) has noticed the flaws, difficulties of cryptography methodology for quantum limits. The application-driven implications of quantum cryptography were related to various applications and worked on the quality and transmission utilizing quantum key trade techniques. The maker gave the expected change to the huge obligation to get correspondence in veritable condition.

Researcher (Goel et al., 2007) has focused on recognizing the material of science law that can merge to enhance the security by analyzing quantum cryptography. Maker also perceived the likely believability of the security strategy to improve the safe correspondence instrument. Maker (Crepeau et al., 1999) used the verification specific correspondence by watching the quantum direction of different machines and delivered the assessment to give the secure message. The

maker gave the run based advancement to cover the problematic estimation with figuring strategy and achieve first in class security.

Researcher (Mandal et al., 2013) implemented a cryptography technique to prevent the fierce brute force attacks. Maker arranged a three-stage show for other photon-based correspondence. The designer analyzed the mathematical response for essential speculative assessment and delivered a probabilistic aide for chairman specific transmission. The maker gave the safe unitary message using empowered correspondence through show encoding.

Researcher (Porzio et al. 2014) has detected a risk in private message communication. A telecom station based composed computation is portrayed to give assurance further developed equality. The author noticed the situation, measures the quality and gave the computational message in real cases. Maker recognized the questionable relations for certain quantum correspondence with show coordination.

Researcher (Shrivastava et al., 2012) used the protected correspondence structure with a key sharing procedure. The maker used to some degree controlled show for string level correspondence and gave the probability driven distinctive verification of any busybody in the framework. Maker achieved the protected parity with a quantum key spread in private condition.

Researcher (Teja et al., 2007) has given the possible improvement to security structure in good condition. Maker recognized the quality and weaknesses of both standard and quantum cryptography methods. Maker associated the imaginative improvement to the system with novel facilitated overhauls. Maker associated the protected correspondence showing in original condition and gets the channel driven quantum correspondence.

Researcher (Bencheikh et al., 2001) has researched the depiction of quantum cryptography under different points. The quantum mechanics show joining, and the maker investigated key sharing methods. Maker perceived various cycle factors to achieve the boundary specific change. Maker earned the schematic change logically condition to deliver banner mode security.

Researcher (Kurochkin et al., 2010) gave the speculative and preliminary examination of the quantum show to achieve the safe correspondence. The maker passed the enamored encoding procedure and its certification in attack driven conditions. The maker gave the speed up the correspondence strategy by perceiving the botches. The maker created the specific methodology in real need and got the safe correspondence measures.

Researcher (Niemiec et al., 2013) gave the combination of security aspects in quantum cryptography program. The author presented the quantum messages and showed the security level improvement consistently place. An encrypted string procedure for controlling the mail direct and its control was in the manner described by the author.

(IJIEST) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

IV. SUGGESTED APPROACH

This framework proposes an approach where we demonstrate how an old strategy, for instance, steganography, can ensure when we go along with it with the extraordinary key scattering segment of quantum cryptography with other additional security features. With quantum PCs, quantum cryptography furthermore came into light and presently is encouraging considering it's anything but benevolent components that make it liberated from listening subtly or whatever other outcast break in the key flow systems.
The suggested technique suggested a technique that mixes old strategies, for example, the use of steganography to hide the quantum key. Further, few components are also presented, making the channel more secure while sharing the key between two parties with the added feature of speed and security.

The fundamental thought of quantum cryptography consolidated with two standard perspectives. The main purpose is to generate the information based on bits using enchanting quantum. The next is to create a quantum key based on physic rules to enhance the particular security. The author described the work to update the cryptographic features to choose the computational trouble and give the factorization to the protected precise technique. The technique of cryptography needs secure communication with confirmation of message standards and generates information factorization by algorithmic model. This factorization is associated at a bit level that works on the particular procedure just as it provides the protected key age in the certified condition. The key age technique under cryptographic showing is showed up in figure 3.

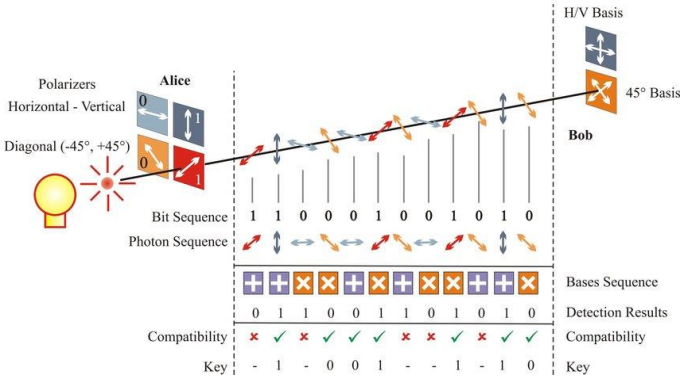

Fig 3: Quantum Cryptography Method based on Bit Polarized

The figure shows the piece absorbed quantum key age method for improving the security points and gives the scattering of the key using the quantum channel. The procedure joins the particular way in an organized edge so will obtain the safe correspondence from the existing system. This system is based on a stream where the matrix size of the data described the association of activity based on the specific condition. These activities can be bearing specific to pick the filtration under the related composed system. The quantum measures are related to these data pieces to ensure the safe remarkable key age.

(IJIEST) 2018, Vol. No. 4, Jan-Dec **e-ISSN: 2454-9584; p-ISSN: 2454-8111**

V. RESULT ANALYSIS

The ordinary cryptography strategies consolidate the RSA system. The unique lead and consistent consolidation show the nature of this cryptographic technique over the conventional cryptography approach. This methodology can recognize the protected estimation to develop the correspondence system further. It gives fast and trustworthy correspondence with low diverse nature-based compromise. The post under the multi-layered nature measure against the standard cryptography method is portrayed in Table 1. Various cryptographic techniques and their properties are indicated with their relation.

Table 1 : Comparative Analysis

Characterization	RSA	Quantum Cryptography
Complexity	$O(N^k)$	O(logN)
Bit size	N	2N
Size of Key	512	1024
Attack Robustness (Brute force)	Largest broken 512 bit value	Largest broken 1024 bit value
Attack Robustness (Random Attack)	2.2 months	Not possible

Cryptography has low diverse nature. It is elaborated in the table that quantum cryptography has a solid security approach and can prevent various attacks. The difference between RSA and the quantum cryptography approaches is shown in the table.

VI. CONCLUSIONS

The Paper focuses on an instrument that joins an old system, for instance, steganography with the astounding key errand piece of quantum cryptography. Quantum cryptography uses material science law to provide certain key ages and scattering. The Paper moreover portrayed the close to insight to show the nature of this cryptography technique.

VII. REFERENCES

[1]. Porzio, "Quantum cryptography: Approaching communication security from a quantum perspective," Photonics Technologies, 2014 Fotonica AEIT Italian Conference on, Naples, 2014, pp. 1-4.

[2]. Shrivastava and M. Singh, "A security enhancement approach in quantum cryptography," Computers and Devices for Communication (CODEC), 2012 5th International Conference on, Kolkata, 2012, pp. 1-4.

[3]. Crepeau, "Cryptography in the quantum world," Information Theory and Networking Workshop, 1999, Metsovo, 1999, pp. 40.

[4]. K. Bencheikh, A. Jankovic, T. Symul and J. A. Levenson, "Quantum cryptography with continuous variables," Quantum Electronics and Laser Science Conference, 2001. QELS '01.

[5]. M. Niemiec and A. R. Pach, "Management of security in quantum cryptography," in IEEE Communications Magazine, vol. 51, no. 8, pp. 36-41, August 2013.

[6]. M. S. Sharbaf, "Quantum Cryptography: A New Generation of Information Technology Security System," Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on, Las Vegas, NV, 2009, pp. 1644-1648.

[7]. M. S. Sharbaf, "Quantum cryptography: An emerging technology in network security," Technologies for Homeland Security (HST), 2011 IEEE International Conference on, Waltham, MA, 2011, pp. 13-19.

[8]. N. I. Mowla, I. Doh and K. Chae, "Securing information flow in content delivery networks with visual and quantum cryptography," 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, 2016, pp. 463-468.

[9]. R. Goel, M. Garuba and A. Girma, "Research Directions in Quantum Cryptography," Information Technology, 2007. ITNG '07. Fourth International Conference on, Las Vegas, NV, 2007, pp. 779-784.

[10]. R. S. Vignesh, S. Sudharssun and K. J. J. Kumar, "Limitations of Quantum & the Versatility of Classical Cryptography: A Comparative Study," Environmental and Computer Science, 2009. ICECS '09. Second International Conference on, Dubai, 2009, pp. 333-337.

[11]. S. Mandal et al., "Multi-photon implementation of three-stage quantum cryptography protocol," Information Networking (ICOIN), 2013 International Conference on, Bangkok, 2013, pp. 6-11.

[12]. S. V. Kartalopoulos, "Identifying vulnerabilities of quantum cryptography in secure optical data transport," Military Communications Conference, 2005. MILCOM 2005. IEEE, Atlantic City, NJ, 2005, pp. 2788-2796 Vol.

[13]. V. L. Kurochkin and I. G. Neizvestny, "Quantum cryptography," Micro/Nanotechnologies and Electron Devices, 2009. EDM 2009. International Conference and Seminar on, Novosibirsk, 2009, pp. 166-170.

[14]. V. Kurochkin and Y. Kurochkin, "Quantum cryptography security improvement with additional states," Micro/Nanotechnologies and Electron Devices (EDM), 2010 International Conference and Seminar on, Novosibirsk, 2010, pp. 231-233.

[15]. V. Teja, P. Banerjee, N. N. Sharma and R. K. Mittal, "Quantum cryptography: State-of-art, challenges and future perspectives," Nanotechnology, 2007. IEEE-NANO 2007. 7th IEEE Conference on, Hong Kong, 2007, pp. 1296-1301.

[16]. R. Canetti, S. Halevi, and J. Katz, ―A forward-secure public-key encryption scheme,‖ in Advances in Cryptology (EUROCRYPT‟03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646.

[17]. D. Boneh and X. Boyen, ―Efficient selective-id secure identity-based encryption without random oracles,‖ in Advances in Cryptology (EUROCRYPT‟04), C. Cachin and J. Camenisch, Eds. Berlin,Germany: Springer, 2004, vol. 3027, pp. 223–238.

[18]. D. Boneh and X. Boyen, ―Secure identity based encryption without random oracles,‖ in Advances in Cryptology (CRYPTO‟04),M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197–206.

[19]. B. Waters, ―Efficient identity-based encryption without random oracles,‖ in Advances in Cryptology (EUROCRYPT‟05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127.

[20]. C. Gentry, ―Practical identity-based encryption without random oracles,‖ in Advances in Cryptology (EUROCRYPT‟06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.

[21]. C. Gentry, C. Peikert, and V. Vaikuntanathan, ―Trapdoors for hard lattices and new cryptographic constructions,‖ in Proc. 40th Annu. ACM Symp. Theory Comput. (STOC‟08), 2008, pp. 197–206.

[22]. S. Agrawal, D. Boneh, and X. Boyen, ―Efficient lattice (h)ibe in the standard model,‖ in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.

[23]. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, ―Bonsai trees, or how to delegate a lattice basis,‖ in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552

[24]. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, ―Identity-based hierarchical strongly key-insulated encryption and its application,‖ in Advances in Cryptology (ASIACRYPT‟05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

[25]. Moni Naor, Adi Shamir,‖ visual cryptography‖

[26]. Jithesh K, 2dr. A V Senthil Kumar, ―Multi-Layer Information Hiding -A Blend Of Steganography And Visual Cryptography,‖

[27]. Young-Chang Hou, ―Visual cryptography for color images,‖