Survey paper on Quantum Cryptography for Improving Security Level and Data Rate

Miss. Nayan Rai[1], Miss. Antara Bhattacharya[2]
Department of Computer science & Engineering
[1] G.H. Raisoni Institute of Engineering & Technology, Nagpur, India
[2] Lecturer ,G.H. Raisoni Institute of Engineering & Technology, Nagpur, India

Abstract-*With rapidly developing technology, the available encryption techniques are becoming more prone to attacks day by day. Focusing this issue, this research work proposing a new encryption technique quantum computing that will enhance the security level by a significant margin and also enhances data transmission rate through exploiting the notion of Superdense Coding. Our proposed technique is a rare trait for currently available encryption technique through which we achieve simultaneous improvement in both security level and data transmission rate. This research work evaluates the performance through analyzing the simulation results in network simulator ns-3. The simulation results demonstrate significant performance improvement compared to available classical alternative*

Keywords-XOR, NS-3

I. INTRODUCTION

Since the ancient times, secured transfer of information has been a matter of concern for people. For this reason, the study of cryptography is becoming more important day-by-day because with the rapidly developing technology, the need for secured data transfer is growing every day. In early ages, the main focus of cryptography was encryption. Encryption still remains a very important part of cryptography though different methods such as encryption, authentication, non-repudiation, etc, have been applied in modern times.

To address this issue, in this research work a new technique is proposed for encryption that will provide enhanced security level and also offers an increased data transmission rate. Here, this research applying a two-level operation on the encryption key. Additionally, exploiting a unique feature of quantum computing, called Superdense Coding, in combination with the two-level operation that contributes in an increasing data transmission rate.

In this proposed technique, first, the actual message is encrypted by exclusive-OR (XOR) operation with an encryption key. The classical channel is used for transmitting the encrypted data. Here, the bits of the key are first permuted and then encoded using Superdense Coding. The advantage of Superdense Coding is that, during the process, the information is transmitted to the receiving end within a very short delay due to having entangled photons. On the other hand, at the receiving end, the qubits are first measured as a part of decoding process. Afterwards, the measured qubits are repermuted. This process reverts back the actual encryption key at the receiver end. Subsequently, the key can be used to decrypt the message. Thus, this proposed technique actually exploits the notion of symmetric key cryptography.

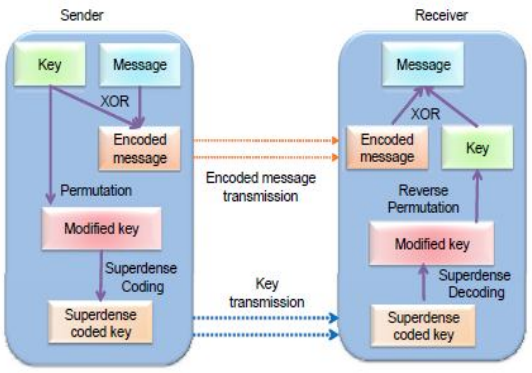


Fig. 1: Block diagram of proposed system

All the operations at sender and receiver ends are mentioned in above figure. In this system, the two-step encryption of the key makes it extremely difficult for any intruder to decrypt and get the key. This proposed technique of encryption focuseson simultaneously improving both security level and data transmission rate.

II. LITERATURE REVIEW

A. Quantum Computing

Quantum computing deals with quantum information, which is based on an analogous concept of bit called quantum bit or qubit. A classical bit has a state of either 0 or 1. This quantum state is a linear combination of the classical states, which is often called superposition state. A quantum bit or qubit, also has a quantum state that can be a superposition of both the classical states (0 & 1) at the same time.

The superposition state can be written as: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are probability amplitudes and both be complex numbers. The states $|0\rangle$ and $|1\rangle$are called computational basis states. Quantum computation allows a huge number of calculations that can be simultaneously carried out with the help of the notion of superposition states. For example, a quantum computer with 400 basic units (qubits) could, simultaneously process more bits of information than the number of atoms in the universe. Such enormous processing power has driven towards devising new coding techniques that can deal with qubits. Superdense Coding is one of such techniques.

In quantum information theory, Superdense Coding refers to a technique used to send two bits of classical information using only one qubit. Superdense Coding requires entanglement between sender device and receiver device. Here, the notion of quantum entanglement refers to a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other even though the individual objects may be spatially separated.

B. Quantum Cryptography

The use of quantum mechanical properties to perform cryptographic tasks can refer as Quantum cryptography. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e., nonquantum) computation. A method of securely communicating a private key from one party to another for using in one-time pad encryption is known as basic protocol of quantum cryptography.

The traditional quantum cryptography depends on correct selection of bases for measurement of qubits. In this protocol, using particular bases a sender encodes his one-time pads in strings of qubits through performing some quantum operations. Then he sends it over a public quantum channel. However, it is impossible for the receiver to distinguish all original states of the qubits because only the sender knows the actual bases of his quantum operations. Here, his probability of guessing the right bases is $\frac{1}{2}$ because as the receiver independently chooses own bases while receiving and decoding the received qubits back to the original pads. Therefore, 2n qubits are needed to be transmitted on an average to construct an n-bit one-time pad. This is certainly a loss of qubits. Behind our proposed technique such loss of qubits is a strong motivation.

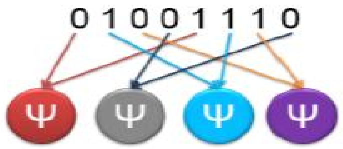
C. Superdense Coding

In this proposed technique, Using one-time padding encryption mechanism we attempt to devise a method for enhancing the security level of the key. The encryption in one-time padding starts through selecting a key at the sender, Bob. Bob performs an exclusive-OR (XOR) operation between the selected key and the message to be transmitted. Then he transmits the encoded message. However, Bob needs to ensure the security of the key itself as the key needs to be transmitted over the same channel.

Key: 10110010

Permutated Key: 01001110

(a) Step 1: Permutation of bits in a key



Key bit positions		Photon position
1	5	1
4	8	2
2	7	3
3	6	4

(b) Step 2: Superdense Coding on the permuted bits

Fig. 2: The sender device encoding process

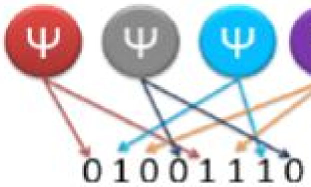
In this proposed technique, to enhance the security of the key to be transmitted Bob needs to perform two operations. First, he performs a permutation operation on the bit sequence of the key. In the second step, he takes a pair of bits from the modified bit sequence and performs Superdense Coding on those. As a result, an n bit key is encoded in $\frac{n}{2}$ qubits. Fig. 2 presents the whole encoding process.

In Superdense Coding, if the sender wants to transmit a 2-bit message, e.g., 00, 01, 10, or 11 to the receiver, he first performs a single qubit operation on his qubits. The sender selects the operation according to the content of the message under transmission as follows:

- I gate operates on message 00
- X gate operates on message 01
- Z gate operates on message 10
- iY gate operates on message 11

Here, X, Y, and Z are the basic quantum gates. Besides, applying I gate refers to doing nothing and applying iY gate refers to applying both X and Z gates together.

Photon position	Key bit positions	
1	1	5
2	4	8
3	2	7
4	3	6



(a) Step 1: Superdense decoding on the permuted bits

Received Key: 01001110

Reverse permutated Key: 10110010

(b) Step 2: Re- permutation of bits in a key

Fig. 3: The receiver device decoding process

The decoding process confirms providing Alice an n bit key from $\frac{n}{2}$ qubits. Subsequently, he performs the permutation as decided earlier and gets the original bit sequence. At the end of this process, to decrypt the message Alice has the exact key or one-time pad. Fig. 3 presents the full decoding process.

III. CONCLUSIONS

This research work attempts to present a new technique of encryption which simultaneously improves both security level and data rate with the help of quantum computing and quantum Cryptography. We outline the theoretical aspects of the proposed system. We will also evaluate the performance of the proposed technique through performing simulation in NS-3.

REFERENCES

[1] Kazi Sinthai Kabir, Tusher Chakraborty and A.B.M. Alim Al Islam, “SuperCrypt: A Technique for Quantum Cryptography through Simultaneously Improving both Security Level and Data Rate” IEEE International Conference on “Networking Systems and Security (NSysS)”, Jan 2016.

[2] Nusrat Jahan Oishi, Md. Arafin Mahamud, Asaduzzaman, “Short Paper: Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6”, International Conference on “Networking Systems and Security (NSysS)”, Jan 2016.

[3] Fahimesh Zarmehi and Monireh Houshmand, “Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement” IEEE Communications Letters, Volume:PP , Issue: 99 , July 2016.

[4] Shenam Chugh, Kamal, ”Securing data transmission over wireless LAN (802.11) by redesigning RC4 Algorithm”, IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), Oct. 2015

[5] Muneer Alshowkan, “Authenticated Multiparty Secret Key Sharing Using Quantum Entanglement Swapping”, Proceedings of 2014 Zone 1 Conference of the “American Society for Engineering Education (ASEE Zone 1)”, April 2014

[6] Gabriel A.J, Alese B.K, Adetunmbi A.O. and Adewale O.S., “Post-Quantum Cryptography: A Combination of Post-Quantum Cryptography and Steganography”, IEEE 8th International Conference on Internet Technology and Secured Transactions (ICITST), Sep 2013.

[7] N. Roch, M. E. Schwartz, F. Motzoi, C. Macklin, R. Vijay, A. W. Eddins, A. N. Korotkov, K. B. Whaley, M. Sarovar, and I. Siddiqi, “Observation of measurement-induced entanglement and quantum trajectories of remote superconducting qubits,” Physical review letters, vol. 112, no. 17, p. 170501, 2014.

[8] D. Riste, M. Dukalski, C. Watson, G. de Lange, M. Tiggelman, Y. M. Blanter, K. Lehnert, R. Schouten, and L. DiCarlo, “Deterministic entanglement of superconducting qubits by parity measurement and feedback,” Nature, vol. 502, no. 7471, pp. 350–354, 2013.

[9] E. Mart´ın-L´opez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O’Brien, “Experimental realization of shor’s quantum factoring algorithm using qubit recycling,” Nature Photonics, vol. 6, no. 11, pp. 773–776, 2012.

[10] A. Bogdanov, D. Khovratovich, and C. Rechberger, “Biclique cryptanalysis of the full aes,” in Advances in Cryptology–ASIACRYPT 2011, pp. 344–371, Springer, 2011.