Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Secure Communication using Quantum Computing Method

Lokesh B S [1]
Asst. Professor,
Dept of ECE, Maharaja Institute of Technology Mysore, India.

Hemanth K Gowda [2], Ganavi B P [3],
Harshitha M C [4], Hurmain Nishath [5]
Student, Dept of ECE, MITM.

***Abstract*—Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. To say a better communication parameters like security, high data rate etc., are important. The paper aims to make the communication more secure by exploring the quantum mechanical phenomena. In our demonstration we have considered the public channel and quantum channel. Public channel uses the classical communication techniques whereas for the quantum channel keys are exchanged using quantum computing methods. The continuous key exchange protocol is implemented using IBM Quantum experience.**

Keywords— IBMQ, CQSD, Quantum computing

I. INTRODUCTION

In today's world, computers are ubiquitous. They can be found in virtually any industry and most households own at least one personal computer or have a mobile phone. What truly transformed our society are large scale networks, like the Internet or mobile telephone networks, which can link billions of devices. Our ways of communicating and conducting business have severely changed over the last decades due to this development. However, most of this communication happens over inherently insecure channels requiring methods to protect our communication. A further issue is the vast amount of data generated, which raises serious privacy concerns. Cryptography provides the key components for protecting our communication. It also secures the passwords and personal data from eavesdroppers. To get a safe strategy to share data between the gatherings is accomplished by the encryption of the information utilizing quantum mechanics standards. Quantum cryptographic actualizes another procedure of cryptanalysis which makes it inconceivable for outsider elements to get these keys. Keys produced between different sides utilizing quantum channels called quantum key conveyances. Quantum key conveyance (QKD) is the principal quantum data undertaking to arrive at the degree of develop innovation. It focuses on the production of a mystery key between approved accomplices associated by a quantum channel. QKD is the way toward utilizing quantum correspondence to build up a mutual key between two gatherings without an outsider (Eve) getting the hang of anything about that key, regardless of whether Eve can listen stealthily on all correspondence between the clients.. In the event that Eve attempts to learn data about the key being set up, errors will emerge making the client notice. When the key is set up, it is then commonly utilized for encoded correspondence utilizing traditional procedures.

II. LITERATURESURVEY

Visible Light Communication (VLC)[1] can be succinctly expressed as Data Transmission through Illumination. Information transmission through noticeable light correspondence is significantly more secure and is fit for accomplishing high information transmission rates when contrasted with existing traditional remote innovations like Wi-Fi, Bluetooth, Wi-max, and so forth, which uses radio recurrence range. Here creator [31] targets assembling a remote VLC framework fit for transmitting content information between two PCs utilizing obvious light. A Light Emitting Diode (LED) is utilized as the transmitter, air as the transmission medium, and a Light emitting Resistor (LER) as the accepting part. Content information gets transmitted as series of 1s and 0s as the LED flashes on and off, quickly at a rate imperceptible to the natural eye. With the quick advancement of the innovation of optical correspondence [2], the security in it has pulled in an ever increasing number of individuals' consideration and even has become a basic segment of national security. Contrasted and the conventional media transmission, optical correspondence is viewed as a sort of secure correspondence on the grounds that optical fiber, transmission vehicle of it, is invulnerable to the average issues of electromagnetic obstruction EMI v/s radio-recurrence impedance (RFI). In any case, the fundamental qualities of the optical fiber make it powerless against an assortment of assaults, including physical framework assaults, listening in, capture attempt, and sticking. The creator proposes another model to infuse the light into a correspondence fiber without harming the cladding or center of it. From the numerical count, the intensity of the infused optical sign can arrive at over 20% of the info power. This degree of infused signal is adequate to meddle with the sign moved in the correspondence. Along these lines, measures to battle this sort of induction and misdirection ought to be taken. In this paper, to meddle with the sign in fiber, a technique for radiation field coupling is proposed. Contrasted and the strategies referenced above aside from fiber twisted, this strategy doesn't harm the center or cladding of correspondence fiber that can guarantee this sort of assault not found. To depict this strategy, right off the bat, a point by point hypothetically examination of the best approach to infuse

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

the optical sign into a correspondence fiber is shown. Besides, a hypothetical examination model and a useful model of this technique are given.

With the enormous mechanical headways being made each year, the requirement for better and quicker information rates, better and improved safety efforts are being given high significance in the exploration network[3]. Along these lines, open space correspondence has become a hotly debated issue as of late of which Visible Light Communication (VLC) is one of the exceptionally looked into zones. The purpose behind its high prevalence is a direct result of its capacity to give high information rates, high data transfer capacity and a safe vehicle of transmission as it can't infiltrate dividers. This paper examines the effect of noticeable light correspondence on sound and video transmissions. A genuine test proving ground is set up to test the presentation of sound transmission over VLC under different conditions, for example, good ways from the source, meddling lighting, and so forth. Emotional tests are completed to survey the nature of the sound VLC connect as apparent by the client. Also, a thorough report on existing synchronous video and sound transmission frameworks over VLC is given and the difficulties and staying open issues are identified. Internet of Things curtailed as IoT[4] has been a worldwide system where articles are connected together so that they can share information among themselves so they interface right away. So also, Ubiquitous processing is the rising pattern of embedding computational capacity into regular items to make them effectively impart to achieve helpful assignments. The advancement of these advances prompts an exponential development of brilliant sensors and gadgets which require quicker, secure, vitality effective information transmission.

III. QUANTUM GATES AND ITS DEFINITION

a) H Gate

The H or Hadamard gate pivots the states |0> and |1> to |+> and |->, individually. It is valuable for making superposition. As a Clifford door, it is helpful for moving data between the x and z bases.

Matrix form: $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

b) cX Gate

The controlled-X entryway is otherwise called the controlled-NOT. It follows up on a couple of qubits; with one is going about as 'control' and the different as 'target'. It plays out a X on the objective at whatever point the control is in state |1>. In the event that the control qubit is in a superposition, this gate creates entanglement.

Matrix form: $CNOT=cX=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

c) X Gate

The Pauli X gate has the property of flipping |0> the state to |1>, and vice versa. It is equivalent to Rx for the angleπ.

Matrix form: $X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

d) Y Gate

The Pauli Y gate is equivalent to Ry for the angleπ . It is also equivalent to the combined effect of X and Z.

Matrix form: $Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$

e) Z Gate

The Pauli Z gate has the property of flipping the |+> to|->, and vice versa. It is equivalent to Rz for the angleπ.

Matrix form: $Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$

f) Swap Gate

The SWAP gate simply swaps the states of two qubits.

Matrix form: $SWAP=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$

The above are some of the gates are used to build the quantum circuits. H and CNOT gates are universal gates as like in NAND and NOR in classical computing. Using CNOT and H gate the most popular Bell states can be build and analyzed. Author in [39] proposes a new quantum communication protocol, called Continuous Quantum Secure Dialogue (CQSD), that allows two parties to continuously exchange messages without halting while ensuring the privacy of the conversation. Compared to existing protocols, CQSD improves the efficiency of quantum communication. The CQSD protocol aims to ensure security while enabling continuous communication. Several types of common eavesdropping attacks and the robustness of CQSD against them like Trojan horse attack, intercept and resend attacks.

Author have used the information as shown in the below Table 1

Table 1 : Operator and its message

Operator	Quantum Gate	Message
U1	I	11
U2	X	10
U3	Z	01
U4	ZX	00

Table 1 input and data is altered

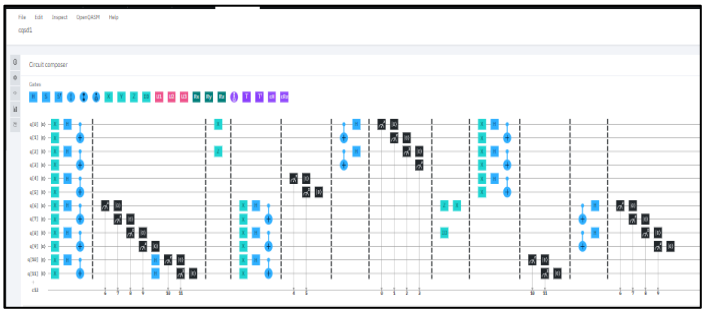

Fig 1: Figure of CQSD

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

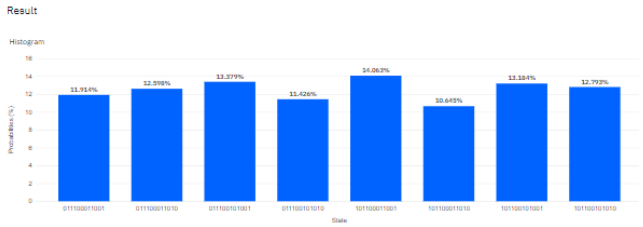

Fig2: Result of CQSD

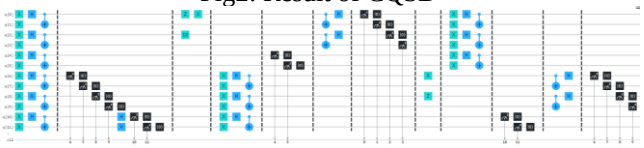

Fig 3: Figure of modified CQSD

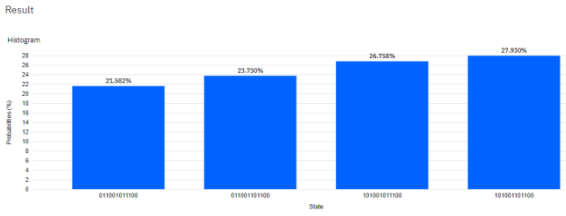

Fig 4: Result of modified CQSD

IV. RESULT

Quantum computing and its quantum mechanical phenomena like entanglement offers a new modality for communications that is different from classical communications. The motivation for use of quantum entanglement (EPR pairs and Bell states) its flexibility and security even though some of the quantum entanglement protocols are non-intuitive. It seems clear that traditional/classical communications engineers will need to develop a new way of thinking that moves them away from classical intuition in order to take advantage of the entanglement resource inbuilding advanced communication systems.

V. REFERENCES

[1] Sandip das, Ankan Chakraborty, Debjani Chakraborty and Sumanjit Moshat. “Pc to Pc Data Transmission Using Visible Light Communication”

[2] Weiming Ding, Junyi Zhang, Hongbin Xia. “Theoretical Demonstration of Light Injection intothe Communication Fiber”.

[3] Fabian Harendran Jesuthasan, Hardik Rohit Kumar, Purav Shah, Huan X. Nguyen and Ramona Trestian. “On The Impact Of Visible Light Communication For Audio And Video Transmissions”.

[4] Saily P. Bhanse and Savita R. Pawar. “Li + Wi-Fi: The Future Of Internet Of Things”.

[5] M. A. Nielsen, and I. L. Chuang, “Quantum computation and quantum information,” (Cambridge University Press, Cambridge,2000).

[6] A. Holevo, “Quantum Systems, Channels, Information: A Mathematical Introduction,” (De Gruyter, BerlinBoston,2012).

[7] I. Bengtsson and K. Zyczkowski, “Geometry of quantum states: An Introduction to Quantum Entanglement,” (Cambridge University Press, Cambridge2006).

[8] M. Hayashi, “Quantum Information Theory: Mathematical Foundation,” (Springer- Verlag, Berlin,2017).

[1] J. Watrous, “The theory of quantum information,” (Cambridge University Press, Cambridge,2018)

[2] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, “Gaussian quantum information,” Rev. Mod. Phys. 84, 621(2012).

[3] S. L. Braunstein, and P. Van Loock, “Quantum information with continuous variables,” Rev. Mod. Phys. 77, 513(2005).

[4] G. Adesso, S. Ragy, and A. R. Lee, “Continuous Variable Quantum Information: the Gaussian States and Beyond,” Open Syst. Inf. Dyn. 21, 1440001(2014).

[5] A. Serafini, “Quantum Continuous Variables: A Primer of Theoretical Methods,” (Taylor & Francis, Oxford,2017).

[6] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, “Hybrid quantum information processing,” Nat. Phys. 11, 713–719(2015)

[7] G. Kurizki, P. Bertet, Y Kubo, K. Mølmer, D. Petrosyan, P. Rabl, J. Schmiedmayer, “Quantum technologies with hybrid systems,” Proc. Natl. Acad. Sci. USA 112, 3866-73 (2015).

[8] J. P. Dowling, G. J. Milburn, “Quantum technology: the second quantum revolution,” Phil. Trans. R. Soc. Lond. A 361, 1655-1674(2003).

[9] J. Lars, “The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies,” (Springer International Publishing,2018).

[10] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, “Quantum entanglement,” Rev. Mod. Phys. 81, 865(2009).

[11] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-PodolskyRosen channels,” Phys. Rev. Lett. 70, 1895 (1993).

[12] S. L. Braunstein and H. J. Kimble, “Teleportation of Continuous Quantum Variables,” Phys. Rev. Lett. 80, 869–872(1998).

[13] S. L. Braunstein, G. M. D’Ariano, G. J. Milburn, and M. F. Sacchi, “Universal Teleportation with a Twist,” Phys. Rev. Lett. 84, 3486(2000)

[14] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, “Advances in Quantum Teleportation,” Nature Photonics 9, 641-652(2015).

[15] W. Wootters, W. Zurek, “A Single quantum cannot be cloned,” Nature 299, 802(1982).

[16] J. Park, “The concept of transition in quantum mechanics,” Found. Phys. 1, 23(1970).

[17] R. J. Schoelkopf and S. M Girvin, “Wiring up quantum systems,” Nature 451, 664 (2008).

[18] P.W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22(1994).

[19] P.W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM J. Comput., 26, 1484(1997).

[20] R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM’, 21, 120(1978).

[21] M. Agrawal, N. Kayal, N. Saxena, “Primes is in P,” Annals of Mathematics 160, 781- 793(2004).

[22] M. Mosca, “Setting the Scene for the ETSI Quantumsafe Cryptography Workshop,” e- proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26- 27 September (2013).

[23] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys. 74, 145(2002)

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du˘sek, N. L¨utkenhaus, and M. Peev, “The Security of Practical Quantum Key Distribution,” Rev. Mod. Phys. 81, 1301 (2009).

[25] E. Diamanti and A. Leverrier, “Distributing Secret Keys with Quantum Continuous Variables: Principle, Security, and Implementations,” Entropy 17, 6072(2015).

[26] E, Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” npj Quantum Information 2, 16025 (2016).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

[27] Sandip das, Ankan Chakraborty, Debjani Chakraborty, and Sumanjit Moshat, "PC to PC Data Transmission using Visible light Communication".

[28] Weiming Ding, Junyi Zhang, Hongbin Xia." Theoretical Demonstration Of Light Injection Into The Communication Fiber".

[29] Fabian Harendran Jesuthasan, Hardik Rohit Kumar, Purav Shah, Huan X. Nguyen, and Ramona Trestian." On the Impact of Visible Light Communication for Audio and Video Transmissions."

[30] Saily P. Bhanse and Savita R. Pawar." Li + Wi-Fi: The Future of the Internet of things".

[31] Shaokai Lin, Zichuan Wang, and LiorHoresh, "Communication over Continuous Quantum Secure Dialogue using Einstein-Podolsky-Rosen States", arXiv:1910.08135v2 [quant-ph] 27 Oct 2019.