Annals of Optimization Theory and Practice

Volume 2, Number 3, 25-32

December 2019

DOI: 10.22121/aotp.2020.217266.1028

An example on elliptic curve cryptography

Javad Sharafi

University of Imam Ali, Tehran, Iran

✉ javadsharafi@grad.kashanu.ac.ir

(Received: November 10, 2019 / Accepted: December 19, 2019)

Abstract Cryptography on Elliptic curve is one of the most important public key encryption systems, whose security depends on difficulty of solving the discrete logarithm problem. The reason of importance is that elliptic curves provide security equivalent to classical systems while using fewer bits. To encrypt a plain message with El-Gamal algorithm, we embed the message to the point on the elliptic curve using the Koblitz technique. In this paper, we explore the conditions that encrypt the message without mapping the point on the elliptic curve.

Keywords El-Gamal algorithm; Elliptic Curve Cryptography; Finite Fields; Point Addition

1. Elliptic Curve

Suppose that K be a field where the characteristic of K is not 2 or 3. An elliptic curve over K is a curve with equation the form

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

Where a and b are elements of K with $4a^3 + 27b^2 \neq 0$. The set of point of E with coordinate in K is defined as:

$$E(K) = \{(x, y) \in E : x, y \in K\} \cup \{O\}, \quad (2)$$

Where is the point at infinity.

1.1. Finite Field Contained Elliptic Curve

If p be a prime number, then E_p is an elliptic curve over a finite field with the equation of the form

$$E_p : y^2 = x^3 + ax + b \pmod{p}, \quad (3)$$

Where a and b are constant with $4a^3 + 27b^2 \neq 0$.

1.2. Important Points

For adding two points P and Q on the elliptic curve, we draw the line L through P and Q. The line L intersects E in a third point R. Then $\acute{R} = P + Q$ is the reflection of R across the x-axis. Negation of a point $P = (x,y)$ is the point $-P = (x, -y)$.

Let E be an elliptic curve. The addition of points on E satisfies the following properties:

1. $P + O = O + P = P \qquad \forall P \in E$
2. $P + (-P) = O \qquad \forall P \in E$
3. $P + (Q + R) = (P + Q) + R \qquad \forall P, Q, R \in E$
4. $P + Q = Q + P \qquad \forall P, Q \in E$

In other words, the points on E form an additive abelian group with O as the identity element.

To add two points P_1 and P_2 on E there are some cases on the coordinates of the points are given as follows:

1) if $P_1 = O$ then $P_1 + P_2 = P_2$.

2) if $P_2 = O$ then $P_1 + P_2 = P_1$.

3) if $P_1 = (x_1,y_1)$ and $P_2 = (x_2,y_2)$ and $x_1 \neq x_2$.

Let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

then:

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1) \tag{4}$$

4) if $P_1 = P_2$, let

$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

then:

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1) \tag{5}$$

2. Cryptosystem on Elliptic Curves

2.1. El-Gamal Public Key

Alice wants to send a message to Bob securely. The first step of El-Gamal elliptic curve cryptosystem converts the plaintext message *m* to a point P_m on the elliptic curve $E(F_p)$. Alice and Bob chooses a private key randomly n_A and n_B respectively from the interval [1, p-1], then they compute a public key by multiplying the private key by the base point *G*:

$$P_A = n_A G \qquad P_B = n_B G,$$

where $n_A G$ is computed as repeated addition $G + G + \cdots + n_A$ times. To encrypt the message P_m, Alice chooses a random number *k* and compute the following values:

$$C_1 = kG \qquad C_2 = P_m + kP_B \quad (6)$$

Alice sends the cipher text message (C_1 , C_2) to Bob. Then Bob decrypts the cipher text message to get the plaintext P_m as follows:

$$C_2 - n_B C_1 = \left(P_m + kP_B\right) - n_B\left(kG\right) = P_m + k\left(n_B G\right) - n_B\left(kG\right) = P_m \quad (7)$$

2.2. Koblitz Encoding Technique

Let $E_P: y^2 = x^3 + ax + b$ be an elliptic curve defined over $E(F_P)$. Let $P \equiv 3\ (mod\ 4)$. We embedded the message *m* to the point P_m on the elliptic curve with the following method:

Suppose that $0 \le m < p/1000 - 1$. For $0 \le j < 1000$, we compute the following values:

$$x_j \equiv 1000m + j \qquad s_j \equiv x_j^3 + ax_j + b \pmod p \quad (8)$$

If $S_j^{(p-1)/2} \equiv 1\ (mod\ p)$, then S_j is a square mod *P* and $y_j = S_j^{(p+1)/4}\ (mod\ p)$. So the plaintext message *m* convert to the point $P_m = (x_j , y_j)$ on E_p. The message *m* can be recovered by the following equation:

$$m = [x_j / 1000]$$

2.3. Example of Koblitz Encoding Technique

Let $E_P: y^2 = x^3 + ax + b$ be an elliptic curve defined over $E(F_P)$, where

p=160815853215891608158515783216621584174015851583063
a= 124587890213264587985421233680147852369 8
b= 356487956451235465485465875487145789654 2 (9)

Clearly $P \equiv 3\ (mod\ 4)$. Suppose we want to encript the persian text shown in Figure 2. Its equivalent ASCII values are:

m=(1570,1578,1588,32,1575,1586,32,1594,1585,1576,32,1705,1588,
1608,1585,32,1589,1608,1585,1578,32,1662,1584,1740,1585,1583).

We put

m_1=157015781588321575158632159415851576321705158 8

m_2=160815853215891608158515783216621584174015851583

Figure1.

First we embed m_1 to the point on the curve. By calculations j=70. So

$$x_1 \equiv 1000m_1 + 70 \equiv 157015781588321575158632159415851576321705158 8070 \pmod{p}$$

and

$$s_1 \equiv x_1^3 + ax_1 + b \equiv 136675430209883314209572962643993168056335694636178 \pmod{p}$$

on the other hand $S_j^{(p-1)/2} \equiv 1\ (mod\ p)$, therefore

$$y_1 = s_1^{(p+1)/4} = 95894767124349928170021515432526550127137810249344 \pmod{p}$$

so the plaintext message m_1 is converted to the point

$$P_{m_1} = (x_1, y_1) = (157015781588321575158632159415851576321705158 8070,$$
$$95894767124349928170021515432526550127137810249344).$$

Now we embed m_2 to the point an curve. So

$$x_2 \equiv 1000m_2 + 70 \equiv 160815853215891608158515783216621584174015851583070 \pmod{p}$$

and

$$s_2 \equiv x_2^3 + ax_2 + b \equiv 122860318794408758138341451124818075627 71 \pmod{p}$$

on the other hand $S_2^{(p-1)/2} \equiv 1\ (mod\ p)$, therefore

$$y_2 = s_2^{(p+1)/4} = 41520670771374945504484550262019312077367105136983 \pmod{p}$$

So the plaintext message m_2 convert to a point

$$P_{m_2} = (x_2, y_2) = (160815853215891608158515783216621584174015851583070,$$
$$41520670771374945504484550262019312077367105136983)$$

Now, Alice encrypts the points P_{m_1} and P_{m_2} on elliptic curve. Bob considers private key n_B and point G on E_P:

$$n_B = 458795654213265487658421356458465789653215465487$$
$$G = (75696702515208745401881713213118145650266650528282,$$
$$798043594736124717609320916174865105629494780222 34) \quad (10)$$

Now Alice encrypts P_{m_1}.

Alice selects random value k:

$$k = 140411536272185229247218214322150490980349894625502$$

Alice computes C_1 and C_2 using 6:

$$C_1 = kG = (42412994553325210342989729025800836703397718743261,$$
$$57496607304417724617097119121339493657804471741440)$$

$$P_B = (14611686117235936577191705428318353997290859418955 6,$$
$$69202370342538795182027117650777103108165558550780)$$

$$C_2 = P_{m_1} + kP_B = (18937610166003692592960373687246817447379976571 17,$$

$$14960979396118523075067727623331532541392550690220 6)$$

Alice sends (C_1 , C_2) as cipher text to Bob. Then Bob decrypts the cipher text message to get the plaintext P_{m_1} as follows:

$$C_2 - n_A C_1 = (15701578158832157515863215941585157632170515880 70,$$
$$95894767124349928170021515432526550127137810249344).$$

Then Bob recovers m_1 by the following equation:

$$m_1 = [x_1 / 1000] \quad (11)$$

3. Main Result

We saw in previous section to encode a message to an elliptic curve, first we embedded the message to the point on the curve and then we encrypted the obtained point. Let's consider the conditions that we can encrypt the message without mapping to the point on the curve. Let $E_P: y^2 = x^3 + ax + b$ be a curve on $E(F_P)$. All the points on E_P forms an abelian group with O as the identity element. According to the previous section, when we add two points on the curve, the third point is also on the curve. If the first point is on the curve, but the second point does not on the curve, then the third point is on the curve or not. Now we show that it is not necessary that the second point is on the curve,

and it is sufficient that the coordinates of the second point is from one to *P*-1. If we show the point on the curve with $P(x_1 , y_1)$ and the second point, which may or may not be on the curve, with $Q(x_2 , y_2)$ and represent the point obtained from the sum of these two points with $R(x_3 , y_3)$, then the following conditions must be established for reversibility of addition:

$$x_1 \neq x_2, \qquad x_1 \neq x_3 \quad (12)$$

In fact we prove $(P + Q) - Q = P$.

If $(P + Q) - Q = (x_4 , y_4)$, then prove $x_1 = x_4$. Denote the slope through $P + Q$ and $-Q$ with *m* and it's equals:

$$m = \frac{-y_2 - y_3}{x_2 - x_3} \quad (13)$$

Then by using 4 we have:

$$x_4 = m^2 - x_3 - x_2 = m^2 - \lambda^2 + x_1 + x_2 - x_2 = m^2 - \lambda^2 + x_1$$

We denote $m^2 - \lambda^2 = 0$, so $x_4 = x_1$. But $m^2 - \lambda^2 = (m\lambda)(m + \lambda)$ therefore we denote $m + \lambda = 0$.

$$m + \lambda = \frac{-y_2 - y_3}{x_2 - x_3} + \frac{y_2 - y_1}{x_2 - x_1} \quad (14)$$

By simplification and substitution values of x_3 and y_3, the numerator of above fraction equals to:

$$2y_2x_1 + 2\lambda x_1^2 +^3 (x_2 - x_1) - \lambda x_1x_2 - x_2^2 - 2y_1x_1 + \lambda^2(y_1 - y_2) + y_2x_2 - y_1x_2 \quad (15)$$

After computation we have $m + \lambda = 0$, so $x_4 = x_1$. By substitution x_4 in the above equation y_4 is obtained. We see that y_4 is also equal to y_1. if $x_1 = x_2$ or $x_1 = x_3$ we obtained point at infinity. In this case by choosing another *k* we resume our calculations.

In fact, we showed that by subtracting *Q* from *R*, the point *P* is obtained, except in cases where the point at infinitely occur. We use this idea in the El-Gamal algorithm and separate calculations for encoding plain message to elliptic curve coordinate is removed, and instead, the message P_m is converted to the point (x_m , y_m), such that x_m and y_m from 1 to *P-1* and

$$x_m \neq x_{Kp_B} \qquad x_m \neq x_{C_2} \quad (16)$$

4. Example and Implementation

Suppose that Bob wants to encrypt the Persian text shown in Figure 1. The number of term of its equivalent ASCII values is 26. Consider the first 13 term as *x*-coordinate and the second 13 term as *y*-coordinate of P_m. Pad with 32 at the end of the above list if the number of term is odd, so that pairing can be done.

$$p_m = [1570157815883215751586321594158515763217051588,$$
$$1608158532158916081585157832166215841740158515 83]$$

Bob considers elliptic curve E_p where in sec 1.2.3. Now Alice encrypts P_m (which is not a point on the curve E_p). Alice selects random value *k*:

$$k=1404115362721852292472182143221504909803498946255 02$$

Alice computes C_1 and C_2 using 6:

$$C_1 = kG = (4241299455332521034298972902580083670339771874326 1$$
$$5749660730441772461709711912133949365780447174144 0)$$

$$P_B = (1461168611723593657719170542831835399729085941895 56,$$
$$6920237034253879518202711765077710310816555855078 0)$$

$$C_2 = P_m + kP_B = (6426641164436459727345210564747895684505872188882 7,$$
$$1159500675448302611872265395946684164459346718087 3)$$

Alice sends (C_1 , C_2) as cipher text to Bob. Then Bob decrypts the cipher text message to get the plaintext P_m as follows:

$$C_2 - n_A C_1 = (1570157815883215751586321594158515763217051588,$$
$$1608158532158916081585157832166215841740158515 83)$$

Now Bob receives the pair of above numbers and splits to four digit numbers. Therefore, we will obtain the following numbers:

$$(1570,1578,1588,32,1575,1586,32,1594,1585,1576,32,1705,1588,$$
$$1608,1585,32,1589,1608,1585,1578,32,1662,1584,1740,1585,1583)$$

Then from this we can recover the message using the ASCII table.

References

1. Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. *Procedia Computer Science*, *54*, 73-82.

2. Singh, L. D., & Singh, K. M. (2017). Medical image encryption based on improved El-Gamal encryption technique. *CDATA [Optik – International Journal for Light and Electron Optics.*

3. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209.

4. J. Ho_stein, J. Pipher, J. H. Silverman (2008). An Introduction to Mathematical Cryptography, *Springer*.

5. Koblitz, N. (1994). *A course in number theory and cryptography* (Vol. 114). Springer Science & Business Media.

6. Washington, L. C. (2008). *Elliptic curves: number theory and cryptography*. CRC press.