International Journal of Pure and Applied Mathematics
Volume 119 No. 10 2018, 1195-1201
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

Elliptic Curve Cryptography Using Chaotic Neural Network

Ayush Sethi[1], Ayush Mittal[2], Ritu Tiwari[3], Deepa Singh[4]
[1234]Robotics & Intelligent System Design Lab,Indian Institute of Information Technology & Management,Gwalior,India
[1]ayushsethi22031992@gmail.com, [2]ayush2709@gmail.com, [3]tiwariritu2@gmail.com, [4]deepa@iiitm.ac.in

Abstract—Cryptography is the science of hiding important information while transmiting over an insecure channel mak-ing it impossible for any adversary to read.Cryptography is very important for transmission and sharing of confidential information preventing any missuse of it.Neural Networks is a mathematical model which simulates the structure and functionality of biological neural network.A chaotic neural network is a network which adds randomness to a signal which is extremely hard to predict.Adding a Chaotic Neural Network to a Cryptographic system enhances the security of the system making it difficult to decode by the adversaries.In this research paper we have collaborated a Chaotic Neural Network with an Elliptic Curve Cryptographic System which is then compared with the conventional models such as RSA,Blowfish and RC2 models and is found to be better than various models based on certainparameters.

Index Terms—Chaotic Neural Networks,Elliptic Curve Arith-metic, Cryptography,Information Security,Logistic Maps.

1. Introduction

The main aim of a cryptographic framework is the exchange of information of among the expected parties with no exposure of data to any adversaries who may get un-authoritative access to it[1].In 1977, Diffie-Hellmann discov-ered that a secret can be computed over any insecure channel which can be transfered safely over the channel. After that period many open key cryptography algorithms came into existence which are dependent on many different theories and need a lot of computation power. Also the time required and computation needed to transfer information was quite high before and thus to limit this disadvantage along with increasing the security of the framework, Neural Networks wereused.

Chaotic Neural Network is a class of Neural Network whose output is a random value dependent upon various parameters[32].The transmission of secret key can be made possible by the sychronization of common learning. The Chaos generated by a Chaotic Neural Network makes it difficult for any adversary to decode the secret message[8] sent by a party as the relationship among various plaintext and ciphertext paris is quite vague[31].Thus making attacks like ciphertext-only and known plaintext attacks impossible. Elliptic Curve Cryptography is a class of Cryptography where instead of using discrete logarithm, we are using Elliptic Curve Arithmetic which is difficult to break than the Integer Factorization Problem[20]. Also the key size for Elliptic Curve Cryptography is typically less due to the extremely hard Elliptic Curve Arithmetic.

In this paper we are using a combination of Elliptic Curve Cryptography along with a Chaotic Neural Network to provide a more secure and faster algorithm.

1.1. Concept of Artificial NeuralNetwork

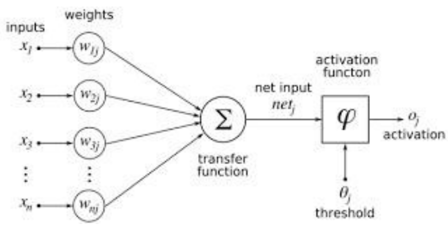

Figure 1. Artificial neural network[1]

Artificial Neural Networks are mathematical models which are used to imitate a biological neural network. ANN's are used to approximate or estimate functions which require a lot of inputs. These mathematical models are used where the human brain is considered to be more efficient in computing a typical function as comparedto a machine e.g identifying various images,or identifying different handwritings [4]etc.

Neural Network is a network of nodes known as neurons which are connected by directed links, where every link (X,Y) that connects the node X and Y has a weight w, also there is an activation function f which depending upon a threshold value maps the input state into an output state[24]. Neural Networks can be differentiated into two types: Feedforward Networks and Recurrent Networks. A Feedforward Neural Network is acyclic and thus it doesnot have any other state rather than the weights themselves. On the opposite side, a Recurrent Network is a cyclic network where the output is fed back into the network along with weights. Becuase of this feedback, Recurrent Networks need small amount of memory to store thatdata.

1.2. RelatedWork

In 2004,Einat Klein presented cryptography framework which was based on a secret-key generation by a neural network in a public channel[4]. The model he proposed had two neural networks trained on their alternate outputs syn-chronized to an equal time dependent weight vector through a chaos synchronization system starting with different initial conditions.In 2011,R. M. Jogdand proposed a model where secret key was generated by neural networks[8]. The neu-ral cryptography hastwo communication networks which receive an identical input vector, generate an output vector and are trained on the output vector. Also in 2012, Pratap Singh generated a secret key over a public channel using a neural network.[9]The model consists of 2 partners which had an input vector and different initial conditions which were syncronised by a common external signal and recieved a common input vector with the machine predicting their output by mutual learning. Zhang, proposed a novel chaotic keyed hash function using a feedforward feedback nonlin-ear filter. Arumugam studied the effective use of logistic map and Lorenz map in generating message authentication codes[25].In 2014, Xiang T. proposed a method where the image is compressed and encrypted by a chaotic map and arithmetic encoding, the encryption and compresseion were done at different stages making it possible for the adver-saries to break the cryptosystem without getting through the compression stage.In 2013,H Zhu and C. Zhao proposed a new encryption and compression scheme using a hyper-chaos and Chinese Remainder Theorem[3].It yielded a co-relation coefficient of 0.0058 and an entropy of 7.98 but its drawback was that it could be easily broken by the adversaries due to its similar plaintext encryptionnature.

2. Preliminaries

2.1. Simulation of a Chaotic NeuralNetwork

The Chaotic Neural Network used in our research work is based on 2 frequency mods which is a modified version of Hebb's Law.The equations for this model are described in thisway:

$$x_i(t + 1) = (1 \quad D_x)x_it+Eg_i(x_it) \tag{1}$$

where

$$g_i(x_i(t))= \sum_{j=1}^{N} w_{ij\,j}(x_j(t)) +I_i(t)$$

Here D is the decay parameter of potentials, E is the excitory rate,I(it) is the external input of the i'thneuron.

2.2. Elliptic CurveCryptography

The locus of a point, whose coordinates conform to a particular cubic equation along with the point at infinity O (the point at which the locus in the projective plane intersects the line at infinity,) is known as an elliptic curve.

The equation of $E(F_p)$ for the characteristic $p > 3$ can be defined as

$$y^2= x^3+ ax+b \tag{2}$$

where a F_p and b F_p are constants suchthat $4a^3+ 27b^2 6= 0$

Key Generation

Key Generation for an Elliptic Curve Cryptosystem is as follows:
Every node needs to have a pair of public and private keys. Every sender will be Encrypting the message with the reciever's Public Key and the reciever will Decrypt the message using it's private key.

Step 1 : Select a number "d" in the range of "N" where N is a primenumber.
Step 2 : Now we can generate the Public Key "Q"as follows:

$$Q = d \ P \tag{3}$$

where P is a point on the Curve

Step 3 : d is our Private Key and Q is the required Public Key.

Encryption

Two Ciphertexts must be generted and let the ciphertexts be C1 and C2. They are generated as follows:
Step 1 : Choose a number "K" less than N.

$$C1 = KP \tag{4}$$

$$C2 = M +KQ \tag{5}$$

where M is the Message we have to send

Step 2 : Now send both of the Ciphertexts.

Decryption

We can get the original message back as follows:

$$M = C2 \ dC1 \tag{6}$$

3. Methodology

Encryption and Decryption Processes

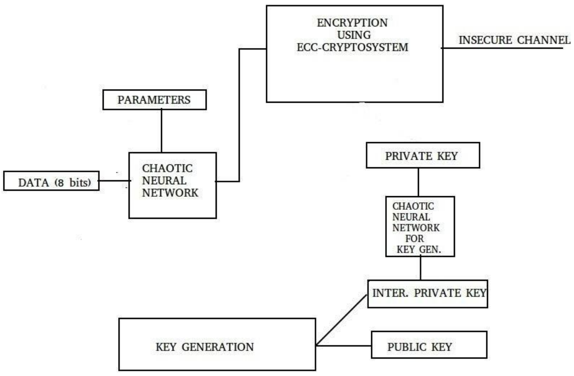

Figure 2. Encryption Using a Chaotic Neural Network

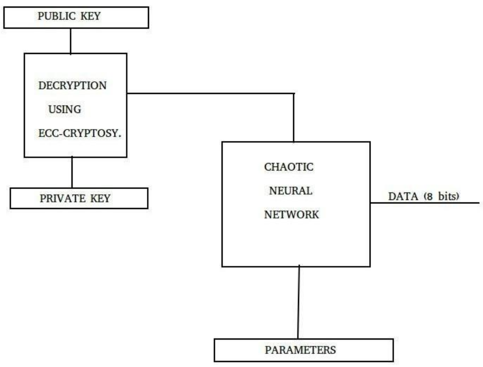

Figure 3. Decryption Using Chaotic Neural Network

3.1. Encryption Process on the SenderSide

First the data is divided into blocks of 8 bits each which will be Encrypted using our Algorithm.The blocks which are left are padded with zeroes.Then the chaos is created using the following algorithm by the Chaotic Neural Network.

STEP 1 : Set the value of parameter M.

STEP 2 :Determine the parameter, U and the initial point x(0) of the 1-D logistic map.

STEP 3 :Evolve the chaotic sequence x(1), x(2), ... , x(M) by x(n+1) = M(n)(1-x(n)).

STEP 4 : Create b(O), b(l), ..., b(8M- 1) from x(l), x(2), ..., x(M) by the generating scheme that 0.b(8m-8)b(8m-7) ..... b(8m-2)b(8m-l) ... is the binary representation of x(m) for m = 1, 2,. . . ., M.

STEP 5 : The weight t and biases O for all the neurons in the hidden layer are calculated given below.

For n : 0 to M-1 Do :

$$g(n)=\sum_{X_i}^{7} d_i 2^i \qquad (7)$$

For i=0 to 7 Do:
if(j eqauls i and b(8*n + i) equals 0)
t=1
else if(j eqauls i and b(8*n + i) equals 1)
t=-1
else if(j not eqauls i)
t=0

if(b*(8*n + i) equals 0)
O = -1/2
else if(b*(8*n + i) equals 1)
O = 1/2
For i=0 to 7 Do :

$$d_i=\left(\sum_{X_i=0}^{7} t_{ij}O_i\right) \qquad (8)$$

Now we can get the final transformed data in bits using the following algorithm.

$$g^0(n) = \sum_{X_i=0}^{7} d_i 2^i \qquad (9)$$

g’(n) is the required data which is to be encrypted using Elliptic Curve Cryptosystem and sent across.
The next part is to generate Private and Public Keys for the CryptoSystem.
As described above, The Elliptic Curve Cryptosystem re-quires to generate a Private Key which is chosen randomly by the Computer. The Public Key of every Node is also dependent on this Private Key. Thus to make system more secure,the randomly generated Private Key is again passed through the Chaotic Neural Network to make the keys even more secure.Then the Encryption process is carried out using the modified Public Key of the reciever and sent across the insecurechannel.

3.2. Decryption on the RecieverSide

The Decryption on the reciever side is exactly opposite in order of the Encryption mechanism. First the Ciphertext is passed into the Elliptic Curve Cryptosystem and decrypted using the Public and the Private keys. The Text decrypted using the Cryptosystem is fed into the Chaotic Neural Network to get the original text.

4. Results

The optimality of the proposed algorithm can be judged based on various parameters. The parameters that we have chosen in our research work are as follows:

Encryption Time Time taken to Encrypt a file of fixed size.The less Encryption time is preffered as the algorithm has to be fast enough to convert the secret message into a hidden message.

Decryption Time Time taken to Dencrypt a file of fixed size.The less Decryption time is preffered as the algorithm has to be fast enough to convert the hidden message back into the secret2 message.

Time to generate keys Time to generate keys should be as less as possible as keys play the most important role in Encrypting and Decrypting data.

Throughput Throughput should be as high as possible as it denotes the amount of data to be transfered from the channel.

Correlation Coeffiecient Correlation function should be close to 1 as a 0 Correlation Coefficient denotes no change in the secret message and the ciphertext.

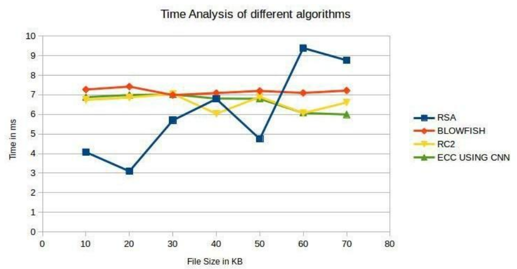

Figure 4. Encryption time for various algorithms

The above graph shows the Encryption time of various algorithms which were used some time ago like Blowfish and some algorithms which are currently in use like RSA. The above diagram shows that for small file RSA outper-forms all other algorithms but as the file size increases, other algorithms catch up and with large file size, our algorithm takes the least amount of time in ms.

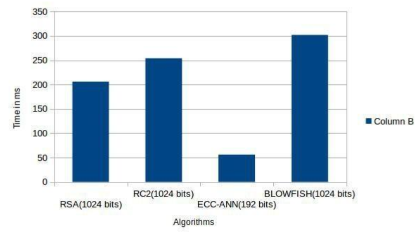

Figure 5. Time required to generate keys

The Bar Graph below shows the time required for gen-erating keys. The key size for all the algorithms except our ECC using ANN is 1024 bits and for our algorithm it is 192 bits.This is done becuase other algorithms with 1024 bits key size provides a same security as ours with 192 bits.

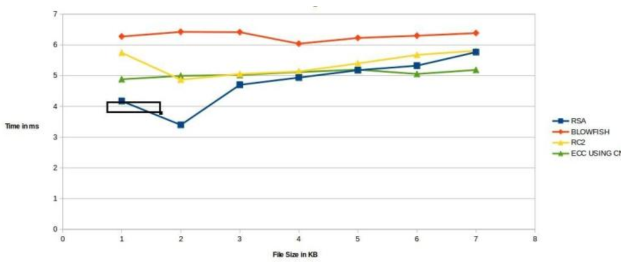

Figure 6. Decryption time for various algorithms

The above graph shows the Decryption time of various algorithms which were used some time ago like Blowfish and some algorithms which are currently in use like RSA. The above diagram shows that for small file RSA outper-forms all other algorithms but as the file size increases, other algorithms catch up and with large file size, our algorithm takes the least amount of time in ms.

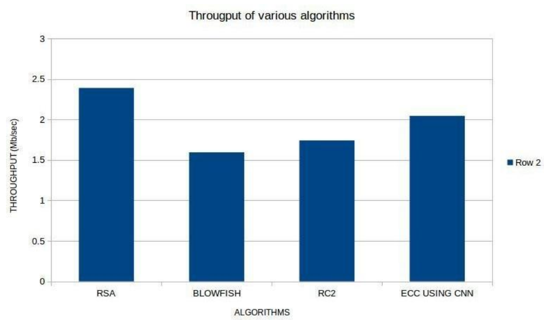

Figure 7. Throughput for various algorithms

The above graphs shows throughput for various alorithms. Throughput is defined as the number of bytes sent across the channel per unit of time. The Results show that RSA has the highest Throughput with our algorithm comingsecond.

$$\text{throughput} = \frac{\text{bytessent}}{\text{timeinseconds}} \qquad (10)$$

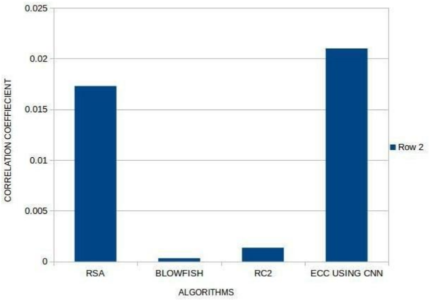

Figure 8. Comparison of various algorithms

The above Bar Graph shows the Corelation Coefficient of various algorithms. The corelation coefficient being close to 0 represents that there is not much change in the plaintext and the ciphertext.The Corelation Coefficient for our algo-rithm is the maximum which shows that our algorithm has changed maximum characters of the plaintext which makes it better than the rest.

TABLE 1. COMAPRISONS OF VARIOUS ALGORITHMS BASED ON DIFFERENT PARAMETERS.

Parameter	RSA	Blowfish	RC 2	ECC-ANN
Encryption time for smallfiles	4.127ms	7.134ms	6.922ms	7.02ms
Encryption time for largefiles	7.65ms	7.172ms	6.656ms	6.245ms
Decryption time for smallfiles	4.213ms	6.49ms	5.257ms	5.05ms
Decryption time for largefiles	5.413ms	6.331ms	5.57ms	5.323ms
Timeto gen-eratekey	59ms	201ms	297ms	251ms
Throughput (inMb/sec)	2.35	1.67	1.86	2.01
Corelation	0.017	0.0015	0.002	0.021

5. Conclusion

This research work has analyzed on various techniques which are used for transfer of data from one end to another in a safe and a secure manner.Chaotic Neural Network has been used to transer data from one end to another. This Neural Network do not require any data set as the input is solely dependent on the chaotic sequence,which makes the process almost impossible to crack by the intruder.The Chaotic Neural Network is used to modify an Elliptic Curve Cryptography framework.The model is compared with few other models that are currently in use and is found to be working better than the conventional models in some aspects.Our model of using Elliptic Curve Cryptography using a Chaotic Neural Network has the highest Co-relation Coefficient and second best in terms of throughput after RSA. Also the Encryption and Decryption time is dependent on the size of the file.The bigger files are fastest Encrypted and Decrypted using our model. This type of cryptography can be used at places where secrecy of data is of utmost importance.Chaotic nature makes it very unpredicatble for intruder to crack the secretmessage.

References

[1] T.P.Wasnik , Vishal S. Patil , Sushant A. Patinge , Sachin R. Dave,Gaurav J. Sayasikamal, “Cryptography as an instrument to network security”, International Journal of Application or Innovation in Engi-neering and Management, Vol. 2, Issue 3, 72-80, 2013.

[2] Wolfgang Kinzel, IdoKanter, “Neural Cryptography”, TH2002 Supple-ment, Vol. 4, 147-153,2003.

[3] Zhu, Hongfeng, Yifeng Zhang, and Yang Sun. “Provably secure multi-server privacy-protection system based on chebyshev chaotic maps without using symmetric cryptography.” International Journal of Net-work Security, vol 18, issue 5,803-815,2016.

[4] Einat Klein,Rachel Mislovaty,IdoKanter,Andreas Ruttor, Wolfgang Kinzel,“Synchronizationofneuralnetworksbymutuallearningandits application to cryptography”, Advances in Neural Information Processing Systems ,Vol. 3, Issue4,37-45,2014

[5] Vaidyanathan, Sundarapandian, Christos K. Volos, and Viet-Thanh Pham. “Hyperchaos, Control, Synchronization and Circuit Simulation of a Novel 4-DHyperchaoticSystemwithThreeQuadraticNonlin-earities.”,Advances in Chaos Theory and Intelligent Control, Springer International Publishing, 297-325,2016.

[6] Vaidyanathan, Sundarapandian. “A Novel 4-D Hyperchaotic Thermal Convection System and Its Adaptive Control.” Advances in Chaos The-ory and Intelligent Control. Springer International Publishing, 2016. 75-100.

[7] N. Prabakaran,P.Vivekanandan,“A New Security on Neural Cryptogra-phy with Queries”, International Journal of Advanced Networking and Applications, Vol. 2, Issue. 1, 437-444,2010.

[8] R. M. Jogdand, Sahana S. Bisalapur, “Design of an efficient neural key generation”, International Journal of Artificial Intelligence and Applications, Vol.2, No.1, 60-69,2011.

[9] Pratap Singh, Harvir Singh, “Cryptography in structure adaptable digital neural networks”, National monthly refereed journal of research in science and technology, Vol.1, Issue.12, 35-44,2012.

[10] Ajit Singh, Aartinandal, “Neu ral Cryptography for Secret Key Ex-change and Encryption with AES”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.5, 376-381, 2013.

[11] Wenwu Yu, Jinde Cao, “Cryptography based on delayed chaotic neural networks”, Physics Letters A, Vol. 356,issue .4, Elsevier, 333338, 2006.

[12] Jiyun Yang, Xiaofeng Liao, Wenwu Yu, Kwok -wo Wong, Jun Wei, “Cryptanalysis of a cryptographic scheme based on delayed chaotic neural networks”, Chaos,Solitons and Fractals, Vol.40, Issue.2, 821-825,2009.

[13] Rajender Singh, Rahul Misra, Abhishek Chaudhary, “Power consumption using artificial neural network in the field of cryptography”, Journal of information, Knowledge and research in computer Engineering, Vol.2, Issue.2, 443-446,2012.

[14] Shweta B. Suryawanshi, Devesh D. Nawgaje, “A triple-key Chaotic neural network for cryptography in image processing”, International Journal of Engineering Sciences and Emerging Technologies, Vol. 2, Issue. 1, 46-50, 2012.

[15] Nitin Shukla, Abhinav Tiwari, “An Empiri cal Investigation of Using ANN Based N-State Sequential Machine and Chaotic Neural Network in the Field of Cryptography”, Global Journal of Computer Science and Technology Neural and Artificial Intelligence, Vol. 12, Issue.10,No.1,17-26,2012.

[16] Tariq A. fadil, Shahrul N. yaakob, Badlishah ahmad, abid yahya, “Encryption of mpeg-2 video signal based on chaotic neural network”, Journal of Engineering and Technology, Vol. 3, 35-42,2012.

[17] Navita Agarwal, Prachi Agarwal, “Use of Artificial Neural Network in the Fie ld of Security”, MIT International Journal of Computer Science and Information Technology, Vol. 3, No. 1, 4244,2013.

[18]B. Geetha vani, E. V. Prasad, “A Hybrid Model for Secure Data Transfer in Audio Signals using HCNN and DD DWT”,International Journal of Advanced Computer Science and Applications, Vol. 4, No.7, 202-208, 2013.

[19] Darrel Hankenson,Alfred Menezes “A guide to Elliptic curve cryptography,Springer”(2014):22-25

[20] Bosmans, Jeroen, et al. “A Tiny Coprocessor for Elliptic Curve Cryptography over the 256-bit NIST Prime Field.” , International Conference on VLSIDesign,IEEE,1-6,2016.

[21] Huaiqin Wu,Xiaoweo Zhang,Ruoxia Li,Rong Yao,“Finite Time synchronisation of chaotic neural networks with mixed time-varying delays and stochastic disturbances”,4 jan 2015, Springer-verlag berlin Heidelberg

[22] Harpreet Kaur “International Journal of Information Technology and Knowledge Management” July-December 2011, Volume 4, No. 2, 417-422.

[23] Farash, Mohammad Sabzinejad, Saru Kumari, and Majid Bakhtiari. “Cryptanalysis and improvement of a robust smart card secured authen-tication scheme on SIP using elliptic curve cryptography.”, Multimedia Tools and Applications,1-20,2015.

[24] Li and M. Bohnerb, “Exponentia l synchronization of chaotic neural networks with mixed delays and impulsive effects via output coupling with delay feedback, Mathematical Computation Model,vol. 52,issue 5,643653,2015.

[25] H. Zhang, L. Cui, X. Zhang, and Y. Luo, “Data-driven robust approx-imate optimal tracking control for unknown general nonlinear systems using adaptive dynamic programming method”, IEEE Transaction on Neural Network, vol. 22, issue no. 12, 2226-2236, Dec.2010.

[26]S. Wen, Z. Zeng, and T. Huang, “Dynamic behaviors of memristor-based delayed recurrent networks”, Journal of Neural Computation Application, vol. 23, issue no.3, 815-821, 2013.

[27]X. He, C. Li, T. Huang, C. Li, and J. Huang, “A recurrent neu-ral network for solving bilevel linear programming problem”, IEEE Transaction on Neural Network Learning Systems, vol. 25, issue no. 4, 824-830, 2014.

[28] A. Zou, X.C Xiao, “An asynchronous encryption arithmetic based on Laguerre chaotic neural networks”,International Conference of the Global Congress on Intelligent System, vol. 4, issue no.3,36-39.

[29] Wang, Leimin, Yi Shen, and Guodong Zhang. “General decay synchronization stability for a class of delayed chaotic neural networks with discontinuous activations.” Neurocomputing, vol. 12 , 169-175,2016.

[30] Li,Yong, and Chuandong Li. “Complete synchronization of delayed chaotic neural networks by intermittent control with two switches in a control period.” Neurocomputing,vol. 173, 1341-1347,2016.

[31] Akhmet, Marat, and Mehmet Onur Fen. “Chaos by Neural Networks.” Replication of Chaos in Neural Networks, Economics and Physics. Springer Berlin Heidelberg. 311-405,2016.

[32] Ch, Shehzad Ashraf, et al. “An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography.” Multimedia Tools and Applications vol .74,issue 5 , 1711-1723,2015.

[33] Huang, Baojun, et al. ”An efficient remote user authentication with key agreement scheme using elliptic curve cryptography.” Wireless Personal Communications,vol 85, issue 1,225-240,2015.