Analysis Of Quantum Cryptography For Secure Satellite Communication

Veenu Yadav, Deepshikha Agarwal

Abstract: This paper present an analysis on the use of Quantum Cryptography (QC) to provide secure communication over the network. The transmission of the data is a very powerful information secure operation to entire Quantum Key Distribution (QKD). This paper presents to communicate satellite-based over the global quantum communication network, to achieve a long distance, to share the data quantum signal by optical fiber to cover the 250 kilometers in distance. Currently, the problem is the transmission of data in quantum communication; the signal weakens for long distances. This paper also proposes an application in satellite communication

Index Terms: Cryptography, Quantum, Qbits, Entanglement, Quantum Key Distribution, Error correction. Secure, Satellite communication

1 INTRODUCTION

In the last century, cryptography has undergone three major changes: firstly the use of cipher machine as an alternative of manual encryption, Secondly, The introduction of the cryptography in the mathematical form made and to improve the complexity of the cryptography. Thirdly, the concept of asymmetric cryptography, which is increased confidentiality. These three changes lead to the new branch of cryptography which we call quantum cryptography (QC) which finds its basis on the well-known quantum physics. on the well-known quantum physics. In quantum cryptography, I also used the concept and derived the principles of quantum physics to provide the unconditional security of data. Also used the classical cryptography to secure and protect the information in two ways 0and 1, 0 and 1 bit also is called the classical bi. Quantum cryptography also protects the information in (qubit) quantum information unit quantum bit as well as classical bits. In Quantum cryptography (QC), the information that it can protect is not only the classical bit but also the quantum information unit quantum bit (qubit). The application is used in, the classical information is more entrance fee in comparison to quantum information. The protection of classical information is very stronger than the quantum information in quantum cryptography (QC). In a few years, the quantum key distribution is more grown-up quantum cryptography. Along with them, Quantum key distribution (QKD) technology is the most grown-up quantum cryptography technology, China has also implemented a large project on quantum cryptography. The random bit of code is generated by a random number generator, this random number is also called the random key. This paper presents a discussion and analysis of the quantum cryptography. Definition of quantum cryptography and basic knowledge of qubit and also discuss the protocol using in quantum cryptography for secure satellite communication. Also, summarize the attacks in quantum cryptography.

- *Veenu Yadav is currently pursuing Ph.D in Computer Science and engineering in Amity University Lucknow campus, India, PH-9161469196. E-mail:yadavveenu402@gmail.com*
- *Dr. Deepshikha Agarwal is Professor in Computer Science and engineering in Amity University Lucknow campus, India, PH-9208205636. E-mail: sun.mita@gmail.com*

Finally, present existing open issues, and proposes a quantum enabled communication system model for entanglement state- Two qubit state $1\div\sqrt{2}(|00>+|11>)$ is maximally entangled. Suppose we have to take a reduce state over either a qubit them, they the result to be get could be not appear, but a mixed state is maximum. That mean the density come out the half. Taking a reduced trace over either the first qubit or the second, we get a maximally mixed state p=½. Fig. 1 shows a quantum enabled communication system.

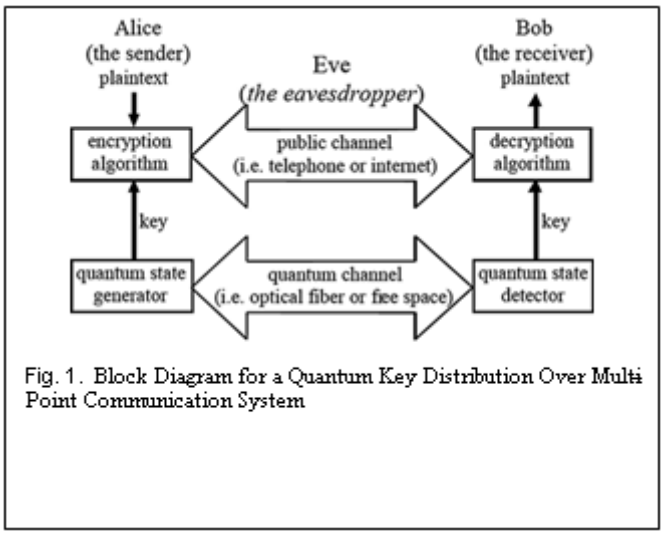

Fig. 1. Block Diagram for a Quantum Key Distribution Over Multi Point Communication System

Suppose we have to take a reduce state over either a qubit

2 QUANTUM CRYPTOGRAPHY- APPROACH

QC can be very well defined as-"Quantum Cryptography is the mechanism and concept of Quantum physics, we have to use the properties of the quantum system for secure communication. Quantum Cryptography is a technology based on the phenomenon of Quantum Mechanism and entanglement, To generate one state at a time. The quantum cryptography is used the polarization properties for encoding the data in photon form. In quantum cryptography, security provides the key to encryption and decryption the information for communication.

2.1 Quantum Key Distribution

The research areas the Quantum Key Distribution mainly

focuses on providing information security by applying the quantum key distribution, asymmetric and symmetric technique in encrypting and decrypt the information for secure communication over the channel [1,2,3,4,5]. The source code future divided in two-part, first one is Discrete variable class protocol (DVCP) and continuous variable class protocol (CVCP) [6]. In quantum key distribution the entanglement of the light source is also divided into two parts prepare and measure class protocol(PMCP) [7] and entanglement based class protocol (EBCP) [8]. In quantum key distribution process, the coding of the finite dimension of the data by which the quantum state refer to the different protocol that the Hilbert space [9]. The phases coding, the polarization of the bit and different phases of the photon. We have to discuss and study the Quantum Key Distribution (QKD) and study the BB84 protocol [10,11]. The Distributed Phase reference (DPC) protocol[12] has too many parts and included single-photon based measure class protocol and entanglement based class protocol (EBCP) also similar to the classical communication channel. The single-photon protocol [13,14,15] is the part of the class of protocol that forms the different –different quantum state by polarization path of a single photon to accomplish key distribution in quantum key distribution processes an encoding and decoding the information. Quantum Key Distribution protocol (QKDP) [1,16] was projected by C.H. Bennett and G. Brassard and socially published in a meeting in 1984, which is referred to as BB84 protocol [17]. In 1992 C.H. Bennet proposed a two-state protocol, called B92 protocol [2,18]. In 1998, D. Brut proposed the six-state protocol, which uses six deferent quantum states for a quantum bit, hence the name [3, 19]. In 2004 V. Scaring proposed the SARG04 protocol [4,20]. The entangled photon protocols (EPP) [21,22,23,24] are a category of protocols to appreciate Quantum Key Distribution protocol (QKPD) by using the properties of quantum entangled states in quantum mechanics. The Communication of the single-photon protocol and an entanglement photon protocol communally entangled photons the earliest protocol was E91 protocol [25,26,27] projected by Arturo Eckert in 1991[5, 28, 29]. In 1992, C.H. Bennett et al. projected the BBM92 protocol [6, 30, 31].

2.2 Quantum Authentication (QA)

Verification can accomplish the distinctiveness frication of the sender, the truthfulness frication of the encode message, as well as more secure for the communication in quantum encryption. There are two main objectives of the Quantum identification authentication (QI) [32] , firstly we have to self identification and more effective it means, Alice can verify to Bob is to be sure Alice. Another is the client does not be imitate that is, after Alice finishing the identification, Bob does not assert to others that he is Alice using the information provided by Alice. One typical schedule is projected through the G.H. Zeng group [33]. In quantum cryptography, the digital signature also provides the more confidential and secure and truthful of the data and the individuality of the encoder in the communication to transfer the data to another side. The digital signature is mainly used to ensure the truthfulness of the data and the individuality of the sender in the communication, asymmetric key encryption also used and provided the more secure data for the end side. This technology, the security for the end side or receiver side. Asymmetric Key encryption is a technology used for encrypting and decrypting the data. In quantum cryptography there are three protocols are used in quantum Arbitrated quantum signature (AQS), Quantum blind signature (QBS) and quantum group signature.

2.3 Quantum Public Key Cryptography

The research on quantum public-key cryptography (QPKC) is separated into two parts, In quantum computing, we to find the character and not easy to solve or remove the problem. The complexity of security is built-in quantum computing. Secondly, we have to generate the secure Key included the quantum bits by the perception of quantum physics with some quantum properties.

2.4 Quantum Information Encryption

Quantum computing is based on the phenomenon fact quantum technicalities, we have to use superposition and entanglement observable is possible to create more than one state at a time. The transmission of the data in quantum computing more secure of classical information than we have to use the classical key to encode the data in quantum bits. The classical information storage and manipulation are based on the quantum bits or qubit. This is also based on the spin of electron or polarization of the single-photon, this behavior is governed on quantum physics.

3 CHALLENGES AND OPPORTUNITIES

The concept of Quantum cryptography (QC) is rewarding, but there are several challenges.Quantum Key Distribution (QKD) is the more important element of Quantum Cryptography is also provides the security of the data for communication by the phenomenon of quantum communication. Quantum computing algorithms to develop secure Quantum Key cryptography. The classical information also contains the lattice codes, can oppose the different attack of the quantum computing In quantum computing, we have to exchange the key by the public key algorithms for secure communication. We have to solve the problem by quantum cryptography to share the key between the sender and receiver with unconditional security. We propose a model for Quantum Cryptography based satellite communication system. Fig 1show the block diagram of the proposed model which is quantum enabled. We aim to secure the quantum information in this system by applying a suitable quantum-based security algorithm which is to be sent via the uplink.

4 CONCLUSION

In Quantum Cryptography we have to store and transfer the secure data by which quantum key, to protect the information for secure communication in satellite system. In the quantum cryptography, system behaves to improve quantum cryptography system for the secure transmission of the information, and prevent hacker attacks. We aim to implement the quantum cryptographic methods on satellite system in future.

REFERENCES

[1]. V. Makarov and D.R. Hjele,“Faked states attack on quantum cryptosystems”, J. Mod. Opt., Vol.52, No.5, pp.691–705,2005.

[2]. V. Makarov, “Controlling passively quenched single photon de- tectors by bright light”, New J. Phys., Vol.11, No.6, Article ID 065003, 18 pages, 2009.

[3]. H.W. Li, S. Wang, J.Z. Huang, et al., “Attacking a practical quantum-key distribution system with wavelength-dependent beam-splitterand multiwavelength sources”, Phys. Rev. A, Vol.84, No.6, Article ID 062308, 5 pages, 2011.
[4]. H.K. Lo, M. Curty and B. Qi, “Measurement-device- independent quantum key distribution”, Phys. Rev. Lett., Vol.108, No.13, Article ID 130503, 5 pages, 2012.
[5]. Y. Liu, T.Y. Chen, L.J. Wang, et al., “Experimental measurement device-independent quantum key distribution”, Phys. Rev. Lett., Vol.111, No.13, Article ID 130502, 5 pages, 2013.
[6]. Z. Tang, Z. Liao, F. Xu, et al., “Experimental demonstration of polarization encoding measurement-device-independent quan- tum key distribution”, Phys. Rev. Lett., Vol.112, No.19, Article ID 190503, 5 pages, 2014.
[7]. H. Inamori, N. Lütkenhaus and D. Mayers, “Unconditional security of practical quantum key distribution”, Eur. Phys. J. D, Vol.41, No.3, pp.599–627, 2007.
[8]. D. Gottesman, H.K. Lo, N. Lütkenhaus, et al., “Security of quantum key distribution with imperfect devices”, Quantum Inf. Comput., Vol.4, No.5, pp.325–360, 2004.
[9]. W.Y. Hwang, H.Y. Su and J. Bae, “Improved measurement- device-independent quantum key distribution with uncharac- terized qubits”, Phys. Rev. A, Vol.95, No.6, Article ID 062313, 4 pages, 2017.
[10]. X.L. Hu, Y.H. Zhou, Z.W. Yu, et al., “Practical measurement- device-independent quantum key distribution without vacuum sources”, Phys. Rev. A, Vol.95, No.3, Article ID 032331, 6 pages, 2017.
[11]. Jiang, Z.W. Yu and X.B. Wang, “Measurement-device- independent quantum key distribution with source state errors and statistical fluctuation”, Phys. Rev. A, Vol.95, No.3, Article ID 032325, 5pages, 2017. [12] C.M. Zhang, J.R. Zhu and Q. Wang, “Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution”, Phys. Rev. A, Vol.95, No.3, Arti- cle ID 032309, 5 pages, 2017.
[12]. N. Lo Piparo, M. Razavi and W.J. Munro, “Measurement- device-independent quantum key distribution with nitrogen va- cancy centers in diamond”, Phys. Rev. A, Vol.95, No.2, Article ID 022338, 12 pages, 2017.
[13]. N. Li, Y. Zhang, S. Wen, et al., “Security analysis of measurement-device-independent quantum key distribution in collective-rotation noisy environment”, Int. J. Theor. Phys., Vol.1, No.12, pp.1–12, 2017.
[14]. J. Li, N. Li, L.L. Li, et al., “One step quantum key distribu- tion based on EPR entanglement”, Sci. Rep., Vol.6, Article ID 28767, 9 pages, 2016.
[15]. N. Li, J. Li, L.L. Li, et al., “Deterministic secure quantum communication and authentication protocol based on extended GHZ-W state and quantum one-time pad”, Int. J. Theor. Phys.,Vol.55, No.8, pp.3579–3587, 2016.
[16].] S.B. Zhang, Z.H. Xie, Y.F. Yin, et al.,“Study on quantum trust model based on node trust evaluation”, Chinese Journal of Electronics, Vol.26, No.3, pp.608–613, 2017.
[17]. Y.J. Zhao, X.W. Chen, Z.G. Shi, et al., “Implementation of one- way quantum computing with a hybrid solid-state quantum sys- tem”, Chinese Journal of Electronics, Vol.26, No.1, pp.27–34, 2017.
[18]. D. Gottesman, H.K. Lo, N. Lütkenhaus, et al.,“Security of quantum key distribution with imperfect devices”, Quantum Inf. Comput., Vol.4, No.5, pp.325–360, 2004.
[19]. W.Y. Hwang, H.Y. Su and J. Bae, “Improved measurement- device-independent quantum key distribution with uncharac- terized qubits”, Phys. Rev. A, Vol.95, No.6, Article ID 062313, 4 pages, 2017.
[20]. X.L. Hu, Y.H. Zhou, Z.W. Yu, et al., “Practical measurement- device-independent quantum key distribution without vacuum sources”, Phys. Rev. A, Vol.95, No.3, Article ID 032331, 6 pages, 2017.
[21]. C. Jiang, Z.W. Yu and X.B. Wang, “Measurement-device- independent quantum key distribution with source state errors and statistical fluctuation”, Phys. Rev. A, Vol.95, No.3, Article ID 032325, 5pages, 2017.
[22]. C.M. Zhang, J.R. Zhu and Q. Wang, “Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution”, Phys. Rev. A, Vol.95, No.3, Arti-cle ID 032309, 5 pages, 2017.
[23]. N. Lo Piparo, M. Razavi and W.J. Munro, “Measurement- device-independent quantum key distribution with nitrogen va- cancy centers in diamond”, Phys. Rev. A, Vol.95, No.2, Article ID 022338, 12 pages, 2017.
[24]. N. Li, Y. Zhang, S. Wen, et al., “Security analysis of measurement-device-independent quantum key distribution in collective-rotation noisy environment”, Int. J. Theor. Phys., Vol.1, No.12, pp.1–12, 2017.
[25]. J. Li, N. Li, L.L. Li, et al., “One step quantum key distribu- tion based on EPR entanglement”, Sci. Rep., Vol.6, Article ID 28767, 9 pages, 2016.
[26]. N. Li, J. Li, L.L. Li, et al., “Deterministic secure quantum communication and authentication protocol based on extended GHZ-W state and quantum one-time pad”, Int. J. Theor. Phys., Vol.55, No.8, pp.3579–3587, 2016.
[27]. S.B. Zhang, Z.H. Xie, Y.F. Yin, et al., “Study on quantum trust model based on node trust evaluation”, Chinese Journal of Electronics, Vol.26, No.3, pp.6086-13, 2017.
[28]. [29] Y.J. Zhao, X.W. Chen, Z.G. Shi, et al., “Implementation of one- way quantum computing with a hybrid solid-state quantum sys- tem”,

Chinese Journal of Electronics, Vol.26, No.1, pp.27–34, 2017.
[29]. H.L. Yin, T.Y. Chen and Z.W. Yu, “Measurement-device- independent quantum key distribution over a 404 km optical fiber”, Phys. Rev. Lett., Vol.117, No.19, Article ID 190501, 5 pages, 2016.
[30]. Z. Li, Y.C. Zhang, F. Xu, et al., “Continuous-variable measurement-device-independent quantum key distribution”, Phys. Rev. A, Vol.89, No.5, Article ID 052301, 8 pages, 2014.
[31]. S. Pirandola, C. Ottaviani, G. Spedalieri, et al., “High-rate measurement-device-independent quantum cryptography”, Na- ture Photon, Vol.9, No.6, pp.397–402, 2015.
[32]. C.H. Bennett, F. Bessette, G. Brassard, et al., “Experimental quantum cryptography”, J. Cryptol., Vol.5, No.1, pp.3–28, 1992.
[33]. P. Jouguet, S. Kunz-Jacques, A. Leverrier, et al., “Experimental demonstration of long-distance continuous-variable quan- tum key distribution”, Nature Photon, Vol.7, No.5, pp.378–381, 2013.
[34]. D. Huang, P. Huang, D. Lin, et al., “Long-distance continuous- variable quantum key distribution by controlling excess noise”, Sci. Rep., Vol.6, Article ID 19201, 9 pages, 2016.