ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 12, No. 2, 2017, *pp*.083-087

A Diffie-Hellman key exchange for self-Encryption over points on the Elliptic Curve Cryptography

B.Ravi Kumar[1], A.Chandra Sekhar[2], G.Appala Naidu[3]
[1]*Department of Mathematics, Gitam University, Visakhapatnam, India;*
[2]*Department of Mathematics, Gitam University, Visakhapatnam, India;*
[3]*Department of Mathematics, Andhra University, Visakhapatnam, India.*
(Received July 23, 2016, accepted January 15, 2017)

Abstract. Cryptography is the combination of Mathematics and Computer Science. Cryptography is used for encryption and decryption of data using mathematics. Cryptography transmit the information in an illegible manner such that only intended recipients will be able to decrypt the information. In the recent years, researchers developed several new encryption methods. Among such Diffie–Hellman encryption is the one laid a concealed platform for the researchers in Cryptography. Ever science several mathematical models were applied for encryption/decryption. In this paper, we introduced a Diffie–Hellman encryption, which uses points on the elliptic curve, and as an additional security the Fibonacci Q-matrix is introduced.

Keywords: Diffie-Hellman; Fibonacci sequence; encryption; decryption.

1. 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 requires. Elliptic curve cryptography, encryption key provides the same security as '1024'-bit RSA encryption key [1][2][3][4][8].

In general, cubic equations for elliptic curves take the following form, known as Weierstrass equation [6]: $y^2 + gxy + hy = x^3 + ix^2 + jx + k$.

Where g, h, i, j, k are real numbers and x,y take on values in the real numbers. For our purpose, it is sufficient to limit ourselves to equations of the form: $y^2 = x^3 + gx + h$.

Where x, y, g, h belong to R, Q, C or Fp. Also include in the definition of an elliptic curve is a single element denoted by O and called the point at infinity or the zero point. There is also a requirement that the discriminant $\Delta = 4g^3 + 27h^2$[4][5][7].

2. Diffie-Hellman algorithm

Alice wants to send a message to Bob using elliptic curve Diffie-Hellman encryption/decryption scheme. Choose the point $C(x_1,y_1)$ on the elliptic curve. Alice selects a private key 'K_A' and generates the public key $P_A = K_A C$ and Bob selects a private key 'K_B' and generates the public key $P_B = K_B C$[9,10,11].

2.1. Encryption

Alice should do the following:
Step 1: Alice selects the Bob public key $P_B = K_B C$.
Step 2: Compute $K_A P_B = K_A (K_B C)$.
Step 3: Represent the message as an integer M in the interval [0, p-2], m is a point on E.
Step 4: Compute $CT_m = M + K_A (K_B C)$.
Step 5: Send the encrypted message 'CT_m' Bob publicly.

2.2. Decryption

To recover the plaintext 'M' from C Bob should do following:
Step 1: First Bob selects the Alice public key $P_A = K_A C$.

Step 2: Compute K_B (K_AC).
Step 3: Now Bob computes the inverse element of K_B (K_AC) is - K_B (K_AC).
Step 4: Recover M = M + K_A K_B C - K_A K_B C.

3. Proposed algorithm

Alice wants to send a message to Bob using elliptic curve Diffie-Hellman 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'.

3.1. Encryption

Step 1: Alice selects the Bob's public key B = bG.
Step 2: Alice uses her own private key 'a' and Computes B = a(bG).
Step 3: Alice chooses a random integer k, where1≤ k ≤ p-2.
Step 4: Compute k (abG).
Step 5: Alice wants to send the message qi to Bob.
Step 6: Alice wants to convert the message into the 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 letter into the points on the elliptic curve.

Let A = {1P, 2P, 3P……255P} and B = {ASCII characters}.

Alice defines one to one correspondence f: A→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 7: To create 2×2 matrix with entries, are the points on the elliptic curve.

$m_1 = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $m_2 = \begin{pmatrix} a_5 & a_6 \\ a_7 & a_8 \end{pmatrix}$, and so on additional which is obtained depending upon the length of the message.

Step 8: 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* $n = 0, \pm1, \pm2 \ldots\ldots\ldots$ and p=1.

Step 9: Alice computes

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

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

Step 10: The resultant set of points are

$$T = \{q_1(x_1, y_1), q_2(x_2, y_2), q_3(x_3, y_3) \ldots\ldots\ldots q_i(x_i, y_i)\} \textit{where } i = 1,2,3\ldots\ldots\ldots$$

Step 11: Compute Ci = qi + kabG.
Step 12: Alice chooses a point R on the elliptic curve E, where k is the x-coordinate of R.
Step 13: Compute R+ abG.
Step 14: Now Alice sends the encrypted message (Ci, R + abG) to Bob.

3.2. Decryption

To recover the plain text q_i from C_i Bob do the following.
Step 1: First Bob selects the Alice public key A= aG.
Step 2: Bob uses his own private key 'b' and Computes bA = b(aG).
Step 3: Now Bob computes the inverse element of b(aG) is - b(aG).
Step 4: Recover 'R' by adding - b(aG) to the second part of the message : -abG + R + abG = R.
Step 5: Compute k(abG) where k is the x-coordinate of R.
Step 6: Now Bob computes the inverse element of k(abG): -kabG.
Step 7: Now Bob adds –kabG to the first part of the message: q_i + kbG – kbG = q_i,
Step 8: After decryption, the obtained points are stored in 2 ×2 matrix as:

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

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

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

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.

4. Example

Alice wants to send a message to Bob using elliptic curve Diffe-Hellman 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), (269,157)}.

The number of points on the elliptic curve is 271 and the prime number is 271. Therefore each point is a generator of an elliptic curve E[12].

Choose the point G=(68,136) on the elliptic curve. Alice selects a private key as 'a'=6, and generates the public key as 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).

4.1. Encryption

Step 1: Alice selects the Bobs public key B = bG = (122 , 259).

Step 2: Alice uses her own private key 'a=6' and Compute aB = a(bG) = 6(122 , 259) = (215,157).

Step 3: Alice chooses a random integer k=64, where $1 \leq k \leq p-2$.

Step 4: Compute 64(215,157) = (246, 38).

Step 5: Alice wants to send the message q_i to Bob.

Step 6: 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 → 76 (172,240) = (120,261),

I → 73 (172,240) = (183, 38),

K→ 75(172,240) = (15, 98),

E → 69(172,240) = (225,189).

Then the points are

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

Step 7: 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 8: Alice chooses a secret key by using Fibonacci recurrence matrix Q^5

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

Step 9: Alice computes

$$p_1 = m_1 \times Q^5 = \begin{pmatrix} (120\ ,261) & (183,38) \\ (15,\ 98) & (225,189) \end{pmatrix} \times \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}$$

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

Then the points are R = {(153, 151), (1,57),(182, 13),(43, 10)}.

Step 10: Alice computes $C_i = q_i + kabG$.

C_1 = (153, 151) + (246, 38) = (12,141),

C_2 = (1, 57) + (246, 38) = (235, 43),

C_3 = (182, 13) + (246, 38) = (38,111),

$C_4 = (43, 10) + (246, 38) = (60, 268)$.

Step 11: Compute R + abG = (64,246) + (215,157) = (1,214).

Step 12: Now Alice sends the encrypted message consisting a pair of points {((12, 141), (1, 214)), ((235, 43), (1, 214)), ((38, 111), (1, 214)), ((60, 268), (1, 214))} to Bob.

4.2. Decryption

To recover the plain text q_i from C_i , Bob will follow the procedure:

Now Bob selects the first encrypted point ((12, 141), (1, 214)) 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) + (1, 214) = (64, 246).

Step 5: Compute 64(64, 246) = (246, 38).

Step 6: Now Bob computes the inverse element of (246, 38) is (246, 233).

Step 7: Bob adds (246, 233) to the first part of the message: (246, 233) + (12, 141) = (153, 151).

∴ The decrypted point $q_1 = (153, 151)$.

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 as a 2×2 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 multiplies 'S_1' with private key (inverse of Fibonacci recurrence matrix):

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

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

Step 10: Then Bob retrieves the letters of the message as:

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

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

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

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

Step 11: Finally, Bob receives the message "LIKE" from Alice.

5. Conclusion

In the proposed work, the plain text is converted to points on the elliptic curve by one to one correspondence using ASCII characters. A Diffie-Hellman key exchange is implemented and 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 enhance the security levels, which are difficult to crack by known attacks.

6. References

[1] N. Koblitz. Elliptic curve Cryptosystems. Mathematics of computation. 48:203- 209(1987).

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

[3] N. Koblitz, Hyper Elliptic Cryptosystem, International Journal of Cryptography. 1:139-150(1989).

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

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

[6] A textbook 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] W. Diffie, P. C. van Oorschot, M. J. Wiener, Authentication and Authenticated Key Exchanges, Designs, Codes and Cryptography Kluwer Academic Publishers). 2(2): 107–125 (1992).

[9] S. Pohlig and M. Hellman, An Improved algorithm for computing Logarithm over GF(p) and its Cryptographic significance, IEEE Transaction on Information Theory, volume 1462, Springer-Verlag,pages. 458-471(1998).

[10] P. Kocher, Timing attacks on Implementations of Diffie-Hellman, RSA DSS and other systems, Advances in Cryptology. 1109: 104- 113(1996).

[11] P. A. Jyotirmie, B.Ravi Kumar, A. Chandra Sekhar, S. Uma Devi , A one to one Correspondence in elliptic curve cryptography, International Journal of Mathematical archive. 4(3):300- 304(2013).

[12] http://www.certicom.com/index.php/ecc-tutorial.

[13] Malek Jakob Kakish, A Secure Diffie-Hellman schemes over elliptic curves, IJRRAS January. (2012).