International Journal of Electrical, Electronics and Computer Engineering **9**(1&2): 12-19(2020)

ISSN No. (Online): 2277-2626

Elliptic Curve Cryptography Involving two Private Keys and Public Keys

***Arun Kumar Sharma*[1] *and Nikhlesh Kumar Badoga*[2]**

[1]*Department of Computer Science & Engineering, NIT Hamirpur, India.*
[2]*Department of Computer Science & Engineering, Thapar Institute of Engineering and Technology, India.*

(Corresponding author: Arun Kumar Sharma)

(Received 13 April 2020, Accepted 27 July 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In the middle of 19th century, study of elliptic curves was started by algebraists, algebraic geometers and number of theorists. But first introduction of Elliptic curve cryptography was given in 1985 by Neal Koblitz and Victor Miller. Elliptic Curve cryptography (ECC) provides same functionality as RSA schemes in public key mechanisms. Difference lies in security of ECC which is based on hardness of elliptic curve discrete logarithmic problem (ECDLP). RSA schemes are used by most products and standards that use public key cryptography for encryption and digital signatures. Elliptic curve cryptography is competing system to RSA. We discuss the elliptic curves and illustrate the mathematical processing of the elliptic curves involving one public key and private key followed by two public keys and private keys.

Keywords: Elliptic Curve, Cryptography, Private Key, Public Key, Encryption, Decryption, Confidentiality, Authenticity, Integrity.

I. INTRODUCTION

Straight lines with the points (x, y) are the simplest curves, where x and y are related as following by an equation:

$$y = ax + b \,. \tag{1.1}$$

The next step up in complexity would involve equations like

$$y = ax^2 + bx + c \,, \tag{1.2}$$

where the right hand side has a quadratic polynomial in x. These type of equations represent parabolas.Now to get something more complicated, we can consider the equations where y also occurs as a square and written as

$$y^2 = ax^2 + bx + c \,. \tag{1.3}$$

The equation (1.3) represents an ellipse or a hyperbola. Equations (1.2) and (1.3) are examples of curves known as conic sections, because they can be obtained by cutting a cone in a suitable way. Once the degree of the polynomial in x on the right side of the equation (1.3)becomes three then, we get

$$y^2 = ax^3 + bx^2 + cx + d \,, \tag{1.4}$$

which is known as the equation of elliptic curves, [6].

Diaphantous [1] in his work gave us elliptic curves for first time. A typical example was given by Diaphantous: a number, say 7, which denotes the difference of two cubes i.e. $(7 = 8 - 1)$, we have to find the rational numbers a and b such that $7 = a^3 + b^3$ (the numbers involving Diaphantous' numbers need to be positive rational numbers, otherwise problem would become trivial). Much later Newton, Lucas and Sylvester discovered that there exists a very important geometric interpretation. The integral solution for the equation $a^3 + b^3 = n$ can be obtained by elliptic curves. Set $a = \frac{36n+y}{6x}$ and $b = \frac{36n-y}{6x}$, we get the transformed equation as $y^2 = x^3 - 432\,n^2$, an elliptic curve. In the above example, if we take the following curve $E: x^3 - y^3 = 7$ and the point $P = (2,1)$ which needs to be rational. Then the tangent to the curve$E$ at P will intersect the curve E in another rational point Q. Fermant and Euler considered Diophantine problems a big thing but then Gauss by providing quadratic reciprocity law started giving number theory a new direction. During these times, elliptic curves were studied mainly by number theorists like Cauchy, Lucas, Sylvester, Poincare and Beppo Lavi as well as by complex algebraic geometers like Clebsch or Juel. In 1890 Juel gave geometric interpretation of group law. Poincare in 1901questioned about rational points on elliptic curves being finitely generated which was proved by Murdell in 1922. The modern theory took off in the 1930 with Hasse's work on the number of points on elliptic curves over finite fields, [5, 17, 19]. The use of elliptic curves for factoring integers was found by Lenstra [8], and their use for proving Fermat's last theorem was discovered by Frey [11] be used for proving Fermat's last theorem and now elliptic curves are used for safe communication.

The general equation of elliptic curve is

$$E(K)\colon\ y^2 + uxy + vy = x^3 + ax^2 + bx + c \,, \tag{1.5}$$

where u, v, a, b, c are elements of field K. Let K be a field of characteristic two, than an elliptic curve over K is the set of points satisfying an equation of type

$$E(K)\colon\ y^2 + xy = x^3 + ax + b \qquad (1.6)$$

or

$$E(K)\colon\ y^2 + xy = x^3 + ax^2 + b. \qquad (1.7)$$

If K denotes the field of characteristic not equal to 2, then by using transformation

$$y \to \frac{y - (ux + v)}{2},$$

equation (1.5) can be simplified as

$$E(K)\colon\ y^2 = x^3 + ax^2 + bx + c, \qquad (1.8)$$

and if K is a field of characteristic not equal to 3 also, then by using transformation

$$x \to x - \frac{d}{3},$$

the equation (1.8) becomes

$$E(K)\colon\ y^2 = x^3 + ax + b\,. \qquad (1.9)$$

(a) Elliptic Curves Over Rationals

If a and b are rational numbers in equation (1.9), then it is known as the elliptic curve over the field $\mathbb{Q}$ of rational numbers. In many areas of number theory, study of the group $E(\mathbb{Q})$continued to play a fundamental role. When a landmark result which described $E(\mathbb{Q})$ was proved by L.J. Mordell, the modern theory of Diophantine equations as well as the solution of polynomial equations using integers or rational numbers was initiated in 1922.

Theorem (Mordell, 1922) [16] : Let E denotes an elliptic curve as defined in (1.9), with $a, b \in \mathbb{Q}$then the group which is formed by rational points on $E(\mathbb{Q})$ is an abelian group that is finitely generated. Moreover, there exista set of points $P_1, P_2, \ldots\ldots.., P_t \in E(\mathbb{Q})$ that are finite such that every point $P \in E(\mathbb{Q})$ could be written in the form

$$P = n_1P_1 + n_2P_2 + \cdots \ldots + n_tP_t \qquad (1.10)$$

for some $n_{1,}n_{2,} \ldots., n_t \in \mathbb{Z}$.

(b) Elliptic Curves Over Real Numbers

Elliptic curves bearing no direct relation to ellipses are cubic equations in 2 variables. These are same as equations used for calculation of length of curve in circumference of an ellipse. The general equation that denotes an elliptic curve is (1.5). A special class of the form (1.9) of elliptic curves is used. In this equation if $4a^3 + 27b^2 \neq 0$, the equation represents a non-singular elliptic curve; or else, the equation represents an elliptic curve that is singular in nature. In case of non-singular elliptic curve, the equation$x^3 + ax + b = 0$, has three distinct roots which may be real or complex, and in case of elliptic curves which are singular, the equation $x^3 + ax + b = 0$ do not contain three distinct roots. Non singular curves are used for data encryption since singular curves cannot be used these days as they now become easy to crack. It is clearly evident that left hand side has a degree two and right hand side has degree 3. If all roots are real, horizontal lines can intersect curves in three points whereas vertical line intersects curves mostly at two points [3].

Example: Let the below mentioned elliptic curves represents two equations:

$$y^2 = x^3 - \qquad (1.11)$$

and

$$y^2 = x^3 + x\,, \qquad (1.12)$$

both are non-singular. However, the equation (1.11) has three real roots $x = -1{,}0{,}1$.
but the equation (1.12)contains only one real root,$x = 0$ and two imaginary ones.

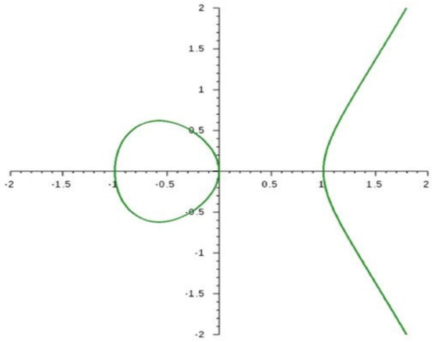


Fig. 1. The Elliptic Curve$y^2 = x^3 - x$

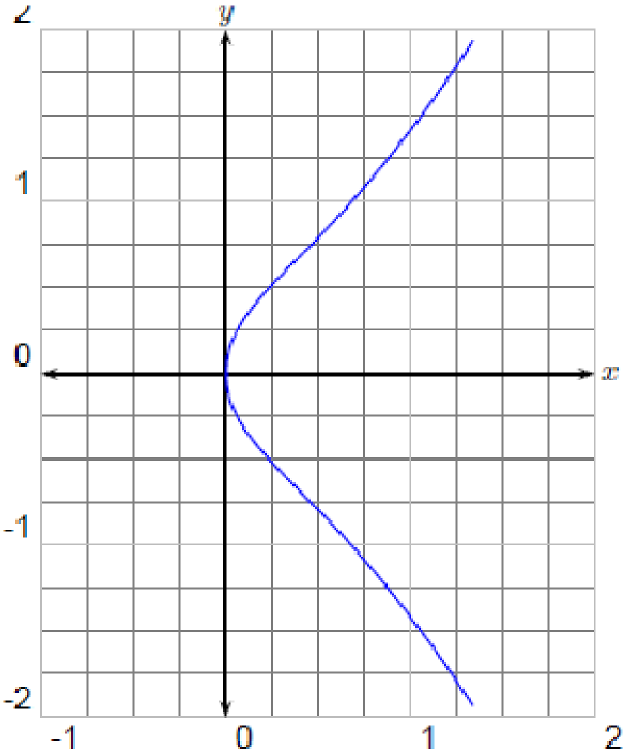


Fig. 2. The elliptic curve $y^2 = x^3 + x$.

(a) Elliptic Curves Over Complex Numbers

Let E denote elliptic curve which is defined over the field $\mathbb{C}$ of complex numbers or say $E(\mathbb{C})$. Thus, E is equal to the set of all pairs (x, y) of complex numbers that satisfy equation (1.9), including the point at infinity$\mathcal{O}$.

Although E denotes curve, if we take into account the concept of geometrical pictures, it is two-dimensional, whose co-ordinates signifies the real and imaginary parts of x and y [7].

(b) Elliptic Curves Over Finite Field

When the coefficients a, b and x, y are restricted to the element of a finite field $\mathbb{Z}_p$ in equation (1.9), then the elliptic curves are known as prime curves. These prime curves are very important for cryptographic applications. To define elliptic curves over $\mathbb{Z}_p$, a cubic equation is used, whose coefficients and variables belong to the set of integers $\mathbb{Z}_p = 0, 1, 2, 3, \ldots, p-1$, which is stated as

$E_p(a, b)$: $y^2 \; mod \; p = (x^3 + ax + b) \; mod \; p$,
(1.13)

with the condition $4a^3 + 27b^2 \neq 0$.

Zero point is the set$E_p(a, b)$, that has all pairs of integers (x, y),which fulfil above equation (1.13), along with point $\mathcal{O}$.

Example: Let $a = -1$, $b = 0$ and $p = 11$, then the equation (1.13) becomes

$E_{11}(-1, 0)$: $y^2 \; mod \; 11 = (x^3 - x) \; mod \; 11$.
(1.14)

The equation (1.14) consist of the following elements:

$$E_{11}(-1,0) = (0,0),(1,0),(4,4),(4,7),(6,1),(6,10),(8,3),(8,8),(9,4),(9,7),(10,0) .$$

(c) Elliptic Curves Over *Gf* (2^n)

The set $GF(2^n)$ consists 2^n elements.An elliptic curve E defined over finite field F_{2^n} is represented with the help of the equation

$$E(F_{2^n}) : \; y^2 + xy = x^3 + ax^2 + b \qquad (1.15)$$

where $x, y, a, b \in F_{2^n}$.The points on E are denoted as$E(F_{2^n}) = \{ (x, y) : x, y \; \in \; F_{2^n}$and satisfy $y^2 + xy = x^3 + ax^2 + b\} \cup \{\mathcal{O}\}$.

The mathematical tools of various cryptosystems are modular multiplication and modular exponentiation. The addition and multiple addition in $E_p(a, b)$ or $E_{2^n}(a, b)$ are the mathematical tools for cryptographic applications. In other words, the addition in elliptic curve cryptography plays same role as modular multiplication in other cryptosystem and multiple addition plays the role which is similar to modular exponentiation in other cryptosystems like RSA cryptosystems [4,10,13, 15, 18].

(II)

(A) ELLIPTIC CURVE CRYPTOGRAPHY INVOLVING SINGLE PRIVATE KEY AND SINGLE PUBLIC KEY

In case of RSA cryptosystem modular multiplication and modular exponentiation are two mathematical tools, which are used for cryptographic applications. In the same way, we use addition and multiple additions in $E_p(a, b)$ or $E_{2^n}(a, b)$ as mathematical tools for cryptographic applications.We know that the security that corresponds to RSA cryptosystem involves a hard problem of factoring the product of two large primes. On the other side, El Gamal cryptosystem signifies the difficulty of discrete logarithm. Now, if we want to design a cryptosystem making use of elliptic curves, we require to search a hard problem similar to RSA and ElGamal. For our purpose, assume the equation $Q = kP$, where $P, Q \in E_p(a, b)$ and $k < p$. In this case Q can be calculated easily for given k and P. But it is relatively very difficult to compute$k$ for a given P and Q. This problem that consists of elliptic curves is called discrete logarithm problem. The number k is called discrete logarithm of Q to the base P, [7, 9].

Example: The elliptic curve which is defined by

$$y^2 = x^3 + 9x + 17 \text{ over} F_{23} ,$$

is a group. The discrete logarithm k of $Q = (4, 5)$that corresponds to the base $= (16, 5)$ is required.To evaluate$k$,we have to compute multiples of P until Q is found. The initial multiples of $P$are $P = (16,5), 2P = (20,20), 3P = (14,14)$, $4P = (19,20)$, $5P = (13,10)$, $6P = (7,3), 7P = (8,7)$, $8P = (12,17)$, $9P = (4,5)$. Since $9P = (4,5) = Q$ the discrete logarithm of Q to the base $P \; is \; k = 9$ .In practical application, k would be large enough such that it would not be possible to determine k particularlyusing this manner.

Key Generation in ECC

To generate the public and private key in ECC. The user A picks a large prime p and elliptic curves parameters$a$ and b for equation

$$y^2 \; mod \; p = (x^3 + ax + b) \; mod \; p .$$

Next he chooses a point $G = (x_1, \, y_1) \in E_p(a, b)$, whose order is very large value n. This point G is called base point and the order of G means,$nG = 0$, such that n is the smallest positive integer. Any user A picks $n_A < n$ and computes

$$P_A = n_A \times G .$$

The number n_A is the private key and P_A is the public key of the user A. It is clear that $P_A \in E_p(a \, , b)$.

Key Exchange in ECC

Consider two users Alice (public key P_A, private key n_A) and Bob (public key P_B, private key n_B) want to exchange their keys. This key exchange depends on the following steps:

1). Alice sends P_A to Bob.
2). Bob calculates$k = n_B \times P_A = n_B \times (n_A \times G)$.
3). Bob sends P_B to Alice.
4). Alice calculates$k = n_A \times P_B = n_A \times (n_B \times G)$.

Thus, they can share the key $k = n_A n_B G$.

Example: Let $p = 211$, $a = 0$, $b = -4$, therefore, the curve is

$y^2 \, mod \, 211 = (x^3 - 4) \, mod \, 211, \qquad G = (2,2)$.

To generate the public key and private key, the user Bob chooses$n_B = 121$, then the public key of user Bob is $P_B = n_B \times G = 121(2,2) = (115,48)$.

Similarly Alice chooses her private key $n_A = 203$ and computes her public key

$$\begin{aligned} P_A &= n_A \times G \\ &= 203\,(2,2) \\ &= (130,203). \end{aligned}$$

The shared key is

$$k = 121(130,203) = 203(115,48) = (161,69).$$

Encryption in ECC

Elliptic curve cryptosystem can be used for encryption and decryption. Let the user Alice wants to encrypt a message m for the user Bob, then the following steps are involved:

Alice encodes the message m as $P_m = (x,y)$.

A random number k is chosen by Alice and produces the cipher text

$$C_m = [k \times G, P_m + k \times P_B]$$

and sends this cipher text C_m to Bob.

Remark: Initially the English language message will be converted into the numerical message m. Then m will be connected with some point of the elliptic curve with given methods discussed in the literature of elliptic curve cryptography.

Decryption in ECC

To decrypt the message, Bob works as follows:

Bob computes $n_B \times k \times G$,

Bob again computes

$$\begin{aligned} &P_m + k \times P_B - n_B \times k \times G \\ &= P_m + k \times P_B - k \times (n_B \times G) \\ &= P_m + k \times P_B - k \times P_B \\ &= P_m. \end{aligned}$$

In other words, we can say Bob picks the first co-ordinate $k \times G$ of C_m, multiply this with his private key and then subtract this from the second point $P_m + kP_B$.

(B) ELLIPTIC CURVE CRYPTOGRAPHY INVOLVING TWO PRIVATE KEYS AND TWO PUBLIC KEYS

The security of the elliptic curve cryptography depends on how difficult it is to find the value of k for given value of kP, the Elliptic Curve Discrete Logarithmic Problem (ECDLP). To enhance the security level in this work, it is proposed that both the sender and the receiver use two private keys and two public keys.

Proposed Method

Considering Alice and Bob as two communicating parties who want to convey the messages they agreed upon using elliptic curves $E_p(a,b)$, where p denotes prime number and a point C which is randomly selected on the elliptic curve. A large number α which is random is selected by Alice which is less than the order of $E_p(a,b)$ and a point A on the elliptic curve. The value of $A_1 = \alpha(C + A)$is computed by Alice and also the value of $A_2 = \alpha A$. The random number α and the point A is chosen as private keys of Alice and publishesA_1 andA_2 as her general public keys. Similarly a large random number β and a point B is selected by Bob on the elliptic curve. Bob further computes the value of $B_1 = \beta(C + B)$ and$B_2 = \beta B$. He keeps the random number β and the point B as his private keys and B_1 andB_2 as his general public keys are published upon. After deciding on publication of public key, calculation of following quantities by communicating parties and their publishment as specific public keys of each other is agreed upon. $A_B = \alpha B_2$ is calculated by Alice and published as specific public key for Bob which is used by Alice.$B_A = \beta A_2$ is calculated by Bob and published as specific public key for Alice which is used by Bob, [5]. We can summerise as follows:

-Alice's private key$_1 = \alpha$, a large random number which is less than the order denoted by the generator.

-Alice's private key$_2 = A$, a point on the elliptic curve$E_p(a,b)$.

-Alice's general public key$_1$ $= A_1$, a pointon the elliptic curve$E_p(a,b)$.

-Alice's general public key$_2$ $= A_2$, a pointon the elliptic curve $E_p(a,b)$.

-Alice's specific public key to be used for Bob $= A_B$, a point on the elliptic curve$E_p(a,b)$.

-The private key$_1$ $of\ Bob = \beta$, a large random number less than the order of the generator.

-The private key$_2$ $of\ Bob = B$, a point on the elliptic curve$E_p(a,b)$.

-General public key$_1$ $of\ Bob = B_1$, a point on the elliptic curve$E_p(a,b)$.

-General public key$_2$ $of\ Bob = B_2$, a point on the elliptic curve$E_p(a,b)$.

-Specific public key for Alice $= B_A$ to be used by Bob, a point on the elliptic curve$E_p(a,b)$.

Encryption

If Bob is willing to communicate message M, then using code table agreed upon by communicating parties Alice and Bob, the characters of message are coded to points on the elliptic curve. After wards each message point is encrypted to cipher pointsE_1, E_2 making a pair. A random number $\gamma$is used which is different for the encryption of different message points. The cipher points are

$$E_1 = \gamma C$$

and

$$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B.$$

Using code table, Bob connects the pair of points of each message point into text characters. Then Alice is communicated the cipher text by Bob in public channel.

Decryption

On receiving cipher text, these texts are converted to points on elliptic curves by Alice and she recognizes the points E_1 and E_2 of each character followed by decryption of message as below:

Decryption Works Out Property:

$$
\begin{aligned}
(\beta+\gamma)A_1-\gamma A_2+A_B &= \gamma(A_1-A_2)+\beta A_1+A_B \\
&= \gamma\alpha C+\beta\alpha C+\beta\alpha A+\beta\alpha B \\
&= \gamma\alpha C+\beta\alpha(A+B+C) \\
\alpha E_1+\alpha B_1+B_A &= \alpha\gamma C+\alpha\beta C+\alpha\beta B+\alpha\beta A \\
&= \gamma\alpha C+\beta\alpha(A+B+C)\,.
\end{aligned}
$$

Therefore,

$$(\beta+\gamma)A_1-\gamma A_2+A_B=\alpha E_1+\alpha B_1+B_A$$

and

$$
\begin{aligned}
E_2-(\alpha E_1+\alpha B_1+B_A) &= [M+(\beta+\gamma)A_1-\gamma A_2+A_B] \\
&\quad -[\alpha E_1+\alpha B_1+B_A] \\
&= M+[\gamma\alpha C+\beta\alpha(A+B+C)] \\
&\quad -[\gamma\alpha C+\beta\alpha(A+B+C)] \\
&= M\,.
\end{aligned}
$$

III. ILLUSTRATION

Example: If the cryptosystem parameters are $E_{23}(1,1)$, $G=(3,10)$ and the private key of the user B is$n_B=4$, then

a) Find the public key of the user B.

b) Find the cipher text C_m for the message $P_m=(6,4)$ by taking $k=2$.

c) How can the user B recover the plain text P_m ?

Solution :

a) The user B's public key is given by

$$
\begin{aligned}
P_B &= n_B\times G \\
&= 4\times(3,10) \\
&= (17,3)\,.
\end{aligned}
$$

b) The cipher text C_m for the message $P_m=(6,4)$ is

$$C_m=[k\times G, P_m+k\times P_B]\,.$$

First compute

$$
\begin{aligned}
k\times G &= 2\times(3,10) \\
&= (7,12)\,,
\end{aligned}
$$

and then

$$
\begin{aligned}
P_m+k\times P_B &= (6,4)+2(17,3) \\
&= (6,4)+(13,16) \\
&= (6,19)\,.
\end{aligned}
$$

c) To recover the plain text P_m from C_m, the user B computes the following steps:

B computes

$$
\begin{aligned}
n_B\times k\times G &= 4\times 2(3,10) \\
&= 8\times(3,10) \\
&= (13,16)\,.
\end{aligned}
$$

Now B computes

$$
\begin{aligned}
P_m+k\times P_B-n_B\times k\times G &= (6,19)-(13,16) \\
&= (6,4) \\
&= P_m\,.
\end{aligned}
$$

Hence, the user B can recover the corresponding plain text

$$P_m=(6,4)\,.$$

Example: Consider an elliptic curve

$$y^2=x^3+2x+9\,.$$

Its graph is shown below:

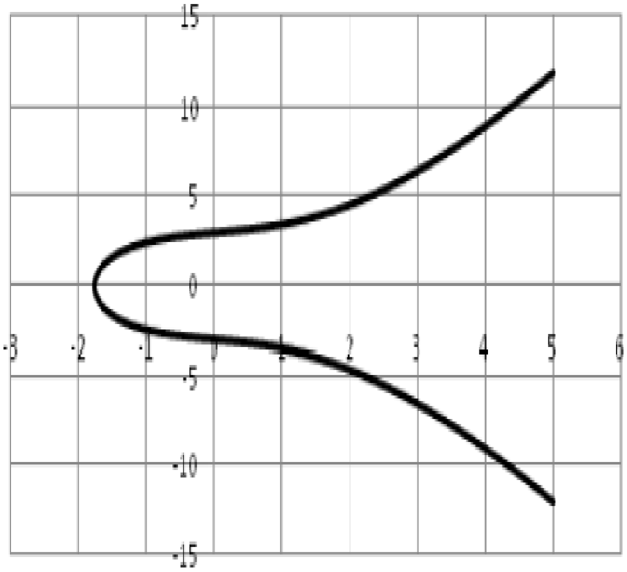


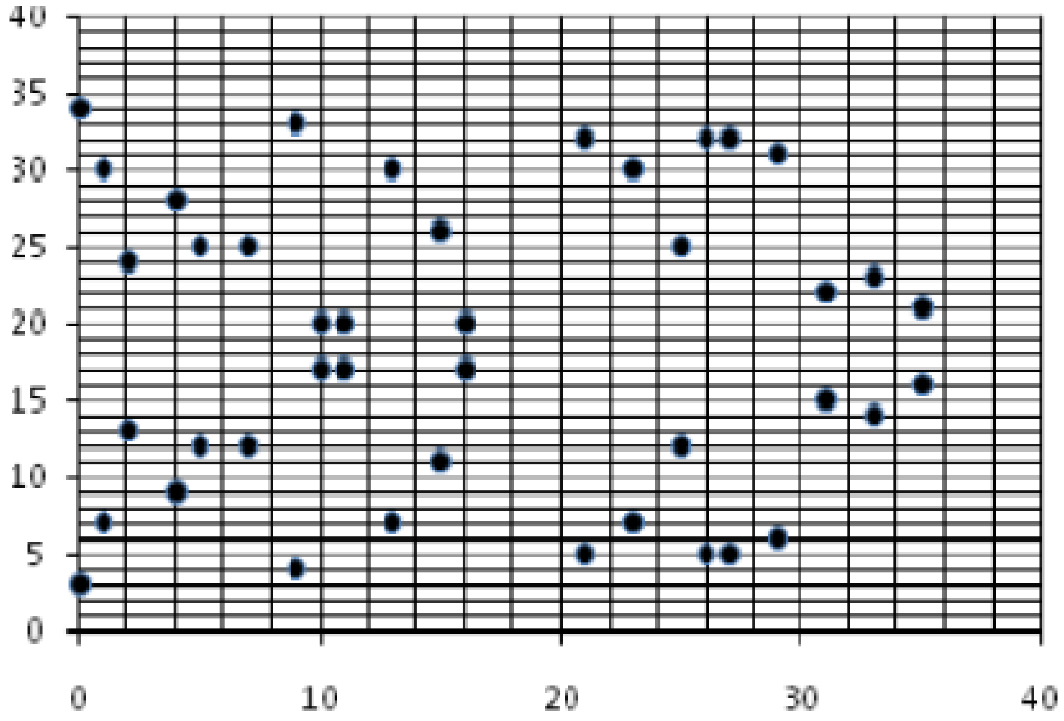
Fig. 3. Elliptic Curve$y^2=x^3+2x+9$.

Now the elliptic curve denoted by:

$E_{37}(2,9)$: $(y^2=x^3+2x+9)\ mod\ 37$,

The points defined for the elliptic curve $E_{37}(2,9)$ are as follows:

$$
\left\{
\begin{array}{c}
\infty,(5,25),(1,30),(21,32),(7,25),(25,12),(4,28),(0,34),(16,17),(15,26), \\
(27,32),(9,4),(2,24),(26\ ,5),(33,14),(11,17),(31,22),(13,30),(35,21), \\
(23,7),(10,17),(29,6),(29,31),(10,20),(23,30),(35,16),(13,7),(31,15), \\
(11,20),(33,23),(26,32),(2,13),(9,33),(27,5),(15,11),(16,20),(0,3), \\
(4,9),(25,25),(7,12),(21,5),(1,7),(5,12),
\end{array}
\right\}
$$



$E_{37}(2,9)\colon\ y^2 = x^3 + 2x + 9\ mod\ 37$

Fig. 4.

Let $C = (9,\ 4)$. A number $\alpha = 5$ which is random is selected by Alice, any let $A = (10,\ 20)$be any point on the elliptic curve. Alice computes

$$A_1 = \alpha(C + A)$$
$$= 5[(9,4) + (10,20)]$$
$$= (1,7)\,,$$
$$A_2\ = \alpha A$$
$$= (33,23)\,.$$

The random number $\alpha\ = 5$ and the point A is kept by Alice on the elliptic curve as her secrete keys and publishesA_1 andA_2 as the public keys of Alice.

The values of $\beta = 7, B = (11,20)$ on the elliptic curve is selected by Bob. He further computes

$$B_1 = \beta(C + B)$$
$$= (11,17)\,,$$
$$B_2 = \beta B$$
$$= (23,30)\,.$$

He keeps the random number $\beta\ = 7$ and the point B on the elliptic curve as his secrete keys and publishesB_1 andB_2 as his public keys.

Alice calculates$A_B = \alpha B_2 = (15,11)$,

and Bob calculates$B_A = \beta A_2 = (2,13)$.

A_B as the specific public key for Bob is published by Alice and B_A as specific public key for Alice is published by Bob.

Encryption

Suppose Bob has to communicate message 'attack' to Alice. He will begin with converting all text characters of message into points on elliptic curves with the help of code table they agreed upon as given below:

*	a	b	c	d	e	f	g	h
∞	(5,25)	(1,30)	(21,32)	(7,25)	(25,12)	(4,28)	(0,34)	(16,17)
I	j	k	l	m	n	o	p	q
(15,26)	(27,32)	(9,4)	(2,24)	(26,5)	(33,14)	(11,17)	(31,22)	(13,30)
r	s	t	u	v	w	x	y	z
(35,21)	(23,7)	(10,17)	(29,6)	(29,31)	(10,20)	(23,30)	(35,16)	(13,7)

1	2	3	4	5	6	7	8	9	0
(31,15)	(11,20)	(33,23)	(26,32)	(2,13)	(9,33)	(27,5)	(15,11)	(16,20)	(0,3)
#	@	!	&	$	%				
(4,9)	(25,25)	(7,12)	(21,5)	(1,7)	(5,12)				

1). In the message 'attack' the first character 'a' signifies the point$(5,25)$using the code table. A random number$\gamma = 8$is selected by Rob for encrypting the character 'a'. Then the point $(5,25)$ is encrypted as $E_1 = \gamma C = (1,30)$ which further points to the character 'b' in the conversion table.

$$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (2,13),$$

this corresponds to '5' in the table. So the character 'a' in the plain text is encrypted to the two characters$\{b,5\}$ in the cipher text.

2). 't' is a point$(10,17)$ in the code table. Let$\gamma = 12$. $E_1 = (21,32)$, this points to 'c' in the code table.

$$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (2,24),$$

this points s to 'l' in the code table. So 'l' is encrypted as$\{c,l\}$.

3). 't' is a point $(10,17)$ in the code table. let$\gamma = 19$.

$$E_1 = (4,9),$$ this points to '#' in the code table.

$$E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (27,32),$$

this pointsto 'j' in the code table. So 't' is encrypted as $\{\#,j\}$.

4). 'a' is a point $(5,25)$ in the code table. Let $\gamma = 2$. $E_1 = (29,31)$, this points to 'v' in the code table. $E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (1,30)$, this points to '$b$' in the code table. So 'c' is encrypted as$\{v,b\}$.

5). 'c' is a point $(21,32)$ in the code table. Let$\gamma = 3$. $E_1 = (1,30)$, this points to 'b' in the code table. $E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (31,22)$, this points to '$p$' in the code table. So 'a' is encrypted as$\{b,p\}$.

6). 'k' is a point $(9,4)$ in the code table. Let$\gamma = 23$. $E_1 = (25,25)$, this points to @ in the code table. $E_2 = M + (\beta + \gamma)A_1 - \gamma A_2 + A_B = (4,28)$, this points to '$f$' in the code table. So 'k' is encrypted as$\{@,f\}$.

Bob communicates $\{b,5; c,l; \#,j; v,b; b,p; @,f\}$ as the cipher text to Alice in public channel.

Decryption

The cipher text $\{b,5; c,l; \#,j; v,b; b,p; @,f\}$ after having been received by Alice is converted by using the cipher characters into the points

$$(1,30),(2,13);\ (21,32),(2,24);\ (4,9),(27,32);\ (29,31),(1,30);\ (1,30),$$
$$(31,22);(25,25),(4,28).$$

By taking two points E_1 andE_2at a time the message is decrypted by Alice.

1).$M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (5,25)$, which is represented by the character 'a' in the code table.

2).$M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (10,17)$, which is represented by the character 't' in the code table.

3).$M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (10,17)$, which is represented by the character 't' in the code table.

4).$M = E_2 - (E_1 + \alpha B_1 + B_A) = (5,25)$, which is represented by the character 'a' in the code table.

5).$M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (21,32)$, which corresponds to the character 'c' in the code table.

6).$M = E_2 - (\alpha E_1 + \alpha B_1 + B_A) = (9,4)$, which is represented by the character 'k' in the code table.

Therefore, '**attack**' is the original message.

IV. APPLICATIONS OF ELLIPTIC CURVES

1). Elliptic Curves used for factoring integers [8].

2). Elliptic Curves used for proving Fermat's Last Theorem [11].

3). Elliptic Curves used for Primality Testing [2].

4). Elliptic Curves used in Public key Cryptography [9].

5). Key exchange.

6). Digital signature.

7). Authentication.

8). Content Based Filtering in Recommender Systems [12].

9). Safety and security of Recommender Systems [14].

10). In Smart card companies such as Gem plus are also using Elliptic Curve Cryptography to improve their product's security.

V. CONCLUSION

We discussed the mathematical structures of Elliptic Curves. The use of these Elliptic curves improved the security of the message which traverse over the insecure channels. Further we discussed the elliptic curves cryptography involving one public key and private key followed by two public keys and private keys. Also we illustrated both of these structures mathematically.

REFERENCES

[1]. Bashmakova, I. G., & Silverman, J. H. (1997). *Diophantus and Diophantine equations* (No. 20). Cambridge University Press.

[2]. Bressoud, D. M. (2012). *Factorization and primality testing*. Springer Science & Business Media.

[3]. Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security*. Mc Graw Hill Education (India) Private Limited.

[4]. Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). *Guide to elliptic curve cryptography*. Springer Science & Business Media.

[5]. Koblitz, N. (1998, August). An elliptic curve implementation of the finite field digital signature algorithm. In *Annual International Cryptology Conference* (pp. 327-337). Springer, Berlin, Heidelberg.

[6]. Koblitz, N. I. (2012). *Introduction to elliptic curves and modular forms* (Vol. 97). Springer Science & Business Media.

[7]. Koblitz, N., & Menezes, A. (2005, December). Pairing-based cryptography at high security levels. In *IMA International Conference on Cryptography and Coding* (pp. 13-36). Springer, Berlin, Heidelberg.

[8]. Lenstra Jr, H. W. (1987). Factoring integers with elliptic curves. *Annals of mathematics*, 649-673.

[9]. Menezes, A. J. (1993). *Elliptic curve public key cryptosystems* (Vol. 234). Springer Science & Business Media.

[10]. Rosing, M. (1999). *Implementing elliptic curve cryptography*. Manning Publications Co.

[11]. Schoen, R. M., & Yau, S. T. (1997). *Lectures on harmonic maps* (Vol. 2). Amer Mathematical Society.

[12]. Sharma, A. K. (2018). Content-Based Filtering in Movie Recommendation. *International Journal of Electrical, Electronics and Computer Engineering*, *7*(2): 106-109.

[13]. Sharma, A. K. (2019). Design and Mathematical Structure of Cryptographic Hash Function SHA-512. *International Journal of Theoretical & Applied Sciences, 11*(2): 41-47.

[14]. Sharma, A. K. (2019). Safety Application in Android. *International Journal on Emerging Technologies, 10*(1): 234-238.

[15]. Sharma, A. K., & Badoga, N. K. (2020). Digital Signatures Using RSA Public Key Cryptosystem Scheme. *International Journal of Theoretical & Applied Sciences, 12*(1): 37-42.

[16]. Silverman, J. H. (2006). An introduction to the theory of elliptic curves. *Brown University. June*, *19*.

[17]. Srinivasa Rao, O., Charan, A., Rauniyar, S., Sannapareddy, P., & Mudrageda, I. (2016). Plain Text Encryption and Decryption Time Comparison Using ECC. *E-Commerce for Future & Trends*, *1*(1), 11-14.

[18]. Stallings, W. (2007). A text book of Cryptography and Network security. *Principles and practices, Pearson education.*

[19]. Sundriyal, S. (2008). Counting points on elliptic curves over Zp.