International Journal of Security and Its Applications
Vol. 11, No. 7 (2017), pp.17-24
http://dx.doi.org/10.14257/ijsia.2017.11.7.02

Introducing Quantum Cryptography Based Secured Encryption and Decryption Algorithms

V. Padmavathi[1], B. Vishnu Vardhan[2] and A. V. N. Krishna[3]

[1]Dept. of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India
chpadmareddy1@gmail.com
[2]Dept. of Computer Science and Engineering, JNTUH College of Engineering, Karimanagar, Telangana, India
mailvishnu@yahoo.com
[3]Dept. of Computer Science and Engineering, Christ University, Bengaluru, Karnataka, India
hari_avn@rediffmail.com

Abstract

With the expansion in electronic communication, the significance of cryptography is apparently increasing every year. Encryption is a cryptography technique to send unintelligible information and decryption to restore the information. These techniques usually undergo difficulty with eavesdropping of plaintext and ciphertext. The conventional cryptography is vulnerable to attacks using high computational resources. Necessarily, an elegant concept of Quantum cryptography based on laws of quantum mechanics is introduced to offer secure and private communication. This paper gives a method for encryption and decryption using Toffoli quantum gate named as VBA Quantum Encryption and Decryption Algorithms. The incorporation of gate renders security which acts as a cumbersome to eavesdropping attack. Besides, a way to detect known plaintext, ciphertext only and chosen plaintext attack through public discussion is explained.

Keywords: *attack; basis; decryption; encryption; quantum cryptography; qubits; Toffoli gate*

1. Introduction

Cryptography is the ability of science which endows security to the information from illicit access and to ensure security services such as authenticity, confidentiality, integrity. The information is being exchanged between two communicating entities usually Sender and Receiver through some channel which may be compromised. Hence cryptography is a way to protect their information from eavesdropping. It involves two algorithms, encryption and decryption and a secret key which is shared between entities. Sender implements encryption algorithm and applies key to it, which follows some rule to scramble the original information or plaintext such that restoring is possible only for Receiver. The scrambled information is usually known as ciphertext. On the other end, Receiver makes use of decryption algorithm and key to the ciphertext to restore the plaintext. Nevertheless, the security provided by conventional cryptography is vulnerable to various threats by means of high computational resources. Consequently, the concept of quantum cryptography based on laws of quantum mechanics is introduced into the world of security by Stephen Wiesner in 1969 [1].

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2017 SERSC

The challenge and the power of conventional cryptography is extended using quantum cryptography. The essential unit of information is qubit and represented with Dirac notation [2].

Quantum cryptography requires two basis specifically rectilinear (R) and diagonal (D) and photon polarized into four states using these bases to encode bits into qubits. A photon polarized in 0° in the rectilinear basis or 45° in the diagonal basis is binary 0. A photon polarized in 90° in the rectilinear bases or 135° in diagonal bases is binary 1 [4]. Figure 1 and 2 shows the bases and four states of polarization respectively.

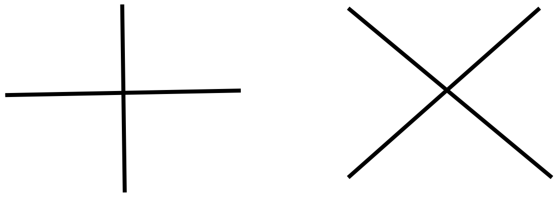

Figure 1. Rectilinear and Diagonal Bases

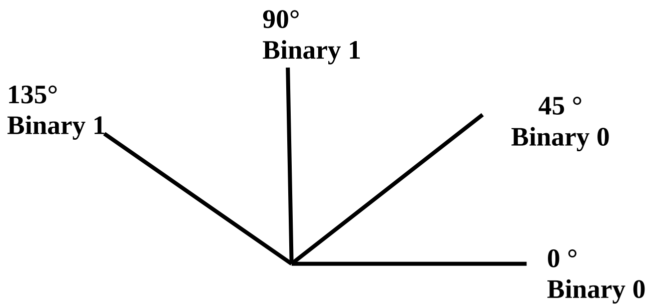

Figure 2. Representation of Qubits using Photon Polarization

The key point of quantum mechanics is its two laws, namely the law of Heisenberg Uncertainty 2) the law of photon polarization. The Heisenberg Uncertainty law says that the measurement of related physical properties simultaneously is not possible [3] [4]. The law of photon polarization says that the replication of qubits cannot be made according to the theorem of no-cloning [5].

This paper proposes new techniques of quantum encryption and decryption algorithms named as VBA Quantum Encryption and Decryption Algorithms with the incorporation of Toffoli quantum gates. The thought of quantum cryptography and Toffoli gate had pioneered in bringing these algorithms. The quantum gate applied on one- qubit can be illustrated by 2 by 2 matrices. [6]. Therefore the quantum gates have exponential time complexity which is 2^n. The exponential complexities proven to be secure, hence the algorithms proposed are secure. By incorporating quantum gate makes difficult for the eavesdropper to know the qubits. Moreover, the public discussion process is embodied into proposed method thereby it offers security services such as authenticity, integrity and confidentiality to the communicating entities. It also used to detect known plaintext, ciphertext only and chosen plaintext attack.

2. Related Work

This part will brief about the limitations of conventional cryptographic algorithms which fail to withstand security. The conventional cryptographic algorithms are based on mathematical problems such as discrete logarithm or integer factoring [7]. However, these

Copyright ⓒ 2017 SERSC

problems are potentially not secure. For instance RSA public key algorithm could simply be broken if factoring of integers are trouble-free. Data Encryption Standard (DES) has issue with weak key as all the rounds will be using the same key. It is exposed to brute force attack and linear cryptanalysis attacks. Triple DES algorithm is susceptible to differential and linear attacks. Moreover, it has become variant to man-in-the-middle attack. Other conventional algorithm IDEA has suffered from differential attack based on chosen plaintext. It also has threat for weak keys. IDEA has exposed to related key differential timing attacks and key schedule attacks. Further, each round had opened to these attacks [8].

3. Proposed Method- VBA Quantum Encyrption and Decryption Algorithms

Quantum cryptography offers potential to develop encryption and decryption algorithms which are resistant to attacks. This paper gives new techniques for encryption and decryption algorithm using Toffoli quantum gate named as VBA Quantum Encyrption and Decryption Algorithms.

Toffoli gate is a 3-qubit quantum gate that is to say it takes three inputs and gives three outputs a, b and c among 2^3 outputs. It is depicted in figure 3. The first two inputs a, b are control qubits that are unaltered by the action of the gate. The third input is a target qubit which is flipped if both a, b control qubits are set to 1 otherwise not. One noteworthy characteristic of Toffoli gate is that applying twice to a set of qubits has reversible effect $|a, b, c\rangle \rightarrow |a, b, c \oplus ab\rangle \rightarrow |a, b, c\rangle$ [6].

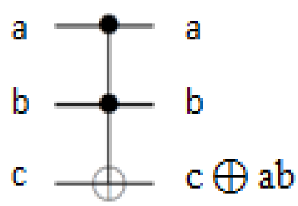

Figure 3. Toffoli Gate

The matrix representation of quantum gates is derived using tensor product. The characteristic of tensor product is it combines two vector spaces to form one large vector space. Consider two vector spaces **U** and V with m and n dimensions respectively then $U \otimes V$ is defined as a space on mn. The elements of $U \otimes V$ are linear combinations of tensor products $|u\rangle \otimes |v\rangle$ of elements of $|u\rangle$ of U and $|v\rangle$ of V. Assume A is a m by n matrix and B is a p by q matrix, then the matrix representation is shown as in figure 4 [6]. Thus the quantum gate with n inputs gives 2^n outputs and has degree 2^n. So, a 1-qubit gate is represented with 2 by 2 matrix. The Toffoli gate which is 3-qubit gate takes three inputs and gives three outputs from 2^3 possible outputs. Therefore, to represent Toffoli gate a 8 by 8 matrix is needed as shown below [2].

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A \otimes B = \left.\overbrace{\begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}}^{nq}\right\} mp$$

Figure 4. Tensor Product

3.1. Properties

The algorithms have the following properties

a) The underlying unit used in these algorithms is qubit, hence it is impossible to clone.

b) The communication is fast due to qubits which are the predominant elements used in these algorithms.

c) Though the purpose of Toffoli quantum gate is known, either plaintext or ciphertext is not revealed because measurement with incorrect basis leads to incorrect qubits.

d) The encryption algorithm obeys the property of unconditionally secure by which it means the ciphertext which is generated does not provide adequate information to know the plaintext.

3.2. Encryption Algorithm

The Plaintext ‘P’ which has ‘n’ bits such that mod(n,7) ==0 and mod(n, 8) ==0 is encrypted by representing with ‘m’ qubits using random basis, where length equal to n i.e. m==n. ‘m’ and key ‘k’ are applied as inputs to 3- qubit Toffoli quantum gate. The resultant is ‘m’ qubits which is ciphertext ‘C’. The flowchart of encryption algorithm is explained in the figure 5.

Encryption Algorithm

Step 1. Consider i) Plaintext ‘P’ of length ‘n’ bits such that n= mod (n, 7) ==0 && mod(n, 8) ==0 ii) Key ‘k’ of length n/2.
Step 2. Choose random basis for each bit.
Step 3. Convert ‘n’ bits into ‘m’ qubits using randomly chosen basis, where length of m==n.
Step 4. Partition ‘m’ qubits into two parts namely a and b each with length m/2.
Step 5. Apply a, b and k as inputs to 3-qubit Toffoli Quantum gate.
Step 6. The result obtained in Step 5 is the ciphertext ‘C’ of length ‘m’.

Copyright ⓒ 2017 SERSC

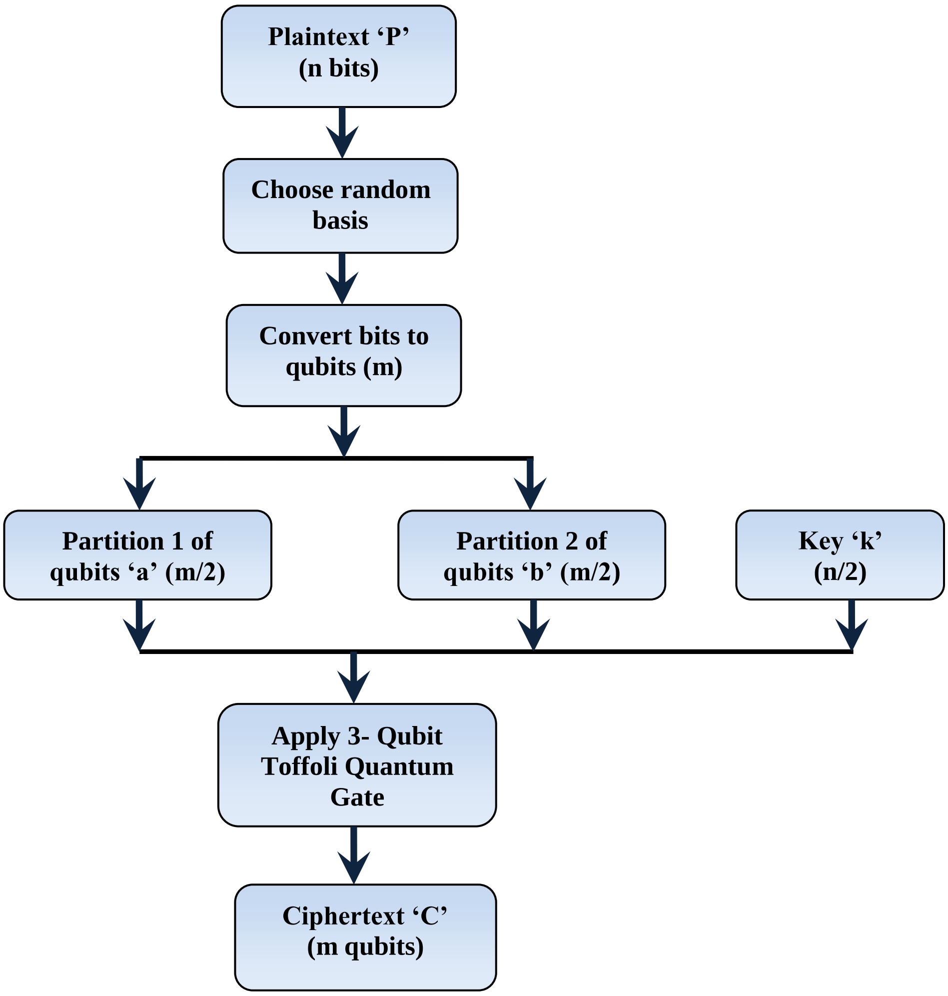

Figure 5. VBA Quantum Encryption Algorithm

3.3. Decryption Algorithm

For ‘C’ and ‘k’ the receiver applies reverse Toffoli quantum gate. The outcome is ‘m’ qubits. This in turn is converted to ‘n’ bits by representing with corresponding basis in order to get plaintext ‘P’. Figure 6 shows the flow of algorithm.

Decryption algorithm

Step 1. Consider key ‘k’ which is shared already.
Step 2. Make ‘C’ into two partitions namely a’ and b’.
Step 3. Apply reverse Toffoli gate to a, b and k, the resultant is qubits of length ‘m’.
Step 4. Choose random basis.
Step 5. Convert qubits into bits using corresponding basis.
Step 6. The result obtained in Step 5 is the Plaintext ‘P’ of length n.

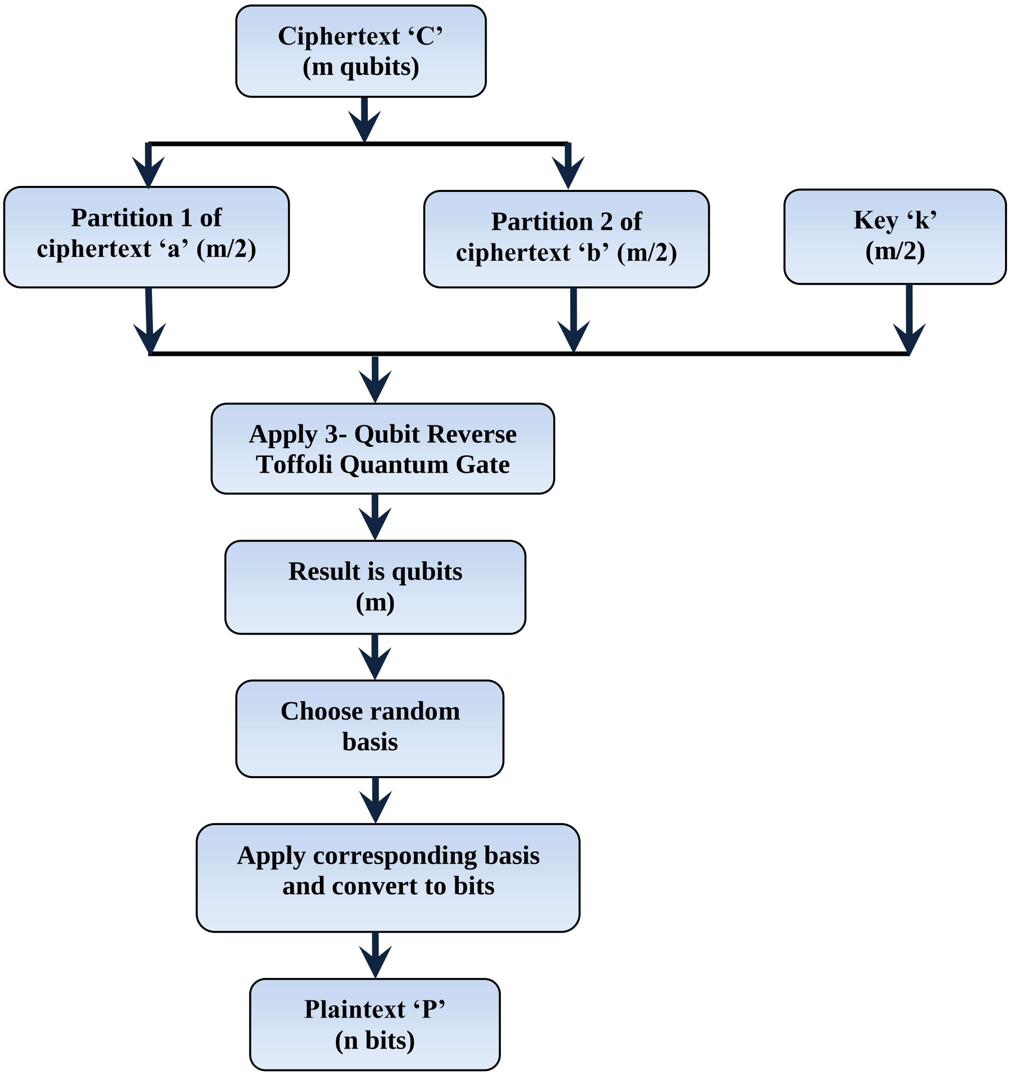

Figure 6. VBA Quantum Decryption Algorithm

4. Public Discussion

The concept of public discussion is employed after the process of encryption and decryption is carried out. It involves the following steps

1) Receiver sends random basis to Sender.
2) Sender checks the correctness of basis.
3) Sender confirms the correct basis to Receiver.

With this Sender and Receiver will get assurance that they are communicating with the authenticated entities which they ought to be. It detects known plaintext, ciphertext only and chosen plaintext attacks.

4.1. Known Plaintext Attack

This is an attack on

- Encryption algorithm

 Copyright ⓒ 2017 SERSC

- Ciphertext
- Possible pairs of plaintext-ciphertext using secret key

If the ciphertext is eavesdropped and intercepted, Receiver cannot be able to restore the original plaintext. Hence the entities detect the attack and conclude the communication. This is attained through discussion.

4.2. Ciphertext only Attack

This is an attack on

- Ciphertext
- Key

Also, if the qubits of ciphertext and key is intercepted, Sender will detect the attack with the process of public discussion.

4.3. Chosen plaintext

Attack takes place by

- Selecting plaintext and obtain corresponding ciphertext

If the selected plaintext is correct, it is impossible to know ciphertext as incorrect measurement of basis gives incorrect qubits. Hence it is detected in the step 1 of public discussion process.

5. Conclusions

As cryptography happened to be essential part in today's world of security, projected method ensures secure communication due to inviolable laws of quantum mechanics. The underlying unit is qubit which is fast in transmission as well as impossible to clone. The algorithms applies Toffoli gate which has exponential complexity and proven to be secure. We have declared that the method proposed does not allow illegitimate user to determine either plaintext or ciphertext by incorporating security services. It also encounters known-plaintext, ciphertext only, chosen plaintext attack and eavesdropping. Besides, we have discussed the properties of algorithms. Thus the proposed VBA quantum encryption and decryption algorithms have potential to guarantee secure system.

References

[1] S. Wiesner, "Conjugate Coding", Sigact News (original manuscript written circa 1969), vol. 15, no. 1, **(1983)**, pp. 78-88.
[2] D. McMahon, "Quantum Computing Explained", IEEE Computer Society, Wiley- Interscience, John Wiley & Sons, Inc., **(2008)**.
[3] D. Wiedemann, "Quantum cryptography", Sigact News, vol. 18, no. 2, **(1987)**, pp. 48-51.
[4] C.H. Bennett, and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing", Bangalore, India, **(1984)**, pp.175-179.
[5] W. K. Wootters and W. H. Zurek , "A Single Quantum Cannot be Cloned", Nature 299, **(1982)**, pp. 802- 803.
[6] M. A. Neilsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 10^{th} Anniversary Edition, **(2010)**.
[7] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe. "Quantum cryptography: A survey." ACM Computing Surveys (CSUR), vol. 39, no. 2, **(2007)**, pp. 6.
[8] L. Elbaz and H. Bar-El, "Strength assessment of encryption algorithms", White paper, **(2000)**.

Copyright ⓒ 2017 SERSC

Authors

Vurubindi Padmavathi is working as an Associate Professor at Sreenidhi Institute of Science and Technology affiliated to Jawarharlal Nehru Technological University, Hyderabad (JNTUH). She has done her Bachelor of Engineering (CSE), M. Tech. (CSE) and is pursuing Ph.D. in Computer Science and Engineering from JNTUH. Having 14 years of teaching experience, her focus is on the research areas like Cryptography, Information Security and Software Engineering. She has conducted and participated in several workshops, seminars and bridge courses. Mrs. Padmavathi has organized a National Conference. She has presented papers in the International Conferences.

Bulusu Vishnu Vardhan is working as a Professor in CSE at JNTUH College of Engineering, Nachupally, Karimnagar, Telangana, Inida. He was the Head of the Department of IT, JNTUH College of Engineering, Nachupally from the year 2010 to 2014. He has completed his M. Tech from Birla Institute of Technology, Mesra, Ranchi in the year 2001 and completed his Ph.D. from JNTUH in the year 2008. He has 20 years of teaching experience, presently he is guiding 16 research scholars in the area of Cryptography and Information Security, Information Retrieval, Linguistic processing, Data mining and other elite areas. Three scholars are awarded with Ph.D., one from JNTUK and two from JNTUH. Dr. Vishnu Vardhan is the member of Board of Studies for Sathavahana University, Karimnagar. He was an active member in Free Software Movement in India. He has completed Government of Andhra Pradesh funded project worth Rs. 5 lacks from Ministry of IT on localization activity. As a co investigator completed another UGC funded project worth Rs. 9 lacks. He has evaluated 4 theses for universities like Osmania, Acharya Nagarjuna University. He visited Singapore and presented paper in International conference ICAEE in 2014. He has more than 40 papers International Journals and Conferences.

Addepalli V N Krishna is a Professor in the department of CSE at Christ University, Bengaluru, India. He has completed M. Tech. and Ph.D. in Computer Science and Engineering discipline. He is in the field of teaching and research since 26 years. He has participated in various National and International Conferences. A V N Krishna has many publications to his credit. His areas of interests are Cryptography, Mathematical Modeling and Data Mining.

 Copyright ⓒ 2017 SERSC