# The analysis of ECC Algorithm

Research question:

“ How can the encryption of transmitted information be achieved using discrete logarithm structure of the Abelian additive group and properties of plane elliptic curve?”

Word counts: 3391

## Table of contents

# Elliptic curve cryptography---A brief review

An elliptic curve is a crossing point of numerous parts of arithmetic, for example, logarithmic math and number hypothesis. Before the complete disclosure of the elliptic curve, the elliptic curve has consistently been considered as a hypothetical subject. As the prime numbers required in the RSA cryptosystem are getting bigger and bigger, numerical acknowledgment turns out to be increasingly troublesome. As of late, individuals have discovered that elliptic curves are a useful asset to defeat this trouble, particularly dependent on the Abelian ground framed by the purposes of the elliptic curve. (Velu, Jacques. "Courbes Elliptiques Munies d'Un Sous-Groupe Z/Zn*Mn.") The acknowledgment of different cryptosystems has been a significant subject in the field of public-key cryptography. Because of the upsides of elliptic curve cryptography, since its presentation during the 1980s, elliptic curve cryptography has step by step become an exceptionally fascinating part of cryptography. Since 1997, an exploration hotspot has been shaped, particularly in the use of versatile correspondence security, which has quickened this pattern.

In general, Elliptic curve cryptography is a cryptographic framework dependent on elliptic curves and points in a finite field. Its numerical establishment is to utilize focuses on the elliptic curve to shape the discrete logarithm structure of the Abelian group theory. This essay aims to investigate and research how can the properties of the elliptic curve and group theory be used to encrypt the information properly and related attacking methods to decode the transmitted information.

# The mathematical foundation of elliptic curve cryptography

## Abelian group

The Abelian group is named after the Norwegian mathematician Niels Abel. An Abelian group $Z$, with two elements $x, y$, and multiple operations can form another group $Z$ which is denoted as $x * y$ or $xy$. Usually, $xy \neq yx$. Also, $(x * y) * (x * y) = x * x * y * y$

## Remainder operation

The Remainder operation is the procedure to receive the return values of the remainder from a division. The correct format of Remainder operation is $number\ mod\ divisor$. Unlike regular division, the Remainder operation returns the value of the remainder directly. For example, when $7 \div 2$, the quotient is 3, and the remainder is 1. In Remainder format, the $7 \bmod 2$ yields 1 directly as the remainder from this division. When dealing with division, the Remainder operation

has its own set of rules to follow. If a module is in a form of $\frac{x}{y} \bmod z$, the answer must not be taken using direct division. Instead, letting $a$ equals to this Remainder:

$a \equiv \frac{x}{y} \bmod z, ay \equiv x \bmod z, ay \bmod z = x \bmod z$. Hence, the value of $a$, which is the value of $\frac{x}{y} \bmod z$ will be obtained.

## Hash table

The Hash calculation is a summed-up calculation, which can likewise be considered as a thought ("Elliptic Curve Discrete Logarithm Based Cryptography."). Utilizing Hash calculation can improve the use of the extra room, and improve the effectiveness of information question, therefore likewise be utilized as an advanced mark to guarantee the security of information transmission. Let alphabets A, B, C, etc. be the specific data stored in a specific position, which can be represented in the following graph:

| A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

If she is requested to locate the C, she needs to look through the table individually to locate the datapoint C. Be that as it may, if she utilizes the data C, which is in position 2, to locate this specific information. The cycle can be moderately simple. Notice that each file number can be determined utilizing the its position in the data group. Thus, the file number is identified with the information itself. Presently, the data points can be represented utilizing the ASCII code - a computer code to represent the subjects such as alphabets. Then, their ASCII code is calculated using the mod function with the total number of data points, where

$\text{file number} = \text{ASCII} \bmod \text{position of the datapoint}$ In this case:

| Datapoints | ASCII codes | Its mod function |
|---|---|---|
| A | 65 | $65 \bmod 11 = 10$ |
| B | 66 | $66 \bmod 11 = 0$ |
| C | 67 | $67 \bmod 11 = 2$ |
| D | 68 | $68 \bmod 11 = 2$ |
| E | 69 | $69 \bmod 11 = 3$ |
| F | 70 | $70 \bmod 11 = 4$ |
| G | 71 | $71 \bmod 11 = 5$ |
| H | 72 | $72 \bmod 11 = 6$ |
| I | 73 | $73 \bmod 11 = 7$ |
| J | 74 | $74 \bmod 11 = 8$ |
| K | 75 | $75 \bmod 11 = 9$ |

Now, the new data table is organized under the previous mathematical operation:

| B | C | D | E | F | G | H | I | J | K | A |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Thus, the computer can find the data in the function faster. Also, the computer can determine whether the data should exist in the table by judging their position (index number) and the mathematical operation that generates the index number. A Hash table can be open addressing, which means data will just fit whatever slot available despite the overlay of the same index number.

## Discrete logarithm structure over the elliptic curve

The aim of the discrete logarithm structure over the elliptic curve is to find the value of the constant $k$ when there is an existed and known point $P = (x, y)$ and the coordinate of $kP$. Operation details will be presented further in this essay.

## Elliptic curve and its related calculations

The general mathematical format of elliptic curve is

$E: y^2 = ax^3 + bx^2 + cx + d$ , where $a, b, c, d$ are real number (Velu, Jacques. “Courbes Elliptiques Munies d’Un Sous-Groupe Z/Zn*Mn.”)

Take an arbitrary elliptic curve as an example, when $a = 1, b = 2, c = 3, d = 4$ , the elliptic curve has the shape:

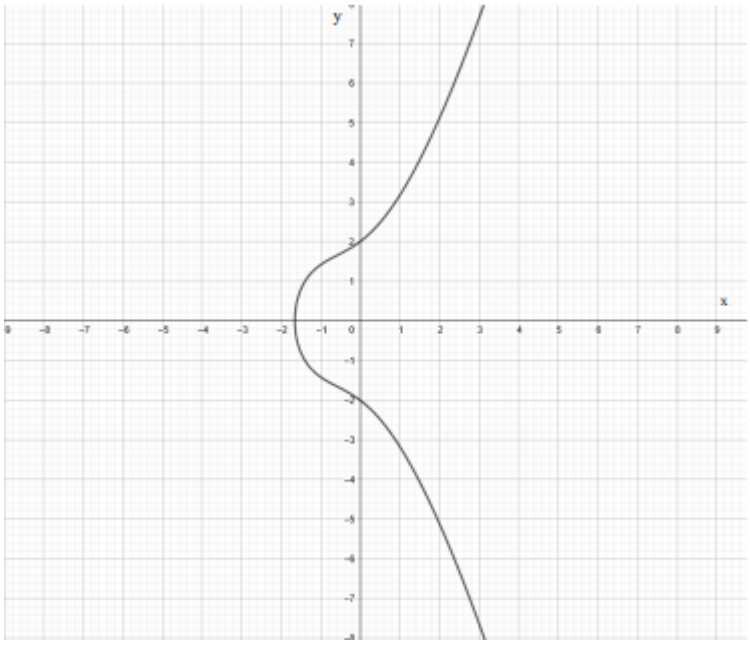


**Figure 1: the shape of the elliptic curve which defined as** $y^2 = x^3 + 2x^2 + 3x + 4$

The calculations regarding the elliptic curve are relatively simple. The addition is the first one to discuss. In the graph below, a straight-line passing point $A$ and $B$ is made. There is also the point of intersection $C$, the values of $x$ of this coordinate and the parallel point $H$ are actually $A+B$. Nonetheless, in an elliptic curve, the arrangement from such addition above is the point on the elliptic curve. Such a mathematical operation is classified as "the basic addition of the elliptic curve".

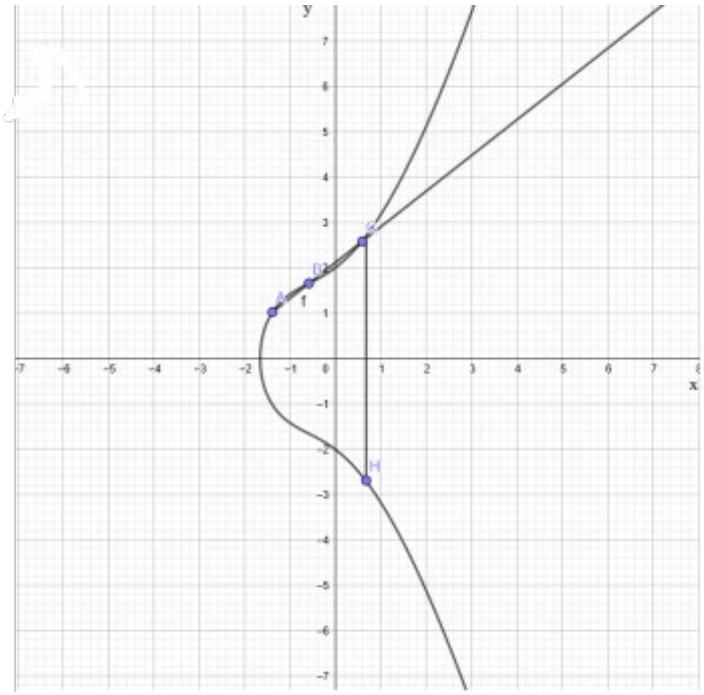

**Figure 2: basic addition of the elliptic curve shown when** $y^2 = x^3 + 2x^2 + 3x + 4$

What if the two points share the same coordinate, what will be the addition? The intersection point will have the value of $x = A + A$.

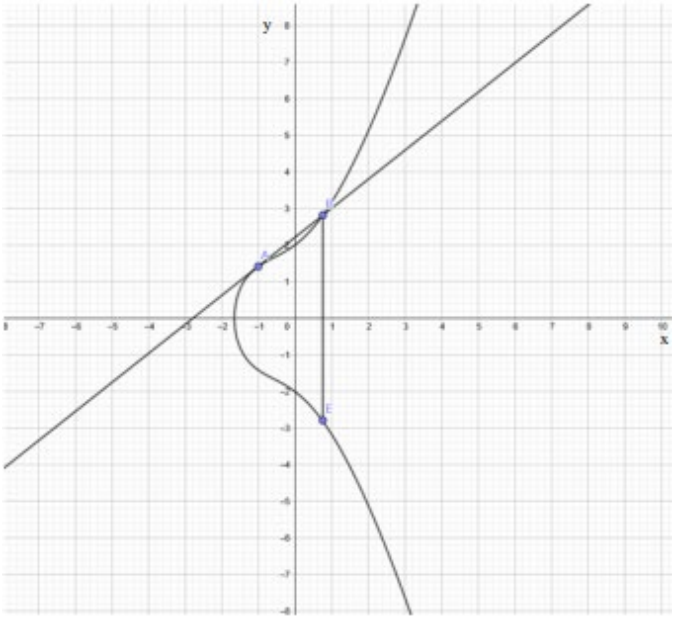

**Figure 3: addition of the same points of the elliptic curve when** $y^2 = x^3 + 2x^2 + 3x + 4$

Additionally, the symmetric point of $A$ on the elliptic curve is denoted as $B$.

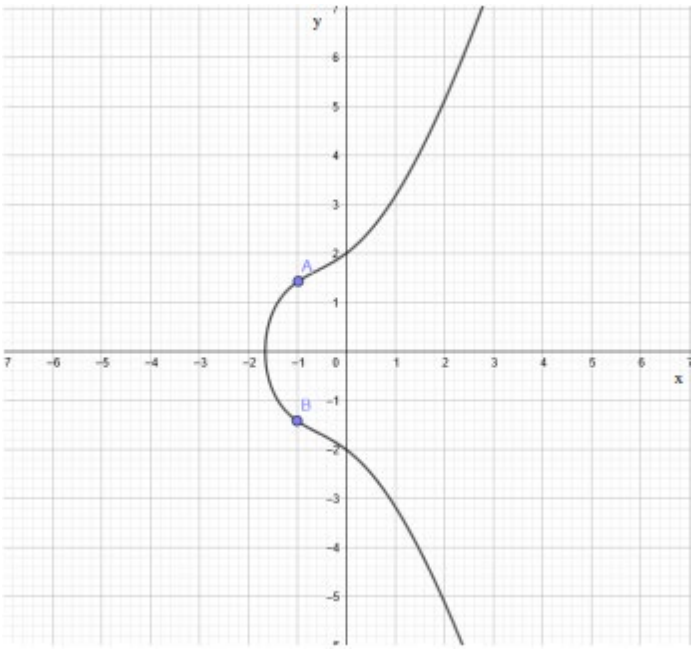


**Figure 4: the symmetry of points of the elliptic curve when** $y^2 = x^3 + 2x^2 + 3x + 4$

If they are added together, the value will be zero.

## The ECC algorithm

## The concept and classification of an elliptic curve and the properties of encryption

The elliptic curve can be classified into two groups, the curve in the finite field $F_p$, and the curve in a finite field $GM(2^m)$. The finite field $GM(2^m)$ is not important in this essay, hence, it is excluded from the explanation. ("The Case for Elliptic Curve Cryptography.")

Let the finite field $F_p$ has an elliptic curve, it has three important definitions as follows. The first definition is about the group of the elements from the elliptic curve, the second definition is about the order and the basic arithmetic operations of the elliptic curve, the third definition describes the behavior of the random point the multiplication of the order or the constant. These three definitions look very abstract and sophisticated. However, they are crucial in the formation of the number generator for the discrete logarithmic problem.

First, a prime number $p$ is the number of elements and the maximum value of the finite field $F_p$ in the elliptic curve equation $E(F_p)$, which is defined on the affine plane with the equation

of $E(F_p) = y^2 = x^3 + ax + b$ . $E(F_p) = y^2 = x^3 + ax + b$ and point of infinity 0 are in the same set on the plane, denoted as $E(F_p) = \{y^2 = x^3 + ax + b \in F_p\} \cup \{0\}$ .

Second, usually, three commonly operations on the elliptic curve over a finite field $F_p$ include addition of points, negation, and multiplication through doubling the same points. The addition of points is fairly straight forward. If $A$ and $B$ are two distinct points on the elliptic curve, where $A = (x_1, y_1)$ and $B = (x_2, y_2)$. Point $C = A + B$, and it has a coordinate of $x_3, y_3$. Since point $C$ lines on the same ray of $A$ and $B$, it shares the same gradient of $A$ and $B$. Thus, the gradient $S$ is calculated $\frac{y_2 - y_1}{x_2 - x_1}$, and the $x$ coordinate of $C$ is obtained through $x_3 = S^2 - x_1 - x_2$, and the coordinate of $y$ is calculated $S * x_1 - S * x_2 - y_1$.

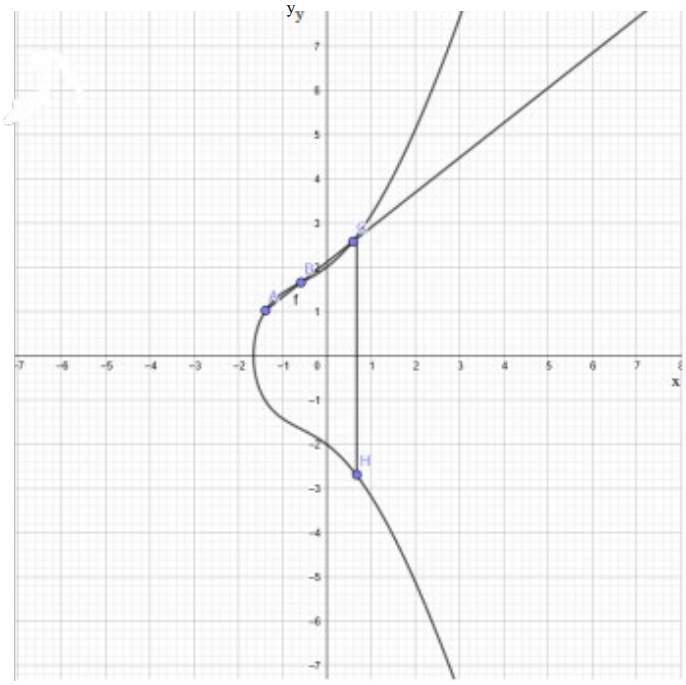


**Figure 5: the elliptic curve when $y^2 = x^3 + 2x^2 + 3x + 4$ and three distinct points**

When two points share the same coordinate, the addition of two points can actually be the multiplication by doubling one of the points. In this scenario, the gradient between two points is given by $S = \frac{3x_1^2 + a}{2y_1}$, and the value of $x$ is given by $x_3 = S^2 - 2x_1$, the value of $y$ is $-x_1 + Sx_1 - Sx_2$.

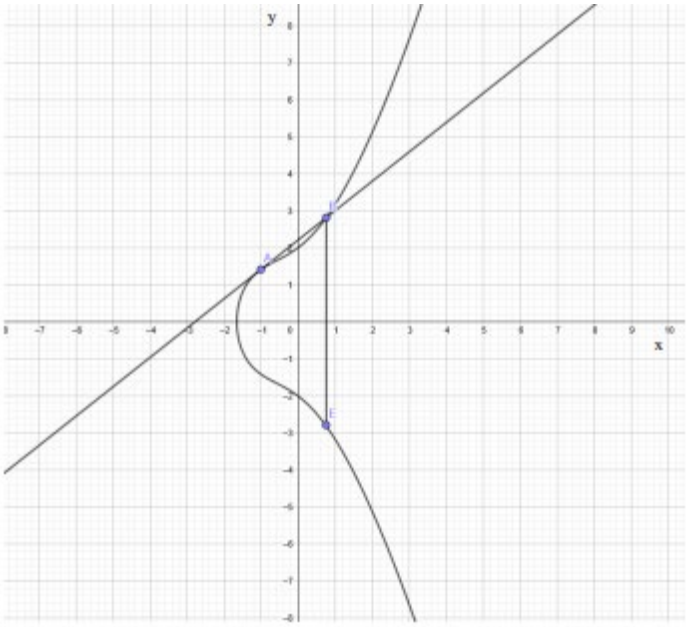


**Figure 5: the elliptic curve when $y^2 = x^3 + 2x^2 + 3x + 4$ and only two distinct points**

The world negation in logic means taking one the opposite value of an existed true value. In the elliptic curve, it means similar. When a point $p = (x, y)$ exists on the plane, and it $-p = (x, -y)$ is the inverse value of $p$. When they are added together, it will share the point of infinity for the value of $y$, which cannot be drawn on the graph.

Third, the order of point $p$: Let $p = (x, y)$, and $k$ is an integer, $kp = k(x, y) = (x, y) + (x, y) + (x, y) + ... + (x, y)$ until the kth term. The order $n$ of point $p$ satisfies $np = 0$ as the smallest integer. In this encryption system, the common base point $p = (x, y)$ is usually chosen $E(F_p)$ and usually requires the order $n$ as a prime number. Also, the order $n$ must be big enough to make $p$ as a generator, which formulate encryption principle using Abelian group as $p = \{p, 2p, 3p, np\}$ repeatedly. This process is also described as the generation of the subgroups.

When an elliptic curve has form $E(F_p) = y^2 = x^3 + ax + b$, the points are all on a designated curve (continues), which is very easy for someone to predict the new coordinate using vector multiplication and addition. Hence, by using the Remainder function, instead of the points resulted from independent variable x, both x and y will share the same reminder and have different values. Thus, the points will scatter all over the plot, and hard for someone to calculate a specific point on the curve. By applying the definitions introduced previously in an example, their effects of encryption become clear. For example, if the elliptic curve $y^2 = x^3 + 2x + 1$ exists on a finite



y

field $F_{53}$. The elliptic curve is then rewritten as $y^2 \equiv x^3 + 2x + 1 \bmod 53$. This equation means that the values of both $y^2$ and $x^3 + 2x + 1$ are evaluated as the dividend and 53 is the divisor. They share the same remainder. Why is remainder important? As examples of the regular elliptic curve, they have geometric shapes with different values of $y$ and $x$. However, if those values are restricted in between the integer of 0 to 53, and they must have the same remainder when they divide 53. The graph will become a plot with scattering points instead of a continuous geometric curve. Specifically, if $y^2 \equiv x^3 + 2x + 1 \bmod 53$, and x=0, the equation becomes $0^3 + 2*0 + 1 \bmod 53 = 1 \bmod 53 = 1 \cup y^2 = 1$, and $y = \pm 1$. Two points $(0,1),(0,-1)$ exist on the graph simultaneously. Using such method, the graph can be drawn:

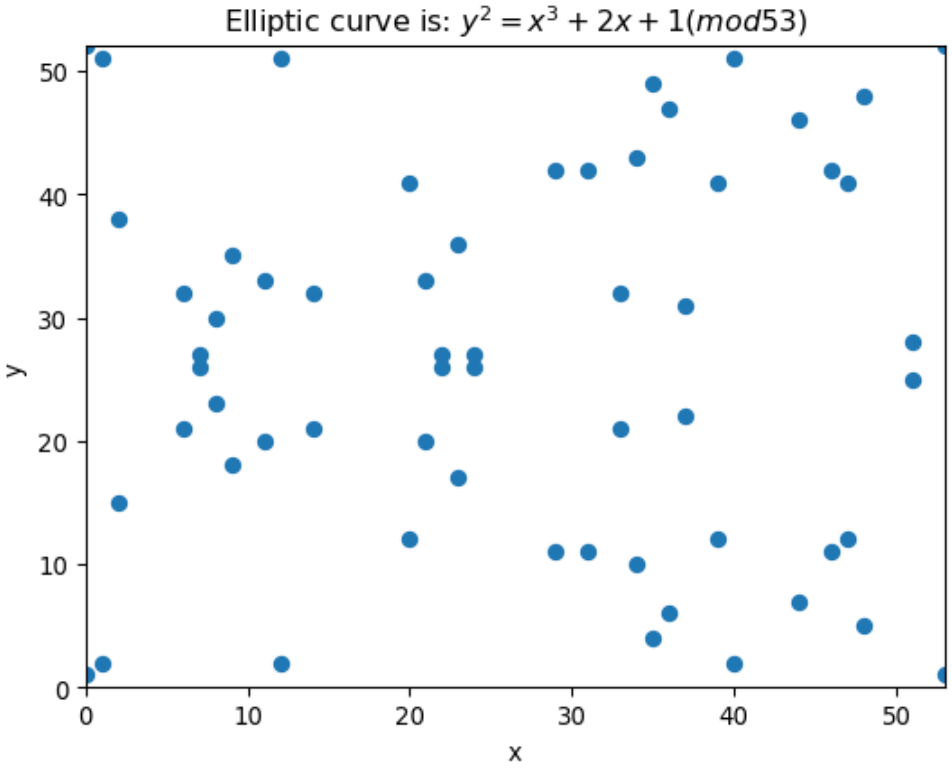


**Figure 6: the actual graph** $y^2 \equiv x^3 + 2x + 1 \bmod 53$ that exists in the finite field $F_{53}$

This graph shows all the scattered points with no observable pattern of distribution, which makes it suitable for encryptions.

The points existed on the graph are:

| |
|---|
| (0,1) (0,52) (1,51) (1,2) (2,15) (2,38) (6,21) (6,32) (7,27) (7,26) (8,23) (8,30) (9,18) (9,35) (11,33) (11,20) (12,51) (12,2) (14,21) (14,32) (20,12) (20,41) (21,33) (21,20) (22,27) (22,26) (23,36) (23,17) (24,27) (24,26) (29,42) (29,11) (31,42) (31,11) (33,21) (33,32) (34,10) (34,43) (35,49) (35,4) (36,47) (36,6) (37,22) (37,31) (39,12) (39,41) (40,51) (40,2) (44,46) (44,7) (46,42) (46,11) (47,12) (47,41) (48,5) (48,48) (51,28) (51,25) (53,1) (53,52) |

Just as what ECDLP describes in definition 3, the arbitrary point $G$ can generate infinite subgroups by multiplying the constant (Semaev, I. A. “Evaluation of Discrete Logarithms in a

Group of p-Torsion Points of an Elliptic Curve in Characteristic p."). In this case, we calculate $E(F_p) = y^2 \equiv x^3 + ax + b \bmod p$. For point addition of $G(x, y)$ calculating the point addition for a given point $G + G$ and represent it by $2G$. For this case, $2G = (x_2, y_2)$. The coordinate of the addition of points can be calculated as

$S \equiv \frac{3x^2 + a}{2y} \bmod p, x_2 = S^2 - 2x \bmod p, y_2 = S(x - x_2) - y \bmod p$ when points are the same. $S \equiv \frac{y_2 - y_1}{x_2 - x_1} \bmod p, x_3 = S^2 - x_1 - x_2 \bmod p, y_3 = S(x_1 - x_3) - y_1 \bmod p$ when there are two distinct points $(x_1, y_1), (x_2, y_2)$. It is important to realize that points cannot be added or multiplied vector wise, it has to follow the formula of the elliptic curve. Worth knowing is that S is required a division, the mod cannot be divided, hence, the division is transformed in another form:

$S \equiv \frac{3x^2 + a}{2y} \bmod p = (3x^2 + a)(2y)^{-1} \bmod p$, this is the special division of Remainder.

Consider $K = kG$, where K and G are points on the elliptic curve $E(F_p)$, n is the order for G, and k is smaller than n. Given k and G, it is anything but difficult to compute K as the way of addition and multiplication. In any case, then again, given K and G, calculating k is exceptionally troublesome. Since the ECC in genuine use, on a fundamental level, takes the finite field p to be very large, and n is additionally very large, it is extremely difficult to calculate each $kG$ with k that get bigger every time. This is the numerical ways of the elliptic curve encryption calculation. Using such an approach can eventually yield successful encryptions.

## Elliptic curve encryption rules and examples

In encryption using ECC, both parties must agree on a finite field and the coefficients in the curve. (Hankerson, Darrel, and Alfred Menezes. "Elliptic Curve Public-Key Encryption Schemes.") Let me use the mathematical format I just formulated, to encrypt certain information. Generally, the steps of encryption can be the following:

1. A elliptic curve is defined by $E(F_p) = y^2 \equiv x^3 + ax + b \bmod p$ is selected by Party A and Party B. A base point G is taken from the range of $E(F_p)$

2. Party A chooses a private key k, and creates a public key K=kG by multiplying positive integer k.

3. Basic parameters such as finite prime field p and the coefficient of an elliptic curve $E(F_p)$ with selected base point G and the results of multiplication K are sent to Party B. Both parties

need to get the correct basic conditions and parameters.

4. Subsequent to accepting the information, Party B encodes the plaintext to be communicated to a point M on $E(F_p)$, and produces a random but big integer number r.

5. $C_1 = M + rK, C_2 = rG$ are calculated by Party B.

6. The calculated $C_1, C_2$ are transmitted to party A by party B.

7. Equation $C_1 - kC_2 = M + rK - krG = M + rkG - krG = M$ is used by Party A after the reception of information.

This method of encryption is more commonly known as the Elgamal password. Let me give you a specific example to apply those procedures (Hankerson 406–407). Alice has selected a elliptic curve $E(F_p) = y^2 \equiv x^3 + 5x + 2 \bmod 53$, this discrete curve looks like the following:

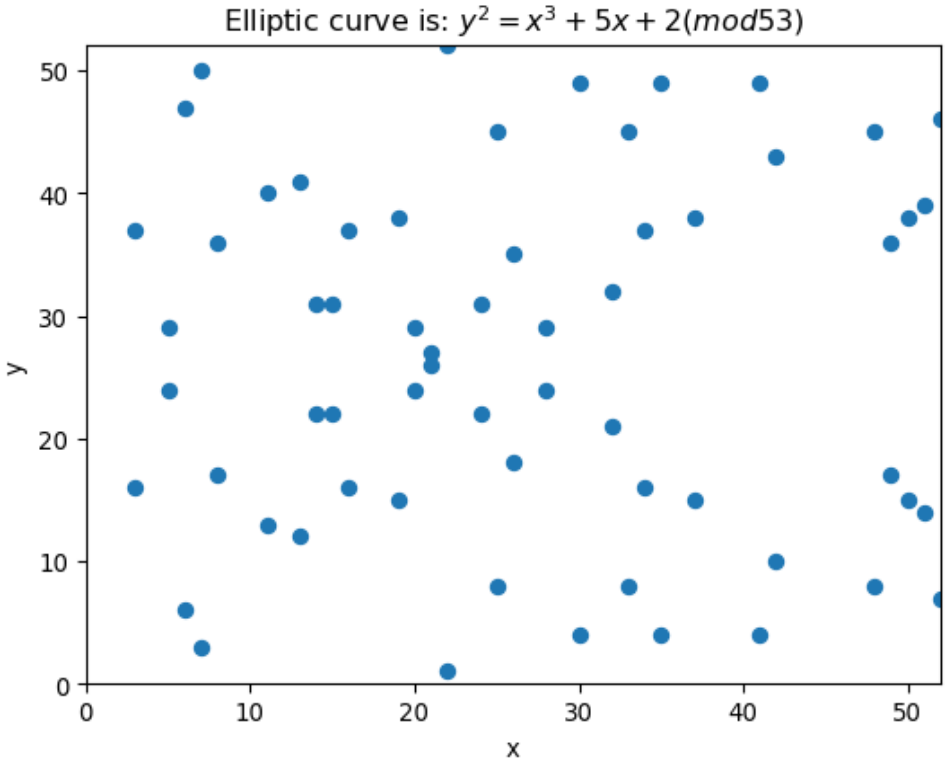


**Figure 6: the plot of an elliptic curve with equation** $E(F_p) = y^2 \equiv x^3 + 5x + 2 \bmod 53$

Alice then selects a base point G (6, 6), with the order of 21. Then, Alice select private key 2, with a public key $2(6,6) = (6,6) + (6,6)$. Using the formula introduced before, this public key has a slope of $S \equiv \frac{3*6^2+5}{2*6} \bmod 53 = (3*6^2+5)(2*6)^{-1} \bmod 53 = 113*12^{-1} \bmod 53$, using Remainder division law, $S \equiv 113*12^{-1} \bmod 53 \quad 12S \equiv 113 \bmod 53 \quad 12S \bmod 53 = 7$.

Using this equation, the value of S will be 58, because $12*58 \bmod 53 = 696 \bmod 53 = 7$.

$x_2 = (58^2 - 2*6) \bmod 53 = 3352 \bmod 53 = 13$,

$y_2 = 58(6-13) - 6 \bmod 53 = -406 - 6 \bmod 53 = -406 \bmod 53 - 6 \bmod 53 = 18 - 6 = 12$.

Therefore, the public key is (13,12). Alice sends the public key (13,12), base point G (6,6) to Bob. After Bob receives the information, he then selected a point of the curve to represent M, which is the information he wants to communicate the Alice. Bod chooses point (7,3) as M on the curve and generates a random number r as 14 (because the point M has an x coordinate of 7). Bob then starts to calculate using the same point doubling and adding formula:

$C_1 = M + rK = (7,3) + 14(13,12)$

$= (7,3) + (13,12) + (13,12) + (13,12)$

$+(13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12) + (13,12)$

$= (7,3) + (32,21)$

Using the addition equations of two distinct points:

$$S \equiv \frac{21-3}{32-7} \bmod 53 = 18*(25)^{-1} \bmod 53$$

$S \equiv 18*(25)^{-1} \bmod 53 \quad 25S \equiv 18 \bmod 53 \quad 25S \bmod 53 = 18$

S is -41 because $41*25 \bmod 53 = 1025 \bmod 53 = 18$.

$x_3 = (41)^2 - 7 - 32 \bmod 53 = 1642 \bmod 53 = 52$

$y_3 = 41(7-52) - 3 \bmod 53 = 1842 \bmod 53 = 7$

$C_1 = (52,7)$

$C_2 = 14(6,6) = (32,32)$

Bob then transmits the points $C_1, C_2$ to Alice. Alice then decodes the information using subtractions of points:

$C_1 - kC_2 = (52,7) - 2*(32,32) = (52,7) - \left[(32,32) + (32,32)\right] = (52,7) - (32,21)$

$= (52,7) + (32,-21)$

$$S \equiv \frac{-21-7}{32-52} \bmod 53 = 28*(20)^{-1} \bmod 53 \;\; S = 12$$

$x_3 = S^2 - x_1 - x_2 \bmod p = 12^2 - 52 - 32 \bmod 53 = 60 \bmod 53 = 7$

$y_3 = S(x_1 - x_3) - y_1 \bmod p = 12(52-7) - 7 \bmod 53 = 533 \bmod 53 = 3$

Hence, the message (7,3) is decrypted by Alice successfully. This example applies the

mathematical way I have deducted for encryptions. The message can be successfully transmitted. However, in real-life, the value of k and base point G is often significantly large---as large as 200 digits. Due to instrumental issue, such big sample of encryption cannot be further demonstrated in this essay, but the encryption works the same way as the encryption with small digits.

## Attacking method

The security of any open key cryptography component depends on certain numerical problems, such as IFP (Integer factorization problem), DLP (Discrete logarithm problem), and ECDLP (Elliptic curve discrete logarithm problem). The public key cryptosystem is dependent on security. Through the definite examination of different assault techniques against ECDLP, searching for specialized measures to oppose these assault strategies to guarantee that ECC has a safe numerical establishment. Summing up the presently known strategies for tackling ECDLP, they can be partitioned into two classes: techniques for general elliptic bends and strategies for exceptional elliptic curves.

## Exhaustive search

The exhaustive search is a technique normally utilized in figuring science and massive computing to discover an answer for a complex problem. It looks through the arrangement space of the issue individually to locate the right arrangement of the issue (Biehl 131–146). Of course, people can use it to try to solve ECDLP. For example, it is known that $p, Q \in E(F_p)$ Basepoint $G$ has an order of $N$. Find $k$, let $i$ satisfied the public key $K = kG$, where $k$ is a constant. The aim is to Calculate the point sequence $G, 2G, 3G, ..., kG \quad E(F_p)$ until $K = kG$ hence $k$ is the private key. Clearly, in the most pessimistic scenario, the calculation needs, at any rate, numerous means to illuminate the ECDLP, so the time unpredictability of the calculation is high, which is exponential. When the number of steps is large enough (currently greater than $2^{80}$), the algorithm becomes infeasible in terms of calculation time, so it fails. It is recommended that the elliptic curve parameters selected for ECC be at least greater than $2^{191}$.

## Baby step giant step

Before anything of this algorithm is discussed further, the basics should be discussed first. For any arbitrary constant $k$, it can be rewritten as $am + b$. For example, the constant 11 and be rewritten in the form of $2*5+1$. Now, to obtain the constant (private) key in the ECC, the ECDLP must be solved, where there is a known point $P \; and \; kP$. Now, let make $kp = A$, where

it can rewrite as $(am+b)p = A \to amp + bp = A \to bp = A - amp$. Individual $bp$ and $A - amp$ are taken and organized in an open addressing Hash table.

| $bp$ (Small step) | $A - amp$ (Giant step) |
|---|---|
| $p$ | $A - mp$ |
| $2p$ | $A - 2mp$ |
| $3p$ | $A - 3mp$ |
| $4p$ | $A - 4mp$ |
| $5p$ | $A - 5mp$ |
| $6p$ | $A - 6mp$ |

How to tell whether each point belongs to the other? When $a$ equals to a certain number, compare $kp$ with $A$ to see if they are equals. Since $k$ must be a positive integer between 0 and $m$, we can compare $A$ with all the points of $0p...mp$. In this case, the when $a = 6, k = 3$, $kp = A$. Hence, $A = (3+6m)P, k = 3+6m$ $A = (3+6m)p, k = 3+6m$. Now, the question is only about setting up the linear equation to find the value of $k$ and cross compare with the public keys $p$ and $kp$.

# Conclusion

In conclusion, using the combination of any random elliptic curve and Remainder function (mod), the keys for encryption and decryption can be hidden in the endless subgroups of any arbitrary point resulted from the function. To achieve successful decryption, methods such as exhaust search or baby-step giant step can be used. However, the keys can be as big as the $2^{191}$. As a result, attacking methods will take a huge amount of time to conduct calculations. However, the attacking method will work faster if the attacker attempts to acquire the private key k by using a quantum computer. However, the limitation of the research exists. In this research, even though the encryption of the information is achieved successfully using properties of an elliptic curve, Remainder operations, additive groups, and discrete logarithm structure, the encryption cannot be fully demonstrated with the large number due to instrumental issues. However, this limitation doesn't impair the validity and correctness of the conclusion.

***Works cited:***


Biehl, Ingrid, et al. “Differential Fault Attacks on Elliptic Curve Cryptosystems.” *Advances in Cryptology — CRYPTO 2000 Lecture Notes in Computer Science*, 2000, pp. 131–146., doi:10.1007/3-540-44598-6_8.

“The Case for Elliptic Curve Cryptography.” *The Case for Elliptic Curve Cryptography - NSA/CSS*, Nation Security Agency, 15 Jan. 2009, web.archive.org/web/20090117023500/www.nsa.gov/business/programs/elliptic_curve.shtml.

“Elliptic Curve Discrete Logarithm Based Cryptography.” *Computational Number Theory and Modern Cryptography*, 2017, pp. 353–376., doi: 10.1002/9781118188606.ch9.

Hankerson, Darrel, and Alfred Menezes. “Elliptic Curve Public-Key Encryption Schemes.” *Encyclopedia of Cryptography and Security*, 2011, pp. 406–407., doi:10.1007/978-1-4419-5906-5_250.

Kumar, D Sravana. “Encryption Of Data Using Elliptic Curve Over Finite Fields.” *International Journal of Distributed and Parallel Systems*, vol. 3, no. 1, 2012, pp. 301–308., doi:10.5121/ijdps.2012.3125.

Semaev, I. A. “Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p.” *Mathematics of Computation of the American Mathematical Society*, vol. 67, no. 221, 1998, pp. 353–356., doi:10.1090/s0025-5718-98-00887-4.

Turner, S., and D. Brown. “Elliptic Curve Private Key Structure.” 2010, doi:10.17487/rfc5915.

Velu, Jacques. “Courbes Elliptiques Munies d’Un Sous-Groupe Z/Zn*Mn.” *Mémoires De La Société Mathématique De France*, vol. 1, 1978, pp. 1–152., doi:10.24033/msmf.241.

Xin, KATIE. “The Elliptic Curve Discrete Logarithm Problem.” *Elliptic Curves in Cryptography*,

1999, pp. 79–100., doi:10.1017/cbo9781107360211.007.