ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

Quantum Cryptography Using SuperCrypt to Improve Security Level and Data Rate

K.KALAISELVI [1], Dr.C.SUMITHRADEVI [2]

1. P.G. Student, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India
2. Assistant Professor, Dept. of MCA, VSB Engineering College, Karur, Tamilnadu, India

Abstract—Secured data transmission has always been a matter of great interest and several encryption techniques for secured data transmission have been devised till now in this regard. However, with rapidly developing technology, the available encryption techniques are becoming more prone to attack every day. Focusing this issue, in this paper, we propose a new technique of encryption that will enhance the security level by a significant margin with the help of quantum computing. Additionally, our proposed technique also enhances data transmission rate through exploiting the notion of Superdense Coding. Such simultaneous improvement in both security level and data transmission rate, which we achieve through our proposed technique, is a rare trait for currently available encryption technique. We name our proposed technique SuperCrypt. We elaborate implementation issues pertinent for SuperCrypt such as recycling qubits and re-establishing entanglement. The simulation results demonstrate significant performance improvement through SuperCrypt compared to available classical alternative. Further, we briefly present a more sophisticated and synchronized version of SuperCrypt that we plan to investigate in future.

1. INTRODUCTION

Since the very early ages, secured transfer of information has been a matter of concern for people. With the rapidly developing technology, the need for secured data transfer is growing every day. For this reason, the study of cryptography is becoming more important day-by-day. At the ancient times, the main focus of cryptography was encryption. Though different methods such as encryption, authentication, nonrepudiation, etc, have been applied in modern times, encryption still remains a very important part of cryptography. There are several techniques of encryption in the literature such as one-time padding [1], RSA [2], AES [2], ElGamal [3], quantum cryptography [1], etc. However, recent studies show that none of these mechanisms is secure enough [1], [3]–[5]. In fact, RSA encryption, which was considered to be the most secure one among all the available alternatives, becomes vulnerable under the exploitation of quantum technology [1], [4]. Therefore, the search for efficient encryption mechanism is still going on. To address this issue, in this paper, we propose a new technique for encryption that will provide enhanced security level. In addition to enhancing the security level, our proposed technique offers an increased data transmission rate, which is a kind of rare for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

conventional cryptography techniques. Here, we apply a two-level operation on the encryption key. Additionally, we exploit a unique feature of quantum computing, called Superdense Coding, in combination with the two-level operation that contributes in an increasing data transmission rate. We term our proposed technique SuperCrypt. In SuperCrypt, first, the actual message is encrypted by exclusive-OR (XOR) operation with an encryption key. The encrypted message is then transmitted through the classical channel. 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, our proposed technique actually exploits the notion of symmetric key cryptography.

2. RELATED WORK

There are several techniques of encryption in the literature such as one-time padding [1], RSA [2], AES [2], ElGamal [3], quantum cryptography [1], etc. In one-time padding, though the level of security of transmitted data is very high, each onetime pad itself needs a secure way of transmission rendering the task of transmitting the pads a bottleneck in implementation of the technique [1]. Therefore, it is difficult (in many cases even impossible) to implement this technique in reality. On the other hand, the RSA technique has been believed to be a strong mechanism for encryption till now. However, recent studies show that this mechanism has become vulnerable to recent advancements of quantum technology [1], [4]. Consequently, other classical techniques such as AES, Elgamal, etc., have also started exhibiting vulnerability to the quantum technology. Now, getting back to the one-time padding technique, quantum cryptography offers a secured technique for transmitting the one-time pads. One popular protocol of quantum cryptography is the BB84 protocol [1]. Unfortunately, several recent research studies demonstrate that this security is also breakable [1]. Moreover, the mechanism of data transmission in quantum cryptography results in a 50% loss of qubits [1]. As a result, the use of BB84 protocol of quantum cryptography in one-time padding suffers from both limited security and limited performance. Another protocol of quantum cryptography is called Ekert protocol [5] which might be used for better security. However, one limitation to quantum cryptography is that a single photon source actually emits two or more photons. This is called photon number splitting (PNS) [1]. The

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

extra emitted photons can be captured by an intruder resulting in PNS attack [1]. The Ekert protocol states that a true single-photon source might be used to reduce the risk of PNS attack [1]. However, the protocol also states that the risk still remains if pair of photons are used. Moreover, the security of the protocol is higher for longer distances [5]. However, the protocol still depends on the choice of bases selection for measurement. Therefore, 50% loss of resources still exists. In addition to that, longer distance communications faces several losses in quantum channel [7]. Before the evolution of quantum cryptography, RSA technique was considered to be a highly-secured encryption mechanism. The main strength of this technique lies in the fact that factorization of the product of two large prime numbers is computationally very expensive. However, recent studies show that the Shor's algorithm of quantum computing can perform this factorization in polynomial time [8]. In fact, a practical experiment with recycled qubits demonstrated successful factorization of 21 using the quantum algorithm [4]. These studies reveal that, with the rapid development of quantum technology, the classical algorithm of RSA encryption is becoming vulnerable day-by-day.

AES or Advanced Encryption Standard algorithm [9] is based on a combination of both substitution and permutation of the message. Until May 2009, it was considered to be a secured mechanism. However, several studies showed that the security of AES encryption is breakable [9]–[11]. Additionally, Elgamal encryption system [3] is another wellinvestigated asymmetric key encryption system. The security of this algorithm depends upon the difficulty of computing discrete logarithms [3]. However, it has been proven that this system is also vulnerable under chosen ciphertext attack [12].

2.1 EXISTING SYSTEM

There are several techniques of encryption in the literature such as one-time padding, RSA, AES, ElGamal, quantum cryptography, etc. In one-time padding, though the level of security of transmitted data is very high, each onetime pad itself needs a secure way of transmission rendering the task of transmitting the pads a bottleneck in implementation of the technique. Therefore, it is difficult (in many cases even impossible) to implement this technique in reality. On the other hand, the RSA technique has been believed to be a strong mechanism for encryption till now. However, recent studies show that this mechanism has become vulnerable to recent advancements of quantum technology. Consequently, other classical techniques such as AES, Elgamal, etc., have also started exhibiting vulnerability to the quantum technology. [6] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC).

AES or Advanced Encryption Standard algorithm is based on a combination of both substitution and permutation of the message. Several studies showed that the security of AES encryption is breakable. Additionally, Elgamal encryption system is another well investigated asymmetric key encryption system. The security of this algorithm depends upon the difficulty of computing discrete logarithms. However, it has been proven that this system is also vulnerable under chosen ciphertext attack.

2.1.1 Disadvantages of Existing System

1. The security of AES encryption is breakable.

2. Elgamal encryption system depends upon the difficulty of computing discrete logarithms.

3. In addition to that, longer distance communications faces several losses in quantum channel.

2.2 PROPOSED SYSTEM

Secured data transmission has always been a matter of great interest and several encryption techniques for secured data transmission have been devised till now in this regard. However, with rapidly developing technology, the available encryption techniques are becoming more prone to attack every day. It proposes a new technique of encryption that will enhance the security level by a significant margin with the help of quantum computing.Quantum computing is a computation theory that makes direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. The phenomena enable several specialized mechanisms such as Superdense Coding. In the proposed technique, a very important step is Superdense Coding of classical information with qubit. The proposed technique of encryption, SuperCrypt focuses on simultaneously improving both data transmission rate and security level.

2.2.1 Advantages of Proposed System:

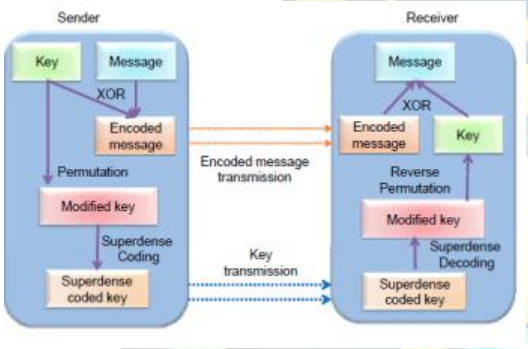
1. Enhancement in Data Transmission Rate
2. Higher Level of Security
3. Computational Complexity for an Intruder

3. SYSTEM MODEL

Among various encryption techniques available now-adays, RSA is considered to be the most widely used one. It is also considered to be one of the most secure encryption techniques for data transmission. However, recent studies demonstrate that the security of RSA technique can be easily broken by Shor's algorithm of quantum computing. Similar

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

outcome is expected for other classical encryption algorithms. Consequently, quantum cryptography seems to be the only possible way-out for securing data transmission. Security in traditional quantum cryptography is based on the selection of bases for measurement of photons, which carry the values of qubits. If an intruder fails to select the bases correctly, he cannot extract the data. However, in recent times, quantum cryptography is also under attack.



A limitation to quantum cryptography is that a single photon source actually can emit two or more photons simultaneously. This is called Photon Number Splitting (PNS. The extra emitted photons can be captured by an intruder resulting in PNS attack. Moreover, the security of traditional quantum cryptography is based on the fact that intruder fails to extract the information if he fails to select the proper basis of measurement. However, in optically controlled quantum systems, there is no need to perform the measurement from any particular basis. This weakens the security of traditional quantum cryptography. Therefore, user needs a more secured encryption method pertinent for the quantum cryptography. Doubled number of photons (i.e., 2n photons) are required to construct an n-bit pad or key in traditional quantum cryptography. This results in half data rate in transmission of the key. As the key is used only once in continuous transmission using one-time padding technique, the resulting half rate can significantly threaten the performance of secured data transmission. Therefore, the system attempt to propose a new technique that will simultaneously improve both the security level and the data transmission rate.

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. A qubit, on the other hand, also has a quantum state that can be a superposition of both the classical states (0 and 1) at the same time. This quantum state is a linear combination of the classical states, which is often called superposition state. The superposition state can be written as: j i = _j0i + _j1i, where _ and _ are probability amplitudes and can, in general, both be complex numbers. The states j0i and j1i are called computational basis states, which form an orthonormal basis for computation in a vector space. With the help of the notion of superposition states, quantum computation allows a huge number of calculations that can be simultaneously carried out. A quantum

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

computer with 400 basic units (qubits) could, for example, 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. In general, Superdense Coding requires entanglement between sender and receiver devices. 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.

Quantum entanglement occurs when particles such as photons, electrons, molecules, or even small diamonds interact physically in a certain way and then get separated. The interaction ensures that each resulting member of a pair is properly described by the same quantum mechanical description or state. The state can correspond to a number of factors such as position, momentum, spin polarization, etc.

Quantum Cryptography

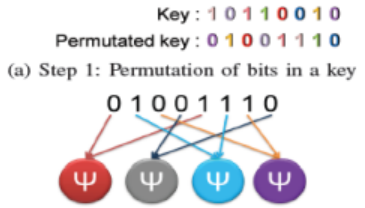
Quantum cryptography refers to the use of quantum mechanical properties to perform cryptographic tasks. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e., nonquantum) computation. The basic protocol of quantum cryptography is usually explained as a method of securely communicating a private key from one party to another for using in one-time pad encryption. The traditional quantum cryptography relies on correct selection of bases for measurement of qubits. In this protocol, a sender encodes her one-time pads in strings of qubits through performing some quantum operations using particular bases. She then sends it over a public quantum channel. However, since only the sender knows the actual bases of her quantum operations, it is impossible for the receiver to distinguish all original states of the qubits. Here, as the receiver independently chooses own bases while receiving and decoding the received qubits back to the original pads, her probability of guessing the right bases is 12. Therefore, to construct an n-bit one-time pad, 2n qubits are needed to be transmitted on an average. This is certainly a loss of qubits. Such loss of qubits is a strong motivation behind proposed technique.

3.1 OVERVIEW OF THE SYSTEM

The encryption in one-time padding starts through selecting a key at the sender, Alice. Alice performs an exclusive-OR (XOR) operation between the selected key and the message to be transmitted. She then transmits the encoded message. However, Alice needs to ensure the security of the key itself as the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

key needs to be transmitted over the same channel.



(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. 1: Encoding process in the sender device

In SuperCrypt, Alice needs to perform two operations to enhance the security of the key to be transmitted. First, she performs a permutation operation on the bit sequence of the key. In the second step, she 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 n 2 qubits in SuperCrypt. Fig. 1 presents the whole encoding process of SuperCrypt. In Superdense Coding, if the sender wants to transmit a 2-bit message, e.g., 00, 01, 10, or 11 to the receiver, she first performs a single qubit operation on her 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

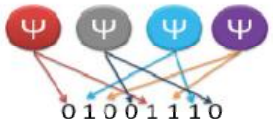
Z gate operates on message 10

iY gate operates on message 11

Here, X, Y , and Z are the basic quantum gates.

The proposed technique of encryption, SuperCrypt focuses on simultaneously improving both data transmission rate and security level.

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 : 0 1 0 0 1 1 1 0

Reverse Permutated Key: 1 0 1 1 0 0 1 0

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

Fig. 2: Decoding process in the receiver device

At the receiving end, the receiver, Bob receives the qubits transmitted by Alice. He performs the same operations performed by Alice in the reverse order. That means, he first decodes the Superdense Coded qubits, and then puts them in correct bit positions.

3.2 STRENGTHS OF PROPOSED TECHNIQUE

Enhancement in Data Transmission Rate

SuperCrypt technique of encryption results in a higher data transmission rate than the existing mechanisms. This happens as one of the steps of the encoding phase involves Superdense Coding. Superdense Coding enables data transmission at double rate through transmitting 2n-bit key using only n

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

photons. Thus, this method supports an increased data transmission rate.

Higher Level of Security

SuperCrypt simultaneously improves both security level and data transmission rate. The encoding mechanism in SuperCrypt involves permutation of the bits and selection of bits for Superdense Coding. This step results in a high computational complexity for an intruder to extract the transmitted information. To better quantify the computational complexity, the following section analyzes the complexity for an intruder to extract the information from an encoded message.

Computational Complexity for an Intruder

According to the decryption method of the proposed technique, the intruder, Trudy needs to perform two steps for successful decryption. First, he has to decode the Superdense Coded information and put the decoded bits in correct positions. Since we can select 2 bits from the n bits of the key in nC2 possible ways, Trudy needs to try nC2 possible combinations. Then, he needs to perform permutation of the bit sequence to find out the correct bit pattern. For this step, he needs to try n! combinations. Therefore, the intruder needs to try X number of bit patterns where,

$$X = n! \times {}^{n}C_2 = n! \times \frac{n^2 - n}{2}$$

This makes the computational complexity of the intruder to be O(n2n!). Obviously, the complexity demonstrates that decoding a key by Trudy demands a significant amount of time in SuperCrypt ensuring a very high level of security.

4. CONCLUSION

Recent technological advancements in computing power leads towards breaking classical encryption techniques. Consequently, the state-of-the-art encryption techniques have started exhibiting their vulnerabilities. For example, RSA (the strongest encryption mechanism available to date) has become vulnerable after the emergence of extremely high computing power through quantum computing. Consequently, it becomes a necessity rather than an ambitious extension to come up with new encryption techniques that will offer more security sustaining system-level performance.

The system presents a new technique of encryption, SuperCrypt to simultaneously improve both security level and data rate with the help of quantum computing and quantum networking. Here, it outlines the theoretical aspects of the proposed system in accordance with portraying its implementation issues. The performance is evaluated of the proposed

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

technique through performing simulation in VB.Net.

FUTURE WORK

The computational power of practical quantum computers is increasing day-by-day, which might cause threat even to the proposed technique in future. This incorporation will increase the level of security at the expense of introducing more complexity in the system. Besides, in the study presented, here mainly focused on encryption of the key while transmitting it through the quantum channel. An important aspect remains for SuperCrypt is that we need to maintain synchronization between transmission of classical information pertinent for the message and transmission of quantum information pertinent for the key, if the users need to retain the classical method of message transmission. This may be needed to continue utilization of already-available classical channels. Now, to develop such a synchronization, to design a hybrid network that will use both classical and quantum channels. Additionally, in recent times, tremendous progress has been made towards building real quantum devices. Therefore, it has been planned to perform real implementation of our proposed technique in near future.

REFERENCES

[1] A. V. Sergienko, Quantum Communications and Cryptography. Taylor and Francis, 2006.

[2] A. S. Tanenbaum, Computer networks, 4th edition. 2003.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Advances in cryptology, pp. 10–18, Springer, 1985.

[4] "University of bristol:quantum computing with recycled particles, sciencedaily. 23 october 2012." www.sciencedaily.com/releases/2012/10/121023112515.htmlast accessed on 16 July, 2015.

[5] D. Naik, C. Peterson, A. White, A. Berglund, and P. Kwiat, "Entangled state quantum cryptography: Eavesdropping on the ekert protocol," Physical Review Letters, vol. 84, no. 20, p. 4733, 2000.

[6] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[7] G. Gilbert and M. Hamrick, "Practical quantum cryptography: A comprehensive

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 17, March 2017

analysis (part one)," arXiv preprint quant-ph/0009027, 2000.

[8] 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.

[9] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full aes-192 and aes-256," in Advances in Cryptology–ASIACRYPT 2009, pp. 1–18, Springer, 2009.

[10] H. Gilbert and T. Peyrin, "Super-sbox cryptanalysis: improved attacks for aes-like permutations," in Fast Software Encryption, pp. 365–383, Springer, 2010.

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

[12] V. Shoup, Why chosen ciphertext security matters. IBM TJ Watson Research Center, 1998.