A Study on Quantum Cryptography and Key Generation Methods

Shally Nagpal
Student, M.Tech (NS), BPSMV, Khanpur, Sonepat,Haryana
Email: shally.ngpl@gmail.com

Abstract

The secure communication in the real global environment is the primary requirement for a web or network user. Quantum cryptography is a environment and the application specific cryptography method that uses the physics law for key generation. The cryptography method extracts the energy features to apply data encoding and embed the key generation algorithm with cryptography process. On the receiver side, the key decoding is used quantum method and this extracted key is then used for data decoding. There are different methods for key generation which are explored in this paper. The paper also explored the scope of quantum key protocol for key generation and encoding.

Keywords - Quantum Cryptography, Encoding, Decoding, Secure Transmission.

1.Introduction

The cryptography is about to encode the information so that the access and communication level security will be achieved. Cryptography method also ensures the authenticated communication. The key specific cryptography saves the information to the authenticated persons hand so that the information transmission in the private and public environment can be more secure. As the security is the primary requirement when information travel in open environment, because of this lot of work is done in cryptography method to improve the security, reliability, robustness and effectiveness of cryptography methods. The complete cryptography process is divided in three main stages. In first stage, the cryptography keys are generated. These keys are generated by sender side. There can be single key for both encryption and decryption or there can be different key for each process. Once the key is generated, the next work is to share the key on receiver side. Different sharing methods are defined for key distribution. The key distribution is either controlled by sender, centralized control or the third party. After distributing the key, the final stage is to use the key-cryptography method for secure communication. On sender side, the key based encoding is performed and on receiver side, the key based decoding is perform. The basic encoding and decoding process is shown in figure 1.

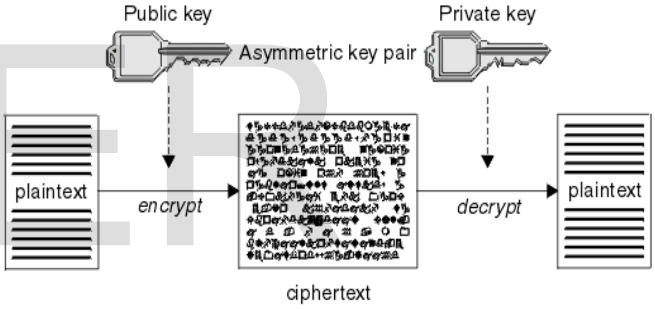

Figure 1 : Key Based Encoding

Different cryptography and method level solutions are provided by different researchers. One of the most effective cryptography methods is a quantum cryptography method. The description of this cryptographic method is described in this section.

1.1 Quantum Cryptography

This cryptographic method uses the physics law or the quantum mechanism to provide secure communication. It is the secure shared communication method with random encoding scheme for applying the key specific encryption and decryption. The characterization of this method can be done under different parameters based on the environment and the application. The key cryptography method uses the quantum transmission to provide the secure communication against the intruders. This cryptography method uses the quantum or the photon polarization method to improve the secure communication. The cryptosystem uses the light photon oriented polarized method to set the cryptographic directions. The method ensures the authentication method with principal communication formation. The process applied by quantum cryptography method against eavesdropper is shown in figure 2. The figure shows that the encryption system is integrated with quantum stage generator on sender side on plain text to apply data encoding. The quantum channel based communication is performed using quantum cryptography method. On receiver side, the encoded data is applied under quantum state detector to extract the hidden key. Based on this key, the decryption algorithm is applied to extract the content back. The work model is able to provide the secure encoded communication in real environment.

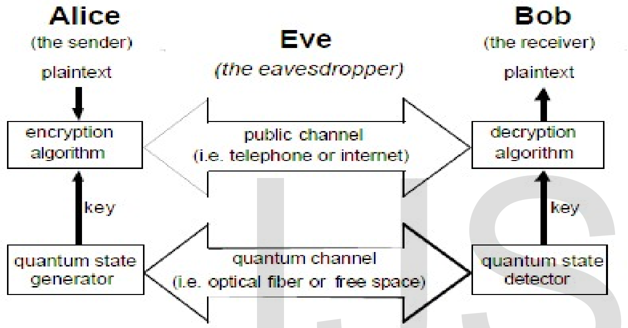

Figure 2 : Quantum Cryptography

In this paper, an exploration to the quantum cryptography methods is defined. The paper has identified the scope of quantum cryptography and explored different key generation and sharing methods. In this section, the requirement of cryptography method for secure communication is defined. The section also identified the scope of quantum cryptography. In section II, the work defined by earlier researchers is discussed. In section III, the secure key generation methods are explored under quantum methods. In section IV, the conclusion of the work is defined.

1. Existing Work

Security is most critical aspect to share the information in the global environment. To provide the secure and authenticated information, there is the requirement of some key specific encoding approach. Cryptography provides different encoding methods based on the requirement. There are a number of existing cryptography that provides authentication under public key, private key or shared key methods. A lot of work defined by different researchers on different key generation, key sharing and key based encoding. Quantum cryptography is one such cryptography form that uses the process level and energy level parameters. Vignesh et. al. (Vignesh et. al., 2009) has provided a comparative analysis on traditional and quantum cryptography methods. Author identified the various characteristics relative to versatility vectors for key sharing and encoding methods. Author defined a restricted quantum key distribution method for secure communication in the network. Sharbaf et. al. (Sharbaf et. al., 2009) has presented a study based work on quantum key cryptography. Author defined a theory based modeling to control network security and provided the real world enhancement to the quantum cryptography model. Author provided a significant improvement to quantum cryptography protocol for secure communication in the network. Kartalopoulos (Kartalopoulos et. al., 2005) provided a work on associated polarization model for intelligent communication using Quantum cryptography methods. Author provided a study on cryptography methods and identified the key generation and identification method. Author applied work on fiber optic transmission for topological improvement. Author also identified the technical issues relative to the communication method and defined the key distribution method for quantum control in dynamic method. Author applied the fiber medium based communication modeling for secure communication in real time environment. Author (Kurochkin et. al., 2009) provided a temporary stage based working on quantum cryptography methods. Author defined the work to apply the solution under polarization method and generated the effective communication line for effective communication control in real time method. (Sharbaf et. al., 2011) has identified the weaknesses, challenges of cryptography methods for quantum parameters. The application driven implication of quantum cryptography was applied for different application and improved the quality and transmission using quantum key exchange methods. Author provided the potential improvement to the valuable contribution to secure communication in real environment.

Author (Goel et. al., 2007) has focused his work on exploration of quantum cryptography and identified the physics law that can be incorporated to improve the security. Author also identified the potential possibility of the security method to improve the secure communication mechanism. Author (Crepeau et. al., 1999) used the evidence specific communication by observing the quantum behavior of different machines and generated the measurement to provide secure communication. Author provided the rule based evolution to cover the difficult computation with factoring method and achieve high end security.

Author (Mandal et. al., 2013) implemented the cryptography model to provide security against brute force attack. Author designed a three stage protocol for multiple photon based communication. Author analyzed the mathematical solution for theoretical requirement analysis and generated a probabilistic map for operator specific transmission. Author provided the secure unitary transmission using polarized communication through protocol encoding. Author (Porzio et. al. 2014) identified the security problems in private communication. A telecom channel based integrated algorithm is defined to provide privacy enhanced communication. Author identified the complexity measures and provided the computational communication in real environment. Author identified the uncertain relations for secure quantum communication with protocol integration. Author (Shrivastava et. al., 2012) used the secure communication system with key sharing method. Author used a bit controlled protocol for string level communication and provided the probability driven identification of any eavesdropper in the network. Author achieved the secure communication with quantum key distribution in private environment. Author (Teja et. al., 2007) has provided the potential enhancement to security system in functional environment. Author identified the strength and weaknesses of both traditional and quantum cryptography method. Author applied the technological enhancement to the system with novel integrated enhancements. Author applied the secure communication modeling in real environment and gains the channel driven quantum communication. Author (Bencheikh et. al., 2001) has explored the characterization of quantum cryptography under different aspects. The quantum mechanics, protocol integration and key sharing methods were explored by the author. Author identified different process factors to achieve the parameter specific improvement. Author achieved the schematic improvement in real time environment to generate signal mode security. Author (Kurochkin et. al., 2010) provided the theoretical and experimental exploration of quantum protocol to achieve the secure communication. Author provided the polarized encoding method and its scope in attack driven environment. Author provided the speed up the communication process by identifying the errors. Author generated the communication method in real environment and gained the secure communication measures. Author (Niemiec et. al., 2013) provided the management of security aspect in quantum cryptography model. Author provided the quantum communication monitoring and provided the security level enhancement in real time environment. A string polarized method for controlling the communication behavior and its control was also described by the author.

Steganography is another effective method applied to achieve secure communication in real time environment. Researchers also integrated the steganography methods with cryptography methods to achieve high end security. Author (Mowla et. al., 2016) has combined the visual cryptography method with quantum cryptography and achieved high end communication against different communication attacks. Author defined the communication modeling under the communication behavior analysis and generated the security with additional correlated method. Author also integrated the steganography method with cryptographic modeling to achieve dual phase security.

2. Quantum cryptographic modeling

The basic concept of quantum cryptography integrated with two main aspects. The first aspect is to generate the data bits using polarized photons and second to apply the physic rules based quantum key generation to enhance the secure communication method. Author defined as the work to improve the cryptographic modeling to resolve the computational difficulty and by providing the factorization for the secure communication method. The cryptography method requires to manage the secure communication with specification of rules and the algorithmic model provide data factorization. This factorization is applied at bit level that not only enhances the communication method but also provide the secure key generation in real environment. The key generation method under cryptographic modeling is shown in figure 3. The figure is showing the bit polarized quantum key generation method for improving the security aspects as well as provide the distribution of the key using quantum channel. The method incorporates the communication method in an integrated form so that the secure communication will be obtained from the method itself. It is a stream based method in which the block size of data bits is defined a series of directional and environment specific operations are applied. These operations can be direction specific to decide the filtration under associated integrated method. The quantum measures are applied on these data block to ensure the secure unique key generation.

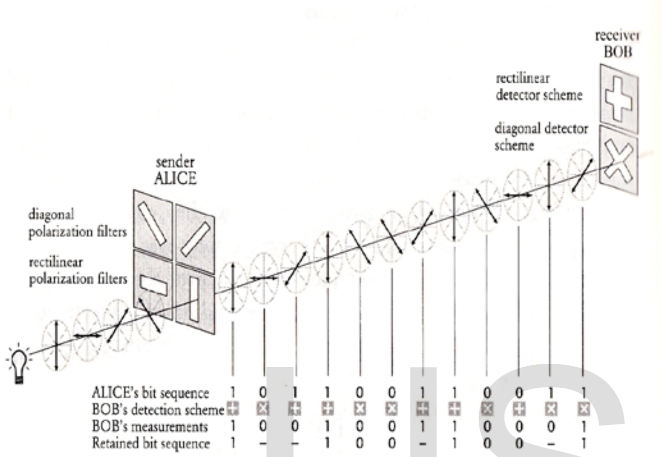
receiver
BOB
rectilinear
detector scheme
diagonal detector
scheme
sender
ALICE
diagonal
polarization filters
rectilinear
polarization filters
ALICE's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1
BOB's detection scheme ⊞ ⊠ ⊞ ⊞ ⊠ ⊠ ⊞ ⊞ ⊠ ⊞ ⊠ ⊠
BOB's measurements 1 0 0 1 0 0 1 1 0 0 0 1
Retained bit sequence 1 – – 1 0 0 – 1 0 0 – 1

Figure 3 : Bit Polarized Quantum Cryptography Method

Once the bit photons for polarized form are generated and measured, the next work is to apply the time padding to control the communication using key exchange methods. The key distribution also controlled using random choices and to provide the communication against different attacks. The knowledge polarization method can be integrated to interpret the meaningful keys and to provide the secure communication modeling against different communication threats in the real environment.

3.1 Comparative observations

The dynamic behavior and real time integration show the strength of this cryptographic method over classical cryptography approach. This approach is able to identify the secure computation to enhance the communication system. It provides the fast and reliable communication to with low complexity based integration. The communication under the complexity measure against traditional cryptography method is defined in table 1. The traditional cryptography methods include RSA method. The comparison is here derived against different cryptographic method properties.

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

The table has provided the clear difference between the RSA and the quantum cryptography methods. The table shows that quantum cryptography provided the secure solution with low complexity and provided more secure encryption against different attacks.

3. Conclusion

In this paper, an exploration to the quantum cryptography methods is provided. The quantum cryptography uses the physics low to provide secure key generation and distribution. The paper also defined the comparative observation to prove the strength of this cryptography method.

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.

Technical Digest. Summaries of Papers Presented at the, Baltimore, MD, USA, 2001, pp. 239-240.

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.