The sum over $E_{a,b}$

A. Chillali, A. Tadmori and M. Ziane

***Abstract*—**Let d is a positive integer. In this article we will study the elliptic curve defined over the ring $\mathbb{F}_{2^d}[\mathcal{E}]$; $\mathcal{E}^2 = 0$. More precisely we will give many various explicit formulas describing the binary operations calculus in $E_{a,b,c}$.

***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: see [1] and [2], $A = \{ a_0 + a_1.\mathcal{E} \mid a_0; a_1 \in \mathbb{F}_{2^d} \}$.

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 and c are in A and c^6b is invertible in A, but we can take c = 1; see, [3].

II. Notations

Let a, $b \in A$ such that b is invertible in A and c = 1. We denote the elliptic curve over A by $E_{a,b}(A)$ and we write:

$E_{a,b}(A) = \{ [X : Y : Z] \in P_2(A) \mid Y^2Z + XYZ = X^3 + aX^2Z + bZ^3\}$.

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

$E_{a_0,b_0}(\mathbb{F}_{2^d}) = \{ [X : Y : Z] \in P_2(\mathbb{F}_{2^d}) \mid Y^2Z + XYZ = X^3 + a_0X^2Z + b_0Z^3\}$.

III. Classification of elements of $E_{A,B}(A)$

Let $[X :Y :Z] \in E_{a,b}(A)$, 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 [4], in this cases we have tow cases for Y.

- 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:

$E_{a,b}(A) = \{[X:Y:1] \in P_2(A) \mid Y^2 + XY = X^3 + aX^2 + b\} \cup \{[x\varepsilon: 1: 0] \mid x \in \mathbb{F}_{2^d} \}$. [1].

IV. Explicit Formulas

We consider the canonical projection π defined by:

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

We have π is a morphism of ring.

* Let π_2 the mapping defined by :

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

The mapping π_2 is a surjective homomorphism of groups.

Theorem1:

Let $P = [X_1: Y_1: Z_1]$, $Q = [X_2: Y_2: Z_2]$ in $E_{a,b}(A)$ then $P + Q = [X_3: Y_3: Z_3]$:

• If $\pi_2(P) = \pi_2(Q)$ then :

✓ $X_3 = X_1Y_1Y_2 + X_2{Y_1}^2Y_2 + {X_2}^2{Y_1}^2 + X_1{X_2}^2Y_1 + a\,{X_1}^2X_2Y_2 + a\,X_1{X_2}^2Y_1 + a\,{X_1}^2{X_2}^2 + b\,X_1Y_1{Z_2}^2 + b\,X_2Y_2{Z_1}^2 + b\,{X_1}^2{Z_2}^2 + b\,Y_1{Z_2}^2Z_1 + b\,Y_2{Z_1}^2Z_2 + b\,X_1{Z_2}^2Z_1$

✓ $Y_3 = {Y_1}^2{Y_2}^2 + X_2{Y_1}^2Y_2 + a\,X_1{X_2}^2Y_1 + a^2\,{X_1}^2{X_2}^2 + b\,{X_1}^2X_2Z_2 + b\,X_1\,{X_2}^2Z_1 + b\,X_1Y_1{Z_2}^2 + b\,{X_1}^2{Z_2}^2 + ab\,{X_2}^2{Z_1}^2 + b\,Y_1{Z_2}^2Z_1 + b\,X_1{Z_2}^2Z_1 + ab\,X_1{Z_2}^2Z_1 + ab\,X_2{Z_1}^2Z_2 + b^2{Z_1}^2{Z_2}^2$

✓ $Z_3 = {X_1}^2X_2Y_2 + X_1{X_2}^2Y_1 + {Y_1}^2Y_2Z_2 + Y_1{Y_2}^2Z_1 + {X_1}^2{X_2}^2 + X_2{Y_1}^2Z_2 + {X_1}^2Y_2Z_2 + a\,{X_1}^2Y_2Z_2 + a\,{X_2}^2Y_1Z_1 + {X_1}^2X_2Z_2 + a\,X_1{X_2}^2Z_1 + b\,Y_1{Z_2}^2Z_1 + b\,Y_2{Z_1}^2Z_2 + b\,X_1{Z_2}^2Z_1$

• If $\pi_2(P) \neq \pi_2(Q)$ then :

A. Chillali is with the USMBA, LST, FPT, Taza, Morocco,
e-mail: abdelhakim.chillali@usmba.ac.ma.
A. Tadmori., is with UMP, FSO , Oujda.
M. Ziane., is with UMP, FSO , Oujda.

ISBN: 978-1-61804-292-7

- ✓ $X_1 = X_1Y_2{}^2Z_1 + X_2Y_1{}^2Z_2 + X_1{}^2Y_2Z_2 + X_2{}^2Y_1Z_1 + a\ X_1{}^2X_2Z_2 + a\ X_1X_2{}^2Z_1 + b\,X_1Z_2{}^2Z_1 + b\,X_2Z_1{}^2Z_2$
- ✓ $Y_3 = X_1{}^2X_2Y_2 + X_1X_2{}^2Y_1 + Y_1{}^2Y_2Z_2 + Y_1Y_2{}^2Z_1 + X_1{}^2Y_2Z_2 + X_2{}^2Y_1Z_1 + a\ X_1{}^2Y_2Z_2 + a\,X_2{}^2Y_1Z_1 + a\ X_1{}^2X_2Z_2 + a\ X_1X_2{}^2Z_1 + b\,Y_1Z_2{}^2Z_1 + b\,Y_2Z_1{}^2Z_2 + b\,X_1Z_2{}^2Z_1 + b\,X_2Z_1{}^2Z_2$
- ✓ $Z_3 = X_1{}^2X_2Z_2 + X_1X_2{}^2Z_1 + Y_1{}^2Z_2{}^2 + Y_2{}^2Z_1{}^2 + X_1Y_1Z_2{}^2 + X_2Y_2Z_1{}^2 + a\ X_1{}^2Z_2{}^2 + a\,X_2{}^2Z_1{}^2$

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

V.MAIN RESULTS

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

Lemma1:
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. . ■

The following lemmas may be proved by using the explicit formulas in [5, p. 236—238].

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 :

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

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 :

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

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 :

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

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 :

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

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 :

$$P + Q = [(t_0{}^2y_1 + h_1x_0{}^2 + a_0x_0{}^2t_1 + a_1x_0{}^2t_0 + a_0x_1t_0{}^2 + a_1x_0t_0{}^2 + b_1x_0 + b_1t_0 + b_0x_1 + b_0t_1 + t_1y_0{}^2 + x_1h_0{}^2)\varepsilon + x_0{}^2h_0 + t_0{}^2y_0 + a_0x_0{}^2t_0 + a_0x_0t_0{}^2 + b_0x_0 + x_0h_0{}^2 + t_0y_0{}^2 + b_0t_0: (a_0x_0{}^2t_1 + b_0x_1 + b_1x_0 + h_1x_0{}^2 + h_1a_0x_0{}^2 + y_1b_0 + h_1b_0 + b_0t_1 + h_1y_0{}^2 + b_1y_0 + y_1h_0{}^2 + b_1h_0 + x_0{}^2t_0h_1 + x_0{}^2t_1h_0 + x_0t_0{}^2y_1 + x_1t_0{}^2y_0 + t_0{}^2y_1 + a_1x_0{}^2h_0 + a_0t_0{}^2y_1 + a_1t_0{}^2y_0 + b_1 + a_1x_0{}^2t_0 + a_0x_1t_0{}^2 + a_1x_0t_0{}^2)\varepsilon + t_0{}^2y_0 + b_0x_0 + x_0t_0{}^2y_0 + x_0{}^2h_0 + x_0{}^2t_0h_0 + a_0x_0{}^2t_0 + a_0x_0t_0{}^2 + b_0y_0 + y_0h_0{}^2 + b_0t_0 + b_0h_0 + y_0{}^2h_0 + a_0t_0{}^2y_0 + a_0x_0{}^2h_0: (x_0{}^2t_1 + t_1h_0 + a_1x_0{}^2 + t_0h_1 + x_1t_0{}^2 + a_1t_0{}^2 + x_0y_1 + x_1y_0)\varepsilon + a_0t_0{}^2 + t_0h_0 + y_0{}^2 + x_0y_0 + x_0{}^2t_0 + x_0t_0{}^2 + h_0{}^2 + a_0x_0{}^2]$$

ACKNOWLEDGMENT

The authors would like to thank University of Mohammed First Oujda and FPT of Taza in MOROCCO for its valued support.

REFERENCES

[1] A. Chillali, The j-invariant over $E_{3^d}{}^n$, 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] 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. Chillali, Elliptic curve over ring, International Mathematical Forum, Vol.6, no.31, 2011 pp.1501-1505
[4] A. Tadmori, A. Chillali and M. Ziane, Elliptic Curves Over SPIR of characteristic Two, proceeding of the 2013 international conference on applied mathematics and Computational Methode, www.europment.org/library/2013/AMCM-05.
[5] 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.
[6] 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).
[7] J.H. SILVERMAN, The Arithmetic of Elliptic curves, Graduate Texts in Mathematcs, Springer, Volume 106(1985).2,19,20,21
[8] J.H. ~SILVERMAN, Advanced Topics in the Arithmetic of Elliptic curves, Graduate Texts in Mathematcs, Volume 151, Springer,(1994).
[9] W. Bosma and H. Lenstra, Complete system of two addition laws for elliptic curved, Journal of Number theory, (1995).