Journal of Mathematics and Statistics 7 (4): 326-331, 2011
ISSN 1549-3644
© 2011 Science Publications

Polynomial Interpolation in the Elliptic Curve Cryptosystem

Liew Khang Jie and Hailiza Kamarulhaili
School of Mathematical Sciences, University Sains Malaysia,
11800 Minden, Penang, Malaysia

Abstract: Problem statement: In this research, we incorporate the polynomial interpolation method in the discrete logarithm problem based cryptosystem which is the elliptic curve cryptosystem. **Approach:** In this study, the polynomial interpolation method to be focused is the Lagrange polynomial interpolation which is the simplest polynomial interpolation method. This method will be incorporated in the encryption algorithm of the elliptic curve ElGamal cryptosystem. **Results:** The scheme modifies the elliptic curve ElGamal cryptosystem by adding few steps in the encryption algorithm. Two polynomials are constructed based on the encrypted points using Lagrange polynomial interpolation and encrypted for the second time using the proposed encryption method. We believe it is safe from the theoretical side as it still relies on the discrete logarithm problem of the elliptic curve. **Conclusion/Recommendations:** The modified scheme is expected to be more secure than the existing scheme as it offers double encryption techniques. On top of the existing encryption algorithm, we managed to encrypt one more time using the polynomial interpolation method. We also have provided detail examples based on the described algorithm.

Key words: Lagrange polynomial interpolation, discrete logarithm problem, elliptic curve, cryptosystem, polynomial interpolation, curve cryptosystem, public key cryptosystem, finite field, advanced cryptography

INTRODUCTION

Whitfield Diffie and Martin Hellman had introduced the Diffie-Hellman key exchange scheme to the cryptography world which later planted the seeds for the development of public key cryptosystem (Diffie and Hellman, 1976). In this scheme, two keys namely public key and secret key are used where public key is made public for encryption steps whereas secret key is kept secretly for decryption steps and it is computationally infeasible. Public Key Cryptosystem (PKC) may have more advantages than Secret Key Cryptosystem (SKC) because in SKC, the encryption key and the decryption key are the same. Therefore, once the encryption key is accidentally known, message can be decrypted using the same key. However the PKC is slower and has larger key size than SKC (Mollin, 2007). Nowadays, there are three mathematical problems of PKC that are considered to be secured and efficient. These three mathematical problems are integer factorization problem, discrete logarithm problem and elliptic curve discrete logarithm problem (Modares *et al*., 2010). Now, we are going to turn our attention to elliptic curve cryptosystem which is the elliptic curve discrete logarithm based public key cryptosystem. Victor Miller and Neal Koblitz had independently proposed elliptic curve cryptosystem (ECC) in 1985 by making use the algebraic properties of the elliptic curve (Miller, 1986; Koblitz, 1987). ECC was based on discrete logarithm problem by using a group of points on an elliptic curve defined over finite field and its running times is fully exponential. The group of points together with a point at infinity eventually forms the Abelian group which is free from sub-exponential algorithms attack. Elliptic curve can be defined over real field, complex field, rational field and finite field. In cryptography, real numbers are not favourable because they are hard to store in computer memory and hard to predict the numbers of storage needed for them. Therefore finite field is preferable because the number of elements is finite and easy to handle and store them (Kaabneh and Al-Bdour, 2005). However, the elliptic curve defined over finite field with characteristic not equal to two or three is the main interest and study object for mathematicians and cryptographers. Taking about its history, the arithmetic

Corresponding Author: Liew Khang Jie, School of Mathematical Sciences, University Sains Malaysia, 11800, Minden, Penang, Malaysia

of the elliptic curve had been studied for theoretical reason for the past hundred years ago and not ever realized that it played important role in cryptography. Advanced cryptography was unimportant compared with the classical cryptography in that particular time probably due to the lack of advancement in computational technology. Besides, ECC has been widely used and also adapted into the existing public key cryptosystems which are known as elliptic curve Diffie and Hellman key exchange scheme, elliptic curve El-Gamal cryptosystem and elliptic curve digital signature algorithm.

MATERIALS AND METHODS

Before going deep into this study, several basic concepts are needed to enhance the understanding for the later part.

Definition: Let F_p be the prime field with characteristic not equal to two or three, an elliptic curve, E defined over field K is given by the smooth short Weierstrass Eq. 1 (Scholten and Vercauteren, 2008):

$$E: y^2 = x^3 + ax + b \quad (1)$$

where, a, b ε K. For every field K, the sets of K-rational points, E (K) is given by Eq. 2:

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\} \cup \{\infty\} \quad (2)$$

Point at infinity, ∞ which is a point sitting at the top or the bottom of the y-axis. This point acts as the identity element for the group law of the elliptic curve. The set of points and point at infinity form an Abelian group. The definition of elliptic curve requires that the elliptic curve is ordinary that is the discriminant of the elliptic curve, $\Delta = -16(4a^3+27b^2) \neq 0$ else is a singular curve. This also means that Eq. 1 has three distinct roots.

Group law of elliptic curve:

- Point at infinity, ∞ is a neutral element for the group such that $P + \infty = \infty + P = P \ \forall \ P \in E(K)$ where a point is denoted as P
- The opposite point is denoted as -P such that $-P = (x, -y) \in E(K)$ which is also a point inside the group of elliptic curve. Then, $P + (-P) = (x, y) + (x, -y) = \infty$
- Let consider the point addition, $P = (x_1, y_1)$ and $Q = (x_2, \mathbf{y}_2)$ such that $Q \neq \pm P$, then $P + Q = (x_3, y_3)$ which can be obtained using the following Eq. 3:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \\ \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \end{aligned} \quad (3)$$

- Let consider the point doubling, such that $P = Q = (x_1, y_1)$, then $P + P = [2]P = (x_3, y_3)$ which can be obtained using the following Eq. 4:

$$\begin{aligned} x_3 &= \lambda^2 - 2x_1 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \\ \lambda &= \frac{3x_1^2 + a}{2y_1} \end{aligned} \quad (4)$$

The method of point addition and point doubling is known as chord and tangent method. Notice that λ is the slope of the straight line in Eq. 3 and the slope of the tangent line in Eq. 4 respectively.

Elliptic Curve Discrete Logarithm Problem (ECDLP):

Definition: The ECDLP can be defined by considering a base point, $P \in F_p$ with order n and a point $Q \in \langle P \rangle$. Then we need to find $t \in [0, n - 1]$ such that (Hankerson *et al*., 2004):

$$P + P + P + \ldots + P = [t]P = Q \quad (5)$$

where, $t \in \mathbb{Z}$. From Eq. 5, the t is known as discrete logarithm of Q to be the base P and denoted as $t = \log_P Q$. Note that we are not going to multiply P with t and the + is a binary operation in the group of elliptic curve. In ECC, the P is the base point which agreed by both parties, Q is the public key and t is the secret key. The difficulty of ECDLP is given P and Q and then it is hard to determine for the value of t.

Lagrange polynomial interpolation:

Theorem: Let a set of k+1 distinct points given as (x_0, y_0), (x_1, y_1), (x_2, y_2),…, (x_k, y_k), then there exist a unique polynomial P (x) with k-th order (Burden and Faires, 1997). The polynomial is given by Eq. 6:

$$P_k(x) = \sum_{i=0}^{k} L_i(x) f(x_i) \quad (6)$$

where, k in P_k (x) stands for the k-th order polynomials and L_i (x) such that Eq. 7:

$$L_i(x) = \frac{(x-x_0)(x-x_1)...(x-x_{i-1})(x-x_{i+1})...(x-x_k)}{(x_i-x_0)(x_i-x_1)...(x_i-x_{i-1})(x_i-x_{i+1})...(x_i-x_k)} = \prod_{\substack{j=0 \\ j\neq i}}^{k} \frac{x-x_j}{x_i-x_j} \quad (7)$$

With these important concepts, we are ready for the discussion of embedding algorithm, the elliptic curve ElGamal cryptosystem and the modified algorithm using Lagrange polynomial interpolation method. Some concrete examples also included for further understanding. This study ends with a conclusion, acknowledgment and references.

RESULTS

To transfer plaintext via insecure channel using elliptic curve cryptosystem, it needs to be embedded into point form using Eq. 1 with appropriate domain parameters for a, b and p. So, we will refer to the text from (Koblitz, 1987; Trappe and Washington, 2006). In order to use the elliptic curve, we need a method to map a message onto a point on elliptic curve. The points yielded known as embedded points. There is unknown polynomial time and deterministic algorithm for embedding the points on an arbitrary elliptic curve defined over prime field, F_p. However, there exists a probabilistic method for embedding plaintext into point form. This method has the property that with small probability it will fail to produce a point. This probability can be made arbitrarily small, let say on the order of $1/2^k$ where $k \in Z$. If message, m is in alphabets such that from A to Z. They can be represented as:

A = 01, B = 02, …, Y = 25, Z = 26

Embedding algorithm:

- Let k be a large positive integer so that a failure rate of $1/2^k$ is acceptable when trying to decode
- Assume $(m + 1)k < p$
- $x = mk + j$, $0 \leq j < k$
- For j = 0, 1, 2,…, .k - 1, compute $y^2 = x^3 + ax + b \pmod p$ and then determine for the square roof for it.
- If get the square root, then $P_m = (x, y)$, else try a new x for $0 \leq j < k$
- To recover the message $P_m = (x, y)$, calculate $m = \lfloor x/k \rfloor$ that is the greatest integer less than or equal to x/k

Example: Let us show how to embed the message "ATTACK" by using the embedding algorithm.

As described earlier, we have:

A = 01, T = 20, T = 20, A = 01, C = 03 and K = 11

Let an elliptic curve E: $y^2 = x^3+26x+87$defined over prime field, F_{829}. Choose k= 30, mk + k < 829 for $0 \leq m \leq 26$:

- m = 01, then x = mk + j = 01 (30) + j for $0 \leq j < 30$. The possible choices for x are 30, 31, …, 59. For x = 31, $y^2 \equiv 20736 \pmod{829}$ and $144^2 \equiv 20736 \pmod{829}$. ∴ So, P_m= (31, 144)
- m = 20, then x = mk + j = 20 (30) + j = 600 + j for $0 \leq j <30$. The possible choices for x are 600, 601, …, 629. For x = 601, $y^2 \equiv 167281 \pmod{829}$ and $144^2 \equiv 167281 \pmod{829}$. ∴ So, P_m= (601, 409)
- m = 03, then x = mk + j = 03 (30) + j = 90 + j for $0 \leq j < 30$. The possible choices for x are 90, 91, …, 119. For x = 93, $y^2 \equiv 103041 \pmod{829}$ and $321^2 \equiv 103041 \pmod{829}$. ∴ So, P_m= (93, 321)
- m =11, then x = mk + j = 11 (30) + j = 330 + j for $0 \leq j < 30$. The possible choices for x are 330, 331, …, 359. For x = 331, $y^2 \equiv 73441 \pmod{829}$ and $271^2 \equiv 73441 \pmod{829}$. ∴ So, P_m= (331, 271)

We have embedded the message "ATTACK" as (31, 144), (601, 409), (601, 409), (31, 144), (93, 321) and (331, 271) respectively as the points.

Elliptic curve ElGamal cryptosystem: Suppose Alice and Bob have agreed on an elliptic curve, E defined over particular finite field with order of n and a base point P. Now Bob wants to send a message, m in term of embedded point, P_m of agreed elliptic curve and the algorithm is presented below:

- Alice chooses her secret key, k_A such that $1 \leq k_A < n$. The gcd $(k_A, n) = 1$. She publishes her public key as k_AP
- Bob chooses k_B such that$1 \leq k_B < n$. The gcd $(k_B, n) = 1$. He sends the encrypted point as $(k_BP, P_m + k_B(k_AP)$
- Alice decrypts the encrypted point by multiplying her secret key such that k_A (k_BP) and then obtains the P_m such that $P_m + k_B$ (k_AP) - k_A (k_BP)

The proposed polynomial interpolation method in the elliptic curve ElGamal cryptosystem: Now, we are going to discuss the algorithm of the modified elliptic curve ElGamal cryptosystem. This modified cryptosystem will send the set of encrypted points as two polynomials which are constructed using Lagrange polynomial interpolation method. The first polynomial will be encrypted as well to ensure the additional steps

in this modified algorithm is meaningful for implementation. Here the algorithm:

- Alice chooses her secret key, k_A such that$1 \le k_A < n$. The gcd (k_A, n) = 1. She publishes her public key as $k_A P$
- Bob chooses k_B such that$1 \le k_B < n$. The gcd (k_B, n) = 1. He encrypts each points such that (x_E, y_E) = P_m + k_B ($k_A P$).
- Bob constructs polynomial A(x) based on the points (1, x_{E1}), (2, x_{E2}), (3, x_{E3}), (I, x_{EI}) where l denotes the number of encrypted points. Another polynomial B(x) is constructed based on the encrypted points (x_{E1}, y_{E1}), (x_{E2}, y_{E2}), (x_{E3}, y_{E3}),…, (x_{EI}, y_{EI}). Both polynomials are constructed using Lagrange polynomial interpolation.
- Bob adds the x-coordinate of k_B ($k_A P$) to each of the coefficients modulo p of the polynomial A(x) whereas the coefficients of polynomial B(x) remain unchanged. The encrypted polynomial A(x) denoted as A' (x). Bob sends ($k_B P$, A'(x), B(x)) to Alice.
- Alice decrypts by multiplying her secret key such that $k_A(k_B P)$. Polynomial A(x) is obtained from A'(x) by deducting each coefficients using the x-coordinate of $k_A(k_B P)$.
- Alice obtains x-coordinate of encrypted points by substituting x = 1, 2,…,I into A(x). Then x-coordinate of encrypted points obtained is substituting into B(x) to get the y-coordinate of encrypted points.
- Alice obtains P_m such that $P_m + k_B (k_A P) - k_A (k_B P)$

Example: An elliptic curve $E: y^2 = x^3 + 26x + 87$ defined over prime field, F_{829}. The base point is P = (360, 220). The order for this group, #E (F_{829}) = 823. Alice chooses k_A such that $1 \le k_A < 823$ and gcd (k_A, 823) = 1. So, Alice chooses k_A = 87 and computes her public key $k_A P$ = (244, 825).

Encryption steps: Bob wishes to send message "ATTACK" to Alice. So, he embeds message in points: (31, 144), (601, 409), (601, 409), (31, 144), (93, 321) and (331, 271). He chooses k_B such that $1 \le k_B < 823$ and gcd (k_B, 823) = 1. Bob chooses k_B = 181 and computes $k_B P$ = (182,403) and also $k_B(k_A P)$ = [181](244, 825) = (523, 167). The set of encrypted points using ElGamal cryptosystem are (350, 355), (530, 534), (530, 534), (350, 355), (379, 194), (302, 715). Bob wishes to send two polynomials instead of points by forming a polynomial A(x) for (1, 350), (2, 530), (3, 530), (4, 350), (5, 379), (6, 302) and a polynomial B(x) for (350, 355), (530, 534), (530, 534), (350, 355), (379, 194), (302, 715) by using Lagrange polynomial interpolation.

To construct A(x), we know that there are 6 distinct points and therefore the degree of A(x), deg (A(x)) = 5. Using the Lagrange polynomial interpolation method:

$$A(x) = \left(\begin{array}{l} \left(\frac{(x-2)(x-3)(x-4)(x-5)(x-6)}{(1-2)(1-3)(1-4)(1-5)(1-6)} \right)(350) + \\ \left(\frac{(x-1)(x-3)(x-4)(x-5)(x-6)}{(2-1)(2-3)(2-4)(2-5)(2-6)} \right)(530) + \\ \left(\frac{(x-1)(x-2)(x-4)(x-5)(x-6)}{(3-1)(3-2)(3-4)(3-5)(3-6)} \right)(530) + \\ \left(\frac{(x-1)(x-2)(x-3)(x-5)(x-6)}{(4-1)(4-2)(4-3)(4-5)(4-6)} \right)(350) + \\ \left(\frac{(x-1)(x-2)(x-3)(x-4)(x-6)}{(5-1)(5-2)(5-3)(5-4)(5-6)} \right)(379) + \\ \left(\frac{(x-1)(x-2)(x-3)(x-4)(x-5)}{(6-1)(6-2)(6-3)(6-4)(6-5)} \right)(302) \end{array} \right) \pmod{829}$$

By taking the multiplicative inverse of modulo 829, we have the following:

$$A(x) = \left[\begin{array}{l} 263550(x-2)(x-3)(x-4)(x-5)(x-6) + \\ 201400(x-1)(x-3)(x-4)(x-5)(x-6) + \\ 36570(x-1)(x-2)(x-4)(x-5)(x-6) + \\ 266000(x-1)(x-2)(x-3)(x-5)(x-6) + \\ 170171(x-1)(x-2)(x-3)(x-4)(x-6) + \\ 22952(x-1)(x-2)(x-3)(x-4)(x-5) \end{array} \right] \pmod{829}$$

$$= 661x^5 + 291x^4 + 549x^3 + 316x^2 + 377x + 643 \pmod{829}$$

Add the x- coordinate of k_B ($k_A P$) = [181](244, 825) = (523, 167) for each coefficients modulo 829 of A(x):

$A'(x) = 355x^5 + 814x^4 + 243x^3 + 10x^2 + 71x + 337 \pmod{829}$

Notice that there are two repetitions for encrypted points and therefore there are only four distinct points. So, the degree of the polynomial B(x), deg (B(x)) = 3. Using the Lagrange polynomial interpolation:

$$B(x) = \left[\begin{array}{l} 182115(x-530)(x-379)(x-302) + \\ 377538(x-350)(x-379)(x-302) + \\ 110386(x-350)(x-530)(x-302) + \\ 499070(x-350)(x-530)(x-379) \end{array} \right] \pmod{829}$$

$$= 219x^3 + 314x^2 + 328x + 120 \pmod{829}$$

Bob sends [(182,403), A' (x), B (x)] to Alice.

DISCUSSION

Decryption steps: Alice receives (182,403), A'(x) and B(x) from Bob. Alice computes $k_A(182, 403) = [87](182, 403) = (523, 167)$. Alice obtains A(x) by deducting each coefficients of A'(x) by using the x-coordinate of $k_A(182, 403)= [87] (182, 403) = (523, 167)$:

$A(x)= 661x^5 + 261x^4 +549x^3 + 316x^2 + 377x + 643 \pmod{829}$

Alice knows this polynomial has 6 points by looking at its degree. She evaluates the polynomial A(x) for x = 1, 2, 3, 4, 5, 6 and obtains 350, 530, 530, 350, 379, 302 respectively. Then Alice evaluates the polynomial B(x) for x = 350, 530, 530, 350, 379, 302 and obtains 355, 534, 534, 355,194, 715.

Therefore, the set of encrypted points is as follows:

(350, 355), (530, 534), (530, 534),
(350, 355), (379, 194), (302, 715)

Alice decrypts the set of points by doing the following:

(350, 355) - (523, 167) = (350, 355) +
(523, -167) = (31, 144)
(530, 534) - (523, 167) = (530, 534) +
(523, -167) = (601, 409)
(530, 534) - (523, 167) = (530, 534) +
(523, -167) = (601, 409)
(350, 355) - (523, 167) = (350, 355) +
(523, -167) = (31, 144)
(379, 194) - (523, 167) = (350, 355) +
(523, -167) = (93, 321)
(302, 715) - (523, 167) = (350, 355) +
(523, -167) = (331, 271)

The message is recovered via $\lfloor x/K \rfloor = \lfloor x/30 \rfloor$:

$$\lfloor 31/30 \rfloor = 01, \lfloor 601/30 \rfloor = 20, \lfloor 601/30 \rfloor = 20,$$
$$\lfloor 31/30 \rfloor = 01, \lfloor 93/30 \rfloor = 03, \lfloor 331/30 \rfloor = 11$$

So, the message received by Alice from Bob is "ATTACK".

CONCLUSION

We have shown a concrete example on the method to embed the message in point form before using the elliptic curve cryptosystem. Also, we have discussed the modified elliptic curve ElGamal cryptosystem using polynomial interpolation method by providing an appropriate example for it. The modified scheme is believed to be secure because it involves double encryptions. Basically, the modified scheme still relies on the elliptic curve discrete logarithm problem. Instead of sending a set of points, we prefer to replace this by encrypted polynomial. Perhaps this can save the space although the computational steps are increasing. We strongly feel that the increment in the computational step is not significant as it only involves the ordinary addition and subtraction operations. However, our future concern is to find out whether or not it is possible to interpolate the embedded points without undergoing the encryption steps using elliptic curve ElGamal cryptosystem since the encrypted polynomial also relies on the elliptic curve discrete logarithm problem.

ACKNOWLEDGMENT

The researchers would like to take this opportunity to thanks Universiti Sains Malaysia, School of Mathematical Sciences and USM short term grant for supporting this research. Liew Khang Jie would like to thanks Institute of Postgraduate Studies for the financial support under the USM Fellowship scheme.

REFERENCES

Burden, R.L. and J.D. Faires, 1997. Numerical Analysis. 6th Edn., Brooks/Cole Publishing Company, United States, ISBN: 0534955320, pp: 811.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654. DOI: 10.1109/TIT.1976.1055638

Hankerson, D.R., S.A. Vanstone and A.J. Menezes, 2004. Guide to Elliptic Curve Cryptography. 1st Edn., Springer-Verlag, New York, USA., ISBN: 038795273X, pp: 311.

Kaabneh, K. and H. Al-Bdour, 2005. Key exchange protocol in elliptic curve cryptography with no public point. Am. J. Applied Sci., 2: 1232-1235. DOI: 10.3844/ajassp.2005.1232.1235

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Miller, V.S., 1986. Use of elliptic curves in cryptography. Adv. Cryptol. CRYPTO Proc., 218: 417-426. DOI: 10.1007/3-540-39799-x_31

Modares, H., Y. Salem, R. Salleh and M.T. Shahgoli, 2010. A bit-serial multiplier architecture for finite fields over galois fields. J. Comput. Sci., 6: 1237-1246. DOI: 10.3844/jcssp.2010.1237.1246

Mollin, R.A., 2007. An Introduction to Cryptography. 2nd Edn., Chapman and Hall/CRC, United States, ISBN: 1584886188, pp: 413.

Scholten, J. and F. Vercauteren, 2008. An Introduction to Elliptic and Hyperelliptic Curve Cryptography and the NTRU.

Trappe, W. and L.C. Washington, 2006. Introduction to Cryptography: With Coding Theory. 2nd Edn., Pearson Prentice Hall, USA., ISBN: 0131862391, pp: 577.