DNA Computing based Elliptic Curve Cryptography

P.Vijayakumar
Research Scholar
Dept., of ECE
Christ College of Engg & Tech

V.Vijayalakshmi
Assistant Professor
Dept., of ECE
Pondicherry Engg College

G.Zayaraz
Associate Professor
Dept., of CSE
Pondicherry Engg College

ABSTRACT
Cryptography is the science of using mathematics to encrypt and decrypt the data for secure communication. It enables the user to transmit the data in insecure network so that it cannot be read by anyone except the intended recipient. RSA and Elliptic Curve Cryptography are the existing public key cryptography technique which is used to provide secure data transmission. Existing DNA based cryptography technique need more computational power and more processing time with larger key sizes to provide higher level of security. This imposes a limitation on public key cryptography scheme. In order to overcome this limitation, a new cryptographic scheme is proposed which provides first level of security with smaller key size and less computation overhead using DNA Computing technique. The second level of security is provided by using low computation ECC encryption and decryption algorithm. The novelty of this proposed scheme is advantages of both ECC and DNA computation is exploited in providing a high level of data security. Finally, the performance of cryptography scheme is compared with the existing cryptographic schemes.

Keywords
Elliptic Curve Cryptography (ECC); Rivest, Shamir and Adleman (RSA); Deoxyribo Nucleic Acid (DNA); Koblitz's Algorithm; Public Key Cryptography.

1. INTRODUCTION
Elliptic Curve Cryptosystem (ECC) is another famous public key cryptography technique proposed by Miller and Koblitz in 1986 and 1987 respectively [1]. ECC provide the same level of security as RSA with a smaller key size. ECC-160 bit key provide the same security level with 1024-bit RSA key size. Therefore, the smaller key size of ECC can be more compact, and it brings many advantages such as circuit area, memory requirement, power consumption, performance and bandwidth. The key size of ECC has also been included in IEEE 1363 and NIST. The ECC operation is known as point scalar multiplication, which can be done by using different elliptic curve arithmetic algorithms [2].

Deoxyribo Nucleic Acid (DNA) is a long linear polymer found in the core part of a cell. DNA is made up of several nucleotides in the form of double helix and it is linked with the transmission of genetic information. Each spiral strand consist of sugar phosphate as backbone and bases are connected to a complementary strand by hydrogen bonding between paired bases Adenine, thymine, guanine and cytosine. Adenine and thymine are connected by two hydrogen bonds while guanine and cytosine are connected by three. In its primitive stage, DNA cryptography is shown to be very effective. Currently, several DNA computing algorithms are proposed for cryptanalysis and steganography problems, and they are very powerful in these areas. The concept of DNA computing combined with fields of cryptography and steganography brings a new hope for powerful, or unbreakable, algorithms [3-5]. This paper is organized as follows. Section 2 describes existing DNA computing based RSA cryptography. In section 3, the proposed DNA computing based ECC cryptography is described. Section 4 discusses the simulation results. The last section concludes this paper.

2. EXISTING SCHEME
The existing scheme implements RSA public key cryptography with DNA computation which achieves better security. This algorithm is quite easy but the real challenge is in the selection and generation of public and private key pairs for RSA. These key pairs should be extremely large prime numbers to overcome the eavesdropper attacks. Hence the existing public key cryptography requires larger key sizes thereby increasing the processing time for encryption and decryption of data.

RSA has the problem of factoring large prime numbers which increases the computation complexity when compared to ECC. The drawback of RSA algorithm is to roundup the power of n prime number with respect to the cipher text size. It results in increase in size of cipher text. So it requires more bandwidth and high power to transmit the data. RSA have more computation overhead for modular exponential algorithm. These are the limitations imposed by implementing RSA in the existing scheme. Existing DNA computing based cryptography converts plaintext into known ASCII value. So eavesdropper can easily achieve the plaintext with the help of encoded plaintext [6-11]. This imposes a serious limitation on the algorithm with added computation complexity, increased processing time and more storage requirement.

3. PROPOSED SCHEME
To overcome the limitations imposed by the existing cryptography scheme such as DNA computing with RSA, the proposed algorithm uses ECC instead of RSA along with data encoding using DNA by Koblitz's method. This proposed scheme provides greater level of security with low computation overhead. The first level of security in this proposed scheme is achieved by mapping the plaintext with DNA Nucleotide which is used to store large amount of data with few grams of DNA. The second level of security is achieved by encrypting the encoded plaintext using ECC encryption algorithm with lesser key size. Thus combination of ECC with DNA provides higher

level of security with less communication and computation complexity. An important advantage of ECC is the shorter key lengths. For example, ECC-160 provides similar security to RSA-1024 and ECC-224 provides equal security to RSA-2048. Further the encoding of data with DNA is carried out using Koblitz's method which is more efficient when compared to the existing scheme.

3.1 DNA Computing based Elliptic Curve Cryptographic Scheme

The proposed cryptographic scheme has advantages of both ECC and DNA based computing. It deals with the encoding and decoding of the given input text message as shown in Fig 3.1. First plaintext is given as input. Each character of the plaintext is mapped with nucleotides which will be the first level of security for secure data communication as shown in Table 3.1. Nucleotides are converted into corresponding numbers as shown in Table 3.2. These numbers are encoded into a ECC curve point using Koblitz's method [12,13]. Next the plaintext is represented in the form of ECC curve points. These points are encrypted using ECC encryption algorithm (Eq.1). ECC encryption is done with the help of its generated keys.The encrypted points from the elliptic curve are in the form of ciphertext points:

$$\{kG, P_m + k P_B\} \quad (1)$$

Where, G - Generated Points
P_m - Plaintext points
k - Random number chosen by user
P_B ` - Public key of another user

The ciphertext points are deciphered using ECC decryption algorithm (Eq.2). Deciphered points are converted into numbers using Koblitz's method. These numbers are decoded with the help of DNA nucleotides and required plaintext is obtained.

$$P_m + kP_B - n_B (kG) = P_m + k (n_B) G - n_B (kG) = P_m \quad (2)$$

Table.3.1: Convert plaintext into nucleotide

A - CCA	K - GAA	U - GTC
B - GTT	L - CGT	V - TCC
C - TTG	M - CCT	X - ACT
D - GGT	N - TCT	Y - AAA
E - TTT	O - CGG	Z - TCA
F - TCG	P - ACA	W - GCC
G - CGC	Q - CAA	
H - ATG	R - ACT	
I - AGT	S - GCA	
J - CGA	T - CTT	

Table.3.2. Convert nucleotides into numbers

A -10	C -20	G -30	T -40

3.2 Proposed Cryptographic Algorithm

The following steps are to be followed to implement the cryptographic scheme using DNA Computing with ECC as shown in Fig.3.3:

- Input the Plaintext
- Convert the Plaintext into DNA nucleotide strands which have unique character.
- Each character of the converted DNA Nucleotide is converted into Numbers.
- If Plaintext consists of the digits 0,1,2,3,4,5,6,7,8,9 are coded as digits itself.
- DNA Nucleotide letters are coded as A = 10, C=20, G=30, T=40.These Numbers are converted into points using Koblitz's method.
- Koblitz's Method: Pick an elliptic curve Ep (a, b).
- Elliptic Curve has N points, which are denoted as (x1,y1),(x2,y2),……..(xn,yn).
- Choose an auxiliary base parameter, for example k = 20. (Both parties should agree upon this)
- Each number mk (say), take $x = mk + 1$ and try to solve for y.
- If not able to solve for x=mk+1, then try x = mk +2 and then x = mk +3 until y value is obtained.
- In practice, y *is* obtained before $x = mk + k - 1$ will hit. Then take the point (x, y). This now converts the number m into a point on the elliptic curve. In this way, the entire message becomes a sequence of points.
- These sequences of points are encrypted using ECC encryption formula to obtain the Ciphertext points. These ciphertext points are deciphered using ECC decryption formula to obtain the plaintext points.
- Consider each plaintext point (x, y) and set m to be the greatest integer less than (x-1)/k. Then the point (x, y) decodes as the symbol m.

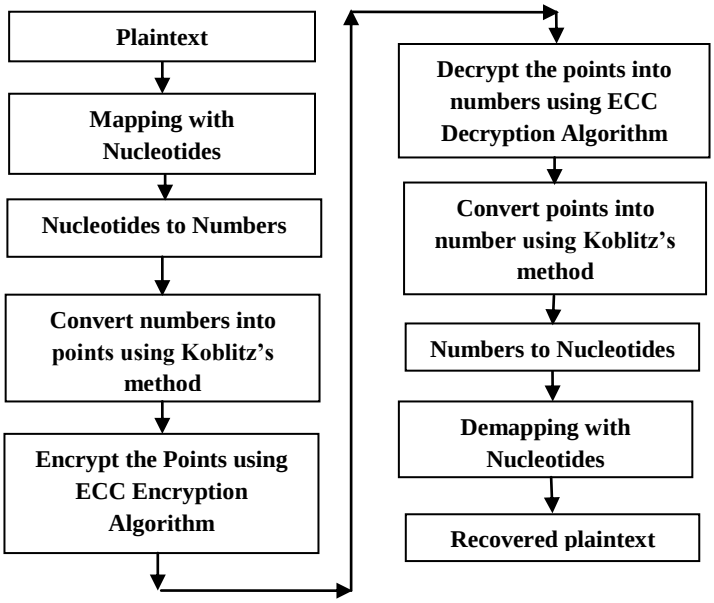

Fig 3.3: Cryptographic scheme using DNA with ECC

4. RESULTS AND DISCUSSION

The proposed cryptographic scheme was simulated for different key size and processing time was analyzed. Fig.4.1 shows that RSA takes more processing time than ECC. For key size of 100 bits, RSA takes processing time of 2.8 seconds whereas ECC takes only 1.5 seconds. From the simulated graph, it is inferred

that as key size increases, the processing time for RSA increases whereas the processing time for ECC decreases.

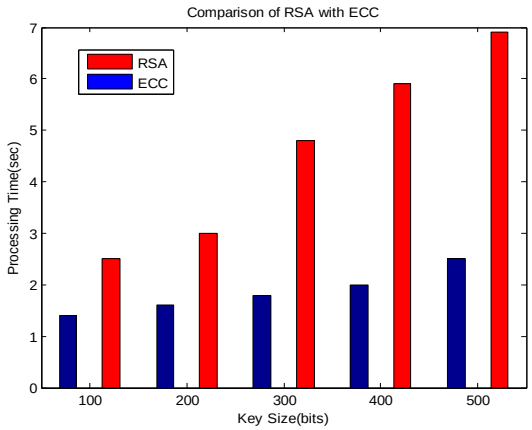

Fig.4.1 Comparison of RSA with ECC

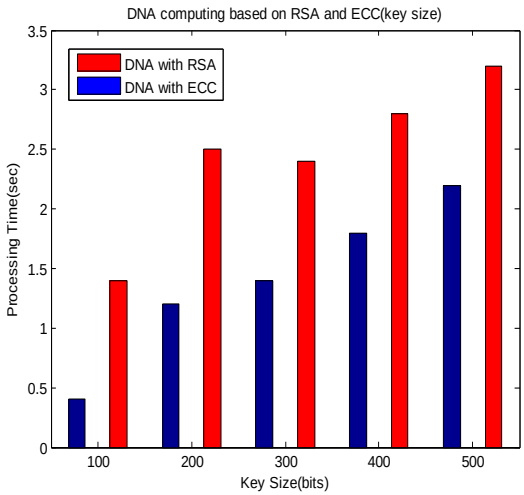

Fig.4.2 DNA Computing based on RSA and ECC (Key size)

Fig.4.2 shows that DNA with RSA takes more processing time than the DNA with ECC. For key size of 200 bits, DNA with RSA takes the processing time of 2.5 second whereas DNA with ECC takes only 1.3 second. Thus the simulated graph shows that as the key size varies from 100 to 500, the processing time of DNA with RSA increases whereas for DNA with ECC decreases.

Fig.4.3 shows the proposed scheme along with the existing scheme for different string lengths. For string length of 3000 bits, DNA with RSA takes the processing time of 0.23 seconds whereas DNA with ECC-160 takes only 0.18 seconds. From the simulated graph, it is inferred that proposed DNA with ECC saves 50ms of processing time for 3000 bits string length than existing scheme.

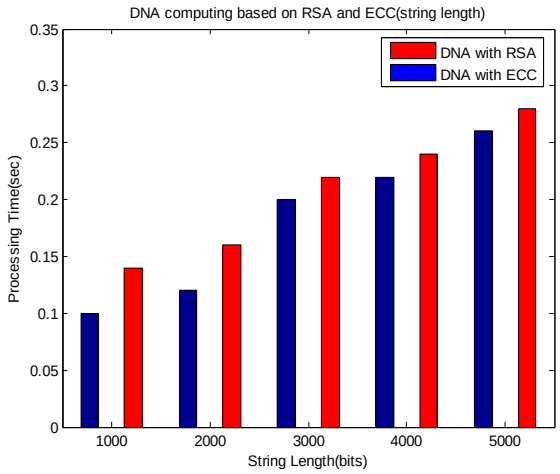

Fig .4.3 DNA Computing based on RSA and ECC (String Length)

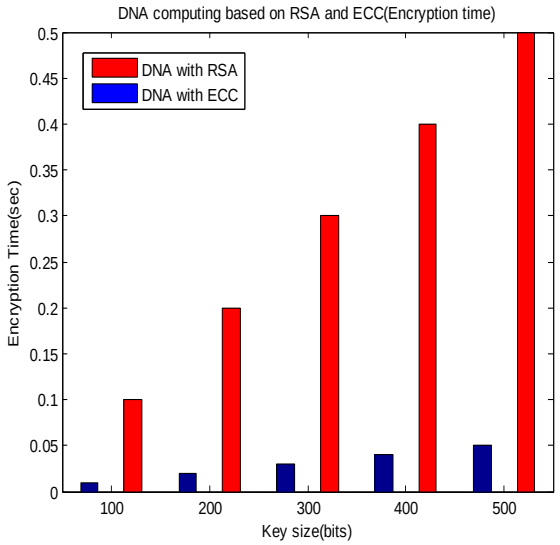

Fig.4.4 DNA computing based RSA and ECC (Encryption Time)

Fig.4.4 shows that analysis of encryption time of the proposed scheme with the existing scheme. From the simulated result, it is inferred that encryption time for DNA with RSA scheme is 0.22 seconds for the key size of 160 bits. Whereas encryption time for proposed DNA with ECC scheme takes only 20ms seconds for 160 bits key size.

5. CONCLUSION

This paper describes a novel cryptographic scheme by combining DNA computing theory with ECC algorithm. Elliptic curve cryptography with DNA Computing offers major advantages over traditional systems such as increased speed, less memory and smaller key size. In addition, less storage, less power and less processing time than other systems make it possible to implement cryptography in many special platforms such as wireless devices, laptop computers and smart cards. It

also provides higher level of security with less key size of ECC-80 bits than RSA-1024 bits.

6.REFERENCES

[1] N.Koblitz, "Elliptic Curve Cryptosystems, Mathematics of Computation", Vol A8, 1987, pp.203 -209.

[2] Amara. M , Siad. A, "Elliptic Curve Cryptography and Its Applications", in the IEEE proceeding of International workshop on Systems, Signal Processing and their Applications, May-2011, pp: 247-250.

[3] Sadeg, S. Gougache, M. Mansouri, N. Drias, H., "An encryption algorithm inspired from DNA"in the IEEE proceedings of International Conference on Machine and Web Intelligence (ICMWI), oct-2010,PP:344-349.

[4] G.Zayaraz, V.Vijayalakshmi et al, "Securing Biometric Authentication Using DNA Sequence and Naccache Stern Knapsack Cryptosystem" in the proceeding of International Conference On Control, Automation, Communication And Energy Conservation, June 2009, pp.1-4.

[5] Guangzhao Cui, Limin Qin et al, "An Encryption Scheme Using DNA Technology," in the IEEE proceeding of Fourth International Conference on Bio-Inspired Computing, Sept 2009, pp. 37-41.

[6] Xing Wang , Qiang Zhang, "DNA computing based Cryptography, in the IEEE proceeding of Fourth International Conference on Bio-Inspired Computing, Nov 2009, pp.1-3.

[7] Liu Feng, Gao Dong-Mei, "DNA Algorithm of Verifiable Secret Sharing," in IEEE Proc International Conference on Future Computer and Communication, June 2009, pp. 244-246.

[8] Li Xin-she, Zhang Lei,Hu Yu-pu, " A novel generation key scheme based on DNA," in the IEEE proceeding of International Conference on Computational Intelligence and Security, December 2008, pp. 264-266.

[9] Otirios A. Tsaftaris, and Aggelos K. Katsaggelos, "Retrieval Efficiency of DNA-Based Databases of Digital Signals, in the IEEE proceeding of Transactions on nanobioscience, vol. 8, no. 3, september 2009, pp. 259-270.

[10] Liu Chang, Yang Chi, "Factoring RSA modulo N with High Bits of P Known Revisited ",in the proceedings of IEEE International Symposium on IT in Medicine & Education, Aug- 2009,pp:495-500.

[11] Qing Liu, Yunfei Li, Lin Hao, Hua Peng," Two Efficient Variants Of The RSA Cryptosystem", in the IEEE proceedings of international conference on computer design and applicaionm,June-2010,PP: V5-550 - V5-553.

[12] Padma .Bh, D.Chandravathi , P.Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method," in the proceeding of International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, pp. 1904-1907.

[13] S.Maria C. Vigila, K.Muneeswaran, "Implementation of Text based Cryptosystem Using ECC," in the IEEE proceeding of ICAC'09, pp. 82-85.