A Novel ElGamal Encryption Scheme of Elliptic Curve Cryptography

B. Ravi Kumar[1] A. Chandra Sekhar[2] G.Appala Naidu[3]

[1,2]Department of Mathematics, GIT, Gitam University, Visakhapatnam, INDIA
[3]Department of Mathematics, Andhra University, Visakhapatnam, INDIA

***Abstract*-Cryptography is the art of using mathematical models to encrypt and decrypt data. Cryptography enables to store sensitive information or transmit across insecure networks so that it cannot be read by anyone except the intended recipient. Ever since the inception of Cryptography, several efficient encryption schemes were introduced by the researches. Among such one is the ElGamal encryption scheme. In the present work, the ElGamal encryption scheme is proposed using the points on an elliptic curve and as an additional security the Fibonacci Q-matrix is introduced.**

***Keywords*- ElGaml, Recurrence relation, Fibonacci sequence.**

I. INTRODUCTION

In the year, 1985 Victor Miller and Neal Koblitz first introduced the Elliptic curve cryptography. Elliptic curve cryptography has proven its security by with standing for a generation of attacks. In the recent years, as the wireless communication has grown rapidly, the numerous companies have adopted Elliptic curve cryptography as an innovative security technology. Elliptic curve employs a relatively short encryption key and the shorter key size is faster and requires less compelling power than the other. Elliptic curve cryptography, encryption key provides the same security as '1024'-bit RSA encryption key [1][2][3][4][8].

Cubic equations for elliptic curves of the following form, known as Weierstrass equation $y^2 + gxy + hy = x^3 + ix^2 + jx + k$ Where g, h, I, j, k, x, y are real numbers [6]: In this work we limit ourselves to the equation of the form $y^2 = x^3 + ax + b$ Where x,y,a,b are reals. The points on the elliptic curve form a cyclic group, including a point O known as the point at infinity. The equation $y^2 = x^3 + ax + b$ is non- singular if $\Delta = 4a^3 + 27b^2 \neq 0$.[4][5][7].

II. THE ELGAMAL CRYPTOSYSTEM

Two communicating parties 'A' and 'B' initially agree upon the Elliptic curve $E_p(x, y)$ and p is sufficiently large prime number and (x,y) is the point on the Elliptic curve. For secure communication over insecure channels, both A and B fixes a point C (x_1, y_1). A initially selects the private key 'K_A' and generates the public key $P_A = K_A \times C.$ Next 'B' selects the private key K_B and generates the public key $P_B = K_B \times C.$ Now A wants send the message M to B for this purpose A choose a random integer 'n' now A encrypts M as $CT_m = \{nC, M + nP_B\}$ and sends to B.

Then 'B' decrypts the CT_m as
$M + nP_B - K_B(nC) = M + n(K_B C) - K_B(Cn) = M$ [9][20].

III. FIBONACCI *Q*-MATRIX

The Fibonacci numbers were introduced by [10][11][12][15][16].

The Fibonacci sequence is $F_{n+1} = F_n + F_{n-1}$ with the initial conditions: $F_0 = F_1 = 1$.

The (2X2) square matrix was introduced in [11][19]:

$$Q = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

The nth power of the Q-matrix is

$$Q^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix},$$

In this proposed work, we introduced Fibonacci Q-matrix as an additional security in addition to the chosen integer where 'k' is the private key. Choose 'n' is sufficiently large then it is difficult to trace 'n' by brute force attack [14][20].

IV. PROPOSED ALGORITHM

Alice wants to send the message to Bob using elliptic curve ElGamal encryption. Alice chooses the elliptic curve $y^2 = x^3 + gx + h$ over the field z_p.

Choose the point G on the elliptic curve. Alice selects a private key 'a' and generates the public key A='aG' and Bob selects a private key 'b' and generates the public key B= 'bG'.

A. *Encryption*:

Step 1: Alice chooses a random integer k, and
Keeps it secret.
Step 2: Compute kG.
Step 3: Alice selects the Bob public key, B=bG.

Step 4: Compute kB=k(bG).
Step 5: Compute aB=a(bG).
Step 6: Alice wants to send the message q_i to Bob.
Step 7: Alice converts the message into points on the elliptic curve. She chooses a point Q, which is a generator of the elliptic curve. By using ASCII characters of upper case into the points on the elliptic curve.

Let $A=\{1P,2P,3P.....255P\}$

$B=\{set\ of\ all\ ASCII\ characters\}$

Alice defines one to one correspondence $f:A\to B$ by $f(nP)=x_n$

Where n=1,2……255 and $\{x_1,x_2,x_3,.....x_{255}\}$ *are the ASCII characters.* Step 8: Generate the following 2×2 matrices with entries as the points on the elliptic curve. $m_1=\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix} m_2=\begin{pmatrix}a_5 & a_6\\ a_7 & a_8\end{pmatrix}$, $m_3=\begin{pmatrix}a_9 & a_{10}\\ a_{11} & a_{12}\end{pmatrix}$, and so on additional which is obtained depending upon the length of the message.

Step 9: Alice chooses a private key from the generalized form of Fibonacci Q-matrix, she selects

$Q_p{}^n=\begin{pmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix} where\ n=0,\pm1,\pm2.....$ and p=1.

Step 10: She Computes $p_1=m_1\times Q^n=\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}\times \begin{pmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix}=\begin{pmatrix}q_1 & q_2\\ q_3 & q_4\end{pmatrix}$,

$p_2=m_2\times Q^n=\begin{pmatrix}a_5 & a_6\\ a_7 & a_8\end{pmatrix}\times \begin{pmatrix}F_{n+1} & F_n\\ F_n & F_{n-1}\end{pmatrix}=\begin{pmatrix}q_5 & q_6\\ q_7 & q_8\end{pmatrix}$,

and so on.

The resulting points are

$R=\{q_1(x_1,y_1),q_2(x_2,y_2),q_3(x_3,y_3),$

$.....,q_i(x_i,y_i)\}where\ i=1,2,3.....$

Step 11: Compute $C_i=q_i+kbG+abG$.

Step 12: Now Alice sends the encrypted message (kG,C_i) to Bob.

A. *Decryption*

To recover the plain text q_i from C_i Bob does the following:

Step 1: First Bob selects the Alice public key A = aG.
Step 2: Compute bA = b(aG).
Step 3: Now Bob computes the inverse element of b(aG) is - b(aG).
Step 4: Add - b(aG)to the second part of the message : $q_i+kbG+abG-abG=q_i+kbG$.
Step 5: Multiply the Bob's own private key 'b'with the first Part of the message kG, we get: keg.
Step 6: Now Bob computes the inverse element of kbG is –kbG.
Step 7: Bob adds -kbG to the second part of the message: $q_i+kbG-kbG=q_i$.
Step 8: After decryption the obtained points are stored as a 2×2 matrix.

$S_1=\begin{pmatrix}q_1 & q_2\\ q_3 & q_4\end{pmatrix}, S_2=\begin{pmatrix}q_5 & q_6\\ q_7 & q_8\end{pmatrix}, and\ so\ on.$

Step 9: Now Bob multiply q_i with a private key (inverse of Fibonacci recurrence matrix):

$S_1\times Q^{-n}=\begin{pmatrix}a_1 & a_2\\ a_3 & a_4\end{pmatrix}, S_2\times Q^{-n}=\begin{pmatrix}a_5 & a_6\\ a_7 & a_8\end{pmatrix}$ and so on,

where $Q^{-n}=\frac{1}{(-1)^n}\begin{pmatrix}F_{n-1} & -F_n\\ -F_n & F_{n+1}\end{pmatrix}$.

and by using the conversion Bob recovers the letters in the message.

V. EXAMPLE

Alice wants to send the message to Bob using elliptic curve ElGamal encryption. Alice chooses the elliptic curve $y^2=x^3-4$ over the field z_{271}.

Then the points on the elliptic curve are
E={O,(1,57),(1,214),(2,2),(2,269),(5,11),(5,260),
(6,36),(6,235),(7,135),(7,136),……
…….....(264,174),(269,114), (69,157)}.

The number of points on the elliptic curve is 271 and the prime number is also 271. Therefore, each point is a generator of an elliptic curve E [17][18].

Choose the point G= (68,136) on the elliptic curve. Alice selects a private key 'a'=6, and generates the public key A='aG' = 6(68,136)= (85, 199) and Bob selects a private key 'b'=8 , and generates the public key B= 'bG' = 8(68,136)= (122 , 259) .

A. Encryption

Step 1: Alice chooses a random integer k =4, and Keeps it secret.
Step 2: Compute kG= 4(68,136)= (250 , 189).
Step 3: Alice selects the Bob public key B=bG= (122 , 259).
Step 4: Compute kB=k(bG)=4(122 , 259) = (132,248).
Step 5: Compute aB=a(bG)=6(122,259) = (215,157).
Step 6: Alice wants to send the message q_i to Bob.

Step 7: Alice wants to convert the message into the points on the elliptic curve. She chooses a point Q = (172,240) which is a generator of the elliptic curve.

By using ASCII characters of upper case letter into the points on the elliptic curve.

$L \to 76(172,240) = (120\ ,261),$

$I \to 73(172,240) = (183\ ,38),$

$K \to 75(172,240) = (15,\ 98),$

$E \to 69(172,240) = (225\ ,189).$

Then the points are

$T = \{(120\ ,261),(183\ ,38),(15,\ 98),(225\ ,189)\}.$

Step 8: To create 2×2 matrix with entries are the points on the elliptic curve.

$$m_1 = \begin{pmatrix} (120\ ,261) & (183\ ,38) \\ (15,\ 98) & (225\ ,189) \end{pmatrix},$$

Step 9: Alice chooses a secret key by using Fibonacci recurrence matrix Q^5.

$$Q^5 = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}.$$

Step 10: Compute

$$p_1 = m_1 \times Q^5$$

$$= \begin{pmatrix} (120\ ,261) & (183\ ,38) \\ (15,\ 98) & (225\ ,189) \end{pmatrix} \times \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} (153\ ,151) & (1\ ,57) \\ (182\ ,13) & (43\ ,10) \end{pmatrix} = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}.$$

Then the points are

$R = \{(153\ ,151),(1\ ,57),(182\ ,13),(43\ ,10)\}.$

Step 11: Compute $C_i = q_i + kbG + abG$.

$C_1 = (153,151) + (132,248) + (215,157) = (7,198),$

$C_2 = (1,57) + (132,248) + (215,157) = (83,100),$

$C_3 = (182,13) + (132,248) + (215,157) = (237,13),$

$C_4 = (43,10) + (132,248) + (215,157) = (183,233).$

Step12: Now Alice sends the encrypted message consisting of the pair of points

$\{(250\ ,189),(207,198)),((250\ ,189),(83,100)),$

$((250\ ,189),(237,13)),((250\ ,189),(183,233)\}$

to Bob.

B. *Decryption*

To recover the plain text q_i from C_i, Bob will follow the procedure: Now Bob selects the first encrypted point $((250\ ,189),(207,198))$ and decrypts the plain text by using the following steps:

Step 1: First Bob selects the Alice public key

A=aG= (85,199).

Step 2: Compute bA=b(aG)= $8(85,199) = (215,157)$.

Step 3: Now Bob computes the inverse element of (215,157) which is (215,114).

Step 4: Add (215,114)) to the second part of the message: $(215,114) + (207,198) = (27,80)$.

Step 5: Multiply the Bob's own private key 'b=8'with the first part of the message

kG= $(250,189)$, we get: b[k G]= (132,248).

Step 6: Now Bob computes the inverse element of $(132,248)$ is $(132,23)$.

Step 7: Bob adds $(132,23)$ to the second part of the message: $(132,23) + (27,80) = (153,151)$.

Then the decrypted point is $q_1 = (153,151)$.

In the similar fashion, Bob decrypts the remaining points

$q_2 = (1,57),\ q_3 = (182,13),\ q_4 = (43,10).$

Step 8: After decryption the obtained points are stored in 2×2 the matrix.

$$S_1 = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix} = \begin{pmatrix} (153,151) & (1,57) \\ (182,13) & (43,10) \end{pmatrix}.$$

Step 9: Now Bob multiply S_1 with the private key (inverse of Fibonacci recurrence matrix):

$$S_1 \times Q^{-5} = \begin{pmatrix} (153,151) & (1,57) \\ (182,13) & (43,10) \end{pmatrix} \times \begin{pmatrix} -3 & 5 \\ 5 & -8 \end{pmatrix}$$

$$= \begin{pmatrix} (120,261) & (183,38) \\ (15,98) & (225,189) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Then Bob retrieves the message as:

$a_1 = (120,261) \to L$

$a_2 = (183,38) \to I$

$a_3 = (15,98) \to K$

$a_4 = (225,189) \to E$

Finally, Bob receives the message "LIKE" from Alice.

VI. CONCLUSIONS

In the proposed work the plain text is converted to points on the elliptic curve by one to one correspondence using ASCII characters. The additional private key has generated using matrix obtained from the Fibonacci sequence. The selection of large prime in Z_p and the selection of 'n' in Fibonacci for generation of the secret key enhances the security levels which are difficult to crack by known attacks.

References

[1] N. Koblitz. Elliptic curve Cryptosystems. Mathematics of computation, 48203-209, 1987.

[2] A text book of Guide to elliptic curve Cryptography by Darrel Hancott Vanstone.

[3] N. Koblitz. Hyper Elliptic Cryptosystem, International Journal of Cryptography, 1,139-150,189.

[4] A Course in Number Theory and Cryptography. By Neal Koblitz.

[5] V. Miller. Uses of Elliptic Curves in Cryptography. In Advances in (CRYPTO 1985), Springer LNCS, 218, 417–426, 1985.

[6] A text book of Cryptography and Network Security by William Stallings.

[7] An introduction to the theory of elliptic curves by Joseph H. Silverman brown University and NTRU Cryptosystems.

[8] A Course in Number Theory and Cryptography –second edition by Neal Koblitz
[9] J ElGamal. A public key Cryptosystem and a signature scheme based on discrete logarithms.In Advances Cryptology (CRYPTO 1984), Springer.
[10] Vorobyov NN. Fibonacci numbers, Moscow: Nauka; 1978 [in Russian].
[11] Hogget VE. Fibonacci and Lucas numbers.Palo Alto,CA: Houghton-Mifflin; 1969.
[12] Vajda S. Fibonacci and Lucas numbers and the golden section. Theory and applications. Ellis Horwood limited; 1989.
[13] Stakhov AP. Introduction into algorithmic measurement theory. Moscow: Soviet Radio; 1977 [in Russian].
[14] A.P. Stakhov,"The ''golden'' matrices and a new kind of cryptography", Chaos, Solutions and Fractals 32 (2007) pp1138–1146.
[15] Stakhov OP.A generalization of the Fibonacci Q-matrix.Rep Nat Acad Sci Ukraine1999 (9):46-9.
[16] Stakhov AP. The golden section and modern harmony mathematics. Applications of Fibonacci numbers,7. Kluwer Academic Publishers; 1998.p.393-99.
[17] A. Chandra Sekhar, S. Uma Devi "A one to one Correspondence in elliptic curve cryptography" International Journal of Mathematical archive-4(3), 2013:300-304.
[18] http://www.certicom.com/index.php/ecc-tutorial.
[19] K.R.Sudha, A.chandra Sekhar ,Prasad Reddy P.V.G.D. "Cryptography protection of Digital Signals using some recurrence relations" International Journal of Computer Science and Network Security, Vol (7) no 5 m may 2007,203-207.
[20] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, on Information Theory, 469- 472, 1985.