ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 2, No. 5, 104-108 (2017)
www.astesj.com
Proceedings of International Conference on Applied Mathematics (ICAM2017), Taza, Morocco

ASTES Journal
ISSN: 2415-6698

Group law and the Security of elliptic curves on $F_p[e_1,...,e_n]$

Abdelalim Seddik*, Chaichaa Abdelhak, Souhail Mohamed

Laboratory of Topology, Algebra, Geometry and Discrete Mathematics, Department of Mathematical and computer sciences, Faculty of sciences Ain Chock Hassan II University of Casablanca.

Emails: seddikabs@hotmail.com, abdelchaichaa@gmail.com, mohamed90souhail@gmail.com

ARTICLEINFO

Article history:
Received: 12 April, 2017
Accepted: 04 May, 2017
Online: 28 December, 2017

Keywords:
The Discrete Logarithm Problem
Group Low
The Localization of the Ring
The maximal ideal
Complexity

ABSTRACT

In this paper, we study the elliptic curve $E_{a,b}(A_P)$, with A_P the localization of the ring $A = \mathbb{F}_p[e_1,...,e_n]$ where $e_ie_i = e_i$ and $e_ie_j = 0$ if $i \neq j$, in the maximal ideal $P = (e_1,...,e_n)$. Finally we show that $Card(E_{a,b}(A_P)) \geqslant (Card(E_{a,b}(\mathbb{F}_p))-3)^n + Card(E_{a,b}(\mathbb{F}_p))$ and the execution time to solve the problem of discrete logarithm in $E_{a,b}(A_P)$ is $\Omega(N)$, sch that the execution time to solve the problem of discrete logarithm in $E_{a,b}(\mathbb{F}_p)$ is $O(\sqrt{N})$. The motivation for this work came from search for new groups with intractable (DLP) discrete logarithm problem is therefore of great importance.

1 Introduction

The elliptic curves are a very fashionable subject in mathematics. They are the basis of the demonstration of Fermat's great theorem by Andrew Wiles, it was proposed for cryptographic use independently by Neal Koblitz[1] and Victor Miller in 1985, claim that elliptic curve cryptography requires much smaller keys than those used in conventional public key cryptosystems, while maintaining an equal level of security. In 2008, Virat introduced the elliptic curves over local ring $\mathbb{F}_p[\epsilon] = \mathbb{F}_p[X]/(X^2)$[2], and a proposed a new public key cryptosystem which is a variant of the ElGamal cryptosystem on an elliptic curve, in 2013 Chillali generalized the Virat result for the ring $\mathbb{F}_p[\epsilon] = \mathbb{F}_p[X]/(X^n)$ [3]. Chillali and Abdelalim constructed a ring $\mathbb{F}_p[e_1,e_2,e_3]$, defined an elliptic curve over $E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])$ and they showed that $Card(E_{a,b}(\mathbb{F}_p[e_1,e_2,e_3])) \geq (Card(E_{a,b}(\mathbb{F}_p))-3)^n + Card(E_{a,b}(\mathbb{F}_p))$ [4].

In this work we will generalize the construction of $\mathbb{F}_p[e_1,e_2,e_3]$ to $\mathbb{F}_p[e_1,..,e_n]$, but not a local ring to define a group law in $\mathbb{F}_p[e_1,..,e_n]$,we localized the ring $\mathbb{F}_p[e_1,..,e_n]$ in a maximal ideal, and we give it a group law and show that $Card(E_{a,b}(\mathbb{F}_p[e_1,..,e_n])) \geq (Card(E_{a,b}(\mathbb{F}_p)) - 3)^n + Card(E_{a,b}(\mathbb{F}_p))$, then shows the discrete logarithmic complexity is $\Omega(N)$ Such that $N = E_{a,b}(\mathbb{F}_p)$ by using the attacks baby step/giant step and ρ–Pollard.

Let p be an odd prime number and n be an integer such that $n \geq 1$. we consider the ring $A_n = \mathbb{F}_p[e_1,...,e_n] = \{a_0+a_1e_1+...+a_ne_n/a_0,a_1,...,a_n \in \mathbb{F}_p, e_ie_i = e_i$ and $e_ie_j = 0$ if $i \neq j\}$. $\mathbb{F}_p[e_1,...,e_n,]$ is vector space over $\mathbb{F}_p$ with basis $(1,e_1,...,e_n)$. We have
$X+Y = (x_0+y_0)+(x_1+x_1)e_1+...+(x_n+y_n)e_n$ and $X.Y = t_0+t_1e_1+...+t_ne_n$ with:

$$\begin{cases} t_0 = x_0y_0 & if \quad i = 0 \\ t_i = x_iy_0 + x_0y_i + x_iy_i & if \quad i \neq 0 \end{cases}$$

Proposition 1. *Let $X = x_0+x_1e_1+...+x_ne_n \in \mathbb{F}_p[e_1,...,e_n]$ then X is invertible if and only if $x_0 \neq 0$ and $x_i \neq -x_0$ for all $i \in \{1,...,n\}$.*

Proof. Let $X = x_0+x_1e_1+...+x_ne_n \in \mathbb{F}_p[e_1,...,e_n]$ a invertible element, there $Y = y_0+y_1e_1+...+y_ne_n \in \mathbb{F}_p[e_1,...,e_n]$ such that $X.Y = 1$, this implies that

$$\begin{cases} x_0y_0 = 1 & if \quad i = 0 \\ x_iy_0 + x_0y_i + x_iy_i = 0 & if \quad i \neq 0 \end{cases}$$

therefore, $x_0 \neq 0$ and $x_i \neq -x_0$ for all $i \in \{1,...,n\}$.
In this case:

$$\begin{cases} y_0 = x_0^{-1} & if \quad i = 0 \\ y_i = -(x_0+x_i)^{-1}x_ix_0^{-1} & if \quad i \neq 0 \end{cases}$$

*Corresponding Author: Abdelalim Seddik , UH2C , CASABLANCA, Morocco. Email:seddikabs@hotmail.com

https://dx.doi.org/10.25046/aj020517

The other since is evident.

Proposition 2. *The ideal $P = (e_1,...,e_n)$ is a maximal (prime) of a ring $\mathbb{F}_p[e_1,...,e_n]$.*

Proof. We have $\mathbb{F}_p[e_1,...,e_n]/P \simeq \mathbb{F}_p$ is a field, there P is maximal.

Proposition 3. *Let $S = \mathbb{F}_p[e_1,...,e_n] - P = \{s_0 + s_1e_1 + ... + s_ne_n / s_0 \in \mathbb{F}_p, s_0 \neq 0\}$. Then the localized of $\mathbb{F}_p[e_1,...,e_n]$ in P is:*
$A_P = \{\frac{x_0+x_1e_1+...+x_ne_n}{s_0+s_1e_1+...+s_ne_n} / x_0, x_1, ..., x_n, s_0, s_1, ..., s_n \in \mathbb{F}_p, s_0 \neq 0\}$

$$= \{\frac{x_0 + x_1e_1 + ... + x_ne_n}{1 + s_1e_1 + ... + s_ne_n} / x_0, x_1, ..., x_n, s_1, ..., s_n \in \mathbb{F}_p\}$$

A_P is a local ring its maximal ideal is
$M = \{\frac{x_1e_1+...+x_ne_n}{1+s_1e_1+...+s_ne_n} / x_1, ..., x_n, s_1, ..., s_n \in \mathbb{F}_p\}$ *and the residual field is $K \simeq \mathbb{F}_p$.*

Proposition 4. *The homomorphism :*

$$\begin{array}{ccc} \pi : A_P & \longrightarrow & \mathbb{F}_p \\ \frac{x_0+x_1e_1+...+x_ne_n}{1+s_1e_1+...+s_ne_n} & \longrightarrow & x_0 \end{array}$$

is a surjective homomorphism of rings.

2 The Elliptic Curve over the ring A_P

Let $n \in \mathbb{N}^*$, $A = \mathbb{F}_p[e_1,...,e_n]$, p a prime number $p \geq 5$, $P = (e_1,...,e_n)$ and A_P the localized of A in P.

Definition 1. *An elliptic curve over ring A_P is curve that is given by such Weierstrass equation:*

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

with $a, b \in A_P$ and $4a^3 + 27b^2$ is invertible on A_P, and the reduction over $\mathbb{F}_p$ is

$$Y^2Z = X^3 + \pi(a)XZ^2 + \pi(b)Z^3$$

$$E_{a,b}(\mathbb{F}_p) = \{[X : Y : Z] \in \mathbb{P}^2(\mathbb{F}_p) / Y^2Z = X^3 + aXZ^2 + bZ^3\}$$

$$E_{a,b}(A) = \{[X : Y : Z] \in \mathbb{P}^2(A) / Y^2Z = X^3 + aXZ^2 + bZ^3\}$$

$$E_{a,b}(A_P) = \{[X : Y : Z] \in \mathbb{P}^2(A_P) / Y^2Z = X^3 + aXZ^2 + bZ^3\}$$

Theorem 1. *The mapping*

$$\begin{array}{ccc} \phi : E_{a,b}(A) & \longrightarrow & E_{a,b}(A_P) \\ [x : y : z] & \longrightarrow & [\frac{x}{1} : \frac{y}{1} : \frac{z}{1}] \end{array}$$

is injective.

Proof. Let $[x : y : z], [x' : y' : z'] \in E_{a,b}(A)$
Suppose that $[x : y : z] = [x' : y' : z']$
$\Rightarrow \exists \lambda \in A$ such that $(x', y', z') = \lambda(x, y, z)$
$\Rightarrow (x', y', z') = (\lambda x, \lambda y, \lambda z)$
$\Rightarrow x' = \lambda x$, $y' = \lambda y$ and $z' = \lambda z$
$\Rightarrow \frac{x'}{1} = \lambda\frac{x}{1}$, $\frac{y'}{1} = \lambda\frac{y}{1}$ and $\frac{z'}{1} = \lambda\frac{z}{1}$
Then $[\frac{x'}{1} : \frac{x'}{1} : \frac{x'}{1}] = [\lambda\frac{x}{1} : \lambda\frac{x}{1} : \lambda\frac{x}{1}] = [\frac{x}{1} : \frac{x}{1} : \frac{x}{1}]$
we deduce that $\phi([x : y : z]) = \phi([x' : y' : z'])$
Then ϕ is well defined.
Note that mapping $\begin{array}{ccc} f : A & \longrightarrow & A_P \\ x & \longrightarrow & \frac{x}{1} \end{array}$ is injective.
We deduce ϕ is injective.

Theorem 2. *Let $a, b \in \mathbb{F}_p$, the mapping*

$$\begin{array}{ccc} \varphi : E_{a,b}(A_P) & \longrightarrow & E_{a,b}(A) \\ [\frac{x}{s_1} : \frac{y}{s_2} : \frac{z}{s_3}] & \longrightarrow & [xs_2s_3 : ys_1s_3 : zs_1s_2] \end{array}$$

is surjective.

Proof. Let $[\frac{x}{s_1} : \frac{y}{s_2} : \frac{z}{s_3}], [\frac{x'}{s_1'} : \frac{y'}{s_2'} : \frac{z'}{s_3'}] \in E_{a,b}(A_P)$
Suppose that $[\frac{x}{s_1} : \frac{y}{s_2} : \frac{z}{s_3}] = [\frac{x'}{s_1'} : \frac{y'}{s_2'} : \frac{z'}{s_3'}]$
Then $\exists \lambda \in A_P^*$ such that $(\frac{x'}{s_1'}, \frac{y'}{s_2'}, \frac{z'}{s_3'}) = \lambda(\frac{x}{s_1}, \frac{y}{s_2}, \frac{z}{s_3})$
$\Rightarrow \frac{x'}{s_1'} = \lambda\frac{x}{s_1}$; $\frac{y'}{s_2'} = \lambda\frac{y}{s_2}$; $\frac{z'}{s_3'} = \lambda\frac{z}{s_3}$
$\Rightarrow s_1s_2s_3\frac{x'}{s_1'} = \lambda s_2s_3x$; $s_1s_2s_3\frac{y'}{s_2'} = \lambda s_1s_3y$; $s_1s_2s_3\frac{z'}{s_3'} = \lambda s_1s_2z$
Then $\varphi[\frac{x'}{s_1'} : \frac{y'}{s_2'} : \frac{y'}{s_2'}] = \varphi[s_1s_2s_3\frac{x'}{s_1'} : s_1s_2s_3\frac{y'}{s_2'} : s_1s_2s_3\frac{z'}{s_3'}]$
$= \varphi[\lambda s_2s_3x : \lambda s_1s_3y : \lambda s_1s_2z]$
$= \varphi[s_2s_3x : s_1s_3y : s_1s_2z]$
$= \varphi[\frac{x}{s_1} : \frac{y}{s_2} : \frac{z}{s_3}]$
Then φ is well defined.
Let $[x : y : z] \in E_{a,b}(A)$, we have $\varphi[\frac{y}{1} : \frac{y}{1} : \frac{z}{1}] = [x : y : z]$.
Finally the mapping φ is surjective.

Corollary 1. *Let $a, b \in \mathbb{F}_p$, then*

$$Card(E_{a,b}(A_P)) = Card(E_{a,b}(A))$$

Proposition 5. *A Weierstrass equation is defined a elliptic curve over A_P if and only if the reduction ever $\mathbb{F}_p$ is a elliptic curve.*

Proposition 6. *Let $a, b \in A_P$ such that $4a^3+27b^2$ is invertible on A_P.The set $E_{a,b}(A_P)$ together with a special point $O = [0 : 1 : 0]$, a commutative binary operation denoted by $+$. It is well known that the binary operation $+$ endows the set $E_{a,b}(A_P)$ with an abelian group with O as identity element.*

Proof. The proof in M.Virat theses[2] page 56, based on [5] page 117 corollary 6.6 and [6] page 63.

Proposition 7. *Let $P = [x : y : z]$ and $P' = [x' : y' : z']$ in $E_{a,b}(A_P)$, we have*

1. *if $\pi_{E_{a,b}(A_P)}(P) \neq \pi_{E_{a,b}(A_P)}(P')$ then $P + P' = [p_1 : q_1 : r_1]$ with*
   $p_1 = y^2x'z' - zxy'^2 - a(zx' + xz')(zx' - xz') + (2yy' - 3bzz')(zx' - xz')$
   $q_1 = yy'(z'y - zy') - a(xyz'^2 - z^2x'y') + (-2azz' - 3xx')(x'y - xy') - 3bzz'(z'y - zy')$
   $r_1 = (zy' + z'y)(z'y - zy') + (3xx' + azz')(zx' - xz')$
2. *if $\pi_{E_{a,b}(R)}(P) = \pi_{E_{a,b}(R)}(P')$ then $P + P' = [p_2 : q_2 : r_2]$ with*
   $p_2 = (yy' - bzz')(x'y + xy') + (a^2zz' - 2axx')(zy' + z'y) - 3b(xyz'^2 + z^2x'y') - a(yzx'^2 + x^2y'z')$

$$q_2 = y^2y'^2 + 3ax^2x'^2 + (-a^3 - 9b^2)z^2z'^2 - a^2(zx' + xz')^2 - 2a^2zxz'x' + (9bxx' - 3abzz')(zx' + xz')$$
$$r_2 = (yy' + 3bzz')(zy' + z'y) + (3xx' + 2azz')(x'y + xy') + a(xyz'^2 + z^2x'y')$$

Proof. The proof in M.Virat theses[2] page 57 Proposition 2.1.2. based on formulas I, II and III in the article of H.Lange and W.Ruppert[7].

Corollary 2. *The mapping*

$$\begin{array}{ccc} \pi_{E(A_P)} : E(A_P) & \longrightarrow & E(\mathbb{F}_p) \\ [x:y:z] & \longrightarrow & [\pi(x):\pi(y):\pi(z)] \end{array} \text{ is a homomorphism of groups.}$$

Theorem 3. *Let $a, b \in \mathbb{F}_p$. Then*

$$Card(E_{a,b}(A)) \geqslant (Card(E_{a,b}(\mathbb{F}_p)) - 3)^n + Card(E_{a,b}(\mathbb{F}_p))$$

Proof. The proof for $n = 3$ exist in article of A.Chilali, S.Abdelalim[4].
For $n \in \mathbb{N}^*$ We consider the set:

$$\begin{aligned} T &= \{[x:y:z]/y^2z = x^3 + axz^2 + bz^3\} \\ &= \{[x:0:z]/0 = x^3 + axz^2 + bz^3\} \\ &= \{[x:0:1]/0 = x^3 + ax + b\} \end{aligned}$$

then $Card(T)$ is exactly the number of the solution of the equation $x^3 + ax + b = 0$
therefore $Card(T) \leq 3$.
Let

$$\begin{aligned} G &= E_{a,n}(\mathbb{F}_p) - T \\ &= \{[x:y:z] \in \mathbb{P}^2(\mathbb{F}_p)/y^2z = x^3 + axz^2 + bz^3 \text{ avec } y \neq 0\} \\ &= \{[x:1:z] \in \mathbb{P}^2(\mathbb{F}_p)/z = x^3 + axz^2 + bz^3\} \\ &= \{[x:1:z] \in \mathbb{P}^2(\mathbb{F}_p)/[x:1:z] \in E_{a,n}(\mathbb{F}_p)\} \end{aligned}$$

therefore $Card(G) \geq Card(E_{a,n}(\mathbb{F}_p)) - 3$
We consider the mapping:

$$\begin{array}{ccc} \alpha : G^n & \longrightarrow & E_{a,b}(A) \\ ([x_i:y_i:z_i])_{i=1}^{i=n} & \longrightarrow & [\sum_{i=0}^n x_ie_i : 1 : \sum_{i=0}^n z_ie_i] \end{array}$$

We have:

$$(\sum_{i=0}^n x_ie_i)^3 = \sum_{i=0}^n (x_ie_i)^3$$
$$(\sum_{i=0}^n z_ie_i)^2 = \sum_{i=0}^n (z_ie_i)^2$$
$$a(\sum_{i=0}^n x_ie_i)(\sum_{i=0}^n z_ie_i)^2 = a\sum_{i=1}^n (x_ie_i)(z_ie_i)^2$$

Since $[x_i : 1 : z_i] \in E_{a,n}(\mathbb{F}_p)$ then $z_i = x_i^3 + ax_iz_i^2 + bz_i^3$. It is clear that :

$$z_ie_i = (x_ie_i)^2 + a(x_ie_i)(z_ie_i)^2 + b(z_ie_i)^3, \ \forall i \in \{1,..,n\}$$
$$\sum_{i=0}^n z_ie_i = \sum_{i=0}^n (x_ie_i)^3 + a\sum_{i=0}^n (x_ie_i)(z_ie_i)^2 + b\sum_{i=0}^n (z_ie_i)^3$$

$$\sum_{i=0}^n z_ie_i = (\sum_{i=0}^n x_ie_i)^3 + a(\sum_{i=0}^n x_ie_i)(\sum_{i=0}^n z_ie_i)^2 + b(\sum_{i=0}^n z_ie_i)^3$$

we deduce that:

$$[\sum_{i=0}^n x_ie_i : 1 : \sum_{i=0}^n z_ie_i] \in E_{a,b}(A)$$

α is injective. Then

$$E_{a,n}(\mathbb{F}_p) \subseteq E_{a,b}(A)$$
$$\alpha(G^n) \subseteq E_{a,b}(A)$$

and $E_{a,n}(\mathbb{F}_p) \cap \alpha(G^n) = \{[0:1:0]\}$
We result that

$$Card(E_{a,b}(A)) \geq Card(\alpha(G^n)) + Card(E_{a,n}(\mathbb{F}_p)) - 1$$

Since α is injective, then

$$Card(G^n) = Card(G)^n \geq Card(E_{a,n}(\mathbb{F}_p) - 3)^n$$

we deduce that:

$$Card(E_{a,b}(A)) \geq Card(E_{a,n}(\mathbb{F}_p) - 1)^n + Card(E_{a,n}(\mathbb{F}_p))$$

Corollary 3. *Let a and b two elements of $\mathbb{F}_p$. Then*

$$Card(E_{a,b}(A_P)) \geqslant (Card(E_{a,b}(\mathbb{F}_p)) - 3)^n + Card(E_{a,b}(\mathbb{F}_p))$$

Proof. In Corollary 1 $Card(E_{a,b}(A_P)) = Card(E_{a,b}(A))$, and in Theorem 3

$$Card(E_{a,b}(A)) \geqslant (Card(E_{a,b}(\mathbb{F}_p)) - 3)^n + Card(E_{a,b}(\mathbb{F}_p))$$

we deduce that:

$$Card(E_{a,b}(A_P)) \geqslant (Card(E_{a,b}(\mathbb{F}_p)) - 3)^n + Card(E_{a,b}(\mathbb{F}_p))$$

3 The discrete logarithm problem: complexity and security

The discrete logarithm problem for G may be stated as: Given $g \in G$ and $h \in < g >$, find an integer x such that $h = g^x$ and $ord(g) = q$ a prime number.

Baby-Step/Giant-Step Method: The idea behind the Baby-Step/Giant-Step method is a standard divide-and-conquer approach found in many areas of computer science. We write

$$x = x_0 + x_1\lceil q \rfloor$$

Now, since $0 \leq x \leq q$, we have that $0 \leq x_0, x_1 \leq \lceil q \rfloor$ We first compute the Baby-Steps

$$g_i \longleftarrow g^i, for 0 \leq i \leq \lceil q \rfloor$$

The pairs (g_i, i) are stored in a table so that one can easily search for items indexed by the first entry in the pair. This can be accomplished by sorting the table on the first entry, or more efficiently by the use of hash tables. To compute and store the Baby-Steps clearly requires $O(\lceil q \rfloor)$ time and a similar amount of storage.
We now compute the Giant-Steps $h_j \longleftarrow h.g^{-j\lceil q \rfloor}$ for

$0 \leq j \leq \lceil q \rceil$, and try to find a match in the table of Baby-Steps, i.e. we try to find a value g_i such that $g_i = h_j$. If such a match occurs we have $x_0 = i$ and $x_1 = j$.
since, if $g_i = h_j$, we have $g^i = h.g^{-j\lceil q \rceil}$
i.e $g^{i+j\lceil q \rceil} = h$
Notice that the time to compute the Giant-Steps is at most $O(\sqrt{q})$.
Hence, the overall time and space complexity of the Baby-Step/Giant-Step method is $O(\sqrt{q})$[8].
Pollard-Type Methods: We define a partition $G = S_0 \cup S_1 \cup S_2$ and the function

$$f(y,a,b) = \begin{cases} (hy, a, a+b \ mod(q)) & if \quad y \in S_0 \\ (y^2, 2a \ mod(q), 2b \ mod(q)) & if \quad y \in S_1 \\ (gy, a+1 \ mod(q), b) & if \quad y \in S_2 \end{cases}$$

Note that if $y = g^a h^b$, Then, taking $(z,k,l) = (y,a,b)$, $z = g^k h^l$.
Then, it is possible to iterate f until finding two identical results: $(y,a,b) = (z,k,l)$ and

$$g^a h^b = y = z = g^k h^l \Rightarrow g^{l-k} = h^{l-b}$$

As $g^x = h$, we have

$$g^{a-k} = g^{x(l-b)} \Rightarrow x(l-b) = (a-k) \ mod(q)$$

if $l-b$ Is invertible modulo q, We find the solution

$$x = (a-k)(l-b)^{-1} \ mod(q)$$

The time and space complexity of the method is $O(\sqrt{q})$.

Let $Card(E_{a,b}(A_P)) = M$ and $Card(E_{a,b})(\mathbb{F}_p) = N$ $n \geq 3$, and $N \geq 7$[8].

Theorem 4. *The time for solving DLP in $E_{a,b}(A_P)$ is $\Omega(N)$, and $O(\sqrt{N})$ for solving DLP in $E_{a,b}(\mathbb{F}_p)$.*

Proof. Its clear that for solving DLP in $E_{a,b}(\mathbb{F}_p)$ is $O(\sqrt{N})$. We have the time for solving DLP in $E_{a,b}(A_P)$ is $O(\sqrt{M})$. And: $M \geq (N-3)^n + N$
$\Rightarrow M \geq (N-3)^3 + N \geq N^2$ because $n \geq 3$ and $N \geq 7$
$\Rightarrow \sqrt{M} \geq N$
$\Rightarrow \sqrt{M} = \Omega(N)$
Then the time complexity for solving DLP in $E_{a,b}(A_P)$ is $\Omega(N)$ Instead of $O(\sqrt{N})$ for $E_{a,b}(\mathbb{F}_p)$.

Example:
Let $n = 3$, $p = 5$, $a = 1$ and $b = 1$.
$E_{1,1}(\mathbb{F}_5) = \{[0:1:0],[0:1:1],[0:4:1],[2:1:1],[2:4:1],[3:1:1],[3:4:1],[4:2:1],[4:3:1]\}$
We have $Card(E_{1,1}(\mathbb{F}_5)) = 9$. Then
$Card(E_{1,1}(A_P)) \geq (E_{1,1}(\mathbb{F}_5) - 3)^3 + Card(E_{1,1}(\mathbb{F}_5)) = 225$
The following table gives the difficulty of calculating in $A = \mathbb{F}_5[e_1,e_2,e_3]$, and in $E_{1,1}(A)$ as a function of the $\mathbb{F}_5$ addition and the multiplication.

Operations	+ in $\mathbb{F}_5$	× in $\mathbb{F}_5$
+ in $\mathbb{F}_5[e_1,e_2,e_3]$	3	0
× in $\mathbb{F}_5[e_1,e_2,e_3]$	6	10
+ in $E_{1,1}(\mathbb{F}_5[e_1,e_2,e_3])$	582	870
+ in $E_{1,1}(\mathbb{F}_5)$	6	4

Note that the computational difficulty in $E_{1,1}(\mathbb{F}_5[e_1,e_2,e_3])$ is much more difficult than in $E_{1,1}(\mathbb{F}_5)$.

4 The fundamental algorithms

4.1 Algorithms in A

Algorithm 1 $sum\_1(p)$
Input:$(X = (x_0,x_1,...,x_n), Y = (y_0,y_1,...,y_n))$;
Output:$(Z = X + Y)$;
for $i = 0$ to n do:
$z_i = x_i + y_i$;
end for;
return $Z = (z_0,z_1,...,z_n)$;
end;

Algorithm 2 $prod\_1(p)$
Input:$(X = (x_0,x_1,...,x_n), Y = (y_0,y_1,...,y_n))$;
Output:$(Z = X.Y)$;
$z_0 = x_0.y_0$;
for $i = 1$ to n do:
$z_i = x_0 y_i + x_i y_i + x_i y_0$;
en for;
return $Z = (z_0,z_1,...,z_n)$;
end;

Algorithm 3 $if\_invertible\_1(p)$
Input:$(X = (x_0,x_1,...,x_n))$
Output:(true,false)
for $i = 1$ to n do
if $(x_0 + x_i == 0 \ mod(p)$ or $x_0 = 0)$
return false;
end if
end for;
return true;
end;

Algorithm 4 $invertible\_1(p)$
Input:$(X = (x_0,x_1,...,x_n))$;
Output:$(Z = X^{-1})$;
if $(if\_invertible\_1(X) == false)$;
print("X is not invertible);
return null;
end if;
$z_0 = x_0^{-1}$;
for $i = 1$ to n do
$z_i = -(x_0 + x_i)^{-1} x_i x_0^{-1}$;
end for;
return $Z = (z_0,z_1,...,z_n)$;
end;

Algorithm 5 $projection\_1(p)$
Input:$(X = (x_0,x_1,...,x_n))$;
Output: x_0;
return x_0;
end;

4.2 Algorithms in A_P

Algorithm 6 $prod\_2(p)$

Input: $(X = ((x_0, x_1, ..., x_n), (1, s_1, ..., s_n)),$
$Y = ((y_0, y_1, ..., y_n), (1, t_1, ..., t_n)));$
Output: XY;
$A = pod\_1((x_0, x_1, ..., x_n), (y_0, y_1, ..., y_n));$
$B = pod\_1((1, s_1, ..., s_n), (1, t_1, ..., t_n));$
$Z = (A, B);$
return Z;
end;

Algorithm 7 $sum\_2(p)$

Input: $(X = ((x_0, x_1, ..., x_n), (1, s_1, ..., s_n)),$
$Y = ((y_0, y_1, ..., y_n), (1, t_1, ..., t_n)));$
Output: $X + Y$;
$A = sum\_1(prod\_1((x_0, x_1, ..., x_n), (1, t_1, ..., t_n)),$
$prod\_1((y_0, y_1, ..., y_n), (1, s_1, ..., s_n)));$
$B = pud\_1((1, s_1, ..., s_n), (1, t_1, ..., t_n));$
$Z = (A, B);$
return Z;
end;

Algorithm 8 $projection\_2(p)$

Input:$(X = ((x_0, x_1, ..., x_n), (1, s_1, ..., s_n)));$
Output: x_0;
return x_0;
end;

4.3 Algorithms in $E_{a,b}(A_P)$

Algorithm 9 $projection\_3(p)$

Input:(X, Y, Z);
Output: $(\pi(X), \pi(Y), \pi(Z))$;
return $(projection\_2(X), projection\_2(Y),$
$projection\_2(Z))$;
end;

In this algorithm the + and . in A_P for simplicity

Algorithm 10 $sum\_3(p)$

Input: $(X = (x, y, z), Y = (x', y', z'))$;
Output: $X + Y = (p, q, r)$;
if $projection\_3(X) = projection\_3(Y)$ then;
$p = y^2x'z' - zxy'^2 - a(zx' + xz')(zx' - xz') + (2yy' - 3bzz')(zx' - xz')$;
$q = yy'(z'y - zy') - a(xyz'^2 - z^2x'y') + (-2azz' - 3xx')(x'y - xy') - 3bzz'(z'y - zy')$;
$r = (zy' + z'y)(z'y - zy') + (3xx' + azz')(zx' - xz')$;
else
$p = (yy' - bzz')(x'y + xy') + (a^2zz' - 2axx')(zy' + z'y) - 3b(xyz'^2 + z^2x'y') - a(yzx'^2 + x^2y'z')$;
$q = y^2y'^2 + 3ax^2x'^2 + (-a^3 - 9b^2)z^2z'^2 - a^2(zx' + xz')^2 - 2a^2zxz'x' + (9bxx' - 3abzz')(zx' + xz')$;
$r = (yy' + 3bzz')(zy' + z'y) + (3xx' + 2azz')(x'y + xy') + a(xyz'^2 + z^2x'y')$;
end if;
return (p, q, r);
fin ;

5 Conclusion

In this work we study the elliptic curves over a special ring, and we construct a new groups with intractable discrete logarithm problem is therefore of great importance, This allows to define more secure cryptographic cryptosystems.

References

[1] N. Koblitz. *Elliptic Curve Cryptosystems*. Mathematics of Computation, (48): 203-209, 1987.

[2] M. Virat. *Courbe elliptique sur un anneau et applications cryptographiques*. Thése Docteur en Sciences, Nice-Sophia Antipolis. (2009).

[3] Abdelhakim Chillali. *Elliptic Curve Over Special Ideal Ring*. Int. J. Open Problems Compt. Math., Vol. 6, No. 2, June 2013.

[4] A. Chilali, S.Abdelalim. *The Eliptic Curves* $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ Gulf Journal of Mathematics Vol 3, Issue 2 (2015) 49-53.

[5] D. Mumford, J. Fogarty, and F. Kirwan.*Geometric Invariant Theory* , volume 34 of A Series of Modern Surveys in Mathematics . Springer-Verlag, 3e edition, 1994.

[6] N.M. Katz and B.Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.

[7] H.Lange and W.Ruppert. *Complete systems of addition laws on abelian varieties*. Invent.Math. 79, 603-610(1985).

[8] Nigel P. Smart. *Cryptography Made Simple*. Springer International Publishing, 2016.

[9] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.

[10] Lawrence C.Washington. *Elliptic Curves Number Theory and Cryptography*. Chapman & HallCRC 2008.

[11] Andreas Enge. *Elleptic Curves And Their Applications To Cryptography, An Introduction*. Kluwers Academic Publishers, 1999.