The Binary Operations Calculus in $E_{a,b,c}$

Abdelhamid Tadmori, Abdelhakim Chillali, M'hammed Ziane

Abstract— In this work, we study the elliptic curve over the ring $\mathbb{F}_{2^d}[\mathcal{E}]$; $\mathcal{E}^2 = 0$; where d is a positive integer. More precisely in cryptography applications, we will give many various explicit formulas describing the binary operations calculus in $E_{a,b,c}$.
The motivation for this work came from the observation that several practical discrete logarithm-based cryptosystems, such as ElGamal, the Elliptic Curve Cryptosystems.

Keywords— Elliptic Curves, Finite Ring, Cryptography..

I. Introduction

LET d be an integer, we consider the quotient ring $A = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$ where $\mathbb{F}_{2^d}$ is the finite field of order 2^d. Then the ring A is identified to the ring $\mathbb{F}_{2^d}[\mathcal{E}]$ with $\mathcal{E}^2 = 0$; ie: A = { $a_0 + a_1.\mathcal{E} \mid a_0; a_1 \in \mathbb{F}_{2^d}$ }, See, [3] and, [5]. We consider the elliptic curve over the ring A which is given by equation $Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3$.where a, b, c are in A and c^6b is inv ertible in A ; but we can take c = 1; see, [4].

- Notation

Let a, b ∈ A such that b is invertible in A and c = 1: So, We denote the elliptic curve over A by $E_{a,b}(A)$ and we write: $E_{a,b}(A)$ = { [X : Y : Z] ∈ $P_2(A)$ | $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$} if $b_0 \in \mathbb{F}_{2^d}\backslash\{0\}$ and $a_0 \in \mathbb{F}_{2^d}$, we also write: $E_{a_0,b_0}(\mathbb{F}_{2^d})$ = { [X : Y : Z] ∈ $P_2(\mathbb{F}_{2^d})$ | $Y^2Z + XYZ = X^3 + a_0X^2Z + b_0Z^3$}.

II. CLSSIFICATION OF ELEMENTS OF $E_{a,b}(A)$

Let [X :Y :Z] ∈ $E_{a,b}(A)$, where X, Y and Z are in A. We have two cases for Z:

* Z invertible: then [X : Y : Z] = [XZ^{-1} : Y Z^{-1}: 1]; hence we take just [X: Y: 1].

* Z non invertible: So Z = $z_1\varepsilon$; see [3] in this cases we have two cases for Y.

This work was supported by the Department of Mathematics in the university of Mohammed First, Oujda MOROCCO.

Abdelhamid Tadmori Author is with the Department of Mathematics FSO UMF Oujda MOROCCO; (e-mail: atadmori@yahoo.fr).
Abdelhakim Chillali Author is the Department of FST USMBA, FEZ, MOROCCO; (e-mail: chil2007@voila.fr)
M'hammed Ziane. Author is with the Department of Mathematics FSO UMF Oujda MOROCCO; (e-mail: ziane20011@yahoo.fr).

- Y invertible: Then [X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}]; so we just take [X : 1 : $z_1\varepsilon$] , then is verified the equation of $E_{a,b}(A)$: $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$.

so we can write:

a = $a_0 + a_1\varepsilon$
b = $b_0 + b_1\varepsilon$
X = $x_0 + x_1\varepsilon$

We have: $z_1\varepsilon + (x_0 + x_1\varepsilon).z_1\varepsilon = (x_0 + x_1\varepsilon)^3 + (a_0 + a_1\varepsilon).(x_0 + x_1\varepsilon)^2.z_1\varepsilon + (b_0 + b_1\varepsilon).{z_1}^3\varepsilon^3$

Which implies that :

$$z_1\varepsilon + x_0z_1\varepsilon = {x_0}^3 + ({x_0}^2x_1 + a_0{x_0}^2z_1)\varepsilon$$

Then :

$$(z_1 + x_0z_1)\varepsilon = {x_0}^3 + ({x_0}^2x_1 + a_0{x_0}^2z_1)\varepsilon$$

Since, $(1, \varepsilon)$ is a base of the vector space 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 $[X{:}\ 1{:}\ z_1\varepsilon] = [x_1\varepsilon : 1 :0]$.

- 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, $1 + a.z_1\varepsilon = 0; ie\ 1 + a_0z_1\varepsilon = 0$ which is absurd.

Proposition 1: Every element of $E_{a,b}(A)$, is of the form $[X{:}Y{:}1]$ or $[x\varepsilon{:}1{:}0]$; where $x \in \mathbb{F}_{2^d}$ and we write $E_{a,b}(A)$ = { [X : Y : 1] ∈ $P_2(A)$ | $Y^2 + XY = X^3 + aX^2 + b$}∪ $\{[x\varepsilon{:}1{:}0] | x \in \mathbb{F}_{2^d}\}$.

III. EXPLICIT FORMULAS

We consider the canonical projection π defined by :

$$\pi{:}\ \mathbb{F}_{2^d}[\varepsilon] \longrightarrow \mathbb{F}_{2^d}$$
$$x_0 + x_1\varepsilon \longmapsto x_0$$

We have π is a morphism of ring.

* Let π_2 the mapping defined by :

$$\pi_2{:}\ E_{a,b}(A) \longrightarrow E_{a_0,b_0}(\mathbb{F}_{2^d})$$
$$[X{:}Y{:}Z] \longmapsto [\pi(X){:}\pi(Y){:}\pi(Z)]$$

The mapping $\pi_2$is a surjective homomorphism of groups.

Theorem 1 :

- If $\pi_2(P) = \pi_2(Q)$ then :

$$X_3 = X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + X_2^2Y_1^2 + X_1X_2^2Y_1 + a\,X_1^2X_2Y_2 + a\,X_1X_2^2Y_1 + a\,X_1^2X_2^2 + b\,X_1Y_1Z_2^2 + b\,X_2Y_2Z_1^2 + b\,X_1^2Z_2^2 + b\,Y_1Z_2^2Z_1 + b\,Y_2Z_1^2Z_2 + b\,X_1Z_2^2Z_1$$

$$Y_3 = Y_1^2Y_2^2 + X_2Y_1^2Y_2 + a\,X_1X_2^2Y_1 + a^2\,X_1^2X_2^2 + b\,X_1^2X_2Z_2 + b\,X_1X_2^2Z_1 + b\,X_1Y_1Z_2^2 + b\,X_1^2Z_2^2 + ab\,X_2^2Z_1^2 + b\,Y_1Z_2^2Z_1 + b\,X_1Z_2^2Z_1 + ab\,X_1Z_2^2Z_1 + ab\,X_2Z_1^2Z_2 + b^2Z_1^2Z_2^2$$

$$Z_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2X_2^2 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + a\,X_1^2Y_2Z_2 + a\,X_2^2Y_1Z_1 + X_1^2X_2Z_2 + a\,X_1X_2^2Z_1 + b\,Y_1Z_2^2Z_1 + b\,Y_2Z_1^2Z_2 + b\,X_1Z_2^2Z_1$$

- If $\pi_2(P) \neq \pi_2(Q)$ then :

$$X_1 = X_1Y_2^2Z_1 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + a\,X_1^2X_2Z_2 + a\,X_1X_2^2Z_1 + b\,X_1Z_2^2Z_1 + b\,X_2Z_1^2Z_2$$

$$Y_3 = X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + a\,X_1^2Y_2Z_2 + a\,X_2^2Y_1Z_1 + a\,X_1^2X_2Z_2 + a\,X_1X_2^2Z_1 + b\,Y_1Z_2^2Z_1 + b\,Y_2Z_1^2Z_2 + b\,X_1Z_2^2Z_1 + b\,X_2Z_1^2Z_2$$

$$Z_3 = X_1^2X_2Z_2 + X_1X_2^2Z_1 + Y_1^2Z_2^2 + Y_2^2Z_1^2 + X_1Y_1Z_2^2 + X_2Y_2Z_1^2 + a\,X_1^2Z_2^2 + a\,X_2^2Z_1^2$$

Proof : Using the explicit formulas in W.Bosma and H.Lenstras article see, [13] we prove the theorem.

IV. MAIN RESULTS

1. Procedures:

The following Maple procedure will help us to calculate, expressively the sum of two points in the elliptic curve $E_{a,b}(A)$.

- **The $f_1$procedure**

This procedure computes the sum of two points of $E_{a,b}(A)$ which verify the condition (1) in the theorem.

```
>f1:= proc(P,Q, a, b)
local x1,y1,z1,x2,y2,z2;
x1:=P[1];y1:=P[2];z1:=P[3]; x2:=Q[1];y2:=Q[2];z2:=Q[3];
expand([y1*y2^2*x1+y1^2*y2*x2+x2^2*y1^2+x1*x2^2*y1+
a*x1^2*x2*y2+a*x1*x2^2*y1+a*x1^2*x2^2+b*x1*z2^2*y1
+b*x2*z1^2*y2+b*x1^2*z2^2+z1*z2^2*b*y1+z1^2*z2*b*y
2+x1*z1*z2^2*b,
y1^2*y2^2+x2*y1^2*y2+a*x1*x2^2*y1+a^2*x1^2*x2^2+b*
x1^2*x2*z2+b*x1*x2^2*z1+b*y1*z2^2*x1+x1^2*z2^2*b+a
*b*x2^2*z1^2+y1*z1*z2^2*b+x1*z1*z2^2*b+x1*z1*z2^2*a
*b+x2*z1^2*z2*a*b+b^2*z1^2*z2^2,
x1^2*x2*y2+x1*x2^2*y1+y1^2*y2*z2+y1*y2^2*z1+x1^2*x
2^2+y1^2*z2*x2+x1^2*y2*z2+a*x1^2*y2*z2+a*x2^2*y1*z
1+x1^2*x2*z2+a*x1*x2^2*z1+b*z1*z2^2*y1+b*z1^2*z2*y
2+b*z1*z2^2*x1] mod 2);
end:
```

- **The $f_2$procedure**

This procedure computes the sum of two points of $E_{a,b}(A)$ which verify the condition (2) in the theorem.

```
>f2:= proc(P,Q, a, b)
local x1,y1,z1,x2,y2,z2;
x1:=P[1];y1:=P[2];z1:=P[3]; x2:=Q[1];y2:=Q[2];z2:=Q[3];
expand([x1*y2^2*z1+x2*y1^2*z2+x1^2*y2*z2+x2^2*y1*z1
+a*x1^2*x2*z2+a*x1*x2^2*z1+b*z1*z2^2*x1+b*z1^2*z2*x
2,
x1^2*x2*y2+x1*x2^2*y1+y1^2*y2*z2+y1*y2^2*z1+x1^2*y
2*z2+x2^2*y1*z1+a*x1^2*y2*z2+a*x2^2*y1*z1+a*x1^2*x
2*z2+a*x1*x2^2*z1+b*z1*z2^2*y1+b*z1^2*z2*y2+b*z1*z2
^2*x1+b*z1^2*z2*x2,
x1^2*x2*z2+x1*x2^2*z1+y1^2*z2^2+y2^2*z1^2+x1*z2^2*
y1+x2*z1^2*y2+a*x1^2*z2^2+a*x2^2*z1^2] mod 2); end:
```

- **The $f_3$procedure**

This procedure gives the image of an element of the ring A by the canonical projection π defined above.

```
f3:=proc(X)
coeff(X, epsilon, 0); end:
```

- **The somme procedure**

This procedure computes the sum of two points chosen arbitraily in $E_{a,b}(A)$, by using the procedures f_1, f_2 and f_3

```
>somme:=proc(P,Q, a, b)
if ([f3 (P[1]),f3 (P[2]),f3 (P[3])]=[f3 (Q[1]),f3 (Q[2]),f3
(Q[3])])
then f1 (P, Q, a, b)
else f2 (P, Q, a, b)
end if;
end:
```

2. Binary operation

Let $a = a_0 + a_1\varepsilon,\ b = b_0 + b_1\varepsilon.$

Lemma 1.
Let $P = [x_1\varepsilon : 1 : 0]$ and $Q = [t_1\varepsilon : 1 : 0]$ two points in $E_{a,b}(A)$ then :

$P + Q = [(x_1 + t_1)\varepsilon : 1 + t_1\varepsilon : 0]$

Proof : As $\pi_2(P) = \pi_2(Q)$, then by applying the formula (1) in theorem, we find the result.

Lemma 2.
Let $P = [x_1\varepsilon : 1 : 0]$ and $Q = [t_0 + t_1\varepsilon : h_0 + h_1\varepsilon : 1]$ two points in $E_{a,b}(A)$, then :

$P + Q = [t_0 + t_1\varepsilon : (x_1t_0^2 + h_1)\varepsilon + h_0 : 1 + x_1\varepsilon]$

Proof : With the somme procedure, we find :

```
> P:=[x1*epsilon, 1, 0];Q:=[t0+t1*epsilon, h0+h1*epsilon, 1];
a:=a0+a1*epsilon; b:=b0+b1*epsilon;
collect(somme(P,Q, a, b), epsilon)mod2:
```

eval(%,epsilon^2=0):eval(%,epsilon^3=0):eval(%,epsilon^4=0):eval(%,epsilon^5=0):eval(%,epsilon^6=0):
eval(%,epsilon^7=0):eval(%,epsilon^8=0):eval(%,epsilon^9=0);

$$P:=[x_1\varepsilon, 1, 0]$$

$$Q:=[t_0+t_1\varepsilon,\ h_0+h_1\varepsilon, 1]$$

$$a:=a_0+a_1\varepsilon$$

$$b:=b_0+b_1\varepsilon$$

$P+Q=[t_0+t_1\varepsilon, (x_1t_0{}^2+h_1)\varepsilon+h_0, 1+x_1\varepsilon]$
which proves the lemma.

Lemma3.
Let $P=[x_0+x_1\varepsilon: y_1\varepsilon: 1]$ and $Q=[x_0+t_1\varepsilon: h_1\varepsilon: 1]$ two points in $E_{a,b}(A)$ then :
$P+Q=[(h_1a_0x_0{}^3+y_1a_0x_0{}^3+a_1x_0{}^4+y_1b_0x_0+h_1b_0x_0+y_1x_0{}^3+x_1b_0+h_1b_0+b_1x_0{}^2+y_1b_0+x_0b_1)\varepsilon+b_0x_0{}^2+a_0x_0{}^4+x_0b_0: (x_1a_0b_0+a_1b_0x_0{}^2+x_1b_0+a_0b_1x_0{}^2+b_0x_0{}^2x_1+x_0b_1+y_1b_0+y_1a_0x_0{}^3+t_1a_0b_0+y_1b_0x_0+b_0x_0{}^2t_1+x_0{}^2b_1)\varepsilon+x_0{}^2b_0+a_0b_0x_0{}^2+b_0{}^2+x_0b_0+a_0{}^2x_0{}^4: (a_1x_0{}^3+h_1x_0{}^2+a_0x_1x_0{}^2+y_1a_0x_0{}^2+h_1a_0x_0{}^2+h_1x_0{}^3+x_0{}^2t_1+b_0x_1+y_1b_0+b_1x_0+y_1x_0{}^3+h_1b_0)\varepsilon+a_0x_0{}^3+x_0{}^4+x_0{}^3+b_0x_0]$

Proof : With the somme procedure we find :

> P:=[x0+x1*epsilon, y1*epsilon, 1];Q:=[x0+t1*epsilon, h1*epsilon, 1];
collect(somme(P, Q, a, b,), epsilon) mod 2:
eval(%,epsilon^2=0):eval(%,epsilon^3=0):
eval(%,epsilon^4=0):eval(%,epsilon^5=0):
eval(%,epsilon^6=0);

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

$$Q:=[x_0+t_1\varepsilon,\ h_1\varepsilon, 1]$$

$P+Q=[(h_1a_0x_0{}^3+y_1a_0x_0{}^3+a_1x_0{}^4+y_1b_0x_0+h_1b_0x_0+y_1x_0{}^3+x_1b_0+h_1b_0+b_1x_0{}^2+y_1b_0+x_0b_1)\varepsilon+b_0x_0{}^2+a_0x_0{}^4+x_0b_0,\ (x_1a_0b_0+a_1b_0x_0{}^2+x_1b_0+a_0b_1x_0{}^2+b_0x_0{}^2x_1+x_0b_1+y_1b_0+y_1a_0x_0{}^3+t_1a_0b_0+y_1b_0x_0+b_0x_0{}^2t_1+x_0{}^2b_1)\varepsilon+x_0{}^2b_0+a_0b_0x_0{}^2+b_0{}^2+x_0b_0+a_0{}^2x_0{}^4, (a_1x_0{}^3+h_1x_0{}^2+a_0x_1x_0{}^2+y_1a_0x_0{}^2+h_1a_0x_0{}^2+h_1x_0{}^3+x_0{}^2t_1+b_0x_1+y_1b_0+b_1x_0+y_1x_0{}^3+h_1b_0)\varepsilon+a_0x_0{}^3+x_0{}^4+x_0{}^3+b_0x_0]$

Which gives the result.

Lemma4.
Let $P=[x_0+x_1\varepsilon: y_0+y_1\varepsilon: 1]$ and $Q=[x_0+t_1\varepsilon: h_1\varepsilon: 1]$ two points in $E_{a,b}(A)$, where $y_0\neq 0$ Then :

$P+Q=[(a_0x_0{}^2t_1+a_0x_0{}^2x_1+x_0{}^2y_1+h_1x_0{}^2+b_0t_1+t_1y_0{}^2+b_0x_1)\varepsilon+x_0{}^2y_0+x_0y_0{}^2: (x_0{}^2x_1y_0+x_0{}^2y_1+y_1x_0{}^3+h_1a_0x_0{}^2+y_1a_0x_0{}^2+h_1b_0+a_0x_1x_0{}^2+b_0t_1+h_1x_0{}^3+b_1y_0+h_1x_0{}^2+a_1x_0{}^2y_0+b_0x_1+y_1b_0+a_0x_0{}^2t_1+h_1y_0{}^2)\varepsilon+a_0x_0{}^2y_0+x_0{}^2y_0+b_0y_0+x_0{}^3y_0: (x_0{}^2x_1+h_1x_0+x_0{}^2t_1+x_0y_1+x_1y_0)\varepsilon+x_0y_0+y_0{}^2]$

Proof : With the somme procedure we find :

> P:=[x0+x1*epsilon, y0+y1*epsilon, 1];Q:=[x0+t1*epsilon, h1*epsilon, 1];
collect(somme(P,Q, a, b,),epsilon) mod2:eval(%,epsilon^2=0):
eval(%,epsilon^3=0):eval(%,epsilon^4=0):eval(%,epsilon^5=0):eval(%,epsilon^6=0);

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

$$Q:=[x_0+t_1\varepsilon,\ h_1\varepsilon, 1]$$

$P+Q=[(a_0x_0{}^2t_1+a_0x_0{}^2x_1+x_0{}^2y_1+h_1x_0{}^2+b_0t_1+t_1y_0{}^2+b_0x_1)\varepsilon+x_0{}^2y_0+x_0y_0{}^2, (x_0{}^2x_1y_0+x_0{}^2y_1+y_1x_0{}^3+h_1a_0x_0{}^2+y_1a_0x_0{}^2+h_1b_0+a_0x_1x_0{}^2+b_0t_1+h_1x_0{}^3+b_1y_0+h_1x_0{}^2+a_1x_0{}^2y_0+b_0x_1+y_1b_0+a_0x_0{}^2t_1+h_1y_0{}^2)\varepsilon+a_0x_0{}^2y_0+x_0{}^2y_0+b_0y_0+x_0{}^3y_0, (x_0{}^2x_1+h_1x_0+x_0{}^2t_1+x_0y_1+x_1y_0)\varepsilon+x_0y_0+y_0{}^2]$

Which gives the result.

Lemma5.
Let $P=[x_0+x_1\varepsilon:\ y_0+y_1\varepsilon: 1]$;
$Q=[x_0+t_1\varepsilon:\ y_0+h_1\varepsilon: 1]$ two points of $E_{a,b}(A)$, where $y_0\neq 0$, then :
$P+Q=[(y_1x_0{}^3+h_1a_0x_0{}^3+y_1a_0x_0{}^3+a_1x_0{}^4+y_1b_0x_0+h_1b_0x_0+b_1x_0{}^2+y_1b_0+h_1b_0+x_0b_1+x_1b_0+y_0{}^3x_1+y_0{}^3t_1+h_1y_0{}^2x_0+y_1y_0{}^2x_0+b_0x_1y_0+b_0t_1y_0+x_1x_0{}^2y_0+a_0x_0{}^2t_1y_0+a_0x_0{}^2x_1y_0)\varepsilon+b_0x_0{}^2+a_0x_0{}^4+x_0b_0+x_0{}^3y_0+x_0{}^2y_0{}^2: (b_0x_0{}^2t_1+b_0x_0{}^2x_1+x_0{}^2b_1+a_0b_1x_0{}^2+a_1b_0x_0{}^2+y_1b_0+x_0b_1+x_1b_0+y_1a_0x_0{}^3+y_1b_0x_0+x_1a_0b_0+t_1a_0b_0+t_1y_0{}^3+y_0b_1+x_0y_0{}^2h_1+a_1x_0{}^3y_0+b_0y_0x_1+b_1y_0x_0+a_0x_1x_0{}^2y_0)\varepsilon+a_0x_0{}^3y_0+y_0{}^4+x_0y_0{}^3+y_0b_0+x_0b_0+b_0{}^2+a_0b_0x_0{}^2+a_0{}^2x_0{}^4+x_0{}^2b_0+b_0y_0x_0: (h_1x_0{}^3+a_0x_1x_0{}^2+a_1x_0{}^3+b_0x_1+b_1x_0+h_1x_0{}^2+h_1a_0x_0{}^2+y_1a_0x_0{}^2+x_0{}^2t_1+y_1x_0{}^3+y_1b_0+h_1b_0+x_0{}^2t_1y_0+x_0{}^2x_1y_0+h_1y_0{}^2+y_1y_0{}^2+t_1y_0{}^2)\varepsilon+x_0y_0{}^2+x_0{}^4+a_0x_0{}^3+x_0{}^2y_0+b_0x_0+x_0{}^3]$

Proof : With the somme procedure we find :

> P:=[x0+x1*epsilon, y0+y1*epsilon, 1];Q:=[x0+t1*epsilon, y0+h1*epsilon,1];
collect(somme(P,Q, a, b,),epsilon) mod2:eval(%,epsilon^2=0):
eval(%,epsilon^3=0):eval(%,epsilon^4=0):
eval(%,epsilon^5=0):eval(%,epsilon^6=0);

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

$$Q:=[x_0+t_1\varepsilon:\ y_0+h_1\varepsilon: 1]$$

$$P+Q=[(y_1x_0{}^3+h_1a_0x_0{}^3+y_1a_0x_0{}^3+a_1x_0{}^4+y_1b_0x_0$$
$$+h_1b_0x_0+b_1x_0{}^2+y_1b_0+h_1b_0+x_0b_1+x_1b_0+y_0{}^3x_1$$
$$+y_0{}^3t_1+h_1y_0{}^2x_0+y_1y_0{}^2x_0+b_0x_1y_0+b_0t_1y_0+x_1x_0{}^2y_0$$
$$+a_0x_0{}^2t_1y_0+a_0x_0{}^2x_1y_0)\varepsilon+b_0x_0{}^2+a_0x_0{}^4$$
$$+x_0b_0+x_0{}^3y_0+x_0{}^2y_0{}^2,(b_0x_0{}^2t_1+b_0x_0{}^2x_1+x_0{}^2b_1+$$
$$a_0b_1x_0{}^2+a_1b_0x_0{}^2+y_1b_0+x_0b_1+x_1b_0+y_1a_0x_0{}^3$$
$$+y_1b_0x_0+x_1a_0b_0+t_1a_0b_0+t_1y_0{}^3+y_0b_1+x_0y_0{}^2h_1$$
$$+a_1x_0{}^3y_0+b_0y_0x_1+b_1y_0x_0+a_0x_1x_0{}^2y_0)\varepsilon+a_0x_0{}^3y_0$$
$$+y_0{}^4+x_0y_0{}^3+y_0b_0+x_0b_0+b_0{}^2+a_0b_0x_0{}^2$$
$$+a_0{}^2x_0{}^4+x_0{}^2b_0+b_0y_0x_0,(h_1x_0{}^3+a_0x_1x_0{}^2+a_1x_0{}^3+$$
$$b_0x_1+b_1x_0+h_1x_0{}^2+h_1a_0x_0{}^2+y_1a_0x_0{}^2+x_0{}^2t_1+y_1x_0{}^3$$
$$+y_1b_0+h_1b_0+x_0{}^2t_1y_0+x_0{}^2x_1y_0+h_1y_0{}^2+y_1y_0{}^2$$
$$+t_1y_0{}^2)\varepsilon+x_0y_0{}^2+x_0{}^4+a_0x_0{}^3+x_0{}^2y_0+b_0x_0+x_0{}^3]$$

This gives the result.

Lemma6.

Let $P=[x_0+x_1\varepsilon:\ y_0+y_1\varepsilon:1]$; $Q=[t_0+t_1\varepsilon:\ h_0+h_1\varepsilon:1]$ two points in $E_{a,b}(A)$, where $x_0\neq t_0$, or $y_0\neq h_0$, then :

$$P+Q=[(t_0{}^2y_1+h_1x_0{}^2+a_0x_0{}^2t_1+a_1x_0{}^2t_0+a_0x_1t_0{}^2$$
$$+a_1x_0t_0{}^2+b_1x_0+b_1t_0+b_0x_1+b_0t_1+t_1y_0{}^2+x_1h_0{}^2)\varepsilon$$
$$+x_0{}^2h_0+t_0{}^2y_0+a_0x_0{}^2t_0+a_0x_0t_0{}^2+b_0x_0+x_0h_0{}^2$$
$$+t_0y_0{}^2+b_0t_0:(a_0x_0{}^2t_1+b_0x_1+b_1x_0+h_1x_0{}^2$$
$$+h_1a_0x_0{}^2+y_1b_0+h_1b_0+b_0t_1+h_1y_0{}^2+b_1y_0+y_1h_0{}^2+$$
$$b_1h_0+x_0{}^2t_0h_1+x_0{}^2t_1h_0+x_0t_0{}^2y_1+x_1t_0{}^2y_0+t_0{}^2y_1$$
$$+a_1x_0{}^2h_0+a_0t_0{}^2y_1+a_1t_0{}^2y_0+b_1t_0+a_1x_0{}^2t_0+a_0x_1t_0{}^2$$
$$+a_1x_0t_0{}^2)\varepsilon+t_0{}^2y_0+b_0x_0+x_0t_0{}^2y_0+x_0{}^2h_0+x_0{}^2t_0h_0$$
$$+a_0x_0{}^2t_0+a_0x_0t_0{}^2+b_0y_0+y_0h_0{}^2+b_0t_0+b_0h_0$$
$$+y_0{}^2h_0+a_0t_0{}^2y_0+a_0x_0{}^2h_0:(x_0{}^2t_1+t_1h_0+a_1x_0{}^2+$$
$$t_0h_1+x_1t_0{}^2+a_1t_0{}^2+x_0y_1+x_1y_0)\varepsilon+a_0t_0{}^2+t_0h_0+y_0{}^2$$
$$+x_0y_0+x_0{}^2t_0+x_0t_0{}^2+h_0{}^2+a_0x_0{}^2]$$

Proof : With the somme procedure we find .

```
> P:=[x0+x1*epsilon, y0+y1*epsilon, 1];Q:=[t0+t1*epsilon, h0+h1*epsilon, 1];
collect(somme(P,Q, a, b,), epsilon) mod 2:
eval(%,epsilon^2=0):eval(%,epsilon^3=0):
eval(%,epsilon^4=0):eval(%,epsilon^5=0):eval(%,epsilon^6=0);
```

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

$$Q=[t_0+t_1\varepsilon,\ \ h_0+h_1\varepsilon,1]$$

$$P+Q=[(t_0{}^2y_1+h_1x_0{}^2+a_0x_0{}^2t_1+a_1x_0{}^2t_0+a_0x_1t_0{}^2$$
$$+a_1x_0t_0{}^2+b_1x_0+b_1t_0+b_0x_1+b_0t_1+t_1y_0{}^2+x_1h_0{}^2)\varepsilon$$
$$+x_0{}^2h_0+t_0{}^2y_0+a_0x_0{}^2t_0+a_0x_0t_0{}^2+b_0x_0+x_0h_0{}^2$$
$$+t_0y_0{}^2+b_0t_0,(a_0x_0{}^2t_1+b_0x_1+b_1x_0+h_1x_0{}^2$$
$$+h_1a_0x_0{}^2+y_1b_0+h_1b_0+b_0t_1+h_1y_0{}^2+b_1y_0+y_1h_0{}^2+$$
$$b_1h_0+x_0{}^2t_0h_1+x_0{}^2t_1h_0+x_0t_0{}^2y_1+x_1t_0{}^2y_0+t_0{}^2y_1$$
$$+a_1x_0{}^2h_0+a_0t_0{}^2y_1+a_1t_0{}^2y_0+b_1t_0+a_1x_0{}^2t_0$$
$$+a_0x_1t_0{}^2+a_1x_0t_0{}^2)\varepsilon+t_0{}^2y_0+b_0x_0+x_0t_0{}^2y_0+x_0{}^2h_0$$
$$+x_0{}^2t_0h_0+a_0x_0{}^2t_0+a_0x_0t_0{}^2+b_0y_0+y_0h_0{}^2+b_0t_0$$
$$+b_0h_0+y_0{}^2h_0+a_0t_0{}^2y_0+a_0x_0{}^2h_0,(x_0{}^2t_1+t_1h_0$$
$$+a_1x_0{}^2+t_0h_1+x_1t_0{}^2+a_1t_0{}^2+x_0y_1+x_1y_0)\varepsilon$$
$$+a_0t_0{}^2+t_0h_0+y_0{}^2+x_0y_0+x_0{}^2t_0+x_0t_0{}^2+h_0{}^2+a_0x_0{}^2]$$

Which gives the result.

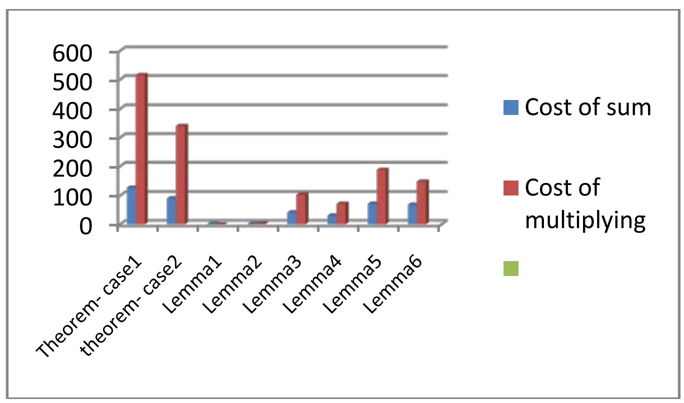
V. Conclusion

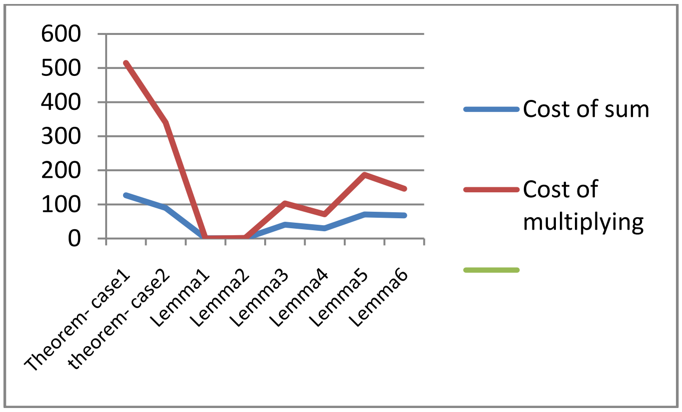
Finally, in the field $\mathbb{F}_{2^d}$; let m is the cost of multiplying; s is the cost of sum, and i is the cost of the reverse. Its clair that $s\leq m\leq i$; we neglect the cost of the reverse and that his comparison. We have the following table:

Table 1:

Cost	Cost of sum	Cost of multiplying
Theorem- case1	$127\times s$	$515\times m$
Theorem- case2	$90\times s$	$340\times m$
Lemma1	$1\times s$	$0\times m$
Lemma2	$1\times s$	$2\times m$
Lemma3	$41\times s$	$103\times m$
Lemma4	$30\times s$	$71\times m$
Lemma5	$71\times s$	$187\times m$
Lemma6	$68\times s$	$146\times m$

- **Graphic interpretation**





- **Result:**

After these graphs, we see that the cost of sum and the cost of Multiplying of lemmas are less weak than those of theorem. Hence the time complexity of lemmas is lower than the time complexity of theorem; which shows the necessity of these lemmas.

Acknowledgments

The authors would like to thank University of Mohammed First Oujda and North Atlantic university Union for its valued support.

References

[1] A. Chillali, the j-invariant over $E_{3^d}{}^n$, Int.j.Open problems Compt. Math (2012).

[2] A. 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 .

[3] A. Tadmori, A. chillali and M. Ziane; Elliptic Curves Over SPIR of characteristic Two; proceeding of the 2013 international conference on applied mathematcs and computational Methode, www.europment.org/library/2013/AMCM.05.

[4] A. Tadmori, A. chillali and M. Ziane; Normal Form of the elliptic Curves over the finite ring; Journal of Mathematics and system Sience 4 (2014) 194-196.

[5] A. Tadmori, A. chillali and M. Ziane Coding over elliptic curves in the ring of characteristic two;International journal of Applied Mathemathics and Informatics, (Volume 8. 2014).

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

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

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

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

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

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

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