International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Elliptic Curve Cryptography using a Diophantine Triple, constructed through Tetradecagonal Numbers

Bindu V. A. [1], Manju Somanath [2], Radhika Das [3]

Submitted: 06/05/2024 **Revised**: 19/06/2024 **Accepted**: 26/06/2024

Abstract The world of Mathematics has time and again thrown mysterious patterns at us and left it for us humans to decipher and unravel the reasons for such consistency. One such structure that has left a mark in its midst is that of a polygonal number. We are all conversant with the Polygon which by mere definition shows that it is a close plane figure of three or more sides and angles. Extending this definition further takes us to Tetradecagon, which is known as a 14-sided polygon. We identified a Diophantine triple from two special Tetradecagonal numbers a, b with property $D(f(n))$. Using this property, we extended our research to include Elliptic Curve Cryptography.

Keywords: *Diophantine triples, Tetradecagonal numbers, Pell equation, Elliptic curve, Elliptic curve cryptography.*

1. Introduction

Let n be an integer. A set of positive integers $\{a_1, a_2, \dots, a_m\}$ is said to have the property $D(n)$, if $a_i\, a_j + n$ is a perfect square for all $1 \le i \le j \le m$; such a set is called a Diophantine m-tuple or a Pn set of size m. The problem of construction of such set was studied by Diophantus. The first set of four positive integers with the above property was found by Fermat and it was $\{1,3,8,120\}$. Many mathematicians considered the problem of the existence of Diophantine quadruples with the property $D(n)$ for any arbitrary integer n and for any linear polynomial and polynomial of degree two in n. Further, various authors considered the connections of the problems of Diophantus.

The concept of the Tetradecagon can be traced back to the times of ancient Greece and the Greek Mathematician Euclid; who has studied these structures in detail and presented them in his book called "Elements" in the year 300BC. Building our knowhow around the Tetradecagon, we find striking properties that emphasises scope for an extensive area of application using these properties. One such property that comes to the fore are the 14 exterior angles which are all equal and measures 25.7142 degrees each and 14 interior angles which are 154.2857 degrees each. Using such unique properties exhibited by the Tetradecagonal structure; we came across to find the Diophantine triples from special polygonal number known by the name Tetradecagonal numbers.

Let's also know a bit of cryptography before we delve into the solution. Cryptography has been in existence since the ancient Greeks, Egyptians. Though it has a simple and humble origin in the past, but it has now culminated into a more advanced stream of science powered by Mathematics. With data being available and shared on the internet and on the Global communication highways; it has become more important and crucial to safeguard the data, protect it and make it more secure. Cryptography can be broadly classified as (1) Secret Key cryptography (2) Public Key cryptography and (3) Hash Functions.

Secret key cryptography falls into the category of Symmetric Encryption. Examples are (i) AES – Advanced Encryption Standard (ii) DES – Data Encryption Standard (iii) Caesar Cipher.

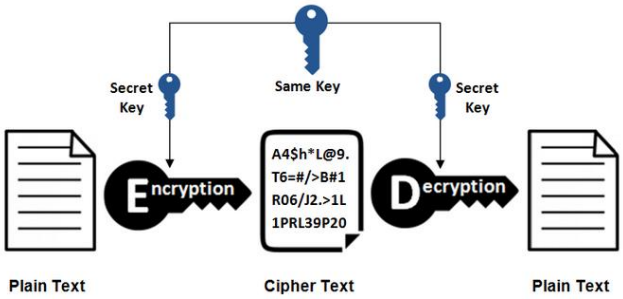

Fig 1: The figure shows the methodology used in implementing the Symmetric Encryption.

Public Key cryptography is categorized as Asymmetric Encryption. Examples are (i) ECC – Elliptic Curve Cryptography (ii) Diffie-Hellman Protocol (iii) DSS – Digital Signature Standard.

[1] *Rajagiri School of Engineering & Technology, Kakkanad, Cochin, Kerala, India*
Research Scholar, Department of Mathematics, National College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India. binduva@rajagiritech.edu.in
[2] *Department of Mathematics, National College, (Affiliated to Bharathidasan University), Tiruchirappalli, Tamil Nadu, India. manjusomanath@nct.ac.in*
[3] *Rajagiri School of Engineering & Technology, Kakkanad, Cochin, Kerala, India*
Research Scholar, Department of Mathematics, National College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India. radhikad@rajagiritech.edu.in

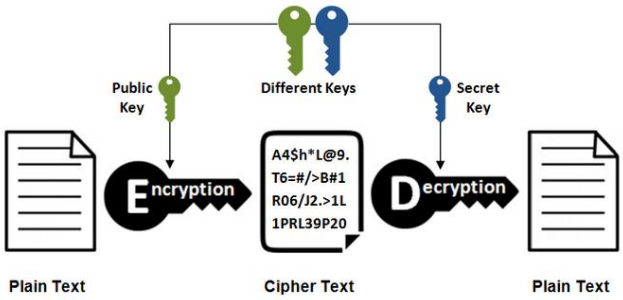

Fig 2: The figure shows the generic implementation of the Elliptic Curve Cryptography exhibiting the Asymmetric nature of encryption/ decryption

2. Priliminaries

An elliptic curve for Elliptic curve cryptography purposes is a plane curve over a finite field which is made up of the points satisfying the equation $E_p(a,b): y^2 = (x^3 + ax + b)$, where the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. If P and Q are two points on the elliptic curve $E_p(a,b)$ then point addition can be done as follows. Assume $P + Q = (x_3, y_3)$ then

$$x_3 = (\lambda^2 - x_1 - x_2)(mod\ p)$$

$$y_3 = (\lambda(x_1 - x_3) - y_1))\ (mod\ p)$$

$$\lambda = \begin{cases} \frac{3x_1^2 + a}{2y_1}(mod\ p), & if\ P = Q \\ \frac{y_2 - y_1}{x_2 - x_1}(mod\ p), & if\ P \neq Q. \end{cases}$$

3. Method of Analysis

Section A

(i) Let $a = 6n^2 - 5n$ and $b = 6n^2 + 7n + 1$ be tetradecagonal numbers of rank n and $n+1$ respectively such that $ab + 42n^2 + 7n + 1$ is a perfect square, say $r^2 = (6n^2 + n + 1)^2$. Let c be any non-zero integer such that

$$ac + 42n^2 + 7n + 1 = s^2 \ldots\ldots\ldots\ldots \quad (1)$$

$$bc + 42n^2 + 7n + 1 = t^2 \ldots\ldots\ldots\ldots \quad (2)$$

Giving a transformation $s = X + aY, t = X + bY$ in equations (1) and (2)we get a Pellian equation $X^2 - abY^2 = 42n^2 + 7n + 1$, has fundamental solution $(X_0, Y_0) = (6n^2 + n + 1, 1)$.The equations (1) and (2) gives the solution $s = 12n^2 - 4n + 1, t = 12n^2 + 6n + 2$ and we get the number $c = 24n^2 + 4n + 3$.

(ii) We approached the problem with the focus on the Diophantine Triples (a, b, c) and its representation. As indicated above, the primary equations are

- $a = 6n^2 - 5n$
- $b = 6n^2 + 7n + 1$
- $c = 24n^2 + 4n + 3$

We can see that the emergence of the consistent pattern enabled us to assume the following.

The assumption going ahead is, the problem of existence of Diophantine 3-tuples is

closely connected with the properties of elliptic curves associated with them.

Let {a, b, c} be a rational Diophantine triple with property $D(x)$. This means that there exist

non-negative rational numbers r, s, t such that

- $(ab + x) = r^2$
- $(ac + x) = s^2$
- $(bc + x) = t^2$

Then $(ab + x)(ac + x)(bc + x) = y^2,\ y = (rst)^2$. In this case, if $n = 1, a = 1, b = 14$ and $c = 31$ (Calculations based on the formulae indicated in point (ii). Refer "Method of Analysis", Section A, Point (ii)).

Giving us an elliptic curve

$$(14 + x)(31 + x)(434 + x) = y^2$$

$$(x^3 + 479x^2 + 19964x + 188356) = y^2 \ldots\ldots\ldots \quad (3)$$

If equation (3) is reduced over the prime field F_p, where $p = 479$ we get an elliptic curve in Weierstrass form $E_{479}(325,109)$.

$$(x^3 + 325x + 109)(mod 479) = y^2(mod 479) \ldots \quad (4)$$

The discriminant of the equation (4)

$$\Delta = -16(4a^3 + 27b^2) = -16(137633287)(mod 479)$$
$$= 453 \neq 0.$$

Hence equation (4) can be used for elliptic curve cryptography.

Section B

Given below is a Java program that uses the conditions to check for the validity of the Elliptic curve points.

```java
import java.util.Scanner;
import java.io.*;
import java.math.RoundingMode;
import java.text.NumberFormat;
import java.lang.Math.*;

public class getSolutionECCplotting
{
    public static void main(String args[]) throws NumberFormatException, IOException {
        double a,b,x,y,intMod;
        double Detr, LHS, RHS;
        a=325;
        b=109;
        intMod=479;
        for (x=1;x<=450;x++) {
            for(y=1;y<=450;y++) {
                        Detr = (-16*Math.pow(a, 3)+27*Math.pow(b, 2));

                        Detr=Detr%19;
                        LHS = (Math.pow(y, 2)%intMod);
                        RHS = (((Math.pow(x, 3))+(a*x)+b)%intMod);

                        if ((Detr)!=0){
                            if(LHS==RHS) {
                                System.out.println(" x = "+x+"\t"+" y = "+y);
                            }
                        }
            }
        }
    }

}
```

Fig 3: The above screenshot image shows the intended Java program that enables us to generate the appropriate ECC points.

Program Outcome:

We have provided a table with corresponding values generated through the program. These values will guide us to understand the intricacies associated with the Elliptic Curve Cryptography. Certain cells have been identified through proper COLOR indicators.

Legend(s):

Point to be encrypted (M)	Generator point (G)	2*G indicator	3*G indicator	Cipher point (C2)

Table 1: The above table shows the generated points corresponding to the Elliptic curve for the given equation

x	y		x	y		x	y	x	y	x	y	x	y
2	151		29	65		51	193	83	11	108	195	138	393
2	328		31	207		51	286	86	99	108	284	140	223
4	**6**	**M**	31	272		54	151	86	380	111	102	140	256
5	204		32	149		54	328	87	1	111	377	141	114
5	275		32	330		57	228	89	190	112	237	141	365
10	124		33	97		57	251	89	289	112	242	143	118
10	355		33	382		59	62	91	112	113	10	143	361
11	15		34	108		60	100	91	367	119	171	146	86
14	207		34	371		60	379	94	1	119	308	146	393
14	272		36	93		61	229	95	47	121	57	151	15
15	185		36	386		61	250	96	26	122	140	153	152
15	294		38	121		66	10	97	34	122	339	153	327
17	**3**	**G**	38	358		67	123	98	226	124	188	157	43
19	230		39	166		67	356	98	253	124	291	158	107
19	249		39	313		73	107	99	6	128	237	158	372
21	48		44	140		73	372	101	81	128	242	159	168
22	195		44	339		78	53	101	398	131	26	159	311
22	284		46	52		79	32	104	164	135	217	160	175
23	152		48	18		80	231	104	315	135	262	160	304
23	327		49	54		80	248	105	167	137	108	163	135
24	67		**50**	**147**	**2*G**	82	211	105	312	137	371	163	344
25	48		50	332		82	268	106	47	138	86	164	182

x	y	x	y	x	y	x	y	x	y	x	y	
164	297	194	212	226	93	248	372	279	210	302	385	
166	89	194	267	226	386	249	233	279	269	303	152	
166	390	195	86	227	220	249	246	280	105	368	274	
167	95	195	393	227	259	250	145	280	374	372	219	
167	384	197	187	230	158	250	334	282	185	**372**	**260**	**C2**
171	23	197	292	230	321	251	104	282	294	375	25	
173	82	199	230	234	33	251	375	283	192	376	6	
173	397	199	249	239	237	252	26	283	287	378	138	
177	2	204	190	239	242	255	145	284	38	378	341	
178	49	204	289	240	209	255	334	285	169	382	44	
180	111	208	45	240	270	259	234	285	310	382	435	
180	368	209	39	241	219	259	245	287	194	383	220	
182	185	210	129	241	260	261	230	287	285	383	259	
182	294	210	350	243	210	261	249	294	130	387	182	
183	148	217	93	243	269	263	180	294	349	387	297	
183	331	217	386	244	142	263	299	295	155	388	59	
186	190	218	105	244	337	265	197	295	324	388	420	
186	289	218	374	246	139	265	282	297	187	391	407	
188	224	222	144	246	340	266	137	297	292	434	207	
188	255	222	335	247	194	266	342	298	1	434	272	
190	35	223	79	247	285	271	45	300	10	**435**	**89**	**3*G**
191	71	223	400	248	107	278	47	302	94	435	390	

The points generated by the program were ported into Excel and plotted using the chart feature. The resultant chart is shown below.

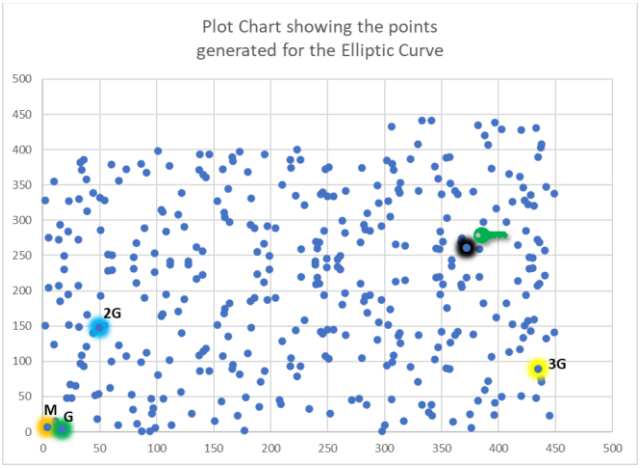

Fig 4: Figure showing the resultant Elliptic Curve points that satisfy the given equation.

Section C

(i) Illustrative steps to Elliptic Curve Cryptography

The equation of an elliptic curve is given as,

$E_p(a,b): y^2 = (x^3 + ax + b)$

Few terms that will be used,

- E_p -> Elliptic Curve defined over the finite field F_p
- p-> The prime number

Note: The elliptic curve generation is based on a maximum limit which is set for the points on the Elliptic curve.

(ii) Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

- Choose a point "M" from $E_p(a,b)$
- Choose a generator point "G" from $E_p(a,b)$
- Select a private key 'n' which is selected from the range $1 \leq n \leq (p-1)$ and compute the public key $P_U = n * G$
- Now, select a number 'k' within the range of $1 \leq k \leq (p-1)$.

(iii) Encryption

Let "M" be a point denoting a message which is also represented as a point on the Elliptic curve.

Two cipher texts will be generated which we will represent as C_1 and C_2.

$C_1 = k * G$

$C_2 = M + k * P_U$

It is thisC_1 and C_2 which will be send to the recipient.

(iv) Decryption

We have to get back the message "M" that was send to the recipient,

$M = C_2 - n * C_1$

"M" is the original message that we have sent.

(v) Illustrative example for the Elliptic curve encryption/ decryption

Consider the elliptic curve

$E_{479}(325,109): y^2 = (x^3 + 325x + 109)$

Step I

Encode a plain text message as a point on the elliptic curve $E_{479}(325,109)$.

From the Table 1, we have $M = (4,6) \in E_{479}(325,109)$.

The point (4,6) is highlighted in Figure 4 for illustrative purpose (Shown in ORANGE hue).

Step II

Establish the public key and the private key as follows. Choose the generator point $G = (17,3) \in E_{479}(325,109)$ from the Table 1. The generator point G is also highlighted in the Figure 4 (Shown in GREEN hue). Please refer. Then select a private key '$n = 3$' which is selected from the range $1 \leq n \leq 478$ and compute $P_U = 3 * G$.

Now $3 * G = 3(17,3) = (17,3) + (17,3) + (17,3)$, first we calculate as $3 * G = (x_3, y_3) = (17,3) + (17,3)$

Using the doubling of points in the elliptic curve we have

$\lambda = \frac{3x_1^2 + a}{2y_1} (mod\ p)$

$\lambda = \frac{3(17)^2 + 325}{6} (mod\ 479) = \frac{1192}{6} (mod 479) = 39.$

Then $x_3 = (\lambda^2 - x_1 - x_2)(mod\ p) = 1487(mod\ 479) = 50$, and

$y_3 = (\lambda(x_1 - x_3) - y_1))\ (mod\ p) = -1290(mod 479) = 147.$

$2 * G = (50,147)$

The point 2*G i.e. (50, 147) is indicated in the Table 1 (Shown in BLUE hue).

Hence $3 * G = (50,147) + (17,3)$, since the points $P_1 = (17,3), P_2 = (50,147)$ are not equal from the rule of addition of two distinct points.

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} (mod\ p)$

$\lambda = \frac{147 - 3}{50 - 17} (mod\ 479) = \frac{48}{11} (mod\ 479) = 135$

Then $x_3 = (\lambda^2 - x_1 - x_2)(modp) = 18158(mod 479) = 435$ and

$y_3 = (\lambda(x_1 - x_3) - y_1))\ (mod\ p)$

$= (-52122)(mod 479) = 89.$

Now $P_U = 3 * G = (435,89)$.

The point 3*G is highlighted in the Figure 4 in the YELLOW hue.

Step III

Consider a random number k such that $1 \leq k \leq (p-1)$, choose $k = 2$

$C_1 = k * G$

$= 2 * (17,3) = (50,147)$

$C_2 = M + k * P_U = (4,6) + 2 * (435,89)$

$= (4,6) + (50,332) = (372,260)$

Step IV

Decryption using the private key

$M = C_2 - n * C_1$

$= (372,260) - 3 * (50,147)$

$= (372,260) - 3(50,332)$

$= (372,260) + (50, -332(mod 479))$

$= (372,260) + (50,147) = (4,6).$

Finally, we are able to generate the Cipher texts C_1 and C_2 using the plotted points provided by the Elliptic Curve representation.

Hence Cipher text

C_1 (Private Key) = (50, 147), and

C_2 (Public Key) = (372,260)

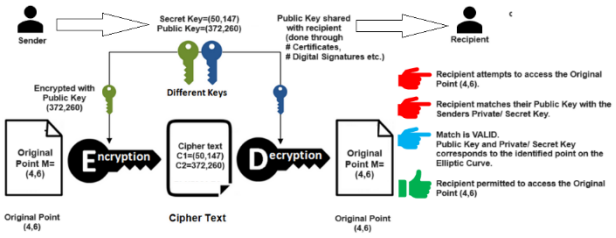

Fig 5: The above figure shows the actual process steps carried out to encrypt/ decrypt an original point and make it accessible to the recipient.

Revisiting the earlier Figure shown for Asymmetric Encryption; let's interpret our solution with respect to the given figure. The analytic representation is shown in Figure 5 above. We have attempted to show the detailed steps that would be activated and enabled for a recipient to match their Public Key with the Senders Private/ Secret Key and access the original point.

NOTE: All the points are part of the Elliptic Curve point representation. It sure is an indication that the recipient will not be able to access the original point if the recipient provides another public key point not related to the equation used in generating these Elliptic curve points.

4. Conclusion

Though ECC was implemented by most web browsers during the early stages; it was replaced with RSA encryption as the Stage 1 encryption. This trend has continued until recently when most Governments around the world have begun implementing ECC cryptography for Government related Digital Signatures to safeguard Government assets.

Some of the striking features and benefits of ECC are:

- It involves smaller ciphertexts, keys, and signatures, and therefore faster generation of keys and signatures is possible,
- The decryption and encryption mechanism speeds are moderately fast,
- The smaller keys mean less data transmitted over the server during security validation,
- Enhanced ECC Mathematical strategies are giving rise to more complicated and stronger encryption models, and
- It is surely providing an alternative to other cryptographic methods.

In this research article, we have generated the cryptographic model by associating the Tetradecagonal structure, its associated Diophantine triples and its properties to generate the cryptographic solution. Combining the most intricate structure in Mathematics to generate a practical application that could in future be an intrinsic part of cryptographic models is the most important takeaway of this research.

The day is not far behind when with more alarming breaches of security being noticed worldwide; we may find that ECC will take its right place and provide a stronger and robust alternative.

References:

[1] Andrej Dujella and Vinko Petri'cevi, Strong Diophantine Triples, Experimental Mathematics 17(1) (2008), 83.

[2] Bashmakova. IG, Diophantus of Alexandria Arithmetic and the Book of Polygonal numbers, Nauka, Moscow, 1974.

[3] Dickson LE, History of theory of numbers, Chelsea, New York, 2 (1966), 513-520.

[4] Gopalan M V and Srividhya G, Two Special Diophantine triples, Diophantus J Math 1(1) (2012), 23-27.

[5] M A Gopalan, V. Sangeetha and Manju Somanath, Construction of the Diophantine Triple involving Polygonal Numbers, Scholars Journal of Engineering and Technology 2(1) (2014).

[6] Manju Somanath, J Kannan and K Raja, Cryptographic Algorithm Based on Prime Assignment, International Journal for Research in Applied Science Engineering Technology (IJRASET) 10(1) (2022),

[7] Manju Somanath, J Kannan and K Raja, Encryption Decryption Algorithm Using Solutions of Pell equation, Int. J. Math. And Appl. 10(1) (2022), 1-8.

[8] Pandichelvi V, Construction of the Diophantine Triple involving Polygonal Numbers, Impact J Sci.Tech. 5(1) (2011), 7-11.

[9] Wade Trappe and Lawrence C Washington, Introduction to Cryptography with Coding Theory, Pearson Education Inc., London, 2006.

[10] William Stallings, Cryptography and Network Security, Pearson Education Inc., London, 2017.