IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-2 E-ISSN: 2347-2693

Robust Quantum Key Distribution Based on Two Level QDNA Technique to Generate Encrypted Key

N.Srilatha[1*], M.Deepthi[2] and I. Rajasekhar Reddy[3]

[1*]Department of Computer Science and Engineering, Rajiv Gandhi University of Knowledge Technology, AP-IIIT, India
[2]Department of Computer Science and Engineering, CMR Engineering College, Hyderabad, India
[3]Department of Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, India

[*]*Corresponding Author: srilathargukt16@gmail.com*

Available online at: www.ijcseonline.org

Received: 29/Jan/2017 Revised: 04/Feb/2017 Accepted: 24/Feb/2017 Published: 28/Feb/2017

***Abstract*— The Privacy is paramount when communicating subtle information, and humans have devised some unusual ways to encode their conversations. The Quantum Key Distribution agrees for the secure transmission of unbreakable encryption keys and it provides a flawless secure coding to solve the problem of key distribution. At present this is more mature application in the field of quantum computing. The fundamental concept of this protocol involves two parties, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. The entanglement distillation approach of BB84 is widely used because the act of reading a quantum bit (QuBits) changes the bit, it is difficult for hackers to interfere without being detected sufficient number of bits. But this technique uses only four directions of electron movements so it is possible to guess the key. To overcome these drawbacks here two level QRNA technique is proposed for security. In first level DNA is applied on plain text after BB84 protocol is applied. This method provides better security than both BB84 protocol and DNA alone.**

Keywords: BB84 protocol, Quantum Cryptography (QC), DNA, QDNA and QuBits

I. INTRODUCTION

Cryptography is the strongest tool for controlling against many kinds of security threats that changes the message from structured data to unstructured data [1][2]. The structure data is easily understood by the every one, so we can convert this format into unstructured data. Now a day we have so many methods for providing the security. The classical cryptography is based on symmetric key or asymmetric key techniques. Symmetric cryptography, also known as secret key cryptography, uses one secret key for both encryption and decryption [3][4]. Symmetric key is provide the security for the possible attacks but it does not work for the brute force attack secret key, by using the DES algorithm we can solve this problem [4][5]. Asymmetric cryptography, also known as public key cryptography, has both a public and a private key, either of which can be used for encryption/decryption. Classical Cryptography suffers from Key Distribution problem, how to communicate the key securely between two pair of users. Deoxyribo Nucleic Acids (DNA) computing is to solve computational problems with the help of biological and chemical methods [6].The use of computing DNA is far from reality and the world of information security is the focus better on other encryption technology for new promising methods [7]. Several DNA-based cryptographic techniques have been proposed [8]. Some of these use Polymerase Chain Reaction (PCR) [9] while others use DNA chip technology [10][11]. Nucleic Acid (RNA) is a copy of the DNA to come out to the cytoplasm to tell the cell what needs to be done in order to survive [12]. This method is to generate a random key using DNA computing technology. DNA is a single-stranded molecule which contains the bases adenine (A), cytosine (C), guanine (G) and uracil (T) base. Data Encryption Algorithms (DEAs) such as 3-DES, AES, and elliptic curves cryptosystems allow to have a good secure encryption using fixed- length keys [13]. They are considered as "unbreakable". But all these algorithms assume that a key is shared between the two endpoints. Thus, security is a problem of key distribution. Quantum Key Distribution is used for providing secure transmission. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. A unique property of Quantum Cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This quantum cryptography enables the transfer of data through quits which have the special property that they change their states if they are copied. In simulation of quantum key exchange and authentication followed by an implementation of DNA based algorithm for secure message exchange was implemented. Various protocols that implement quantum key distribution are BB84, B92, Ekert protocols . Generally, the

BB84 protocol coding scheme uses four non-orthogonal polarization states where as B92 protocol uses only two orthogonal states that will polarize each of the photon that will be transmitted. In this protocol, sender and receiver have to communicate within two channels, Quantum channel and public channel to share a secret key. In [14] Ekert protocol is a 3-state protocol that uses three non-orthogonal polarization states that will polarize each of the photon.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. non-quantum) communication Various security problems exist in designed key distribution protocols; for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority.

II. BACKGROUND WORK

Two existing methods first is Quantum cryptography and second is DNA are briefly explained to provide security to the data.

A. Quantum key Distribution Technique

In Quantum Cryptography (using BB84 protocol) a Quantum Key Distribution is used for providing secure transmission. In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol. It was based on Heisenberg's Uncertainty Principle and is simply known as the BB84 protocol after the author's names and the year in which it was published. The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. **Table1** shows how a bit can be encoded in the polarization state of photon in BB84.

TABLE I. BB84 LOOKUP TABLE

Direction	→	↑	↖	↗
Symbols	H	V	L	R
Bits	0	1	0	1

In BB84 protocol, only four directions are used for generating the key. Hacker easily guesses the key from these four directions.

B. DNA Technique

1. In DNA Technique, plain text is converted into DNA sequence by using DNA sequence which is as shown in table
2. In this method also four letters are using so it is also somewhat easy to hack original data by black hat hacker. To overcome these limitations here proposing new technique by combining both the methods.

III. REELATED WORK

This paper proposes a new technique by combining the DNA and Quantum Cryptography (BB84 protocol) is called QRNA Technique. To overcome the drawbacks of Existing systems here two level QDNA technique is proposed for providing more security. In first level apply the BB84 protocol method on plain text. In the second level apply the DNA technique. The sequence of steps for encryption process.

A. Encryption

Step 1: plain text is **HAI**.
Step 2: Take the Alice and Bob patterns as s1 and s2 strings. Alice string s1= HRLVLHRLHRLLVHRHRVLRHVVH Bob string s2= HRVHRVLHLRVRHVRHLLLLHHRR
Step 3: Generate the actual key of Alice and Bob patterns by using BB84 protocol.
key1=011010101101001011110011
key2=010010110111001010110000
Step 3: Compare the key1 and key2 bits for generating key3.
If key1 bit equal to key2 bit then key3 value is 1 otherwise 0.
key3=1101111001011111101111
00
Step 4: Convert key3 from binary to decimal.
11011110|01011111|1011110
0
222 195 188 Decimal values are 222,195,188.
Step 5: If decimal value is even then add 2 or else add 3 to the plain text.
H+2 = J
A+3 = D
I+2 = K
Step 6: After applying BB84 protocol, cipher text is JDK.
Step 7: Output of BB84 protocol is converted into DNA sequence by the following steps.
1. Plain text = JDK
2. Convert the plain text into Binary format and perform the reverse operation on the bits.
J (74) = 01010010 D (68) = 00100010 K (75) = 11010010

3. Convert the binary format into DNA sequence by using the DNA sequence table.

TABLE II. DNA SEQUENTIAL TABLE

Alphabets	Binary Format
A	00
C	01
G	10
T	11

RNA sequence for the plain text is:

CCAGAGAGTCAG. Step 8: Final Cipher text is

CCAGAGAGTCAG.

B. Decryption

Step 1: Cipher text is CCAGAGAGTCAG.

tep 2: Convert it into binary format by using DNA sequence table.

010100100010001011010010

TABLE III. ENCRYPTION TIME FOR EXISTING AND PROPOSED METHODS

File size (KB)	DNA (msec)	Quantum (msec)	QDNA (msec)
123	2678	3657	3743
165	1087	2094	2125
250	2985	3922	3954
294	678	844	4016
336	765	859	3656
772	256	313	516
1926	1865	2078	2140
2258	12345	14672	14625
2475	867	1000	1094
3761	7687	8253	8360

Step 3: Perform the reverse operation on the bits and convert the binary format into decimal value.

01001010 ----> 74 (J)

01000100 ----> 68 (D)

01001011 ----> 75 b (K)

Step 4: Output of the DNA technique is JDK.

Step 5: The result of DNA technique is given as a input to the Quantum Cryptography (BB84 protocol).

1. Take the Alice and ob patterns as s1 and s2 strings. Alice string s1= HRLVLHRLHRLLVHRHRVLRHVVH Bob string s2= HRVHRVLHLRVRHVRHLLLLHHRR

2. Generate the key of Alice and Bob patterns by using bb84 protocol.

key1=011010101101001011110011

key2=010010110111001010110000

3. Compare the key1 and key2 bits for generating key3. If key1 bit equal to key2 bit then key3 value is 1 otherwise 0.

key3=110111100101111110111100

4. Convert key3 from binary to decimal. Decimal values are 222,195,188

5. If decimal value is even then subtract 2 or else subtract 3 from the Cipher text. J-2 = H D-3 = A K-2 = I

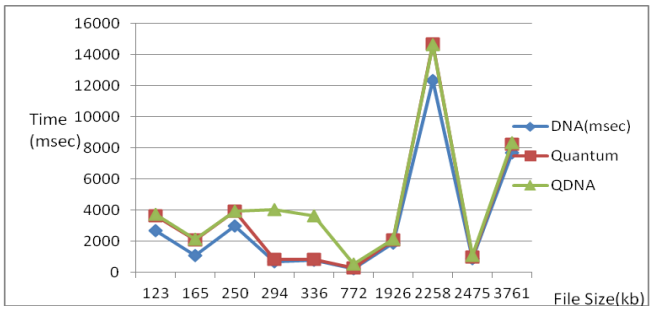
Step 7: Plain text is **HAI**.

IV. EXPERMENTAL RESULTS

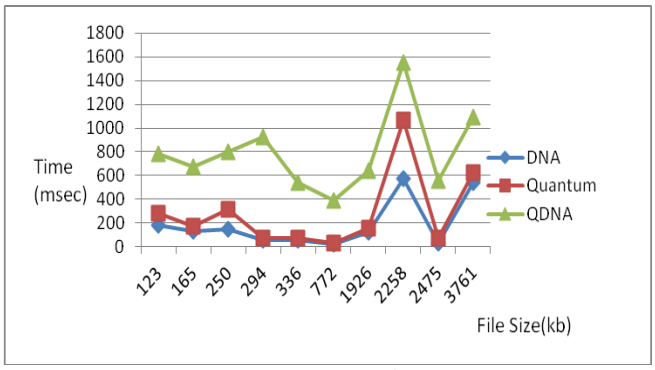
In this paper we considered documents like text, pdf, document with full of mathematical equations and document with full of images and constructed the tables and drawn the graphs. The tables and graphs shown that the document with full of mathematical equations with PDF of 2258KB, and 250KB documents with Images. And with images have taken more time than plain text 2475KB. The below table 3 and table 4 shows the Encryption, Decryption time for existing and proposed methods. The below graph 1 and graph 2 shows the time complexity for encryption and decryption process of the DNA, Quantum Cryptography (BB84 protocol) and Quantum DNA (QDNA) technique. The QDNA has taken more time than DNA and Quantum cryptograph. But it provides more security than both existing methods.

TABL IV. DECRYPTION TIME FOR EXISTING AND PROPOSED METHODS

File size (KB)	DNA (msec)	Quantum (msec)	QDNA (msec)
123	186	281	781
165	134	172	672
250	150	313	797
294	58	78	922
336	58	78	544
772	24	32	390
1926	126	156	640
2258	578	1063	1547
2475	34	78	562
3761	545	625	1094



Graph 1: Time complexity for Encryption



Graph 2: Time complexity for Decryption

V. CONCLUSION

The proposed method of encryption and decryption is far better than existing methods like DNA and Quantum Key Distribution (BB84 protocol). The strength of the proposed method is the complex cipher generation from two strong keys. As DNA computing is a very promising field that keeps the ability to overcome many limitations of silicon computers.. Quantum cryptography indicates that it is uncompromisingly secure key distribution, faster key refresh rate than traditional approaches, truly random key generation. In this paper, the proposed method is combining the both two strong encryption techniques. The proposed method works in two levels, the first level is convert the plain text into cipher text by using BB84 protocol, the second level is convert the first level of cipher text into another cipher text by using DNA technique. This method provides better security than both BB84 protocol and DNA alone. There is a limitation with this method is that. it takes more time to perform encryption and decryption process than existing methods. Future enhancement of this paper is performs the optimization techniques for reducing the time complexity.

REFERENCES

[1] B.Jyoshna"Mechanisms for secure data transmission A Survey", Published in International of Computer Science and Engineering(IJCSE), Vol.-2(8), PP(82-83) August 2014.

[2] R.Shah and Y. S. Chouhan, "Encoding of Hindi Text Using Steganography Technique", International Journal of Scientific Research in Computer Science and Engineering, Vol.2(1),pp. 22-28, Feb 2014

[3] Alia, M.A., Yahya,A., "Public–Key Steganography Based on Matching Method", European Journal of Scientific Research, Vol(2), PP223-231 Aug (2010).

[4] G. Cui, L. Qin, Y. Wang and X. Zhang, "An encryption scheme using DNA technology", Bio Inspired Computing: Theories and Applications, pp. 37-42, 2008.

[5] Z. Chen and J. Xu, "One-time-pads encryption in the tile assembly model," Bio-Inspired Computing: Theories and Applications,Vol-46 pp.23- 30,may 2008.

[6] E Suresh Babu, C Nagaraju, MHM Krishna Prasad "Analysis of Secure Routing Protocol for Wireless Adhoc Networks Using Efficient DNA Based Cryptographic Mechanism" published in Procedia Computer Sciencedec-. Vol-70PP:341-347 , Oct 2015.

[7] Ashok Sharma, R S Thakur and Shailesh Jaloree, "Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud", International Journal of Scientific Research in Computer Science and Engineering, Vol. 4(5), pp.5-11, Oct 2016

[8] R Pradeep Kumar Reddy, C Nagaraju, N Subramanyam "Text encryption through level based privacy using dna steganography" published in International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) ,vol-3 PP168-172,May-jun 2014.

[9] Mamta Rani1 and Sandeep Jain,"DNA Computing and Recent Developments". International journal of computer science and Engineering, Vol.2, PP.16-19,April 2014.

[10] Kritika Gupta, " DNA Based Cryptographic Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering,vol(3), pp. 607-610, March 2013.

[11] Komal Kumbharkar, "An improved Symmetric key cryptography with DNA based strong cipher", international journal of advanced and innovative research, (IJCSE) ,Vol(2),PP2278-7844,May-jun2013.

[12] Sharmeen kaur, Raveena Singh and Shivya Gagneja "Network Security and Methods of Encoding and Decoding". International journal of computer science and Engineering, Vol.-2(2), pp (11-15) Feb 2014.

[13] Pallab Banerjee1 and Anita Kumari2,Puja Jha3 "Comparative Performance Analysis of Optimized Performance Round Robin Scheduling Algorithm(OPRR) with AN Based Round Robin Scheduling Algorithm using Dynamic Time Quantum in Real Time System with Arrival Time". International journal of computer sciences and Engineering, Vol.-3(5), pp. 309-316, May 2015.

[14] Azarderakhsh, mehran mozaffar kermani, David jao,"post quantum cryptography on FPGA based on isolegines on elliptic curves" IEEE journal,VOL(64),pp86-99,2017

Authors Profile

Ms.N.Srilatha in pursed Bachelor of Science from Yogi Vemana University, Proddatur in 2013 and Master of Science from JNTUA College Of Engineering in year 2016.she is currently working as Acedamic Assistant in Department of Computational Sciences, RajivGandhi University of Knoweledge Technology,AP IIIT since 2016. She has attended 2 IEEE conferences and it's also available online. Her main research work focuses on Cryptography Algorithm.

Ms.M.Deepthi in pursed Bachelor of Science from Yogi Vemana University, Proddatur in 2012 and Master of Science from JNTUA College Of Engineering in year 2016. She is currently working as Assistant Professor in Department of Computer Sciences and Engineering in CMR Engineering College. She has attended 2 IEEE conferences and it's also available online. Her main research work focuses on Cryptography Algorithm

Mr I. Rajasekhar Reddy pursed Bachelor of Technology in Department of Computer Science and Engineering from Yogi Vemana University, Proddatur in year 2015. He is currently pursuing Master of Technology in Department of Computer Science and Engineering, JNTUACEP, Pulivendula since 2015. He has published 6 research papers in reputed international journals and 5 conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Image Processing.

