Grenze International Journal of Engineering and Technology, Jan Issue

Data Security Architecture in Cloud Computing based on Elliptic Curve Cryptography with Special Focus on Lowering the Cipher Space

CH. Neelima[1] and CH. Suneetha[2]
[1]Assistant Professor, Dept. of Mathematics ANITS, Visakhapatnam, India
Email: neelimachallarapu@gmail.com
[2]Associate Professor, Dept. of Mathematics GITAM University, Visakhapatnam, India
Email: gurukripachs@gmail.com

***Abstract*— Public key Cryptography which is associated with pair of public and private keys is an important requirement for electronic commence in the history of cryptography. Since public key is shared it should be digitally stored in the software in the form of public key Infrastructure (PKI) certificates Elliptic Curve Cryptography plays major role in cloud computing due to the exceptional property of smaller key size. ECC has wide range of applications in Secure Socket Layers (SSL) of cloud computing. The main disadvantage of ECC is the cipher space is two times the message. The present paper explains an innovative elliptic curve cryptosystem that reduces the cipher space, equal to the original message.**

***Index Terms*— Elliptic Curve Cryptography, Encryption, Decryption**

I. INTRODUCTION

A key exchange algorithm by Diffie – Hellman is an attractive protocol for communication between two unfamiliar users that uses power of large prime numbers. It greatly enhances the security of the internet and is proposed as internet standard. But the algorithm is suffered with security implication as man-in-middle attack. Later on, there were many modifications to D H Key Exchange algorithm. On the other hand, RSA is a public key cryptosystem which obtains its security from the difficulty of factorizing large integers into their prime. Though the public key operations are faster in RSA the strength of the algorithm will not be increased even if the key size is doubled. An alternative of RSA algorithm to achieve the same security certificate with considerably shorter key length is elliptic curve cryptography came to light in 1985 by Victor and Miller. Elliptic curve cryptography is based on a discrete logarithmic problem called (ECDLP). Since there are no exponential operations in ECDLP limited processing power, finite storage space with little band width is required for ECC. The hardness of ECDLP makes ECC less vulnerable compared with other classical cryptographic algorithms. So, ECC is especially viable for limited applications such as smart cards, cellular phones and wireless communication devices. Same elliptic curve may be used by many people with distinct key pairs. In spite of these advantages as ECC has similar structure with ELGamal, one message point maps to two cipher points on the curve. There is a small disadvantage that the encrypted message is twice than that of the unencrypted message. This leads to network congestion and communication risk. The present paper aims at reduction of the size of the cipher besides providing the security.

Grenze ID: 01.GIJET.10.1.64_1

II. Literature Survey

Several researchers in literature studied the benefits of ECC over conventional cryptosystems and deployed elliptic curves over finite fields for security applications. Many authors proposed text-based encryption algorithms using ECC. Benjamin Sebastina, Ugar Alpay Cenar (7) studied and compared significant advantages of ECC over RSA in SSL and TLS certificates. L. Dolendro and K Manglem (8) implemented text encryption using elliptic curve cryptography. In this chapter authors proposed a classical method of assigning characters to points on the elliptic curve, by pairing the ASCII values of the plain text characters. Renee Brady et.al. (9) proposed encryption scheme with elliptic curve cryptography. In that paper they discussed the limitations of communicating text messages through the sites like twitter and used Unicode to encode the text message as a number, Koblitz method to encode the text as a point on elliptic curve. A. Shamir (10) was the first to propose Identity-based cryptosystem to overcome the authenticity issues in a different way to traditional public key infrastructure. Aziz and Diffie [11] also suggested a secure and an authentic technique which requires prior communication. S. Thiraviya and S. Britto (12) proposed enhanced elliptic curve cryptography for online social network users. In that paper they implemented encryption, decryption time analysis, plain text, cipher text size analysis. KolhekarM, Jadhav A (13) proposed encryption technique based on elliptic curve. F. Amounas and E.H. EI Kinani [14] emphasized the advantage of a nonsingular matrix used to map similar characters to different points on the curve. T.N. Shankar and G. Sahoo (15) showed how an alphabetic table of two dimensions is used for conversion of two-dimensional plain text co-ordinate representation. These points are then added with elliptic curve points for encryption. K. Agrawal and A. Gera [16] designed message encryption with the help of Hill Cipher, where Cipher ASCII values are used to locate EC points. All these algorithms explain only the encryption methods, but they have not encountered the variation issue of the cipher size. The present text-based encryption algorithm protects the cipher from all types of attacks as well as considers the fixation of the cipher size to that of the original text.

III. Elliptic Curve Arithmetic

An affine equation E: $y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6$is called weierstrass equation on real field, for real b_1, b_2, $b_{3,\ b4}$, b_6 and x, y for encryption purpose, the curve is restricted to $y^2 = x^3 + ax + b$, $4a^3+27b^2 \neq 0$ on Ƒq.

Elliptic Curve group laws: - There are some special laws for adding two points on the elliptic curve unlike normal addition. Point addition on the curve uses chord -and – tangent rule to find out the resulting point [1, 2, 3]. All the points on the curve over finite field, with addition as binary composition will form a commutative group whose identity is point at ∞.

Addition Rules: - For two points P (x1, y1) and Q (x2, y2) of the curve, sum of P and Q is R (x3, y3). R (x3, y3) is obtained by considering the reflection point of the line passing through P, Q and the curve with respect to X- axis. Same geometric procedure applies for P and -P also. For P and -P the line is vertical. Where the addition of P and -P is ∞ [1, 2, 3].

Point Doubling on the Curve: - For P (x1, y1), the double point 2P is reflection of intersection point of tangent at P, with respect to X- axis [1, 2, 3]. Below given are examples for addition and doubling for the curve $y^2 = x^3-x$.

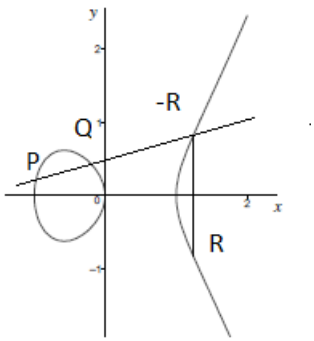


Figure 1. Geometric addition

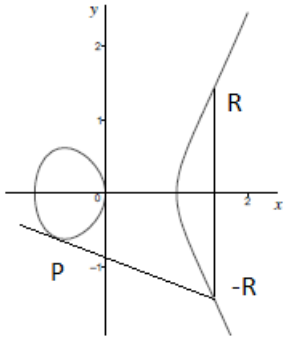


Figure 2. Geometric doubling

Identity: - Infinity point is identity.

Negatives: - A point with same X- co-ordinate and negative of Y- co-ordinate is called the negative of the point.

Point addition: - If Ꝑ ($\dot{x}_1$, $\dot{y}_1$), Ꝗ ($\dot{x}_2$, $\dot{y}_2$) are two points where Ꝑ ≠ Ꝗ. Then Ꝑ + Ꝗ = ($\dot{x}_3$, $\dot{y}_3$) [1,2] $\dot{x}_3 = [(\dot{y}_2 - \dot{y}_1)/(\dot{x}_2 - \dot{x}_1)]^2 - \dot{x}_1 - \dot{x}_2$ and $\dot{y}_3 = [(\dot{y}_2 - \dot{y}_1)/(\dot{x}_2 - \dot{x}_1)](\dot{x}_1 - \dot{x}_3) - \dot{y}_1$

Point Doubling: - Let p $(\dot{x}_1, \dot{y}_1) \in E(F_q)$ where $p \neq -p$ then

$$2P = (x_3, y_3)\ [1,2] \text{where } x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \text{ and } y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

Point Multiplication: - Addition of points n times is called multiplication of point n times,
nP = P+P+……. n times.

ECDLP (Elliptic Curve Discrete Logarithmic Problem): - Elliptic Curve Cryptography mainly depends on hardness of Elliptic Curve Discrete Logarithmic Problem (ECDLP). It is a mathematical logic that finding a point Q on the curve for given n and P, Q = nP is simple whereas finding n = $\log_P Q$ is very difficult.

V. Proposed Method

In the present paper the authors designed a new technique to encrypt the message and to reduce the size of the cipher text to that of the plain text so that the computational strain, communication risk, storage space, processing power consumption can be considerably reduced. If two genuine users want to send messages to each other first they agree upon a curve Eq (a, b) over finite field with as many points as possible on it and publish. A secure elliptic curve is a curve that protects an elliptic curve protected by main physical attacks is secure. Some desired features in curve selection are

- The order of the curve should not have prime factors to face 1 attack by Pollig-Hellman attack
- It is not super singular
- It is non-anomalous curve order is not same as q.

A common look up table by assigning ASCII characters to points on the curve and a random function f (x, y) is shared between the users.

Alice selects a random point A, a large number at random α smaller than the order computes

$$A1 = [A/\alpha + \alpha^{\wedge}2\ A] \bmod q$$

$$A2 = [\alpha A] \bmod q$$

Keeping α as secret key she publishes A1, A2 as her general public keys.

In the same way Bob chooses big number β, a point B, calculates B1= [B/β+β^2 B]modq, B2=[βB]modq. He publishes B1, B2 as his general public keys and keeps β, B as his secret keys.

Again, Alice computes AB=[αB2]modq which is a specific to Bob. Bob computes BA=[βA2]modq which is specific to Alice to converse with her.

VI. Enciphering

Suppose Bob wants to send message M, with characters

M1, M2, ……Mn

1. First, characters are converted to points with the help of common look up table. P1, P2, P3…….Pn.
2. He selects a random point P0 with coordinates (x0, y0) on the curve and generates an integer r = [f (x0, y0)]modq using the published random function f(x,y).
3. He encrypts the point P0 as C0 = [P0+βA1]modq
4. Each point P1, P2…. Pn is encrypted as Ci= r^i [Pi+ β A1]modq i= 1,2,3……. n
5. He writes the corresponding text characters and sends the cipher text to achieve public medium.

VII. Decryption

Alice first decrypts Co as

$$P0 = \{C0 - [1/\alpha^{\wedge}2 + \alpha]\ BA\} \bmod q$$

Then Alice decrypts the cipher text as

$$Pi = \{Ci/r^{\wedge}i - [1/\alpha^{\wedge}2 + \alpha]\ BA\} \bmod q\ i = 1,2\ldots n$$

Decryption works out properly:

Pi= Ci/r^i -[1/α^2 +α] BA = Ci= r^i/r^i [Pi+ β A1]- [1/α^2 +α] BA

= [Pi+ β {A/α+α^2 A}]- [1/α^2 +α] βαA

= Pi+ β/α A+ βα^2 A- β/α A- βα^2 A = Pi

User 1	Public channel	User 2
A1= $\left[\frac{A}{\alpha} + \alpha^2 A\right] modq$		{B1= $\left[\frac{B}{\beta} + \beta^2 B\right] modq$,
$A2 = [\alpha A] modq$		$B2 = [\beta B] modq$}, B, β are secret
A, α are secret		BA = βA2
AB = αB2		

Enciphering technique

Input: original message
Output: Cipher
Step1: Begin
Step2: i: Message M1, M2, Mn
ii: Assigned points P1, P2, Pn
by table
Step3: Consider P0(x0, y0) at random and calculate r = [f (x0, y0)] modq
Step4: encrypt P0 as $C0 = [P0 + \beta A1]$
Step5: Each point P1, P2… is encrypted as $Ci = \{r^i[Pi + \beta A1]\} modq$ i= 1,2,3……. n
Step6: convert the points to the characters from table
Step7: End

Decryption

Input: Cipher
Output: Original message
Step1: Begin
Step2: i: Cipher characters C1, C2, C3, …
ii: Characters to points P1, P2, P3… of the curve by using table
Step3: C0 is decrypted as $P0 = \left\{C0 - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\} modq$
Step4: Compute r = [f (x0, y0)]$_{modq}$ using the first point P0(x0,y0)
Step4: Each point P1, P2… is decrypted as $Pi = \left\{\frac{Ci}{r^i} - \left[\frac{1}{\alpha^2} + \alpha\right] BA\right\} modq$ i=1,2…. n
Step5: convert the points to the characters from table
Step6: End

VIII. IMPLEMENTATION OF THE ALGORITHM

Two users Alice and Bob select an elliptic curve $y^2 = x^3 + 3x + 27$ mod 331 with prime order is 317 possessing all the above-mentioned desired features. The curve, an EC coded ASCII table by mapping the 256 ASCII characters to first 256 affine points on the curve and a random function

$f(x, y) = [x^2y^2 + xy + x + y] mod\ 331$ are public.

Alice	Bob
$\alpha = 17$, A = (296,210)	$\beta = 19$, B = (231,3)
A1 = (8,296) A2 = (61,159)	B1 = (43,47) B2 = (88,123)
AB = (127,35)	BA = (9,320)

If Bob wants to send the message “SSSS” to Alice, the EC affine point corresponding to the character ‘S’ from the look up table is (39,144). He selects a random point

P0 = (36,38) and generates ‘r’ value as 68.

He encrypts the plain text as cipher points C1, C2, C3, C4

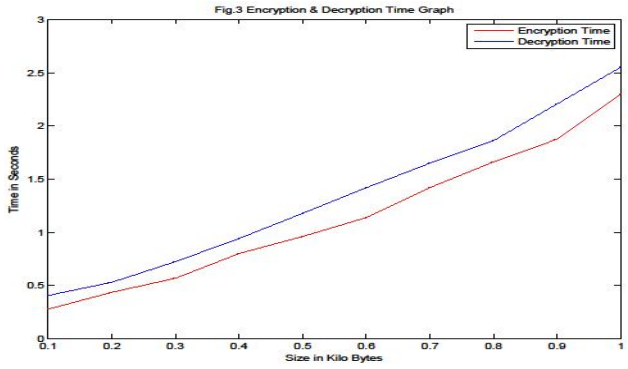
Message	Cipher
(39,144), (39,144), (39,144), (39,144)	(320,283)(248,60), (184,330)(257,52),(212,306)

IX. Implementation Results and Performance Analysis

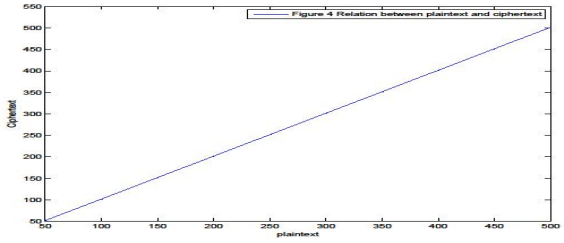
The encryption and decryption times for different size messages are recorded on a machine with 1GB RAM and 1.6 GHz processor speed on Win XP platform using MATLAB14. The following table gives encryption and decryption times in seconds for different size data. The time required for encryption and decryption for different size data are calculated and tabulated as follows

These values are plotted in the graph. The encryption and decryption time plots in figure 3 show that the execution time is very less when compared to other conventional cryptosystems. The time recorded for both encryption and decryption is below3 seconds. So, the computational and communication risk will be considerably reduced to the required levels.

Size of the message (in kilo bytes)	Encryption time (in seconds)	Decryption time (in seconds)
0.1	0.2774	0.4064
0.2	0.4372	0.5313
0.3	0.5695	0.7256
0.4	0.8023	0.9439
0.5	0.9617	1.1807
0.6	1.1400	1.4205
0.7	1.4218	1.6523
0.8	1.6627	1.8646
0.9	1.8768	2.2093
1.0	2.2986	2.555

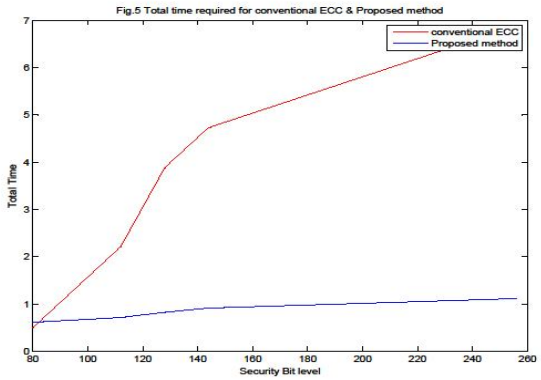


Since the cipher text size is fixed except one-point P0 or one-character C0 appended at the beginning of the cipher there is no network congestion in communication. The graph in figure 4 represents the relationship between plaintext and cipher text size. The graph is linear with negligible variation. So, the present technique is suitable for not only small, medium size messages but also for bigdata.



IX. Comparative Analysis Of Conventional ECC And The Proposed Method

A comparative study on total execution time is implemented between conventional ECC and the present method. The graph in fig. 5 shows that the present algorithm is faster than the conventional algorithm.



X. Security Analysis

General attacks are effective same message character maps to same cipher character. In the present algorithm each plain text character is encrypted using the value 'r' raised to the power of its position r^i , i = 1,2,3…. Since r^i , i = 1,2,3…. Different repetition will not occur. characters for small and medium size messages. In the example shown above all the same 'S' are encrypted to different EC points. To estimate the frequency of the characters a big message of size 1 kilobyte is encrypted using the present technique. Repetition of English alphabets is shown by the bar diagrams in figure 6. It is clear from the graph that the most frequently repeated English alphabets like A, E, S, T are negligible in number and all the other characters are numerals, special ASCII characters. So, the frequency analysis is impossible to execute here even for big data also.

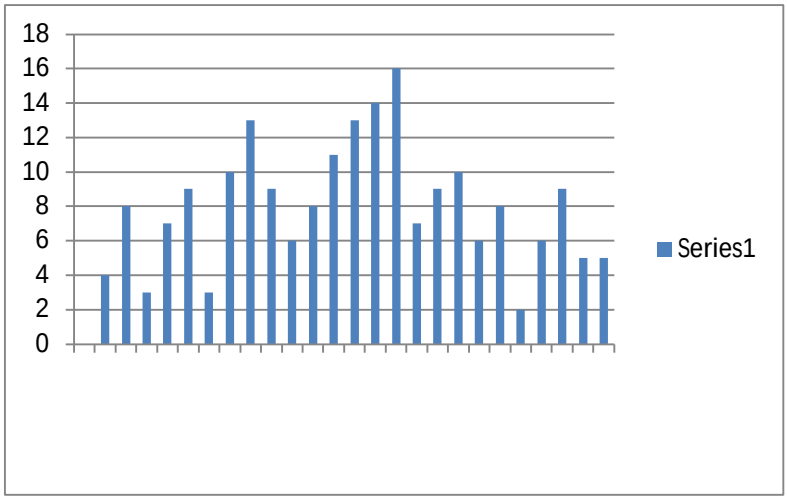


Fig.6 1

The hardness of ECC depends on the strength of ECDLP). A common attack on ECC is pollard Rho to solve ECDLP. The process of applying the Pollard Rho attack to solve ECDLP does not arise here since each character is encrypted different r^i.

XI. Advantage Of The Present Scheme Over The Earlier Schemes

In ECC a l bit key yields pair of points consisting of 4*l bits due to the two coordinates x and y. Each cipher character has bandwidth 4*l. Thus, the plain text coded to N points on the curve is encrypted as 2*N points with 4*l*N bit bandwidth which is significantly large. This results the transmission expensive and leads to network

congestion. But in the present method the plain text with N characters is encrypted as (N+1) affine points with bandwidth 2*l*(N+1) almost equal to the size of the plain text. Each character is encrypted to a random character as long as q<n. If n = q+1 and if P0 = P(q+1) they are coded to the same cipher point, since r is a number in the finite field less than q which is the generator of the cyclic group. In ECC generally q is very large so that large volumes of data can be transmitted by communicating parties. The case of n>q occurs rarely. In such a case it is recommended to change either the secret key or the function f(x,y) to calculate r value after communicating q characters.

XII. Conclusions

The encryption technique proposed here offers same level of security as the conventional ECC protocol as it is highly difficult to calculate the secret keys of both the legitimate entities; α, A of Alice and β, B of Bob from the public keys A1, A2 and B1, B2, if the order of the elliptic curve is very large. Also, it reduces the size of the cipher text to that of the plain text. So, the ECC algorithm designed here is faster than previously proposed schemes. Another special feature of this algorithm is there is no pre sharing of the data before transmission. The curve, EC coded ASCII table and function are public. The keys A1, A2, AB; B1,B2,BA are communicated via public channel only. So, the present cipher is very useful for long messages because the cipher length is same as that of the plain text.

References

[1] Koblitz N., "Elliptic curve cryptosystems, mathematics of computation", Vol. 48, No.177, pp. 203-209, January 1987.v
[2] Miller V., "Uses of elliptic curves in cryptography". In advances in Cryptography (CRYPTO 1985), Springer LNCS, 1985, vol. 218, pp 417-4 26.
[3] Maurer U., A. Menzes and E. Teske, "Analysis of GHS weil decent attack on the ECDLP over characteristic two fields of composite degree". LMS journal of computation and Mathematics, 5:127-174, 2002.
[4] Arron Blumenfeld, "Discrete logarithms on Elliptic curves", 2011
[5] Menzes A., and Vanstone S. "Handbook of applied cryptography", The CRC-Press series of Discrete Mathematics and its Applications CRC-Press,1997.
[6] Miyaji, Nakabayashi and Takano "Elliptic curves with low embedding degree", Journal of Cryptology, 2006, Volume 19, Number 4, Pages 553-562.
[7] Benjamin Clement Sebastin, Ugar Alpay Cenar "Advantage of using elliptic curve cryptography in SSL/TLA, https://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Cenar+Sebastian
[8] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh "Implementation of Text Encryption using Elliptic Curve Cryptography", Procedia Computer Science 54 (2015) 73-82, www. Sciencedirect.com.
[9] Rene'e Brady, Naleceia David and Anna Tracy, "Encrypting with Elliptic Curve Cryptography, www.math.purdue.edu//Encrypting
[10] A. Shamir, "Identity- based cryptosystems and signature schemes", In Proc. CRYPTO 1984, LNCS Vol. 196, pp. 47-53, Springer 1984.
[11] A.Aziz & W. Diffie, "A secure communications protocol to prevent unauthorized access: privacy and authentication for wireless local area networks, IEEE personal communications, pages 25-31, first quarter 1994.
[12] S. Thiraviya Regina Rajam and S. Britto Ramesh Kumar, "Enhanced Elliptic curve Cryptography", Indian Journal of science and technology, Vol. 8 (26), Oct 2015.
[13] Megha Kohelekar, Anita Jadhav, "Implementation Of Elliptic Curve Cryptography On Text And Image", International Journal of Enterprise Computing and Business Systems, Vol. 1 Issue 2 July 2011
[14] F. Amounas and E.H. EI Kinani, Fast Mapping Method based on Matrix Approach for Elliptic Curve Cryptography, Int J of Information and Network Security 1, 54–59 (2012).
[15] T.N. Shankar and G. Sahoo, Cryptography with Elliptic Curves, Int J of Computer Science and Applications 2, 38– 42 (2009).
[16] K. Agrawal and A. Gera, Elliptic Curve Cryptography with Hill Cipher Generation for secure Text Cryptosystem. Int J of Computer Applications 106, 18–24 (2014).