Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Secure Communication System for Free Space Utilizing Quantum Computing Based Multiple Bits Encryption and Decryption

Kavita R. Singh[1], Kapil Gupta[2], Sagarkumar S. Badhiye[3], Roshni S. Khedgaonkar[4], Pravinkumar M. Sonsare[5]

[1]Professor, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra
[2]Assistant Professor, Department of Computer Science and Engineering, Vincent Palloti College of Engineering and Technology, Nagpur
[3]Assistant Professor ,Symbiosis Institute of Technology, Nagpur Campus, Symbiosis International (Deemed University), Pune, India
[4]Assistant Professor, Department of Computer Technology, YeshwantraoChavan College of Engineering, Nagpur
[5]Assistant Professor, Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur
Email:singhkavita19@gmail.com

In this research, an embedded system based quantum encryption and decryption using polarization scheme is proposed in the transmitter and receiver side .The information data andencryption code is fed into quantum encryption setup, where the encryption takes place and ispassed to the LED's polarizer form where it is converted as photons and passed to the receiver. At the receiver end, LDR's (light dependent resistor) are used, which act as a detector forconversion of light energy to optical energy. LDR output is decrypted using quantum decryptingand the original message is recovered. In the proposed system, the polarization state of photoncarries, quantum encryption key (private key if user). The property of photons is used in errordetection in the proposed system.The significant outcome of this research is that eaves dropping in quantumcommunication channel are always detected and the proposed system does not implementcomplex mathematical algorithms for its security. This research work is implemented in anembedded hardware for different transmission lengths for which encryption and decryption isperformed at a faster rate, when compared to implementation involving software simulationalone. The future enhancement of the above research would involve avoiding the usage ofquantum repeaters to achieve significant data transmission and reception.

Keywords: Embedded system, Quantum encryption, Decryption, Light dependent resistor

(LDR).

1. Introduction

In today's world, security in data communication has become a top most priority every organization and entity swears by it. In general, cryptography is defined as the methodology to ensure data is secure by employing suitable encryption and decryption techniques. In the transmitter side, the original message is encrypted using a key. Then the encrypted data is decrypted with the duplicate key at the receiver side as per the accepted protocol between the two parties. [1].

In the realm of secure communication, the burgeoning field of quantum computing has emerged as a promising frontier. Leveraging the principles of quantum mechanics, particularly the unique properties of quantum bits (qubits), quantum computing offers unprecedented capabilities in encryption and decryption. In this context, we propose a novel secure communication system designed for free space transmission, harnessing the power of Quantum Computing Based Multiple Bits Encryption and Decryption (QCMBED)[2].

Traditional encryption methods often rely on mathematical algorithms that, while robust, may eventually succumb to advancements in computational power or algorithmic breakthroughs.[3] Quantum computing, on the other hand, operates on fundamentally different principles, exploiting quantum phenomena such as superposition and entanglement to perform operations at speeds exponentially faster than classical computers[4].

Our proposed system integrates quantum encryption and decryption techniques within a free space communication framework, offering unparalleled security and efficiency[4][5]. Unlike conventional systems, which typically encrypt and decrypt data one bit at a time, QCMBED enables simultaneous encryption and decryption of multiple bits using quantum states[5].

At the heart of our communication system lies a quantum encryption setup, where information data and encryption codes are encoded onto qubits utilizing polarization schemes[6]. These qubits serve as carriers of information, their polarization states representing the encryption keys.

In the transmitter side, the encoded qubits are converted into photons and transmitted through free space. This process involves passing the qubits through LED-based polarizers, ensuring their conversion into photons with the desired polarization states intact. This ensures that the information remains secure during transmission.Upon reception, the photons are detected by Light Dependent Resistors (LDRs) acting as detectors. The output from the LDRs undergoes quantum decryption, where the quantum states of the received photons are utilized to recover the original message. The decryption process occurs simultaneously across multiple bits, enhancing the speed and efficiency of communication[7].

Furthermore, the implementation of our system in embedded hardware facilitates faster encryption and decryption rates compared to software simulations alone.

This hardware-based approach ensures efficient communication even over extended transmission lengths.In conventional cryptographic techniques, eaves dropping are prevented from accessing the contents of encrypted message by employing certain mathematical function and techniques, but this security methodology does not guarantee any key security[8]. In many scenarios, a secure communication link is established by using key but a third party with a mollified intent may steal the session keys, giving rise to data security, getting compromised. So in this regard, quantum cryptography is a better alternative when it comes to data security integrity[9]. The main objective of providing security is to restrict information and resource access to the authorized people who utilize the system. In general, security breach can be classified in four categories (a) interrupter (b) interceptor(c) modification (d) fabrication interruption implies, the main core of the system which gets destroyed or becomes unavailable on unusable interceptor implies that an unauthorized party has hacked the service or data[10]. Modification implies unauthorized alternator of data or service tempering such that it no longer adheres to its original specification, fabrication infers to the situation where are additional data or activity gets generated that would normally won't exist.

2. Cryptography is Conventional Sense

A technique involving the usage of mathematical formula to covert a plain text to cipher text and vice versa to ensure secure data transmission between transmitter and receiver. Encryption is a process which produce a cipher text from plain text[11]. The reverse process is termed as decryption. In this Digital age, attackers and hackers are at large, eaves dropping and performing cyber fraud, leading to the necessity of storing the information in a secure manner. This has also led to massive awareness campaign for protecting digital assets from being disclosed, ensuring the authenticity of data and messages and also ensuring that system is protected from network based attacks smart phone, ATM cards, digital signatures, all employ cryptography in one form to other to ensure data protection[12].The schematic employs two important channel of communication. The first is the quantum channel which transmits and receives quantum bits and generates session key. The second is the channel which forms the link between the sender and receiver to compare whether the quantum's bits are tapped[13]. Encryption decryption takes place between sender and receiver, keeping the communication secure, the function of eaves dropping detection block is to check whether a change in the quantum state occurs due to eaves dropper obtaining the guarantee bits to compose session key there by detecting the eaves dropper. Therefore this scheme is more practical and efficient when compared to conventional cryptographic system

3. Quantum Cryptography

Quantum cryptography the involve the usage of quantum communication and quantum computation to perform various cryptographic tasks. The most important mathematical tools involved are (a) complex numbers, (b) vertical representation of function having infinite components (c) energy function and wave nature of the particle .unlike conventional cryptographic, where certain task are perceived to impossible ,quantum cryptography makes

it possible to impossible, quantum cryptography make it possible by employing protocols such as bb84 for a single by employing protocols such as bb84 for a single photon and E91 for entangled particle in quantum cryptography, quantum channel are employed generously for key distribution and the encoded message are sent through public channels. In conventional communication, the signal is split and amplified so the communication parties completely unaware whether eaves dropping has taken place or not, leading to jeopardizing the sharing of private keys. The no cloning theorem in completely eliminates and duplication of unknown state of a particle and thereby preventing the copies of original particle

Loss of data in quantum computing creates vulnerabilities in system that implements quantum cryptographic techniques. One of the major threats in a quantum cryptographic system is the tampering of quantum key distributer, leading to generation of duplicate key due to random number generator attack. The attacks can be classified in various categories namely Trojan those attack and time shift attack. The those attack can be detected to check the non-legitimate signal from entering the transmitter. Similarly time shift attack can also be detected by modifying the implementation accordingly. A part from these two attacks. There are many type like faked state attacks phase remapping and time shift attacks to name a few.

4. Quantum Random Access memories (QRAM)

N = 2n unique memory cells can be randomly addressed by a Random Access Memory (RAM) using n bits. Any quantum superposition of N memory cells can be addressed by n qubits in a quantum random access memory (qRAM). This study presents an architecture that drastically decreases the number of switches that must be thrown during a memory call: O(logN) switches, as opposed to the N required in traditional (classical or quantum) RAM systems. This results in an exponential reduction in the power required for addressing and produces a more resilient qRAM algorithm overall. It also requires entanglement among exponentially fewer gates.The ability to store data in a variety of memory cells is a basic feature of any computing device.

Random access memory, or RAM, is the most adaptable architecture for memory arrays because it allows any memory cell to be addressed whenever necessary. An input register, also known as a "address register," an output register, and a memory array make up a RAM. Every cell in the array has a distinct numerical address assigned to it. The content of a memory cell is returned to the output register ("decoding") once the address register is initialised with the address of the memory cell. If big quantum computers are ever constructed, quantum random access memory, or RAM, will be a crucial component, just as RAM is a crucial component of classical computers[14]. Its three fundamental parts are the same as those of the RAM, except instead of bits, qubits (quantum bits) make up the address and output registers. [The memory array may be quantum or classical, contingent on the application of qRAM].

RAMs, both quantum and classical, are computationally costly: Conventional architectures require throwing O(N1/d) switches, or two-body interactions, in order to access one of the N = 2n memory slots, where n is the number of bits in the address register, if the memory array is arranged in a d-dimensional lattice. This exponential resource consumption results in a

significant decoherence rate for QRAMs and a comparatively poor decoding speed and energy consumption for traditional RAMs. This is the reason that the development of a QRAM has received little attention thus far. A novel RAM architecture called "bucket-brigade" is given in this study, which lowers the number of switches that must be thrown during a RAM call—quantum or classical—from O(N1/d) to O(logN). When compared to typical configurations, the running time computational complexity at the information theoretical level is exponentially reduced if the travel time of the signals along the wires connecting the device's components is neglected[15]. It involves simplifying the QRAM circuit in comparison to standard architectures, cutting down on the number of gates that must be entangled for each memory call, and eliminating the requirement for costly error correction procedures. Furthermore, fewer switchings means less energy used for routing, which could result in RAMs that are more energy-efficient and consume less power during decoding than existing architectures[3].[4]. By making the fan out scheme and the bucket-brigade scheme reversible processes and necessitating the preservation of quantum coherence, they can both be converted into quantum RAM algorithms. This is accomplished, in abstract, by linking the quantum bus—a quantum signal—with the memory cell through an H-gate and transmitting it back and forth in a binary trees fashion[4][7].

5. Quantum Error Correction Code

Achieving fault-tolerant quantum computation that can handle noise, stored quantum information, and quantum gates with flawed design, preparation, and measurements relies heavily on quantum error correction codes, which play a critical role in protecting information from errors caused by de coherence and other sources of quantum noise [9]. To ensure the safety of data transmission, quantum key distribution makes use of individual photons. Assuming absolutely no turbulence in the air, the polarisation state of a photon travelling through open space will not change. The polarisation state of a photon, however, varies significantly as it passes through an optical fibre. By taking use of the characteristics of quantum objects like photons, this study is able to accomplish quantum encryption and decryption.

As a rule, both classical error correction codes and quantum error correction utilise syndrome measuring methods to encode data. This study employs a multi-qubit measurement on the encoded state to enable the retrieval of error information while preserving the integrity of the encoded state's quantum information. By measuring syndromes, quantum error correction codes may determine whether a qubit is damaged and, if so, in what ways. This study revealed not just which physical qubit was impacted, but also the potential ways in which it was affected. Bit flip, sign flip, or a mix of the two is usually at blame for the mistake. The measurement effect in a quantum experiment might be the culprit. Put differently, if the noise-induced error is completely random, then the error may be represented by a superposition of Pauli matrices and identification operators [12]. The quantification of syndrome allows the qubit to decide on a particular Pauli mistake that may have occurred, and the syndrome itself identifies the fault. The corrupted qubit is subjected to the Pauli operator in order to undo the mistake's impact. Although the syndrome measurement provides extensive details on the mistake that happened, it provides very little details regarding the value stored in the logical qubit in relation to other qubits inside the quantum computer.

6. Quantum key distribution

In communication, data is encrypted for confidentiality. In conventional method, the existing encryption techniques depends on the encryption key (private key) and it is used for one session only and then rejected. The need for reliable and effective methods for the distribution of the encryption keys is required in conventional method. The secure and reliable methods for cryptographic key distribution is an active research area in communication. In this research work polarization based quntum key distribution is proposed[13]. In this work, vertical /horizontal or diagonal polarized photons can be transmitted by the proposed system. If the photon with horizontal/vertical polarization is used in transmitter, then the photon with vertical polarization will transmit '1' and the photon with horizontal polarization will transmit '0'. If the photon with diagonal polarization is used, then the photon with θ1 degree is encrypted form of '1' and photon with θ2 degree is encrypted form of '0'. In receiver side, photons are seperated with different polarization. In tramsmitter side, the encryption key is selected with the length of 'x'. In transmitter side, two random strings (S1 and S2) are generated with the length of (4+δ)x. By choosing 'δ' sufficiently large transmitter and receiver ensures that the number of bits used is close to '2x' with a very high probability. A substring of length 'x' of the bits in string 'S1' is used as the qunatum encryption key and the bits in string 'S2' is used by transmitter to select the (V/H) polarization or (DG) polarization for each photon transmit to receiver. The binary form of the data in string 'S1' is encrypted based upon the corresponding values of the bits in string 'S2'. The encryption process is shown in table 1 and the decryption process is shown in table 2. The original data is reconstructed by using table4.4 in receiver side.

Table 1. Encryption process based on polarization

i th bit of the string S2.	Polarization type	Binary form of data in 'S1' encrypted into photon polarizationParameter	
		1	0
1	V/H polarization	Vertical polarization	Horizontal Polarization
2	Diagonal polarization	Photon with 'θ1' polarization	Photon with 'θ2' polarization

Table 2. Decryption process based on polarization

Encrypted data in 'S1'	Decrypted data
Vertical polarization	1
Horizontal polarization	0
Photon with 'θ1' polarization	1
Photon with 'θ2' polarization	0

Using polarisation, this study proposes quantum encryption and decryption for embedded systems. Quantum encryption encrypts data by taking in both the data and the encryption algorithm. The data is transformed to photons and sent to the transmitter after passing via an LED polarised system. At the receiving end, a light-dependent resistor (LDR) serves as a detector to convert light energy into an electrical signal. The receiver side retrieves the original message after decrypting the LDR output using a quantum decryption technique. The suggested approach makes use of photon properties for error detection and their polarisation states to transport a quantum encryption key (the user's private key).

7. Conclusion

In this research, a quantum based multiple bit crypto scheme using qcl and quipper simulator is discussed. The oracles are implemented using the functional programming language in GHC script. Polarization based encryption and decryption is demonstrated and proved as a secure mode of communication in free space. Significant aspect of this research involves implementing embedded system based quantum encryption and decryption using polarization in hardware. Implemented hardware is analyzed for three different transmission lengths (1/X, 2/X and X), from which it is found that encryption & decryption using polarization having length 1/X has relatively produced efficient results, when compared to other analysis methods(2/x and x),in terms of faster rates of encryption &decryption.

Conflicts of Interest

The authors declare that they have no competing interests.

References

1. Koch, C. P., Boscain, U., Calarco, T., Dirr, G., Filipp, S., Glaser, S. J., et al. (2022). Quantum optimal control in quantum technologies. Strategic report on current status visions and goals for research in Europe. EPJ Quantum Technol., 9(1), 203-228.
2. Abushgra, A. A. (2022). Variations of QKD protocols based on conventional system measurements: A literature review. Cryptography, 6(1), 12.
3. Hasan, S. R., Chowdhury, M. Z., &Saiam, M. (2022). A new quantum visible light communication for future wireless network systems. In Proc. Int. Conf. Advancement Electr. Electron. Eng. (ICAEEE) (pp. 1-4).
4. Ingole, K., &Padole, D. (2023). Design Approaches for Internet of Things Based System Model for Agricultural Applications. In 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) (pp. 1-5).
5. Perumal, A. M., &Nadar, E. R. S. (2022). Retraction note to: Architectural framework and simulation of quantum key optimization techniques in healthcare networks for data security. J. Ambient Intell. Humanized Comput., 12, 7173-7180.
6. Wang, P., Zhang, R., & Sun, Z. (2022). Practical quantum key agreement protocol based on BB84. Quantum Inf. Comput., 22(3), 241-250.
7. Tian, Y., Li, J., Chen, X.-B., Ye, C.-Q., & Li, H.-J. (2021). An efficient semi-quantum secret sharing protocol of specific bits. Quantum Inf. Process., 20(6), 1-11.
8. Alshaer, N., Moawad, A., & Ismail, T. (2021). Reliability and security analysis of an entanglement-based QKD protocol in a dynamic Ground-to-UAV FSO communications system. IEEE Access, 9, 168052-168067.
9. Singh, A., Dev, K., Siljak, H., Joshi, H. D., &Magarini, M. (2021). Quantum internet—Applications functionalities enabling technologies challenges and research directions. IEEE Commun. Surveys Tuts., 23(4), 2218-2247.
10. Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). 6G wireless communication systems: Applications requirements technologies challenges and research directions. IEEE Open J. Commun. Soc., 1, 957-975.
11. Nguyen, Q. N., Aboura, S., Chevallier, J., Zhang, L., & Zhu, B. (2020). Local Gaussian correlations in financial and commodity markets. European Journal of Operational Research, 285(1), 306–323.

12. Wang, L., & Alexander, C. A. (2020). Quantum science and quantum technology: Progress and challenges. Amer. J. Elect. Electron. Eng., 8(2), 43-50.
13. Nejrs, Salwa Mohammed(2023) Medical images utilization for significant data hiding based on machine learning, Journal of Discrete Mathematical Sciences and Cryptography, 26:7, 1971–1979, DOI: 10.47974/JDMSC-1785
14. Lin, Lon, Lee, Chun-Chang, Yeh, Wen-Chih& Yu, Zheng(2022) The influence of ethical climate and personality traits on the performance of housing agents, Journal of Information and Optimization Sciences, 43:2, 371-399, DOI: 10.1080/02522667.2021.2016986
15. Johri, P., Khatri, S.K., Al-Taani, A.T., Sabharwal, M., Suvanov, S., Kumar, A. (2021). Natural Language Processing: History, Evolution, Application, and Future Work. In: Abraham, A., Castillo, O., Virmani, D. (eds) Proceedings of 3rd International Conference on Computing Informatics and Networks. Lecture Notes in Networks and Systems, vol 167. Springer, Singapore. https://doi.org/10.1007/978-981-15-9712-1_31