International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

Design and Mathematical Model of Hybrid Cryptographic Algorithm- A^{3}D Algorithm

Anjan K[1], Abhijith C[2], Arunraj[3], Deekshith N[4], Jibi Abraham[5]

Department of Computer Science and Engineering, R. V. College of Engineering, Bangalore, India[1,2,3,4]

Department of CEIT, College of Engineering, Pune, India[5]

Abstract: With the advent of network technology, internet attacks are also versatile. So, the traditional encryption algorithms (single data encryption) may not suffice securing the information over network. The alternative is to design an algorithm, that addresses the urgent need of security with less computational effort. This paper presents complete mathematical model required for designing a cryptographic algorithm that incorporates point curve in Jacobian symbol. The encryption process is based on a secured multilevel pseudo random number generator that helps in obscuring key generation process.

Keywords: Multilevel random number generator; Elliptic curve cryptography(ECC); Jacobian symbol; Goldwasser-Micali

I. INTRODUCTION

Every commercial application on network requires different levels of security, certain application requires high security and confidentiality of information over the network[1]. To enhance the confidentiality various measures have been taken up to improve cryptographic algorithm. These measures may not have remarkable effect on attacks that compromises security.

Cryptographic algorithm need to be designed with a balance on computational power and security. Most of the algorithms either symmetric or asymmetric caters to any one of these needs. Hence to implement an algorithm that takes case of these two factors is tedious or difficult, however certain changes in the existing algorithms like inclusion of point curve of Elliptic curve cryptography in GoldWasser Micali Algorithm would answer the needs.

A. *Elliptic curve cryptography(ECC)*

Elliptic Curve Cryptography is a promising asymmetric cryptographic algorithm with an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [2][3][4]. The primary benefit of ECC is that it requires a smaller key size compared to other cryptographic algorithms [5]. This reduces storage and transmission requirements, which leads to faster processing. This is very useful for implementing encryption on small devices with limited resources in terms of power, CPU and memory [6]. It is also very helpful in handling many encrypted sessions for large web servers. The strength of an asymmetric encryption algorithm such as ECC is found in the complexity of computing the inverse of the function used to generate the key. Creating the key is straight forward, but finding the inputs that were used to create the key is computationally infeasible. In ECC, the computationally intense problem is called “Elliptic Curve Discrete Logarithm Problem”, and involves the difficulty in computing the discrete logarithm (exponent) from the result. And there are many hybrid cryptographic algorithms which uses ECC cryptosystem as a base making it an ideal choice.

B. *GoldWasser Micali Cryptosystem*

Goldwasser-Micali cryptosystem is an asymmetric key encryption[7] algorithm, which is based on probabilistic public-key encryption scheme. It is highly secured algorithm as the ciphertext generated will be several times larger than the initial plaintext [8]. Since the algorithm uses probabilistic encryption technique, a given plaintext may produce different ciphertexts each time it is encrypted. This has significant advantages, as it prevents from recognizing intercepted messages by comparing them to a set of known ciphertexts.

II. MULTILEVEL RANDOM NUMBER GENERATOR

The details of the custom designed multilevel random number generator are given below. Flow of the generation is depicted in Fig 1.

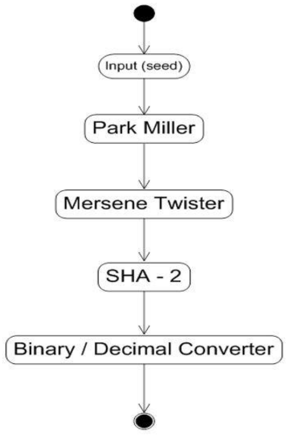

Fig 1 : Multi level random number generator

A random number obtained from java in built function is fed to Park-Miller algorithm as initial seed. The outcome of it is given to standard Mersenne-Twister algorithm as seed and output of it is given to SHA-2 hash function. 64 bit random number is taken randomly from the hash string obtained and number is returned to calling function [9][10][11]. Refer Figure above for activity diagram of this module.

III. MATHEMATICAL MODEL OF HYBRID ALGORITHM.

Let p be a prime number, which is chosen randomly. The elliptic curve $Y^2 = X^3 + AX^2 + B$ is chosen such that, A and B should satisfy the condition: $4A^3 + 27B^2 \neq 0$.This is to avoid duplication of roots. Since ECC is based on prime fields, curve equation and the conditions changes to equation 1 and 2 respectively.

$$Y^2 mod\ P\ = (X^3 + AX^2 + B) mod\ P \qquad (1)$$

$$(4A^3 + 27B^2) mod\ P \neq 0 \qquad (2)$$

By assigning a random value for X, corresponding value of Y can be found using the equation 3 in order to get the base point:

$$Y =\ \pm\sqrt{(X^3 + AX^2 + B) mod\ P} \qquad (3)$$

Let a=$X^3 + AX^2 + B$. Therefore,

$$Y =\ \pm\sqrt{a\ mod\ P}$$

Now `a' is a quadratic residue if $a^{\frac{P-1}{2}} \equiv 1\ (mod\ P)$. Also, `a' is not a quadratic residue if $a^{\frac{P-1}{2}} \equiv -1\ (mod\ P)$. Assuming that `a' is a quadratic residue, then $\sqrt{a\ mod\ P}$ is calculated as shown below:

$P - 1 = 2^S.m$

z = any non residue mod p

$c\ \equiv z^m (mod\ P)$

$u\ \equiv a^m (mod\ P)$

$v\ \equiv a^{\frac{m+1}{2}}\ (mod\ P)$

Note that o(c) is 2^s and o(u) divides 2^{s-1}, as u is a quadratic residue. Also, $v^2 \equiv ua\ (mod\ P)$. Each pass starts with o(u) dividing 2^i . Either o(u) divides 2^{i-1}, or $u^{2^{i-1}}\ \equiv 1\ (mod\ P)$. In the latter case u and v can be modified as to make o(u) divide 2^{i-1}, while maintaining the property $v^2 \equiv ua\ (mod\ P)$. Finally v is the square root of `a mod P' . Hence (X, Y) forms the base point G.

Now the order `n' of point G is found such that n(G)=O by performing scalar multiplication. Scalar multiplication requires two important operations namely point addition and point doubling [2].

A. Point Addition

Let P(x1, y1) and Q(x2, y2) ∈ E(K) where P ≠ Q. Then P + Q = (x3, y3), where coordinates x3 and y3 are found using equation 4 and 5 respectively.

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \qquad (4)$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 - x_3) - y_1 \qquad (5)$$

B. Point Doubling

Let P(x1, y1) ∈ E_K(a,b) where P≠ -P then, 2P=(x3, y3); where coordinates x3 and y3 are found using equation 6 and 7 respectively.

$$x_3 = \left(\frac{3x^2{}_1 + a}{2y_1}\right)^2 - 2x_1 \qquad (6)$$

$$y_3 = \left(\frac{3x^2{}_1 + a}{2y_1}\right)^2 - (x_1 - x_3) - y_1 \qquad (7)$$

C. Point Multiplication

Let P be any point on the elliptic curve(K). Then the multiplication operation of the point P is defined as repeated addition, i.e. kP = P + P + ...k times. So, a random value k <n is chosen as ECC private key and perform scalar multiplication with base point in order to obtain the ECC Public Key PK, i.e. PK = k * G.

Further, prime numbers p and q which are nearest to the coordinates of PK are obtained and are used to find jacobian symbols in Goldwasser Micali algorithm.

D. Integration

The pair (p,q) acts as private key for Goldwasser Micali algorithm. Public key is constructed using N = p_q. Then, y is found such that Jacobian condition[12] is satisfied which is given as,

$\frac{y}{N} = 1$ ie

$\frac{y}{p} = \frac{y}{q} = 1$

where y is a pseudo square modulo Zn. Now (n,y) pair is the obtained public key.

E. Encryption and Decryption

Let's assume that, sender A wants to send a message M to the receiver B. Through a standard key exchange mechanism, A obtains B's public Key i.e. (n, y). Message translator converts message M into a binary string as $m_0 m_1 m_2 \ldots m_i \ldots m_n$. If i^{th} bit of the message is m_i, then using a pseudo random number x, corresponding cipher bit c_i is computed as,

$$c_i = (y.x^2\ mod\ n) if\ m_i = 1$$

$$c_i = (x^2\ mod\ n) if\ m_i = 0$$

So $c_0 c_1 c_2 \ldots \ldots \ldots c_i \ldots \ldots c_n$ is the generated string of cipher bits.

While decrypting, receiver B obtains the cipher from A through communication channel. B uses its private key (p, q) to decipher the message. For each cipher bit c_i, Legendre symbol [18] is computed as:

$$e_i = \frac{c_i}{p}$$

If $e_i = 1$, then set $m_i = 0$ else set $m_i = 1$. Finally, $m_0 m_1 m_2 \ldots \ldots \ldots m_i \ldots \ldots \ldots m_n$ is the decrypted message in the form of binary string. Message translator at receiver end converts this binary string into original message.

IV. SYSTEM DESIGN

In any system, each component that makes complete system, contributes to the system with its own function. It is important to identify those components in order understand those in a better way. The initial design process of identifying these components, establishing a connection between those and understanding about their organization within the system is known as system organization. In this section overall system organization is described along with brief description of components that makes the system. Figure 2 shows the system organization which involves certain components that makes entire system. Each block represents a module or an entity involved with the system. Each module has its own function that is to be performed and is itself comprised of smaller tasks.

A. *Sender and Receiver*

Sender is a person who wants to send a message securely to receiver over a communication channel using the hybrid cryptosystem. The message which sender wants to send is called cipher text. Sender needs to create a file which contains the message he wants to send. Then using user interface he needs to browse the file to encrypt it. The encrypted message will be transferred to the receiver over a communication channel. Before delivering the message to receiver, the cipher text is converted back to original message by decryptor.

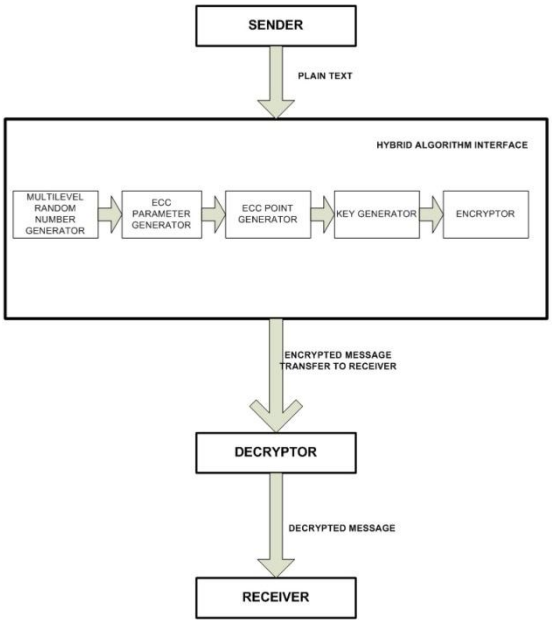

Fig 2 : System design of Hybrid Algorithm

B. *Random Number Generator*

The random number generator [9][10][11][13][14] is important component of hybrid algorithm interface. This module computes pseudo random numbers and provides it to key generation process and ECC parameter generator.

C. *ECC Parameter Generator*

This component finds suitable values for the elliptic curve parameters [15][16][17]. Elliptic curve has three parameters: p, a and b. Parameter p is obtained using random number generator. Parameters a and b should be generated such that, they should satisfy condition the condition:

$(4A^3 + 27B^2) mod\ P$ =0.

D. *ECC Point Generator*

This component computes the point P(X,Y) such that, it should lie on the ECC curve$Y^2 = X^3 + AX^2 + B$. Since ECC is implemented using prime field F(P), the condition: Y^2 mod P $= (X^3 + AX + B) mod\ P$ should be satisfied by the generated point [18][19][20].

E. *Key Generator*

This component generates key required by encryptor and decryptor [21][22]. Using ECC parameters base point G is generated using point generator. Scalar multiplication is performed as k(G) which generates ECC public key. The points coordinates are converted as nearest primes as (p,q) which is used as Goldwaser Micali Algorithms private key. From the private key, public key (n,y) is obtained as explained in mathematical design in this paper.

F. *Encryptor and Decryptor*

Using keys generated by key generator, encryptor will encrypt the message using bit-wise encryption technique [23][24]. Similarly, using bit-wise decryption technique the original message is retrieved by receiver.

V. CONCLUSION

Cryptographic algorithms are integral part of the secured communication over the internet. The existing well known algorithms may not be feasible against security attacks in future. Hybrid cryptosystem developed in this project provides a shield against brute force attacks and the cryptosystem mainly concentrates on increased level of security. Key features of ECC algorithm and Goldwasser-Micali algorithm have been implemented in this project successfully. An effective random number generator have been developed to strengthen the cryptosystem. The developed cryptographic algorithm uses 64-bit key for encryption and decryption. The encrypted message is semantically secure because of the bit-wise probabilistic encryption technique used and hence process of deciphering is impossible for the intermediaries. Performance analysis shows that the ratio of plaintext size to cipher text size is constant. Also, the encryption and decryption time are less in comparison with other existing standard algorithms under similar specifications.

REFERENCES

[1] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol. 1(1), 2010, pp. 01-05.

[2] Sravana Kumar D, Suneeth, Chandrasekhar A, "Encryption of data using Elliptic Curve over finite fields", International Journal of Distributed and Parallel Systems (IJDPS), Vol.3(1), 2012 , pp. 301-308.

[3] Moncef Amara, Amar Siad, "Elliptic Curve cryptography and its applications", Proceeding of the 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), France, 2011, pp. 247-250.

[4] Prabu M, Shanmugalakshmi R, "A Comparative and Overview Analysis of Elliptic Curve Cryptography Over Finite Fields", Proceeding of the International Conference on Information and Multimedia Technology, 2009, pp. 495-499.

[5] Nafeesa Begum J, Kumar K, Sumathy V, "Multilevel Access Control in Defense Messaging System Using Elliptic Curve Cryptography", Proceeding of the second International conference on Computing, Communication and Networking Technologies, 2010.

[6] Song Ju, "A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography", IEEE, 2012, pp. 138-141.

[7] Shafi Goldwasser, Silvio Micali, "Probabilistic Encryption", Journal of computer and system sciences, 1984, pp. 270-299.

[8] Orhio Mark Creado, Xianping Wu, Yiling Wang, Phu Dung Le, "Probabilistic Encryption: A Comparative Analysis against RSA and ECC", Proceeding of the Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009, pp. 1123-1129.

[9] Sammy Kwok, Edmund Lam, "FPGA based High speed True Random Number Generator for Cryptographic Applications", IEEE, 2006.

[10] Bang-Ju Wang, Hong-Jiang Cao, Yu-Hua Wang, Huan-Guo Zhang, "Random Number Generator of BP Neural Network Based on

SHA-2 (512)”, Proceeding of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 2008, pp. 2708-2712.

[11]] Langdon W B, “A Fast High Quality Pseudo Random Number Generator for Graphics Processing Units”, Proceeding of the IEEE Congress on Evolutionary Computation, 2008, pp. 459-465.

[12] Shruthi R, Sumana P, Anjan Koundinya K, “Performance Analysis of Goldwasser-Micali Cryptosystem”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2(7), July 2013, pp. 2818-2822.

[13] Lih-Yuan Deng, Olusegun George E, Yu-Chm Chu, “On Improving Pseudo- Random Number Generators”, Proceeding of the Winter Simulation Conference, Memphis, 1991, pp. 1035-1042.

[14] Manuel Blum, Silvio Micali, “How To Generate Cryptographically Strong Sequences Of Pseudo Random Bits”, IEEE, 1982.

[15] Xiaoqiang Zhang, Guiliang Zhu, Weiping Wang, Mengmeng Wang, “Design and Realization of Elliptic Curve Cryptosystem”, Proceeding of the International Symposium on Instrumentation & Measurement, Sensor network and Automation, China, 2012, pp. 302-305.

[16] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, “Elliptic Curve Cryptography”, ACM Ubiquity, Vol. 9(20), 2008.

[17] BAI Qing-hai, ZHANG Wen-bo, JIANG Peng, LU Xu, “Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation”,Proceeding of the International Conference on Computer Science and Service System, China, 2012, pp. 1224-1227.

[18] Jaydip Sen, “Cryptography and Security in Computing”, 5th Ed., InTech publications, ISBN 978-953-51-0179-6, 2012.

[19] Apostolos Fournaris P, Odysseas Koufopavlou, “Creating an Elliptic Curve Arithmetic unit for use in Elliptic Curve cryptography”, IEEE, 2012, pp. 1457-1464.

[20] Kimmo Jarvinen U, Jorma Skytta O, “High-Speed Elliptic Curve Cryptography Accelerator for Koblitz Curves”, Proceeding of the 16th International Symposium on Field-Programmable Custom Computing Machines, Finland, 2008, pp. 109-118.

[21]] MariaCelestin Vigila S, Muneeswaran K, “Implementation of Text based Cryptosystem using Elliptic Curve Cryptography”, Proceeding of the International Conference on Automatic Computing, Sivakasi, 2009, pp. 82-85.

[22] Sukalyan Goswami, Subarna Laha, Satarupa Chakraborty, Ankana Dhar, “Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm”, Proceeding of the Third International Conference on Intelligent Systems Modelling and Simulation, Kolkata, 2012, pp. 639-644.

[23] Orhio Mark Creado, Xianping Wu, Yiling Wang, Phu Dung Le, “Probabilistic Encryption: A Practical Implementation”, Proceeding of the Fourth International Conference on Computer Sciences and Convergence Information Technology, Melbourne, Australia, 2009, pp. 1130-1136.

[24] Julien Bringer, Herve Chabanne, Malika Izabachene, David Pointcheval, Qiang Tang, Sebastien Zimmer, “An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication”, Proceeding of the 12th Australasian Conference on Information Security and Privacy, Queensland, Australia, 2007, pp. 1-10.

BIOGRAPHIES

Anjan K Koundinya has received his B.E degree from Visveswariah Technological University, Belgaum, India in 2007 And his master degree from Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore, India. He has been awarded Best Performer PG 2010 and rank holder for his academic excellence. His areas of research includes Network Security and Cryptology, Adhoc Networks, Mobile Computing, Agile Software Engineering and Advanced Computing Infrastructure. He is currently working as Assistant Professor in Dept. of Computer Science and Engineering, R V College of Engineering.

Abhijith C has received his B.E degree in Computer Science and Engineering from R V College of Engineering, Bangalore, India in 2014. His areas of research interests include Computer Networks, Cryptography, Network Security. He is currently working as a Graduate Software Engineer at Aurigo Software Technologies Pvt. Ltd.

Arunraj has received his B.E degree in Computer Science and Engineering from R V College of Engineering, Bangalore, India in 2014. His areas of research interests include Computer Networks, Cryptography, Network Security. He is currently working as a Graduate Software Engineer at Sapient.

Deekshith N has received his B.E degree in Computer Science and Engineering from R V College of Engineering, Bangalore, India in 2014. His areas of research interests include Computer Networks, Cryptography, Network Security. He is currently working as a Graduate Software Engineer at Tesco Hindustan Service Centre.