INTERNATIONAL JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS
DOI: 10.46300/91014.2020.14.11 Volume 14, 2020

Elliptic Curve Over SPIR Of Characteristic Two

Abdelhamid TADMORI
Departement of Mathematics
Faculty of science Mohamed first
University Oujda MOROCCO
atadmori@yahoo.fr

Abdelhakim CHILLALI
FST
USMBA, FES
MORROCO
chil2007@voila.fr

M'hamed ZIANE
Departement of Mathematics
Faculty of science Mohamed first
University Oujda MOROCCO
Ziane20011@yahoo.fr

***Abstract*—In [1] and [4] we defined the elliptic curve over the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^2 = 0$. In this work, we will study the elliptic curve over the ring $\mathbf{A} = \mathbb{F}_{2^d}[\varepsilon]$, where d is a positive integer and $\varepsilon^2 = 0$. More precisely we will establish a group homomorphism between the abulia group $(\mathbf{E}_{a,b,c}(\mathbb{F}_{2^d}), +)$ and $(\mathbb{F}_{2^d}, +)$.**

I. Introduction

Let d be an integer, we consider the quotient ring

$$\mathbf{A} = \frac{\mathbb{F}_{2^d}[X]}{(X^2)},$$

where $\mathbb{F}_{2^d}$ is the finite field of order 2^d.
Then the ring $\mathbf{A}$ is identified to the ring $\mathbb{F}_{2^d}[\varepsilon]$ with $\varepsilon^2 = 0$, ie:

$$\mathbf{A} = \{ a_0 + a_1 \cdot \varepsilon \mid a_0, a_1 \in \mathbb{F}_{2^d} \}.$$

We consider the elliptic curve over the ring $\mathbf{A}$ which is given by equation $Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3$, where a,b,c are in $\mathbf{A}$ and c^6b is invertible in $\mathbf{A}$, see [1] and [2].

II. Notations

Let a,b,c $\in \mathbf{A}$, such that c^6b is invertible in $\mathbf{A}$. We denote the elliptic curve over $\mathbf{A}$ by $\mathbf{E}_{a,b,c}(\mathbf{A})$ and we write:

$$\mathbf{E}_{a,b,c}(\mathbf{A}) = \{ [X : Y : Z] \in \mathbb{P}_2(\mathbf{A}) \mid Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3 \}.$$

If $b_0, c_0 \in \mathbb{F}_{2^d} \setminus \{0\}$ and $a_0 \in \mathbb{F}_{2^d}$, we also write:

$$\mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d}) = \{ [X : Y : Z] \in \mathbb{P}_2(\mathbb{F}_{2^d}) \mid Y^2Z + c_0XYZ = X^3 + a_0X^2Z + b_0Z^3 \}.$$

III. Classification of elements of $\mathbf{E}_{a,b,c}(\mathbf{A})$

Let $[X : Y : Z] \in \mathbf{E}_{a,b,c}(\mathbf{A})$, where X, Y and Z are in $\mathbf{A}$. We have tow cases for Z:

- Z invertible: then $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1]$ hence we take just [X:Y:1].
- Z non invertible: so $Z = z_1\varepsilon$, see [3] in this cases we have tow cases for Y.

- If Y invertible: then $[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}]$, so we just take $[X : 1 : z_1\varepsilon] \in \mathbf{E}_{a,b,c}(\mathbf{A})$, then is verified the equation of

$$\mathbf{E}_{a,b,c}(\mathbf{A}) : Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3,$$

so we can write:

$$a = a_0 + a_1$$

$$b = b_0 + b_1$$

$$c = c_0 + c_1$$

$$X = x_0 + x_1$$

- We have:

$$z_1\varepsilon + (c_0 + c_1\varepsilon) \cdot (x_0 + x_1\varepsilon) \cdot z_1\varepsilon = (x_0 + x_1\varepsilon)^3 + (a_0 + a_1\varepsilon) \cdot (x_0 + x_1\varepsilon)^2 \cdot z_1\varepsilon + (b_0 + b_1\varepsilon) \cdot z_1^3\varepsilon^3,$$

which implies that

$$z_1\varepsilon + (c_0 + c_1\varepsilon) \cdot (x_0z_1\varepsilon) = x_0^3 + (x_0^2x_1 + a_0x_0^2z_1)\varepsilon$$

so

$$z_1\varepsilon + c_0x_0z_1\varepsilon = x_0^3 + (x_0^2x_1 + a_0x_0^2z_1)\varepsilon$$

then

$$(z_1 + c_0x_0z_1) \cdot \varepsilon = x_0^3 + (x_0^2x_1 + a_0x_0^2z_1)\varepsilon$$

since $(1, \varepsilon)$ is a base of the vector space $\mathbf{A}$ over $\mathbb{F}_{2^d}$ then $x_0 = 0$, so $X = x_1\varepsilon$ and $z_1\varepsilon = 0$ (ie $z_1 = 0$) hence $[X : 1 : z_1\varepsilon] = [x_1\varepsilon : 1 : 0]$.

- If Y non invertible: then we have $Y = y_1\varepsilon$, so $x = x_0 + x_1\varepsilon$ is invertible so we take $[X : Y : Z] \sim [1 : y_1\varepsilon : z_1\varepsilon]$, thus $1 + a.z_1\varepsilon = 0$, ie: $1 + a_0.z_1\varepsilon = 0$, which is absurd

Proposition 1. *Every element of $\mathbf{E}_{a,b,c}(\mathbf{A})$ is of the form $[X : Y : 1]$ or $[x\varepsilon : 1 : 0]$, where $x \in \mathbb{F}_{2^d}$ and we write*

$$\mathbf{E}_{a,b,c}(\mathbf{A}) = \{ [X : Y : 1] \in \mathbb{P}_2(\mathbf{A}) \mid Y^2 + cXY = X^3 + aX^2 + b \} \bigcup \{ [x\varepsilon : 1 : 0] \mid x \in \mathbb{F}_{2^d} \}.$$

IV. The π_2 homomorphism

We consider the canonical projection π defined by:

$$\pi : \mathbb{F}_{2^d}[\varepsilon] \longrightarrow \mathbb{F}_{2^d}$$

$$x_0 + x_1\varepsilon \longmapsto x_0$$

Lemma 2. *π is a morphism of rings.*

Proof.. let $X = x_0 + x_1\varepsilon$ and $Y = y_0 + y_1\varepsilon$ then:

$$X + Y = x_0 + y_0 + (x_1 + y_1)\varepsilon$$

$$X \cdot Y = (x_0 + x_1\varepsilon) \cdot (y_0 + y_1\varepsilon)$$

$$= x_0 \cdot y_0 + x_0y_1\varepsilon + y_0x_1\varepsilon$$

$$= x_0 \cdot y_0 + (x_0y_1 + y_0x_1)\varepsilon,$$

DOI: 10.46300/91014.2020.14.11 Volume 14, 2020

so :

$$\pi(X+Y) = \pi(X) + \pi(y)$$

$$\pi(X \cdot Y) = \pi(X) \times \pi(Y),$$

therefore π is a morphism of rings. □

Lemma 3. *Let* $[X : Y : Z] \in \mathbb{P}_2(\mathbf{A})$, *where*

$$X = x_0 + x_1\varepsilon$$

$$Y = y_0 + y_1\varepsilon$$

$$Z = z_0 + z_1\varepsilon$$

$$a = a_0 + a_1\varepsilon$$

$$b = b_0 + b_1\varepsilon$$

$$c = c_0 + c_1\varepsilon$$

then $[X : Y : Z] \in \mathbf{E}_{a,b,c}(\mathbf{A})$ *if and only if*

$$y_0^2 z_0 + c_0 x_0 y_0 z_0 = x_0^3 + a_0 x_0^2 z_0 + b_0 z_0^3$$

$$y_0^2 z_1 + c_0 x_0 (y_0 z_1 + y_1 z_0) + y_0 z_0 (c_0 x_1 + c_1 x_0) = a_0 x_0^2 z_1 + b_1 z_0^3 + a_1 x_0^2 z_0 + x_0^2 x_1 + b_0 z_0^2 z_1$$

Proof.. Since $(1, \varepsilon)$ is a base of the vector space $\mathbf{A}$ over $\mathbb{F}_{2^d}$, and $[X : Y : Z] \in \mathbf{E}_{a,b,c}(\mathbf{A})$, then

$$Y^2 Z + cXYZ = X^3 + aX^2 Z + bZ^3,$$

so after the compute, we find the result. □

⋆ Let π_2 the mapping defined by:

$$\mathbf{E}_{a,b,c}(\mathbf{A}) \xrightarrow{\pi_2} \mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$$

$$[X : Y : Z] \longmapsto [\pi(X) : \pi(Y) : \pi(Z)]$$

We proof that the mapping π_2 is a surjective homomorphism of groups.

Theorem 4. *Let* $\mathbf{P} = [X_1 : Y_1 : Z_1]$ *and* $\mathbf{Q} = [X_2 : Y_2 : Z_2]$ *tow points in* $\mathbf{E}_{a,b,c}(\mathbf{A})$, *and* $\mathbf{P} + \mathbf{Q} = [X_3 : Y_3 : Z_3]$.

- *If* $\pi_2(\mathbf{P}) = \pi_2(\mathbf{Q})$, *then:*
  $X_3 = X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + cX_2^2Y_1^2 + c^2X_1X_2^2Y_1 + aX_1^2X_2Y_2 + aX_1X_2^2Y_1 + acX_1^2X_2^2 + bX_1Y_1Z_2^2 + bX_2Y_2Z_1^2 + bcX_1^2Z_2^2 + c^2bY_1Z_2^2Z_1 + c^2bY_2Z_1^2Z_2 + c^3bX_1Z_2^2Z_1$
  $Y_3 = Y_1^2Y_2^2 + cX_2Y_1^2Y_2 + acX_1X_2^2Y_1 + a^2X_1^2X_2^2 + bX_1^2X_2Z_2 + bX_1X_2^2Z_1 + bcX_1Y_1Z_2^2 + bc^2X_1^2Z_2^2 + abX_2^2Z_1^2 + bc^3Y_1Z_1Z_2^2 + bc^4X_1Z_1Z_2^2 + abc^2X_1Z_1Z_2^2 + abc^2X_2Z_1^2Z_2 + b^2Z_1^2Z_2^2$
  $Z_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + cX_1^2X_2^2 + cY_1^2X_2Z_2 + c^2X_1^2Y_2Z_2 + aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1 + c^3X_1^2X_2Z_2 + acX_1X_2^2Z_1 + bY_1Z_1Z_2^2 + bY_2Z_1^2Z_2 + bcX_1Z_1Z_2^2$
- *If* $\pi_2(\mathbf{P}) \neq \pi_2(\mathbf{Q})$, *then:*
  $X_3 = X_1Y_2^2Z_1 + X_2Y_1^2Z_2 + cX_1^2Y_2Z_2 + cX_2^2Y_1Z_1 + aX_1^2X_2Z_2 + aX_1X_2^2Z_1 + bX_1Z_1Z_2^2 + bX_2Z_1^2Z_2$
  $Y_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + c^2X_1^2Y_2Z_2 + c^2X_2^2Y_1Z_1 + aX_1^2Y_2Z_2 + aX_2^2Y_1Z_1 + acX_1^2X_2Z_2 + acX_1X_2^2Z_1 + bY_1Z_1Z_2^2 + bY_2Z_1^2Z_2 + bcX_1Z_1Z_2^2 + bcX_2Z_1^2Z_2$
  $Z_3 = X_1^2X_2Z_2 + X_1X_2^2Z_1 + Y_1^2Z_2^2 + Y_2^2Z_1^2 + cX_1Y_1Z_2^2 + cX_2Y_2Z_1^2 + aX_1^2Z_2^2 + aX_2^2Z_1^2$

Proof.. Using the explicit formulas in W.Bosma and H.Lenstra article , see [5], we prove the theorem. □

Lemma 5. *The mapping* π_2 *is a surjective homomorphism of groups*

Proof.. The formula of lemma(3) means that $\pi_2([X : Y : Z]) = [x_0 : y_0 : z_0]$, and $[x_0 : y_0 : z_0] \in \mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$, so π_2 is well defined.
π_2 is surjective: let $[x_0 : y_0 : z_0] \in \mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$ we will show that $[x_0 : y_0 : z_0]$ have an antecedent

$$[x : y : z] \in \mathbf{E}_{a,b,c}(\mathbf{A})$$

- Case 1: $z_0 = 0$, then $[x_0 : y_0 : z_0] = [0 : 1 : 0]$ and we just take $[X : Y : Z] = [0 : 1 : 0]$.
- Case 2: $z_0 \neq 0$, then $[x_0 : y_0 : z_0] = [z_0^{-1}x_0 : z_0^{-1}y_0 : 1]$ so we just take $[x_0 : y_0 : 1]$.

so we will find an antecedent $[X : Y : Z]$ of $[x_0 : y_0 : 1]$ of the form

$$[x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : 1],$$

from the formulas of the lemma (3) we have:

$$y_0^2 + c_0x_0y_0 = x_0^3 + a_0x_0^2 + b_0,$$

and

$$c_0(x_0y_1 + y_0x_1) + c_1x_0y_0 = a_1x_0^2 + x_0^2x_1 + b_1,$$

there is three sub-cases:

- Case 2,1: $x_0 \neq 0$, then we just take
  $$[X : Y : Z] = [x_0 : \ y_0 + (c_0x_0)^{-1} \cdot (a_1x_0^2 + c_1x_0y_0 + b_1)\varepsilon : \ 1],$$
  because $c^6 b$ is invertible so $c_0 \neq 0$
- Case 2,2: $y_0 \neq 0$, then,we just take
  $$[X : Y : Z] = [(c_0y_0)^{-1} \cdot b_1\varepsilon : \ y_0 : \ 1]$$
- Case 2,3: $y_0 = 0$ and $x_0 = 0$ then we have $b_0 = 0$ absurd because $c^6 b$ is invertible ie $b_0 \neq 0$ and $c_0 \neq 0$

π_2 is an homomorphism: we just use the theorem(4) and lemma(2) □

Lemma 6.

$$[x\varepsilon : 1 : 0] + [y\varepsilon : 1 : 0] = [(x+y)\varepsilon : 1 : 0]$$

Proof.. We have $\pi_2([x\varepsilon : 1 : 0]) = \pi_2([y\varepsilon : 1 : 0])$, so by applying the formula in theorem (4)we have:

$$X_3 = (x+y)\varepsilon, Y_3 = 1 + cy\varepsilon \ \texttt{and} \ Z_3 = 0,$$

so

$$[x\varepsilon : 1 : 0] + [y\varepsilon : 1 : 0] = [(x+y)\varepsilon : 1 + cy\varepsilon : 0] = [(x+y)\varepsilon : 1 : 0]$$

□

Lemma 7. *The mapping*

$$\mathbb{F}_{2^d} \xrightarrow{\theta} \mathbf{E}_{a,b,c}(\mathbf{A})$$

$$x \longmapsto [x\varepsilon : 1 : 0]$$

is an injective morphism of groups.

Proof.. θ is well defined because

$$[x\varepsilon : 1 : 0] \in \mathbf{E}_{a,b,c}(\mathbf{A}),$$

see proposition (1) and from the lemma (6)we have:

$$\theta(x+y) = [(x+y)\varepsilon : 1 : 0] = [x\varepsilon : 1 : 0]+[y\varepsilon : 1 : 0] = \theta(x)+\theta(y),$$

then θ is a morphism.
•θ is injective (evidently) □

Lemma 8.

$$\textbf{\textit{Ker}}(\pi_2) = \theta(\mathbb{F}_{2^d})$$

Proof.. Evidently we have: $\theta(\mathbb{F}_{2^d}) \subseteq \mathbf{Ker}(\pi_2)$, now let,

$$\mathbf{P} = [X : Y : Z] = [x_0+x_1\varepsilon : y_0+y_1\varepsilon : z_0+z_1\varepsilon] \in \mathbf{Ker}(\pi_2),$$

implies that $\pi_2(\mathbf{P}) = [x_0 : y_0 : z_0] = [0 : 1 : 0]$, implies that $\mathbf{P} = [x_1\varepsilon : 1 : z_1\varepsilon] \in \mathbf{E}_{a,b,c}(\mathbf{A})$ and from the proposition (1) we have:
$\mathbf{P} = [x\varepsilon : 1 : 0] \in \theta(\mathbb{F}_{2^d})$, ie: $\mathbf{Ker}(\pi_2) \subseteq \theta(\mathbb{F}_{2^d})$, hence $\mathbf{Ker}(\pi_2) = \theta(\mathbb{F}_{2^d})$ □

From lemmas (5), (7) and (8) we deduce the following corollary:

Corollary 9. *The sequence*

$$0 \longrightarrow \textbf{\textit{Ker}}(\pi_2) \xrightarrow{i} \mathbf{E}_{a,b,c}(\mathbf{A}) \xrightarrow{\pi_2} \mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d}) \longrightarrow 0$$

is a short exact sequence which defines the group extension $\mathbf{E}_{a,b,c}(\mathbf{A})$ of $\mathbf{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$ by $\textbf{\textit{Ker}}(\pi_2)$, where i is the canonical injection.

V. CRYPTOGRAPHIC APPLICATION

Let $\mathbf{E}_{a,b,c}(\mathbf{A})$ an elliptic curve over A and $P \in \mathbf{E}_{a,b,c}(\mathbf{A})$ of order l . We will use the subgroup $< P >$ of $\mathbf{E}_{a,b,c}(\mathbf{A})$ to encrypt messages, and we denote $G =< P >$.

1) Coding of elements of G
We will give a code to each element $Q = mP$ where $m \in \{1, 2, .., l\}$ defined as it follows:
if $Q = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : Z]$ where $x_i, y_i \in A$ for $i = 0$ or 1 and $Z = 0$ or 1. We set:

$$x_i = c_{0i} + c_{1i}\alpha$$

$$y_i = d_{0i} + d_{1i}\alpha$$

where α is primitive root of an irreducible polynomial of degree 2 over $\mathbb{F}_2$ and $c_{ij}, d_{ij} \in \mathbb{F}_2$.
Then we code Q as it follows:
If $Z = 1$ then: $Q = c_{00}c_{10}c_{01}c_{11}d_{00}d_{10}d_{01}d_{11}1$
If $Z = 0$ then: $Q = 00c_{01}c_{11}10000$
2) Example Let $a = 0$, $b = 1 + \varepsilon$ and $c = 1$.
So the elliptic curve $\mathbf{E}_{a,b,c}(\mathbf{A})$ has 32 elements: $\{[0 : 1 : 0], [1 : \varepsilon : 1], [1 : 1 + \varepsilon : 1], [\alpha : (\alpha + 1)\epsilon : 1], [\alpha : \alpha + (\alpha + 1)\varepsilon : 1], [\epsilon : 1 : 0], [\varepsilon : 1 : 1], [\varepsilon : 1 + \varepsilon : 1], [\varepsilon : 1 + \alpha\varepsilon : 1], [\varepsilon : 1 + (\alpha + 1)\varepsilon : 1], [\alpha\varepsilon : 1 : 0], [(\alpha + 1)\varepsilon : 1 : 0], [1+\varepsilon : 0 : 1], [1+\varepsilon : 1+\varepsilon : 1], [1+\alpha\varepsilon : (\alpha+1)\varepsilon : 1], [1+\alpha\varepsilon : 1+\varepsilon : 1], [1+(\alpha+1)\varepsilon : \alpha\epsilon : 1], [1+(\alpha+1)\varepsilon : 1+\varepsilon : 1], [\alpha+1 : \alpha\varepsilon : 1], [\alpha+1 : \alpha+1+\alpha\varepsilon : 1], [\alpha+\varepsilon : \alpha : 1], [\alpha + \varepsilon : \varepsilon : 1], [\alpha + \alpha\varepsilon : 0 : 1], [\alpha + \alpha\varepsilon : \alpha + \alpha\varepsilon : 1], [\alpha + (\alpha + 1)\varepsilon : \alpha\varepsilon : 1], [\alpha + (\alpha + 1)\varepsilon : \alpha + \varepsilon : 1], [\alpha+1+\varepsilon : \epsilon : 1], [\alpha+1+\varepsilon : \alpha+1 : 1], [\alpha+1+\alpha\varepsilon : (\alpha+1)\varepsilon : 1], [\alpha+1+\alpha\varepsilon : \alpha+1+\varepsilon : 1], [\alpha+1+(\alpha+1)\varepsilon : 0 : 1], [\alpha + 1 + (\alpha + 1)\varepsilon : \alpha + 1 + (\alpha + 1)\varepsilon : 1]\}$
Let
$P = [\alpha+1+(\alpha+1)\varepsilon : \alpha+1+(\alpha+1)\varepsilon : 1] = 111111111$,
we have:

$$2P = [1 + \alpha\varepsilon + \varepsilon : 1 + \varepsilon : 1] = 101110101$$

$$3P = [\alpha + \varepsilon : \varepsilon : 1] = 011000101$$

$$4P = [\varepsilon : 1 + \varepsilon : 1] = 001010101$$

$$5P = [\alpha + (\alpha + 1)\varepsilon : \alpha + \varepsilon : 1] = 011101101$$

$$6P = [1 + \alpha\varepsilon : \alpha\varepsilon + \varepsilon : 1] = 1001001111$$

$$7P = [\alpha + 1 : \alpha\varepsilon : 1] = 110000011$$

$$8P = [\varepsilon : 1 + \alpha\varepsilon : 0] = 010010011$$

$$9P = [\alpha + 1 : \alpha + 1 + \alpha\varepsilon : 1] = 1100110111$$

$$10P = [1 + \alpha\varepsilon : 1 + \varepsilon : 1] = 100111001$$

$$11P = [\alpha + (\alpha + 1)\varepsilon : \alpha\varepsilon : 1] = 011100011$$

$$12P = [\varepsilon : 1 : 1] = 010010001$$

$$13P = [\alpha + \varepsilon : \alpha : 1] = 011001001$$

$$14P = [1 + \alpha\varepsilon + \varepsilon : \alpha\varepsilon : 1] = 110100011$$

$$15P = [\alpha + 1 + \alpha\varepsilon + \varepsilon : 0 : 1] = 111100001$$

and $16P = [0 : 1 : 0] = 000010000$
so, $G = \{111111111, 101110101, 011000101, 001010101, 011101101, 1001001111, 110000011, 010010011, 1100110111, 100111001, 011100011, 010010001, 011001001, 110100011, 111100001, 000010000\}$.

VI. CONCLUSION

In this work we have studed the elliptic curve over the ring $\mathbf{A} = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$, precisely we have established the short exact sequence that defines the group extension $\mathbf{E}_{a,b,c}(\mathbf{A})$ of $\mathbf{E}_{\pi_2(a),\pi_2(b),\pi_2(c)}(\mathbb{F}_{2^d})$ by $\mathbf{Ker}(\pi_2)$, and we have gived an example of cryptography over this ring.

REFERENCES

[1] Abdelhakim chillali, *the j-invariant over* $\mathbf{E}^n_{3^d}$. Int.j.Open problems Compt. Math.,Vol.5,No.4,December 2012,ISSN 1998-6262; Copyright ICSRS Publication,WWW.i-csrs.org,pp.106-111 (2012).

[2] Abdelhakim chillali, *Elliptic curve over ring,* International Mathematical Forum,Vol.6,no.31,2011 pp.1501-1505

[3] Abdelhakim chillali, *Cryptography over elliptic curve of the ring* $\mathbb{F}_q[\varepsilon]$,$\varepsilon^4 = 0$ World Academy of science Engineering and Technology,78 (2011),pp.848-850

[4] M.H. Hassib and A. Chillali, *Example of cryptography over the ring* $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^2 = 0$, Latest trends in Applied Informatics and Computing, p.71-73, ISBN 978-1-61804-130-2, (2012).

[5] W.Bosma and H.Lenstra, *Complete system of two addition laws for eliptic curved,* Journal of Number theory (1995).

[6] J. Lenstra, H.W, *Elliptic curves and number-theoretic algorithms*, Processing of the International Congress of Mathematicians, Berkely, California, USA,(1986).

[7] M.VIRAT. *courbe elliptique sur un anneau et applications cryptographiques*, These Docteur en Sciences, Nice-Sophia Antipolis. (2009)

[8] N.KOBLITZ. *Elliptic Curve Cryptosystems*,Mathematics of Computation.48,203,209,(1987).2,6,21,37

[9] R.LERCIER. *Algorithmique de courbes elliptiques dans les corps finis*, PhD thesis, Ecole polytechnique. juin (1997).

[10] J.H.SILVERMAN. *The Arithmetic of Elliptic curves*,Graduate Texts in Mathematcs. Springer.Volume 106(1985).2,19,20,21

[11] J.H.SILVERMAN. *Advanced Topics in the Arithmetic of Elliptic curves*,Graduate Texts in Mathematcs. Volume 151, Springer,(1994).

[12] V.CHANDRASEKARAN, N.NAGARAJAN. *Novel Approach Design of Elliptic curve Cryptography Implementation in VLSI*,RECENT ADVANCES in NETWORKING, VLSI and SIGNAL PROCESSING. www.wseas.us/e-library/conferences/2010/Cambridge/.../ICNVS-17.pdf

[13] Kapil A. Gwalani, Omar Elkeelany. *Design and Evaluation of Hardware Accelerator for Elliptic Curve Cryptography Point Multiplication*, RECENT ADVANCES IN APPLIED MATHEMATICS AND COMPUTATIONAL AND INFORMATION SCIENCES - Volume II.www.wseas.us/e-library/conferences/2009/houston/.../AAMCIS2-29.pdf