Elliptic Curve Public-Key Cryptosystem Over Z(i)

Soram Ranbir Singh
Department of Computer Science & Engineering,
Manipur Institute of Technology, Takyelpat, Imphal-795001, India.

Khomdram Memeta Chanu
Department of Electronics Accreditation of Computer Courses Centre, Akampat
Imphal-795001, India.

Abstract— **A method to implement elliptic curve public-key cryptosystem over Z(i) is discussed. The method is in fact the same as the technique that works on Galois fields but here works on Z(i). The curve under Z(i) generates more points as compared to the curve under Galois fields. The security of the system is better due to more number of points on the curve. But there are some difficulties in the new system and through this paper; we try to discuss some of the pitfalls of the new system.**

Keywords- Elliptic Curve Cryptography, ECDLP, Gaussian Integer, Unique Factorization Domain.

I. INTRODUCTION

We live in an information age where information is treated as an asset that has a value like any other asset that we possess. So, we need to keep information secured from attacks and hackers. To keep information safe and secured it needs to be hidden from unauthorized access, protected from unauthorized modification and so on. Just a few decades from today, computer networks had been created and it has been creating a change in the use of information in the sense that information is distributed. It is now required to an authorized person to send and procure information from a far off place using computer networks. A new requirement has come up in the picture when the information is transmitted from one computer to another i.e., there should be a way to maintain its confidentiality on the way when it is transported from one computer to another in the network. So, the need for the public-key cryptography comes into picture. In public-key cryptography, there are two keys:- a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. There are numerous public-key cryptography algorithms in the literature but many of these are found to be insecure and many are impractical to implement and use. As of now, only a few of those algorithms are considered both secure and practical. Of these secure and practical public-key algorithms, a few are suitable for encryption and still others are only useful for authentication. For example, RSA is presently used for both encryption and authentication. It is very slow in actual practice. Elliptic Curve Cryptography(ECC) is one of a few public-key algorithms that can be used in place of RSA.

II. WHY ECC

One of the main problems of RSA is its demand for a huge key length to meet the challenges in today's security scenario. When you create an RSA key pair, you specify a key length in bits, as generally you would for other algorithms. Specifically, the key length of an RSA key specifies the number of bits in the modulus. But the million dollar question is "what RSA key length should we choose".

Experts say that an RSA key length of 1024 bits is sufficient for many medium-security purposes such as web site logins but for high-security applications such as online financial fund transfers or for data that need to remain confidential for more than a few years; you should use at least a 2048-bit key and it can be confirmed using table 1. To keep data confidential for more than the next two decades, RSA experts recommend a key size larger than 2048 bits [1]. A larger key increases the security of the encryption. But it has a serious problem in practice. With every doubling of the RSA key length, decryption is about 8 times slower. The size of ciphertext also become huge considerably. The key length also affects the speed of encryption, which is slower by a factor of 4. The comparisons in Table 2 demonstrate that smaller parameters can be used in elliptic curve cryptography (ECC) than with RSA system at a given security level. By a security level of k bits we mean that the best algorithm known for breaking the system takes approximately 2^k steps. At the 132-bit ECC/1024-bit RSA

security level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations.

TABLE 1. RSA KEY LENGTH OF SOME ORGANIZATIONS

Organization	**RSA Key length**
Google	1024
Yahoo	1024
eBay	2048
Online SBI	2048
Bank Asia	2048
Vijaya Bank	2048

TABLE 2. RSA AND ECC KEY SIZES

Security level	80	112	120	128	256
ECC	132	185	237	256	512
RSA	1024	2048	2560	3072	15360

At the 256-bit ECC/3072-bit RSA security level the ratio has already increased to between 20 and 60, depending on optimizations. To secure a 256-bit AES key, ECC-521 can be expected to be on average 400 times faster than 15,360-bit RSA [1]. The advantages that can be gained from smaller parameters include speed (faster computations) and smaller keys and certificates.

III. ELLIPTIC CURVE

Elliptic curves are a specific class of algebraic curves. The "Weierstrass form" of an elliptic curve equation is [2],[4],[11]:-

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

The constant $a_1,\ a_2,\ a_3,\ a_4,\ a_6$ and the variables x, y can be complex, real, integers, polynomials, or even any other field elements. So, the mathematics of elliptic curve cryptography is so deep and complicated. But in practice we must specify which field, F, these constants and the variables, x, y belong to and $\Delta \neq 0$, where Δ is the discriminant of E and is defined as follows [2]:-

$$\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$$
$$d_2 = a_1^2 + 4a_2$$
$$d_4 = 2a_4 + a_1 a_3$$
$$d_6 = a_3^2 + 4a_6$$
$$d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$$

We say that E is defined over K when the coefficients $a_1,\ a_2,\ a_3,\ a_4,\ a_6$ (and of course, the variables x and y) of the equations come from the elements of the field K. So, we sometimes write $E(K)$ to emphasize that E is defined over K, and K is called the underlying field. If E is defined over K, then E is also defined over any extension field of K.

A. Elliptic Curve Over Galois fields

Using the real numbers for cryptography has a lot of problems as it is very difficult to store them precisely in computer memory and predict how much storage will be needed for them. The difficulty can be solved by using Galois fields. In a Galois field, the number of elements is finite [16]. Since the number of elements if finite, we can find a unique representation for each of them, which allows us to store and handle the elements in an efficient way. Galois showed that the number of elements in a Galois field is always a positive prime power, and is denoted by $GF(p^n)$. Two special Galois fields are common in Elliptic Curve Cryptography. They are $GF(p)$ when $n=1$ and $GF(2^n)$ when $p=2$.

B. Elliptic Curve Over Prime Galois Fields

An elliptic group over a prime Galois Field uses a special elliptic curve of the form

$$y^2 (\text{mod } p) = x^3 + ax + b (\text{mod } p)$$

where $a, b \in GF(p), 0 \le x \le p$ and $-16(4a^3 + 27b^2) \bmod p \neq 0$. The constants ***a*** and ***b*** are non-negative integers smaller than the prime p. The condition that $-16(4a^3 + 27b^2) \bmod p \neq 0$ implies that the curve has no "singular points" [3].

C. Group Law

The mathematical property that makes elliptic curves useful for cryptography is simply that if we take two (distinct) points on the curve, then the chord joining them intercepts the curve in a third point (because we have a cubic curve). If we then reflect that point in the x-axis we get another point on the curve (since the curve is symmetric about the x-axis). This is the "sum" of the first two points. Together with this addition operation, the set of points $E(K)$ forms an abelian group with **0** serving as its identity [4]. It is this group that is used in the construction of elliptic curve cryptographic systems. Algebraic formulae for the group law can be derived from the geometric description.

Group law for $y^2 = x^3 + ax + b$ over $GF(p)$.

(1) Identity: $P + 0 = 0 + P = P$ for all $P \in E(K)$.

(2) Negative: If $P = (x, y) \in E(K)$, then $(x, y) + (x, -y) = 0$. The point $(x, -y)$ is denoted by -P and is called the negative of P; note that -P is indeed a point in $E(K)$. Also, $-0 = 0$.

(3) Point addition: Let $P = (x_1, y_1) \in E(K)$ and $Q = (x_2, y_2) \in E(K)$ where $P \neq \pm Q$ .Then $P + Q = R(x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

(4) Point doubling: Let $P = (x_1, y_1) \in E(K)$, where $P \neq \pm P$. Then $2P = R(x_3, y_3)$, where $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = \dfrac{3x_1^2 + a}{2y_1}$.

D. Geometrical Interpretation of Group Law

1. Negative of a Point

Let's take a point $P = (x, y)$. The formula for finding $-P$ is $-P = (x, -y)$ as shown in the fig. 1.

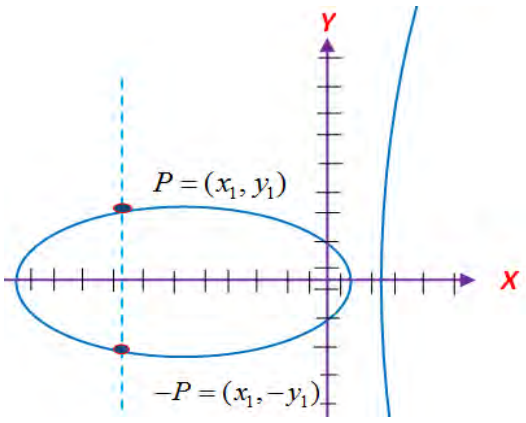

Fig.1.Negative of a Point

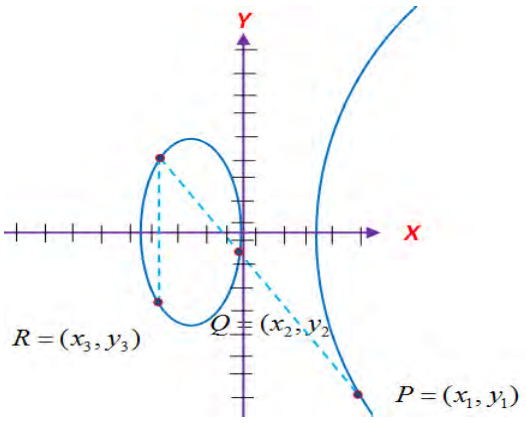

Fig. 2. Addition of two Points

2. Addition of two Points

As mentioned above, we can define the addition of any two points on an elliptic curve by drawing a line between the two points and finding the point at which the line intersects the curve. The negative of the intersection point is defined as the "elliptic sum" by mathematicians as shown in fig. 2.

Mathematically we write:

R = *P* + *Q*.

This "addition" satisfies all the usual algebraic properties that we associate with integers, provided we define a single additional point "the point at infinity", which plays the role of 0 in the integers. In mathematical terms, we can define a finite additive abelian group on the points of the curve, with the zero being the point at infinity [4].

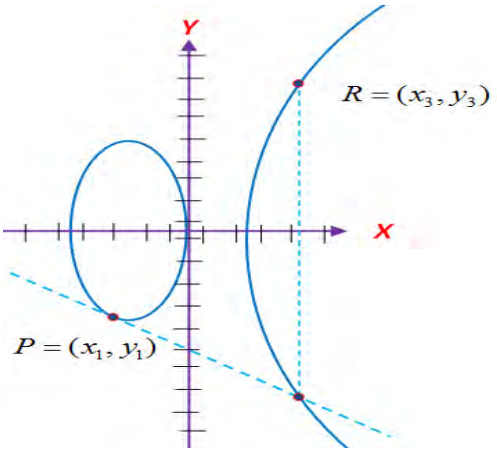

Fig. 3. Doubling a Point

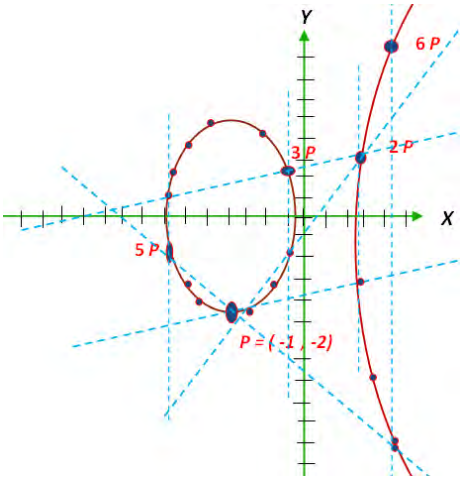

Fig. 4. Some multiples of $P = (-1, -2)$.

3. Doubling of a Point

If $P = (x_1, y_1)$, then the double of *P*, denoted by, $R = (x_3, y_3)$, is defined as follows. First draw the tangent line to the elliptic curve at *P*. This line intersects the elliptic curve in a second point. Then *R* is the reflection of this point in the x –axis. This is depicted in fig. 3. We can extend this idea to define $P + P + P = 3P$, and extending this idea further, we can define $P + P + P + ... + k$ times $= kP$, for any integer *k*, and hence define the order of P, being the smallest integer k such that $kP = 0$, where 0 denotes the point at infinity[4]. Fig. 4 shows some multiples of $P = (-1, -2)$ on the curve $y^2 = x^3 - 5x$.

To elucidate doubling of a point, consider the elliptic curve

$$y^2 = x^3 + x + 4$$

defined over $GF(23)$. This curve is represented by $E_{23}(1,4)$. We first note that $4a^3 + 27b^2 = 4 + 432 = 436 \equiv 22 (\text{mod } 23) \neq 0 (\text{mod } 23)$. The points in $E_{23}(1,4)$ are the following:-

Table 3. Points on the curve $E_{23}(1,4)$

0	*(0,2)*	*(0,21)*	*(1,11)*	*(1,12)*	*(4,7)*
(4,16)	*(7,3)*	*(7,20)*	*(8,8)*	*(8,15)*	*(9,11)*
(9,12)	*(10,5)*	*(10,18)*	*(11,9)*	*(11,14)*	*(13,11)*
(13,12)	*(14,5)*	*(14,18)*	*(15,6)*	*(15,17)*	*(17,9)*
(17,14)	*(18,9)*	*(18,14)*	*(22,5)*	*(22,19)*	

Let $P = (4,7)$ and $Q = (13,11)$. Then $P + Q = R(x_3, y_3)$ is computed as follows-

$$\lambda = \frac{11-7}{13-4} = \frac{4}{9} = 4 \text{X} 9^{-1} (\text{ mod } 23) = 4 \text{X} 18 (\text{ mod } 23) = 72 \text{ mod } 23 = 3$$

$$x_3 = 3^2 - 4 - 13 = -8 \equiv 15 (\text{mod } 23), \quad \text{and } y_3 = 3(4-15) - 7 = -40 \equiv 6 (\text{mod } 23)$$

Hence, $R = (15, 6).$

Again, let $P = (4, 7).$ Then $2P = P + P$ is calculated as follows:-

$$\lambda = \left(\frac{3 \mathrm{X} 4^2 + 1}{14} \right) = 49 \mathrm{X} 14^{-1} = 49 \mathrm{X} 5 = 245 \, (\mathrm{mod}\, 23) = 15$$

$x_3 = 15^2 - 8 = 217 \equiv 10 (\mathrm{mod}\, 23)$ and $y_3 = 15(4 - 10) = -97 \equiv 18 (\mathrm{mod}\, 23).$

Hence, $2P = (10, 18).$

E. Elliptic Curve Over Binary Galois Fields

Let's look at elliptic curves over $GF(2^n)$.That means our constants are either polynomial or normal basis numbers. It also means we cannot use the simplified version of equation, which we used for integer numbers, for our elliptic curve equations.

The mathematicians tell us that we need to use either this version:

$$y^2 + xy = x^3 + ax^2 + b \qquad (1)$$

or this version

$$y^2 + y = x^3 + ax + b \qquad (2)$$

But, the mathematicians say that the second form above, (2), has the advantage that it can be computed quickly and has some very special properties. These properties make such curves unsuitable for cryptography.

The curves of (1) are excellent for cryptographic applications. One must be careful in choosing the coefficients to get maximum benefit of security. A poor choice can create a curve that is easier for the cryptanalyst to attack. For equation (1) to be valid, *b* must never be 0. However, *a* can be 0. Here we give the group laws of the first form of the curve[3].

Group law for $y^2 + xy = x^3 + ax^2 + b$ over $GF(2^n)$

1. Identity: $P + 0 = 0 + P = P$ for all $P \in E.$
2. Negative: If $P = (x, y) \in E,$ then $(x, y) + (x, x + y) = 0.$ The point $(x, x + y)$ is denoted by $-P$ and is called the negative of *P*; note that -*P* is indeed a point in E. Also, $-0 = 0.$
3. Point addition: Let $P = (x_1, y_1) \in E$ and $Q = (x_2, y_2) \in E$ where $P \neq \pm Q$ .Then $P + Q = R(x_3, y_3)$, where $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$ and $y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ with $\lambda = \frac{y_2 + y_1}{x_2 + x_1}.$
4. Point doubling: Let $P = (x_1, y_1) \in E,$ where $P \neq -P$. Then $2P = R = (x_3, y_3),$ where $x_3 = \lambda^2 + \lambda + a$ and $y_3 = x_1^2 + \lambda x_3 + x_3$ with $\lambda = x_1 + \frac{y_1}{x_1}.$

Let us take an elliptic curve [9] $y^2 + xy = x^3 + g^3 x^2 + 1$ over $GF(2^3)$ under the irreducible polynomial $f(x) = x^3 + x + 1.$ Here the generator, g, satisfies the relation $g^3 + g + 1 = 0$ or $g^3 = g + 1$ as the arithmetic is over $GF(2).$ The following table 4 shows the values of $g's$ and the points on the curve are given in table 5.

TABLE 4: POSSIBLE VALUES OF g's

0	*000*	*g*	*010*	$g^3 = g + 1$	*011*	$g^5 = g^2 + g + 1$	*111*
1	*001*	g^2	*100*	$g^4 = g^2 + g$	*110*	$g^6 = g^2 + 1$	*101*

TABLE 5: POINTS ON THE GIVEN CURVE $y^2 + xy = x^3 + g^3x^2 + 1$

0	$(0,1)$	$(g^2,1)$	(g^2,g^6)	(g^3,g^2)
(g^3,g^5)	$(g^5,1)$	(g^5,g^4)	(g^6,g)	(g^6,g^5)

Let $P=(0,1)$ and $Q=(g^2,1)$. We have $P+Q=R=(x_3,y_3)$ is computed as follows.

$$\lambda = \frac{1+1}{g^2+0} = 0$$

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a = 0+0+0+g^2+g^3 = g^5 \text{ and } y_3 = \lambda(x_1+x_3)+x_3+y_1 = 0(0+g^5)+g^5+1$$
$$= g^5+1 = g^2+g = g^4.$$

So, $R=(g^5,g^4)=(111,110)$.

Again take $P=(g^2,1)$. $2P = P+P = R(x_3,y_3)$.

$$\lambda = g^2 + \frac{1}{g^2} = g^2+g^5 = g+1 = g^3$$

$$x_3 = \lambda^2+\lambda+a = g^6+g^3+g^3 = g^6 \text{ and } y_3 = x_1^2+\lambda x_3 + x_3$$
$$= g^4+g^9+g^6 = g^4+g^2+(g^2+1)$$
$$= g^4+1 = (g^2+g)+1 = g^5$$

Therefore, $R=(x_3,y_3)=(g^6,g^5)=(101,111)$.

F. An important Theorem

Let *E* be an elliptic curve defined over F_q. Then $E(F_q)$ is isomorphic to $Z_{n1} \oplus Z_{n2}$ where n_1 and n_2 are uniquely determined positive integers such that n_2 divides both n_1 and $q-1$. Note that $\#E(F_q) = n_1 n_2$. If $n_2 = 1$, then $E(F_q)$ is a cyclic group. If $n_2 > 1$, then $E(F_q)$ is said to have rank *2*. If n_2 is a small integer (e.g., n = 2 ,3 or 4), we sometimes say that $E(F_q)$ is almost cyclic[4]. Since n_2 divides n_1 and $q-1$, one expects that $E(F_q)$ is cyclic or almost cyclic for most elliptic curves *E* over F_q.

G. Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve defined over a finite field and let, P be a point (called base point) on E of order n and k is a scalar. Calculating the point $Q = kP$ from P is very easy and $Q = kP$ can be computed by repeated point additions of P. However, it is very hard to determine the value of k knowing the two points: kP and P. This lead leads to the definition of Elliptic Curve Logarithm Problem (ECDLP) [3], which is defined as: "Given a base point P and the point $Q = kP$, lying on the curve, find the value of scalar k". The integer k is called the elliptic curve discrete logarithm of Q to the base P, denoted as $k = \log_P Q$.

IV. THE SET $Z(i)$

We have studied in our high school classes that all complex numbers can be written as $a+ib$, where a and b are real numbers and $i = \sqrt{-1}$. If we only allow integer values for a and b we have the set $Z(i)$. This set is also called Gaussian Integers[15]. So, a Gaussian integer is a complex number whose real and imaginary part are both integers. The set $Z(i)$ forms a ring rather than a field, meaning that addition, subtraction, and multiplication are well-behaved, but inversion is not[15]. The reciprocal of an element $a \in Z(i)$ in general need

not exist within the set $Z(i)$. As a ring, the set $Z(i)$ behaves similarly to the rational integers Z. The units (multiplicatively invertible elements) of the $Z(i)$ are $Z(i)^+ = \{\pm 1, \pm i\}$ a multiplicative group. Every nonzero element of $Z(i)$ factors uniquely (up to units) into prime in $Z(i)$ and so on. Prime numbers in Z are called rational primes to distinguish them from prime numbers in the set $Z(i)$.

The norm of a Gaussian integer is the natural number defined as [15]:-

$$N(x+iy) = x^2 + y^2 = (x+iy)(x-iy)$$

The norm is multiplicative, i.e.

$$N(m*n) = N(n)*N(m)$$

The units of $Z(i)$ are therefore precisely those elements with norm 1, i.e. the elements 1,-1, i,-i.

A Gaussian integer $a+ib$ in $Z(i)$ is Gaussian prime in $Z(i)$ if and only if $a+ib$ is the product of a unit and one of the following[16]:

(i) $1+i$,

(ii) a prime number $p \in Z$, where $p \equiv 3 \pmod 4$, or

(iii) $x+iy$, where $x^2 + y^2 = p$, and p is a prime in Z with $p \equiv 1 \pmod 4$.

The necessary conditions can be stated as following: if a Gaussian integer *a* + *bi* is a Gaussian prime, then either its norm is a prime number, or its norm is a square of a prime number.

We will assume that every Gaussian Integer whose norm is greater than 1 and less than n has a prime factorization. A Gaussian Integer with norm n is either prime or composite. If it is a prime, we have found a prime factorization. If it is composite, then we can factor it into two Gaussian Integers both of whose norms are less than n. Thus both of these Gaussian Integers will have prime factorizations, so the prime factorization of the Gaussian Integer in question will be the product of those two prime factorizations.

The ring of $Z(i)$ is a unique factorization domain, which means that, just like in the integers, every element of $Z(i)$ has a unique decomposition into prime elements [15]. Since the norm is a multiplicative map, an element with prime norm must be prime. Thus $x \pm iy$ are both prime. So if $p = (x+iy)(x-iy)$, by unique factorization this means p cannot be a prime element of $Z(i)$. In this case, the prime p is said to split in $Z(i)$. We note also that if p splits in $Z(i)$, then the minimal polynomial of i, $x^2 + 1$, factors modulo p. For example, $x^2 + 1 = (x + 2)(x - 2)$ modulo 5.

A. Elliptic Curve Over $Z(i)$

In this version of elliptic curves, the elliptic curve points will be elements of $Z(i)$ and therefore will have complex coordinates. As an example, consider the elliptic curve $y^2 = x^3 + x$ over $F_p(i) = \{a+ib : a,b \in GF(3)\}$ of $Z(i)$. It has 16 points. The points are given in table 6 below.

TABLE 6: POINTS ON $y^2 = x^3 + x$ OVER $F_p(i) = \{a+ib : a,b \in GF(3)\}$.

x	*y*	*Point*	*x*	*y*	*Point*
0	*0*	*(0, 0)*	*1+2i*	*±i*	*(1+2i, i),(2i, 2i)*
i	*0*	*(i, 0)*	*2*	*±1*	*(2, 1),(2, 2)*
2i	*0*	*(2i, 0)*	*2+ i*	*±1*	*(i, 1),(i, 2)*
1	*±i*	*(1,i),(1, 2i)*	*2+2i*	*±1*	*(2+2i, 1),(2i, 2)*
1+i	*±i*	*(i, i),(i, 2i)*			*0*

To show the idea and the distribution of points, a full enumeration of curve points has been done. The following fig.5. shows the complex points on the complex plane. The x and y coordinates are represented separately as each coordinate is complex. The *x* and *y* coordinate fall within the planar square limited by 0, *p*, *ip* and (1 + *i*)*p*.

The prime p can be a Gaussian prime of the form $p = a + ib$ in $Z(i)$ and if so, the real part of *x* and *y* falls between *a* and – *b*. The imaginary part falls between 0 and *a* + *b*.

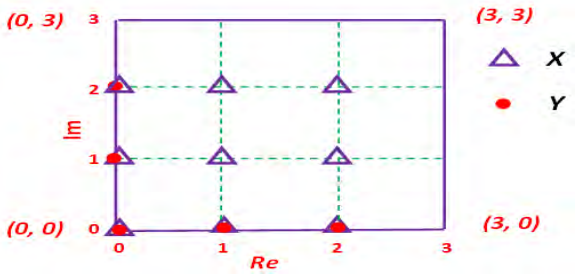

Fig. 5. Point on $y^2 = x^3 + x$ over $F_p(i) = \{a + ib : a, b \in GF(3)\}$.

If the same curve is implemented under $GF(3)$, then it has 4 points as shown below in table 7.

TABLE 7. POINTS ON $y^2 = x^3 + x$ *OVER* $GF(3)$

x	*y*	*point*
0	*0*	*(0, 0)*
2	*±1*	*(2, 1),(2,2)*
		0

B. Point counting

Let *E* be an elliptic curve defined over F_q. The number of points in $E(F_q)$, denoted by $\#E(F_q)$ or $|E(F_q)|$, is called the order of *E* over F_q. Then Hasse's theorem says that the order of $E(F_q)$ satisfies the inequality [4]

$$q + 1 - 2\sqrt{q} \le |E(F_q)| \le q + 1 + 2\sqrt{q}.$$

An alternate formulation of Hasse's theorem can be stated as:- if *E* is defined over F_q, then $\#E(F_q) = q + 1 - t$ where $|t| \le 2\sqrt{q}$; *t* is called the trace of *E* over F_q. Since $2\sqrt{q}$ is small relative to *q*, we have $|E(F_q)| \approx q$.

There are several methods presently known that can quickly determine the order of $E(F_q)$. Unfortunately none of them is effective once q is very large. An alternative approach is to use the order of certain points in $E(F_q)$. Since $E(F_q)$ is a group, and then the order of any point in $E(F_q)$ must divide $|E(F_q)|$, by Lagrange's theorem. In Hasse's theorem, we know that $|E(F_q)|$ is bounded in an interval of length $4\sqrt{q}$. If we can find a point in $E(F_q)$ of order $m > 4\sqrt{q}$, then there will be only one multiple of m lying in that interval, which must be $|E(F_q)|$. For example, let E be the elliptic curve $y^2 = x^3 - 10x + 21$ over $GF(557)$. It can be shown that the point (2, 3) has order 189. Hasse's theorem says that

$$557 + 1 - 2\sqrt{557} \le |E(F_{557})| \le 557 + 1 + 2\sqrt{557}$$

$$\text{i.e, } 511 \le |E(F_{557})| \le 605$$

But the only multiple of 189 in this interval is 3 as 3X189 = 576. Hence, $|E(F_{557})| = 567$.

Now let us take this theorem to elliptic curve over $Z(i)$. In this case, our field is $F_p(i) = \{a + ib : a, b \in F_p$ with p = 3 mod 4. Now q is the norm of the $x \in Z(i)$ i.e, Gaussian integer. In other words, this field is isomorphic to F_{p^2} . So, the Hasse's theorem says

$$q+1-2\sqrt{q} \le \left|E(F_q)\right| \le q+1+2\sqrt{q}$$

$$9+1-2\sqrt{9} \le \left|E(F_p(i))\right| \le 9+1+2\sqrt{9} \qquad \left[\because q = p^2 = 3^2 = 9\right]$$

$$10-6 \le \left|E(F_p(i))\right| \le 10+6$$

$$4 \le \left|E(F_p(i))\right| \le 16.$$

The actual number of points is 16 which is again within the bound of Hasse's theorem.

C. Elliptic Curve Arithmetic

The arithmetic for adding two points can be done in the same way we do over F_q. Similar is the case for each of negation and doubling of a point.

Multiplication of a point by the imaginary number *i* transform a point (*x*, *y*) to the point (–*x*, *iy*). Depending on the equation of the elliptic curve, it may be a new point either on the curve itself or not on the original curve but to a new curve. As an example, consider the elliptic curve

$E_1 : y^2 = x^3 + x.$

It has complex multiplication

$f(x, y) = (-x, iy)$

because $(iy)^2 = -y^2 = -x^3 - x.$ It is easy to see that $f(x, y)$ is indeed a point on the curve E_1. In this type of elliptic curve, multiplication of a point by *i* is still a point on the same curve.

Again consider the elliptic curve equation

$E_2 : y^2 = x^3 + ax + b$

If all the points on this curve are multiplied by *i*, this generates all the points that are on another curve whose equation is $y^2 = x^3 + ax - b$. Thus, depending on curves, multiplication by *i* introduces a shift that transforms all the points of the curve to another one. This is one the problems of elliptic curve cryptography over $Z(i)$.

D. Supersingular Curves

Elliptic curves defined over a finite field are of two types. Most are what are called ordinary or non-supersingular curves, but a small number are supersingular. As mentioned above, the order or cardinality of an elliptic curve is $\left|E(F_q)\right| = q+1-t$, where $|t| \le 2\sqrt{q}$. Let *p* be the characteristic of F_q. An elliptic curve *E* defined over F_q is supersingular if *p* divides *t*. If *p* does not divide *t*, then *E* is non-supersingular [4]. The problem with the supersingular elliptic curve is that the ECDLP in an elliptic curve E defined over a field F_q can be reduced to the ordinary DLP in the multiplicative group of some finite extension field of $F_q k$ for some $k \ge 1$. It follows that the reduction of ECDLP to ordinary DLP can be solved in a sub-exponential time, thus, compromising security of the system. To ensure that the reduction does not apply to a particular curve, one need to make sure that n, the order of the point P, does that divide $q^k - 1$ for small k.

In the case of $Z(i)$, *p* is replaced by its norm in the condition. Using a Weil pairing on *E*, there is a polynomial time reduction of ECDLP to DLP. These curves are exposed to the MOV attack that runs in sub exponential time. Although the computations of the attack are longer with $Z(i)$, those curves should be avoided.

E. Implementation Speed and Complexity

The number of digits involved in arithmetic over the prime $p \in Z(i)$ is similar to the number of digits handled in the arithmetic on the same elliptic curve over a field of the order of p^2. However; complex arithmetic enables multipliers to compute the real and imaginary parts of the output independently. The multiplication of $(a+ib)$ and $(c+id)$ gives (*ac* - *bd*) as the real part and (*ad* + *bc*) as the imaginary part of the operation. Both the real and imaginary parts can be calculated independently. This leads to quicker operations. The hardware implementation of the arithmetic will use less electronic components because the required multipliers work on inputs that are on the order of *p* rather than p^2. This implies that the multipliers used in case of $Z(i)$ will handle digits that is roughly half the number of digits needed to handle the larger integers on the order of p^2. As an example, the complexity of a typical multiplication is $0(n^2)$ where *n* is the number of digits in each of the two inputs. For rational primes on the order of p^2 that have *n* digits the complexity is $0(n^2)$ while the equivalent Gaussian integers with real and imaginary parts on the order of *p* each will have a complexity $O\left(\frac{n}{2}\right)^2 = O\left(\frac{n^2}{4}\right)$. If two multipliers are run in parallel to calculate the real and imaginary parts the total time complexity remains $O\left(\frac{n^2}{4}\right)$, which is $\frac{1}{4}$ of the time needed in the case of rational integer.

But an elliptic curve defined over $Z(i)$ requires double the space and bandwidth as used by elliptic curve over Galois fields of the same prime *p* because the points on elliptic curve over $Z(i)$ are Gaussian integers. Point compression techniques [4] can be used to decrease the memory space requirements sacrificing speed.

F. Security Issues

An elliptic curve defined over $Z(i)$ results in an elliptic curve group that is much larger than the group of the same curve over Galois Fields. The security is greatly improved as the order of the curve becomes squared. For systems with limited computational capacity like smart cards, a very high level of security can be achieved using elliptic curve cryptography over $Z(i)$.

ACKNOWLEDGMENT

The first author thanks his daughter Java Soram and son Chandrayan Soram for not complaining anything to him when he was spending too much time with his Laptop in the preparation of the manuscript.

REFERENCES

[1] Kristin Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security", Microsoft Corporation.
[2] Ian Blake, Gadiel Seroussi, Higel Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.
[3] Lawrence C. Washington, Elliptic Curves, Number Theory and Cryptography, CRC Press, 2008.
[4] Ian Blake, Gadiel Seroussi, Higel Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press, 2005
[5] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.
[6] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards," IEEE Trans. Consumer Electronic, vol. 49, no. 2, pp. 414-416, May 2003.
[7] Neal Koblitz, Alfred J. Menezes, "A survey of public-key cryptosystems,", Aug 7. 2004.
[8] Rotman, Galois Theory, Springer International Edition, 2010
[9] William Stallings, Cryptography & Network Security, PHI, 2006
[10] Atul Kahate, Cryptography and Network Security, 2E, Tata McGraw, 2011.
[11] Henri Cohen, Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press, 2006.
[12] Thomas Koshy, Elementary Number Theory with Applications, Academic Press, 2009.
[13] Erdinc Ozturk, "Low Power Elliptic Curve Cryptography" M.Sc thesis, Worcester Polytechnic Institute, April 2004
[14] Menezes, Okamoto, Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, IEEE Transaction on Information Theory, vol. 39, 1993.
[15] Gaussian Integers from The Wikipedia website. [Online]. Available: http://en.wikipedia.org/
[16] Bhattacharya, Jain, Nagpaul, Basic Abstract Algebra, Cambridge University Press, 2002.
[17] Joseph H. Silverman, John Tate, Rational Points on Elliptic Curves, Springer, 1992.
[18] Bruice Schneier, Applied Cryptography, Wiley India, 2007.
[19] ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, 1999.

[20] A. Antipa, D. Brown, A. Menezea, R. Struik, and S. Vanstone,. Validation of elliptic curve public keys. Public Key Cryptography—PKC 2003, 211–223, 2003.
[21] M. Bellare , A. Boldyreva,and S. Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. Advances in Cryptology—EUROCRYPT 2000 , 259–274, 2000.
[22] W. Diffie, P Vanoorschot, and M. Wiener. Authentication and authenticated key exchanges. Designs, Codes and Cryptography, 2:107–125, 1992.
[23] R. Canetti and H. Krawczyk , Analysis of key-exchange protocols and their use for building secure channels. Advances in Cryptology—EUROCRYPT 2001, 453–474, 2001.