JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

A Novel Encryption Technique Using DNA Encoding and Single Qubit Rotations

Partha Sarathi Goswami[1*], Tamal Chakraborty[2], Harekrishna Chatterjee[3]

[1*]Dept. of Computer Application, A.J.C.Bose Polytechnic, Department of Technical Education & Training, Government of West Bengal, India
[2] Mrinalini Dutta Mahavidyapith, West Bengal State University, Kolkata, India
[3]University of Engineering & Management, Kolkata, India
[*]*Corresponding Author: goswamipsg@rediffmail.com, Tel: +91-9230649935*

Available online at: www.ijcseonline.org

Received: 23/Feb//2018, Revised: 28/Feb2018, Accepted: 21/Mar/2018, Published: 30/Mar/2018

Abstract- In today's world security has become a major threat over the transmission channel. To overcome this DNA cryptography is used to encrypt and transfer the message from sender to receiver over a secured communication network. This paper focuses on the encryption and decryption of the message using DNA encoded sequences and discusses the cryptographic applications of single qubit rotations from the view of one-way trapdoor functions. For encryption quantum public key is used and for decryption the concept of classical private key is used. The mapping between integer numbers and quantum states is done using one way trapdoor function.

Keywords- Quantum Cryptography, DNA Cryptography, One-way trapdoor function, Qubit.

I. Introduction

Security is a very fundamental and significant issue of data transmission today. DNA cryptography is a new and promising field in information security. It combines classical solutions in cryptography with the strength of the genetic material. A plaintext message is encoded in DNA sequences. DNA sequences get powerful, when combined with nucleotide base A-T and C-G. DNA cryptography technology is needed in information security to protect and hide data. Genetic information is encoded as a sequence of nucleotides Guanine-G, Adenine-A, Thymine-T and Cytosine-C. Adenine, Thymine and Guanine, Cytosine are base pairs. Modern public-key (or else asymmetric) cryptography relies on numerical trapdoor one-way functions, i.e., functions that are "easy" to compute, but "hard" to invert without some additional information (the so-called trapdoor information). The main characteristic of these mathematical objects is that they provide the legitimate users with a tractable problem, while at the same time any unauthorized user (adversary) has to face a computationally infeasible problem. This barrier between legitimate users and adversaries, due to complexity of effort, is the key idea behind most of the known public-key cryptosystems. Each participant in such a cryptosystem has to have a personal key consisting of two parts, i.e., the public and the secret (also known as private) part. Messages are encrypted with use of the public key and the decryption of the resulting cipher text is possible by means of the private key. Thus generation of the pair of keys (public and private) plays a vitally important part in any cryptosystem. This paper introduces a one-way trapdoor function based on the principles of quantum theory. The unit of quantum information is a quantum bit or qubit. A qubit has two quantum states polarization of a single photon namely vertical polarization and horizontal polarization. In classical computing a bit should be in one state or the other whereas a quantum bit (qubit) can exist as the superposition of two quantum states |0> and |1>. The proposed algorithm generates the pair of keys by rotating a single qubit, which are then applied for encryption of a DNA encoded plaintext.

The paper is organised as -- Section II contains the related work in the field of Quantum cryptography and DNA cryptography. Section III gives a brief discussion about DNA Cryptography with tables for conversion of Binary to DNA and DNA code set. Section IV gives a brief overview of Quantum cryptography. Section V gives a glimpse about one way trapdoor function. Section VI explains the rotation of a single qubit based on quantum trapdoor function. Section VII explains the algorithm for key generation, encryption and decryption of the plain text using single rotations of the qubit and the concept of DNA coding. Section VIII discusses about the security aspect of the encryption algorithm. Finally section IX concludes the research work.

II. Related Work

A. Related Work in Quantum Cryptography

In 1984 Charles H. Bennett and Gilles Brassard [1] was the first to propose the protocol on quantum cryptography named as BB84. The protocol was based on Heisenberg's Uncertainty principle. In 1992 Charles H. Bennett [2] proposed a much simplified version of BB84, in which only two polarization states are necessary, named as B92. In 2002 Ching-Nung Yang and Chen-Chin Kuo [3] proposed an enhanced quantum key distribution protocol using BB84 and B92. One is to enhance the idealized maximum efficiency to 28.6 % with the average complexity order 2, and the other with an efficiency of 42.9 % and has the average complexity order of 2.86. In 2011 M. Houshmand and S. Hosseini-Khayat [4] an entanglement-based quantum key distribution where they used an updated version of Cabello's definition of efficiency of quantum key distribution protocols to compare between their protocol and BB84. A sequence of qubit pairs is obtained by separating the stream of qubits. The protocol gives less information about the key bit than BB84. This is because before the beginning of the protocol the participants publically agree on two 2-qubit unitary transformations say U_1 and U_2 and all transmitted qubits are useful in contradictory to BB84 where half of qubits are discarded on average. In this protocol one classical bit is used to acknowledge receiving each of the qubit and one classical bit is used for determining the basis of each of the group of qubits thereby giving an advantage against eavesdropper under an intercept resent attack. In 2014, Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari Hussam [5] proposed a novel secure quantum key distribution algorithm in which they overcame the drawbacks in BB84 and B92 protocols. It was done by eliminating the need for two communicating parties to confirm their used basis over a public channel. In their work session key is exchanged over the quantum channel. Also the users' authentication and confidentiality is maintained by exchanging random basis and nonce. In 2013 Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Ema Abdelfattah [6] introduced a new model for QKD between three parties where there is a trusted centre providing clients with the necessary secret information to securely communicate with each other. Here there is no need of physical channel to check the qubits sequence. The algorithm has two parts firstly the user authentication and quantum bases distribution and secondly the data transfer over the quantum channel. The algorithm improves the efficiency by eliminating the rounds required to check the quantum bases and provide authentication.

B. Related Work in DNA Cryptography

In the year 1994, Adleman [7] first introduced the concept of DNA computing by giving solutions to the combinatorial problems using molecular computation such as the "Hamiltonian path" problem. He solved the graph containing seven vertices by encoding it into the molecular form with the help of an algorithm and then computational operations were performed by brute force method. In the year 1995, Lipton [8] extended the findings of Adleman by solving another NP-complete problem called "satisfaction" by using DNA molecules in a test tube to encode the graph for 2 bit numbers. In the year 1996, Dan Boneh [9] applied DNA computing concept used by Adleman and Lipton, in order to break one of the symmetric key algorithm of cryptography known as DES (Data Encryption Standard). He performed biological operations on the DNA strands in a test tube, such as extraction, polymerization via DNA polymerase, amplification via PCR and perform operations on the DNA strands which have the encoding of binary strings. Then DES attack is planned by generating the inverse DES solution, due to which key can be easily guessed from the cipher-text and further evaluate the DES circuit, lookup table and XOR gates. By using their molecular approach they broke DES in 4 months. In the year 1997, Ouyang Qi, D. Peter Kaplan, Liu Shumao and Albert Libchaber [10] applied the concept of DNA cryptography to generate the solution for maximal clique problem, a NP-complete problem. Thus showing the efficiency of DNA computing to solve Hard-problems and vast parallelism inherent in it which makes operations fast. In the year 2004, Ashish Gehani, La Bean Thomas and John Reif [11] introduced DNA cryptography by combining molecular biology with the concept of one-time pad which has perfect confidentiality. They proposed a method of encryption and decryption which based on DNA chip and one-time-pad thus making it difficult for the intruder to guess the encrypted message. In year 2006, Sherif T. Amin, Magdy Saeb and El-Gindi Salah [12] proposed the DNA cryptographic approach using symmetric key, where key sequences were obtained from the genetic database and remained unaltered on both the sender and receiver end. Using this technique real message is not transferred over network and message is scalable for large digital information products but in the process the size of plain text increases the encryption time and decryption time. In the year 2012, Sabari Pramanik and Sanjit Kumar Setua [13] proposed parallel DNA cryptography technique by means of DNA molecular structure and hybridization technique that reduces the time requirement. They explained how message can be exchanged safely between the sender and the receiver. Here they used one-time-pad as the encryption key. In year 2012, Yunpeng Zhang, Bochen Fu and Xianwei Zhang [14] proposed a DNA cryptography using DNA fragment assembly. In their algorithm they explained how sender translates the plaintext into a binary sequence and then to along chain of DNA that is again fragmented into small DNA chains. The key of short chain embedding took place in the fragments and then forwarded to the receiver as a ciphertext, the receiver then deciphers it and reassembles the fragments to obtain the plaintext again. Here the length of ciphertext is secure and short. But as the length of the DNA fragment is short, attacker can easily detect it. In the year 2013, Olga Tornea and Monica E. Borda [15] proposed a DNA based cipher based on DNA indexing. They used the random DNA sequence from the genetic database as one-time pad key, that is send to the receiver using secure communication channel. The encryption mechanisms occur by converting the plaintext into its corresponding ASCII code, then to the binary format and finally into the DNA sequence (A, C, G, and T). Now the DNA sequence formed is searched in the key sequence and record the index numbers. The array of integer numbers so obtained is the ciphertext that is decrypted by the receiver only by using the key and index pointer. In the year 2015, Ashish Kumar Kaundal, A.K Verma [16] proposed DNA cryptographic approach based on feistel inspired structure and compared it with traditional algorithm, one-time-pad.

III. DNA CRYPTOGRAPHY

The encryption process begins with the input message which is nothing but the plaintext being applied to the cryptography scheme. This plaintext is then given for DNA encryption. The output of the encryption process is DNA triplet code for the corresponding plaintext input. This cipher text in turn is given to receiver through the communication channel. The receiver receives the cipher text which is DNA coded message and converts them into plaintext. Decryption is the reverse process of encryption. The triplet code is now converted back to the original plaintext message.

Table 1: Conversion Table from Binary to DNA

A=CGA	H=CGC	O=GGA	V=CCT	.=GAT	5=AGA
B=CCA	I=ATG	P=GTG	W=CCG	:=GCT	6=TTA
C=GTT	J=AGT	Q=AAC	X=CTA	0=ACT	7=ACA
D=TTG	K=AAG	R=TCA	Y=AAA	1=ACC	8=AGG
E=GGC	L=TGC	S=ACG	Z=CTT	2=TAG	9=GCG
F=GGT	M=TCC	T=TTC	_=ATA	3=GCA	space= CCC
G=TTT	N=TCT	U=CTG	,=TCG	4=GAG	

Table 2: DNA Code Set

Binary	DNA
00	A
01	C
10	G
11	T

IV. QUANTUM CRYPTOGRAPHY

Quantum cryptography uses the basic concept of physics to develop a cryptosystem that is completely secure against being compromised without the knowledge of the sender or the receiver of the messages. The word quantum refers to the most fundamental comportment of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation of it. Quantum key distribution is based on the principles of quantum physics as well as on the classical information theory. The distributed key must be both common and secret. Quantum key distribution guarantees long-term secrecy of confidential data transmission. A crucial and rather important feature of quantum mechanics is quantum entanglement, a physical phenomenon that occurs when quantum particles behave in such a way that the quantum state of each particle cannot be described individually.

V. ONE WAY TRAPDOOR FUNCTION

To define one way trapdoor function let S be a set of numbers and Q be the set of quantum states of a system. Then one way function can be represented as a mapping M: $S \rightarrow Q$ that is easy to calculate but difficult to crack. A quantum one way function whose reverse is possible by means of some trapdoor information is a quantum trapdoor one way function.

Let $S \in Z_n := \{0,1,2,...,n-1|n \in N\}$ be the input set of integers for the one way trapdoor functions and let its output be the quantum state $|\varphi_s>$.Let the initial quantum state be $|0>$ corresponding to the Hilbert space H. Then for any randomly chosen $S \in Z_n$, $\hat{O}: H \rightarrow H$ will change the initial state to

$|0> \rightarrow |\varphi_s> = \hat{O}|0>$. Therefore all possible output state sets of the one way trapdoor function will be $Q \equiv \{|\varphi_s>|S \in Z_n\}$ which belongs to the Hilbert space H. So, if M: $Z_n \rightarrow Q$ is a bijection mapping then there exists a unique $S \in Z_n$ such that $|0> \rightarrow |\varphi_s>$ or in other words M is a one-to-one mapping and $|Z_n| = |Q|$.

VI. ROTATIONS OF SINGLE QUBIT BASED ON QUANTUM TRAPDOOR FUNCTION

A general qubit state lying on the $x - z$ plane of the Bloch sphere is

$|\psi(\theta)> = \cos(\theta/2)\,|0_z> + \sin(\theta/2)\,|1_z>$,

where $0 \leq \theta < 2\pi$.

Therefore a qubit can represent a range of states on the $x-z$ Bloch plane unlike the conventional method which stores a discrete variable taking only two real values i.e. “0” and “1”. Now a rotation on the y-axis $\hat{R}(\theta) = e^{-i\theta\hat{y}/2}$ with $\hat{y}= i(|1z> <0z| -|0z> <1z|)$ being the Pauli operator gives $|\psi(\theta)> = \hat{R}(\theta)\,|0_z>$.

The input of the quantum trapdoor function is a random integer S uniformly distributed over Z_2^n with $n \in N$, and a qubit initially prepared in $|0z>$. Thus, an n-bit strings is sufficient to identify the input s for fixed n. Now for $n \in N$ and $S\in Z_2^n$, the qubit state is rotated by $S\theta_n$ around the y-axis with $\theta_n = \pi/2^{n-1}$.

Therefore for any fixed $n\in N$, the one way trapdoor function $Q_n=\{|\psi_S(\theta_n)>|S\in Z_2^n,\ \theta_n= \pi/2^{n-1}\}$, can be written as

$$|\psi_S(\theta_n)> \equiv \hat{R}(S\theta_n)|0z>$$
$$= \cos(\frac{S\theta n}{2})\ |0_z> + \sin(\frac{S\theta n}{2})\ |1_z> \qquad (1)$$

Hence, both Z_2^n and Q_n remain unknown if n is not known. So it is concluded that for any given pair of integers {n,S}, the mapping $S\rightarrow|\psi_S(\theta_n)>$ is easy to compute as it contains only a single-qubit rotations.

Inverse of the mapping $S\rightarrow|\psi_S(\theta_n)>$ is to recover S from the given qubit $|\psi_S(\theta_n)>$ chosen randomly from the known set $Q_{n.}$ Let n is known then the inverse of the function is to find the different non-orthogonal states chosen randomly from Q_n. So, as n increases the number of non-orthogonal states also increases and for n>>1, the nearest overlapping so obtained

$< \psi_S(\theta_n)|\ \psi_{S+1}(\theta_n)> = \cos(\theta_n/2) \rightarrow 1$.

Therefore, a projective Von Neumann cannot discriminate all of the states for n >> 1, as the number of possible results in such calculation is limited by the dimensions of the qubit.

VII. Encryption And Decryption Of The Plain Text Using Qubit And Dna Concept

A. Key Generation

Every user in the cryptosystem will generate a key having a Private Key K_{pv} and a Public Key K_{pb} as under.

Step 1: Let n>>1 be a random positive integer.

Step 2: Let S be a set of random integer strings of length N where $S=(S_1,S_2,S_3,\ldots\ldots\ldots.,S_N)$ with S_j chosen independently from Z_2^n and $S\in Z_2^n$.

Step 3: Obtain N qubits in the state $|0_z>\otimes^N$.

Step 4: Rotate the j^{th} qubit $\hat{R}^{(j)}(S_j\theta_n)$ by $\theta_n= \pi/2^{n-1}$.

So, the j^{th} qubit $|\psi_{Sj}(\theta_n)>_j = \hat{R}^{(j)}(S_j\theta_n)|0z>$

This takes the form $|\psi_S(\theta_n)> \equiv \hat{R}(S\theta_n)|0z>$

$$= \cos(\frac{S\theta n}{2})\ |0_z> + \sin(\frac{S\theta n}{2})\ |1_z>$$

where $0 \leq \theta < 2\pi$.

Step 5: Private Key $K_{pv} =\{n,S\}$ and

Public Key $K_{pb} = \{N, |\Psi^{(pk)}(\theta_n)>\}$ with the N qubits states $|\Psi^{(pk)}(\theta_n)> \equiv \otimes^N{}_j|\psi_{Sj}(\theta_n)>_j$.

B. Encryption

Let Bob be the sender and Alice be the receiver. Now Bob wants to send Alice an r-bit message $M = (M_1, M_2, \ldots, M_r)$, with $M_j \in \{0, 1\}$ and $r \leq N$.

To encrypt the plain text the following steps are done without altering the order of the public-key qubits:

Step 1: Obtain Alice's authentic public key K_{pb}. If r > N, Bob requests Alice to increase the length of her public key.

Step 2: Convert the Plain text into its Binary equivalent. Replace the 4th bit of the code set so obtained by – 0 if it is 1 and 1 if it is 0.

Step 3: According to the DNA base binary coding, every two bit is considered as one DNA base. Since a byte consists of eight bits, so, each byte represents four bases, for example, 01101100 will be as CGTA. Convert the plain text into its DNA equivalent form.

Step 4: Apply the Watson-Crick transformation A↔T and C↔G on the plain text so obtained.

Step 5: Convert the text into its binary equivalent code. Replace the 1st bit of the 4 group code set so obtained by 0 if it is 1 and 1 if it is 0. Let the message so obtained be M.

Step 6: Encrypt the j^{th} bit of his message M_j by the rotation $\hat{R}_j(m_j\pi)$ on the qubits of the public key, which becomes

$|\psi_{Sj,Mj}(\theta_n)>_j= \hat{R}(M_j\pi)|\psi_{Sj}(\theta_n)>_j$

Step 7: The quantum encrypted message

$|\Psi^{(Kpy)}{}_{S,M}(\theta_n)> = \otimes^N{}_{j=1}|\psi_{Sj,Mj}(\theta_n)>_j$ is send to Alice.

Observe here that the message is encoded in the first r qubits of the cipher text so that, in the decryption process Alice only focus on this part of the cipher text, neglecting the remaining N − r qubits, which do not have any additional information.

C. Decryption

The following steps are done by Alice to decrypt the cipher text $|\Psi^{(Kpy)}{}_{s,M}(\theta_n)>$ to obtain the message m.

Step 1: Apply $\hat{R}^{(j)}(S_j\theta_n)^{-1}$ on the j^{th} qubit of the cipher text.

Step 2: Measure each qubit of the cipher text in the basis {|0z>,|1z>}.

Step 3: Replace the 1st bit of the 4 group code set so obtained by 0 if it is 1 and 1 if it is 0. Convert the binary message into its DNA equivalent form.

Step 4: Apply the Watson-Crick transformation A↔T and C↔G on the message.

Step 5: Replace the 4th bit of the code set so obtained by – 0 if it is 1 and 1 if it is 0. Convert it into its equivalent binary form so as to obtain the plain text send by Bob.

VIII. SECURITY

The main objective of an eavesdropper is to recover the plaintext from the cipher text meant for Alice. But there is always a more determined objective relating to the recovery of the private key from Alice's public key. A cryptosystem is said to be cracked if any of the two objectives are not full filled. Moreover the opponent has access to all of the messages sent to Alice.

Authentication is vital for secure quantum encryption for without it any encryption is susceptible to an impersonation attack. To emphasize on the importance of authenticity, it is described in Step 1 of Encryption that Bob should obtain an authentic copy of Alice's public key.

The Private Key (K_{pv}) of each entity is $K_{pv} = \{n,S\}$ where n>>1 is a random positive integer and S is a set of random integer strings of length N where $S=(S_1,S_2,S_3,\ldots\ldots\ldots,S_N)$ with S_j chosen independently from Z_2^n and $S\in Z_2^n$.

The entropy for n is $H(n) = \log_2(|\tilde{N}|)$, where $|\tilde{N}|$ denotes the number of elements in $\tilde{N}$.

Also the entropy for S is $H(S|n) = N_n$

Therefore the entropy of the private key K_{pv} is,

$$H(K_{pv}) = H(n) + H(S|n) = \log_2(|\tilde{N}|) + N_n >> N$$

To satisfy the above condition it is sufficient to have either $n \gg 1$ or $\log_2(|\tilde{N}|) >> N$. In Section VII both of these are satisfied concurrently as n is a randomly chosen from the integer set N with the constraint n>>1. Hence Eve's information gain is much smaller than $H(K_{pv})$, which therefore remains practically unknown to her.

IX. CONCLUSIONS

In this paper cryptographic applications of single-qubit rotations in the context of quantum one way trapdoor functions and DNA encoding is discussed. It is shown how one way trapdoor functions can be used for a quantum public-key cryptosystem, whose security, in comparison to classical cryptosystem depends on the principles of quantum mechanics. Specifically, in the proposed encryption, each user creates a key having two parts: a private key, that is purely classical, and a public key, that contains a number of qubits prepared independently in states specified by the private key. The sender encrypts his message on the recipient's public key by rotating the state of its qubits. An eavesdropper cannot deduce the encrypted message without knowing the recipient's private key. The main aim of the work is to focus on the concepts that form the basis of quantum public key encryption and establish a correct theoretical framework. The paper also shows how significant properties of quantum system may provide a barrier, due to complexity of effort, between authentic users and eavesdropper, which is the foundation of quantum public-key encryption.

REFERENCES

[1] 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, pp. 175-179, December 1984.

[2] C. Bennett, "*Quantum cryptography using any two non-orthogonal states*" Physical Review Letters, 68:3121–3124, 1992.

[3] Ching-Nung Yang, Chen-Chin Kuo, "*Enhanced Quantum Key Distribution Protocols Using BB84 and B92*", 2002.

[4] M. Houshmand and S. Hosseini-Khayat, "*An Entanglement- base Quantum Key Distribution Protocol"*, Information Security and cryptology (ISCISC), 8th International ISC Conference, IEEE, pp. 45-48, 2011.

[5] Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam, "*A Novel Secure Quantum Key Distribution Algorithm*", University of Bridgeport, 2014.

[6] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, "*Quantum Key Distribution by Using Public Key Algorithm (RSA)*", London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH),IEEE, August 2013.

[7] Adleman. M. L, "*Molecular Computation of Solutions to Combinatorial Problems*", Science, vol.266, pp.1021-1024, 1994.

[8] J. Lipton. R,"*Using DNA to Solve NP Complete Problems*", Science, Vol.268, pp.542-545, 1995.

[9] Boneh. D,"*Breaking DES using Molecular computer*", American Mathematical Society, pp 37-65.1996.

[10] Ouyang Qi, D. Peter Kaplan, Liu Shumao and Albert Libchaber,"*DNA Solution of the Maximal Clique Problem*", Science 278, 5337, 446-449, 1997.

[11] Ashish Gehani, LaBean Thomas and John Reif, "*DNA-based cryptography*", Aspects of Molecular Computing, Springer Berlin Heidelberg, pp.167-188.2004.

[12] Sherif T. Amin, Magdy Saeb and El-Gindi Salah, "*A DNA-Based Implementation of YAEA Encryption Algorithm*", Computational Intelligence, pp.120-125, 2006.

[13] Pramanik Sabari and Kumar Sanjit Setua, "*DNA cryptography*", Electrical & Computer Engineering (ICECE), 7th IEEE International Conference, pp.551-554, 2012.

[14] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "*DNA cryptography based on DNA Fragment assembly* ", Information Science and Digital Content Technology (ICIDT), 8th IEEE International Conference, Vol.1, pp.179-182, 2012.

[15] Olga Tornea, and Borda E. Monica, "*Security And Complexity Of A DNA-Based Cipher*", Roedunet International Conference (Ro Edu Net), 11th IEEE International Conference,pp.1-5, 2013 .

[16] Ashish Kumar Kaundal, A.K Verma,"*Extending Feistel structure to DNA Cryptography*", Journal of Discrete Mathematical Sciences and Cryptography Volume 18, Issue 4, pp.349-362, 2015.

[17] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, "*Public-Key System Using DNA as a One-Way Function for Key Distribution*", Biosystems 81, pp.25-29, 2005.

[18] A. Menezes, P. Van Oorschot and S. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1996.

[19] M. A. Nielsen and I. L. Chuang, "*Quantum Computation and Quantum Information*", Cambridge University Press, Cambridge, London, 2000.

[20] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "*Performance of two quantum key- distribution Protocols*," Phys. Rev. A vol. 73, 2006.

[21] Simmon, G. J., "*Symmetric and Asymmetric Encryption*", ACM Computing Surveys, 11(4), pp. 305-330, 1979.

[22] W. K. Wooters and W. H. Zurek, "*A single quantum cannot be cloned*", Nature 299, 802, 1982

[23] Young, A., "*The future of cryptography: Practice and theory*", IEEE IT Professional Journal, pp. 62-64, 2003.

[24] Vishnu Teja, Payel Banerjee, N. N. Sharma and R. K. Mittal, "*Quantum Cryptography: State-of-Art, Challenges and Future Perspectives*". 7th IEEE International Conference on Nanotechnology, pp. 1296-1301, 2007.

[25] C. Elliott, D. Pearson and G. Troxel, "*Quantum Cryptography in Practice*", Preprint of SIGCOMM 2003.

[26] Mehrdad S. Sharbaf, "*Quantum Cryptography: An Emerging Technplogy in Network Security*". IEEE, 2011.

[27] Partha Sarathi Goswami, Prasun Chakrabarti "*Approach towards realizing resource mining and secured information transfer*", International Journal of Computer Science and Network Security, pp. 345-350 Vol. 8, No. 7, 2008.

[28] Partha Sarathi Goswami, Pabitra Kumar Dey, Dr. A.C. Mandal, "*Quantum Cryptography: Security through Uncertainty*", National Conference on Computing & Systems 2010, pp 86-89, 2010.

[29] Partha Sarathi Goswami, Tamal Chakraborty, Sourav Saha, "*Cryptographic Scheme using the Biological Properties of DNA-RNA - A Review*", American Journal of Advanced Computing, Vancouver, Canada, Vol III(2), pp.61-65, 2016. ISSN: 2368-1209129.

Authors Profile

Mr. P.S. Goswami is pursuing his Ph.D.(Engg.) from University of Engineering and Management, Kolkata. He did his graduation (B.Sc., Hons) in Mathematics in 2000, MCA in 2003, M.Phil. in Computer Science in 2007 and M.Tech. in Computer Science and Engineering in 2010. He is an IBM certified specialist in DB2. He is an Associate Member of the Institute of Engineers, Kolkata. He is currently working as a Lecturer (W.B.G.S.) in Computer Applications at A.J.C. Bose Polytechnic, Govt. of West Bengal under Department of Technical Education and Training, Govt. of West Bengal. Previously he worked as a Lecturer in different Engineering and Management colleges in India. He has published several papers in journals and conferences. He has also reviewed several research papers and has contributed in a few books also. His research interests include Bio-informatics, Cryptography Algorithms, DNA Cryptography, Quantum Cryptography, Network Security and Computer Graphics. He has more than 15 years of teaching and research experience.

Dr.Tamal Chakraborty is working as Assistant Professor, Department of Computer Science in Mrinalini Datta Mahavidyapith, Kolkata. He started his career with Wipro Technologies, India as a Software Engineer. Then he joined Flextronics Software Systems, India as a Technical Leader. After that he was associated with IBM India Pvt. Limited, where he was leading a software development team. Subsequently, he worked with Infosys Technologies, India, as a Project Manager. Since 2009 till 2016 he was teaching in Institute of Engineering and Management. He did his graduation (B.Sc., Hons.) in Physics from University of Calcutta in 1997, and B.Tech. in Computer Science and Engineering from University of Calcutta in 2000. In 2006 He received his MS degree from BITS Pilani, India. He was awarded with PhD (Tech.) by University of Calcutta in 2014. He has been presented with numerous awards from professional bodies and academia; including ―Feather in My Cap Award (twice) by Wipro Technologies, ―Spot Award by Lucent Technologies, ―Bravo Award by IBM India Pvt. Ltd. and ―Award of Excellence for contribution in the ―International Conference on innovative techno-management solution for social sector, in 2012. He has participated in various projects in India, Belgium and Ireland. IBM India Pvt. Ltd. had honoured him with ―Mentor Award for guiding a project in ―The Great Mind Challenge, 2011. Prof. Chakraborty is a member of the Computer Society of India (CSI). He has authored numerous papers in journals and conferences. His research interests include, Bio-informatics, Programming Languages and Design and Analysis of Algorithms.

Dr. Harekrishna Chattopadhyay is a faculty of University of Engineering & Management, Kolkata. Previously he worked as the Head of the Department, Electronics and Communications Engineering, Camellia School of Engineering and Technology. He has several years of teaching and research experience, including numerous publications in reputed Journals. In 2016 he was awarded PhD (Tech.) by University of Calcutta. His research interest includes Electro Cardiogram Signal Analysis, Quantum Computing and DNA Cryptography.