Coding over elliptic curves in the ring of characteristic two

Abdelhamid Tadmori, Abdelhakim Chillali, M'hammed Ziane

***Abstract*—**In this article we will study the elliptic curve over the ring $\boldsymbol{A} = \mathbb{F}_{2^d}[\boldsymbol{\varepsilon}]$, where d is a positive integer and $\boldsymbol{\varepsilon^2 = 0}$. More precisely we will establish a group homomorphism between the abulia group $(\boldsymbol{E_{a,b,c}}(\mathbb{F}_{2^d}), +)$ and $(\mathbb{F}_{2^d}, +)$, and we have given an example for coding elements over this ring.

***Keywords*—**Elliptic curve over ring, Finite ring, Finite field, Coding.

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 $\mathbb{F}_{2^d}[\boldsymbol{\varepsilon}]$with $\boldsymbol{\varepsilon^2 = 0}$. ie: $A = \{a_0 + a_1.\varepsilon \,|a_0, a_1 \in \mathbb{F}_{2^d}\}$. 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, c are in A and c^6b is invertible in A, see [1] and [2].

II. NOTAIONS

Let $a, b, c \in A$, such that c^6b is invertible in A. We denote the elliptic curve over A by $E_{a,b,c}(A)$ and we write: $E_{a,b,c}(A) = \{[X:Y:Z] \in \mathbb{P}_2(A) | Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3\}$. If $b_0, c_0 \in \mathbb{F}_{2^d}\backslash\{0\}$ and $a_0 \in \mathbb{F}_{2^d}$, we also write: $E_{a_0,b_0,c_0}(\mathbb{F}_{2^d}) = \{[X:Y:Z] \in \mathbb{P}_2(\mathbb{F}_{2^d}) \big| Y^2Z + c_0XYZ = X^3 + a_0X^2Z + b_0Z^3\}$.

III. Classification of elements of $E_{a,b,c}(A)$

Let [X : Y : Z] ∈ $E_{a,b,c}(A)$, 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.

- 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 $E_{a,b,c}(A)$: $Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3$.

So we can write:

$$a = a_0 + a_1\varepsilon$$
$$b = b_0 + b_1\varepsilon$$
$$c = c_0 + c_1\varepsilon$$
$$X = x_0 + x_1\varepsilon$$

We have:

$$z_1\varepsilon + (c_0 + c_1\varepsilon).(x_0 + x_1\varepsilon).z_1\varepsilon = (x_0 + x_1\varepsilon)^3 + (a_0 + a_1\varepsilon).(x_0 + x_1\varepsilon)^2.z_1\varepsilon + (b_0 + b_1\varepsilon).{z_1}^3\varepsilon^3$$

Which implies that

$$z_1\varepsilon + (c_0 + c_1\varepsilon).(x_0z_1\varepsilon) = {x_0}^3 + ({x_0}^2x_1 + a_0{x_0}^2z_1)\varepsilon$$

Then

$$(z_1 + c_0x_0z_1)\varepsilon = {x_0}^3 + ({x_0}^2x_1 + a_0{x_0}^2z_1)\varepsilon$$

Since $(1, \varepsilon)$ is a basis 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 $E_{a,b,c}(A)$, is of the form $[X:Y:1]$ or $[x\varepsilon: 1: 0]$; where $x \in \mathbb{F}_{2^d}$ and we write $E_{a,b,c}(A) = \{\, [X : Y : 1] \in P_2(A) \,|Y^2 + cXY = X^3 + aX^2 + b\} \cup \{[x\varepsilon: 1: 0] \big| x \in \mathbb{F}_{2^d}\, \}$

IV. THE π_2 HOMOMORPHISM

We consider the canonical projection π defined by

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

Lemma 1: π is a morphism of rings.

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

$$X + Y = x_0 + y_0 + (x_1 + y_1)\varepsilon$$
$$\begin{aligned} X.Y &= (x_0 + x_1\varepsilon).(y_0 + y_1\varepsilon) \\ &= x_0.y_0 + x_0y_1\varepsilon + y_0x_1\varepsilon \\ &= x_0y_0 + (x_0y_1 + y_0x_1)\varepsilon \end{aligned}$$

So :

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

Therefore π is a morphism of rings.

Lemma 2: Let [X : Y : Z] ∈ $\mathbb{P}_2(A)$, where

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

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

We would also like to thank FST, FEZ; MOROCCO for its valued support.

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).

$$Z = z_0 + z_1\varepsilon$$
$$a = a_0 + a_1\varepsilon$$
$$b = b_0 + b_1\varepsilon$$
$$c = c_0 + c_1\varepsilon$$
$$X = x_0 + x_1\varepsilon.$$

Then $[X : Y : Z] \in E_{a,b,c}(A)$ 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 basis of the vector space A over $\mathbb{F}_{2^d}$ and $[X : Y : Z] \in E_{a,b,c}(A)$, then $Y^2Z + cXYZ = X^3 + aX^2Z + bZ^3$, so after the compute, we find the result.

* Let π_2 the mapping defined by:

$$\pi_2 : E_{a,b,c}(A) \longrightarrow E_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$$
$$[X : Y : Z] \longmapsto [\pi(X) : \pi(Y) : \pi(Z)]$$

We proof that the mapping $\pi_2$is a surjective homomorphism of groups.

Theorem 1: Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in $E_{a,b,c}(A)$ and $P + Q = [X_3 : Y_3 : Z_3]$.

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

$$X_3 = X_1Y_1Y_2{}^2 + X_2Y_1{}^2Y_2 + c\,X_2{}^2Y_1{}^2 + c^2X_1X_2{}^2Y_1 + a\,X_1{}^2X_2Y_2 + a\,X_1X_2{}^2Y_1 + ac\,X_1{}^2X_2{}^2 + b\,X_1Y_1Z_2{}^2 + b\,X_2Y_2Z_1{}^2 + bc\,X_1{}^2Z_2{}^2 + c^2b\,Y_1Z_2{}^2Z_1 + c^2b\,Y_2Z_1{}^2Z_2 + c^3b\,X_1Z_2{}^2Z_1.$$

$$Y_3 = Y_1{}^2Y_2{}^2 + c\,X_2Y_1{}^2Y_2 + ac\,X_1X_2{}^2Y_1 + a^2\,X_1{}^2X_2{}^2 + b\,X_1{}^2X_2Z_2 + b\,X_1\,X_2{}^2Z_1 + bc\,X_1Y_1Z_2{}^2 + bc^2\,X_1{}^2Z_2{}^2 + ab\,X_2{}^2Z_1{}^2 + bc^3\,Y_1Z_2{}^2Z_1 + bc^4\,X_1Z_2{}^2Z_1 + abc^2\,X_1Z_2{}^2Z_1 + abc^2\,X_2Z_1{}^2Z_2 + b^2Z_1{}^2Z_2{}^2.$$

$$Z_3 = X_1{}^2X_2Y_2 + X_1X_2{}^2Y_1 + Y_1{}^2Y_2Z_2 + Y_1Y_2{}^2Z_1 + c\,X_1{}^2X_2{}^2 + c\,X_2Y_1{}^2Z_2 + c^2\,X_1{}^2Y_2Z_2 + a\,X_1{}^2Y_2Z_2 + a\,X_2{}^2Y_1Z_1 + c^3\,X_1{}^2X_2Z_2 + ac\,X_1X_2{}^2Z_1 + b\,Y_1Z_2{}^2Z_1 + b\,Y_2Z_1{}^2Z_2 + bc\,X_1Z_2{}^2Z_1.$$

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

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

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

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

Proof. Using the explicit formulas in W. Bosma and H. Lenstras article see [4] we prove the theorem.

Lemma 3. The mapping $\pi_2$is a surjective homomorphism of groups.

Proof. The formula of lemma (2) means that $\pi_2([X : Y : Z]) = [x_0 : y_0 : z_0]$, and $[x_0 : y_0 : z_0] \in \mathrm{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$ so π_2 is well defined.

π_2 is surjective: Let $[x_0 : y_0 : z_0] \in \mathrm{E}_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$, we will show that $[x_0 : y_0 : z_0]$ have an antecedent $[X : Y : Z] \in E_{a,b,c}(A)$.

• 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 : $z_0 \neq 0$, so z_0 is invertible 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 lemma (2) we have :

$$y_0{}^2 + c_0x_0y_0 = x_0{}^3 + a_0x_0{}^2 + b_0$$
$$c_0(x_0y_1 + y_0x_1) + c_1x_0y_0 = a_1x_0{}^2 + x_0{}^2x_1 + b_1$$

There is three sub-cases :

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

• Case 2,2 : $y_0 \neq 0$, then we just take $[X : Y : Z] = [(c_0y_0)^{-1}.b_1\varepsilon : y_0 : 1]$.

• Case 2,3 : $y_0 = 0$ and $x_0 = 0$ then we have $b_0 = 0$ absurd because c^6b is invertible ie, $b_0 \neq 0$ and $c_0 \neq 0$.

π_2 is an homomorphism : We just use the theorem (1) and lemma (1).

Lemma 4: $[x\varepsilon : 1 : 0] + [y\varepsilon : 1 : 0] = [(x + y)\varepsilon : 1 : 0]$

Proof. We have $\pi_2([x\varepsilon : 1 : 0]) = \pi_2([y\varepsilon : 1 : 0])$, so by applying the formula in theorem (1) we have : $X_3 = (x + y)\varepsilon, Y_3 = 1 + cy\varepsilon$ 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 5: The mapping

$$\mathbb{F}_{2^d} \xrightarrow{\theta} E_{a,b,c}(A)$$
$$x \longmapsto [x\varepsilon : 1 : 0]$$

Is an injective morphism of groups.

Proof. θ is well defined because $[x\varepsilon : 1 : 0] \in E_{a,b,c}(A)$, see proposition (1) and from the lemma (4) 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 6: $Ker(\pi_2) = \theta(\mathbb{F}_{2^d})$

Proof. Evidently we have $\theta(\mathbb{F}_{2^d}) \subseteq Ker(\pi_2)$, now let $P = [X : Y : Z] = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : z_0 + z_1\varepsilon] \in Ker(\pi_2)$, implies that $\pi_2(P) = [x_0 : y_0 : z_0] = [0 : 1 : 0]$, implies that $P = [x_1\varepsilon : 1 : z_1\varepsilon] \in E_{a,b,c}(A)$ and from the proposition (1), we have $P = [x\varepsilon : 1 : 0] \in \theta(\mathbb{F}_{2^d})$, ie $Ker(\pi_2) \subseteq \theta(\mathbb{F}_{2^d})$, hence $\theta(\mathbb{F}_{2^d}) = Ker(\pi_2)$.

From lemmas (3), (5), and (6) we deduce the following corollary :

Corollary 1: The sequence

$$0 \rightarrow Ker(\pi_2) \xrightarrow{i} E_{a,b,c}(A) \xrightarrow{\pi_2} E_{a_0,b_0,c_0}(\mathbb{F}_{2^d}) \rightarrow 0$$

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

V. CODING APPLICAION

Let $E_{a,b,c}(A)$ an elliptic curve over A and $P \in E_{a,b,c}(A)$ of order l. We will use the subgroup $< P >$ of $E_{a,b,c}(A)$ 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 $m \in \{1,2, \ldots, l\}$ which $\boldsymbol{A} = \mathbb{F}_{2^2}[\boldsymbol{\varepsilon}]$**;** defined as it follows:
If $Q = [x_0 + x_1\varepsilon : y_0 + y_1\varepsilon : Z]$, where $x_i, y_i \in \mathbb{F}_{2^2}$ for $i = 0$ or 1 and $Z = 0$ or 1. We set :

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

, where α is primitive root of an irreducible polynomal of degree 2 over $\mathbb{F}_2$ and $c_{i,j}, d_{i,j} \in \mathbb{F}_2$. Then we code Q as it follows:
If $Z = 1$ then : $Q = c_{0,0}c_{1,0}c_{0,1}c_{1,1}d_{0,0}d_{1,0}d_{0,1}d_{1,1}1$
If $Z = 0$ then : $Q = 00c_{0,1}c_{1,1}10000$

2. Example:

Let $a = 0, b = 1 + \varepsilon$ and $c = 1$. So the elliptic curve $E_{a,b,c}(A)$ has 32 elements :
Let $P = [\alpha + 1 + (\alpha + 1)\varepsilon : \alpha + 1 + (\alpha + 1)\varepsilon : 1] = 111111111 \in E_{a,b,c}(A)$, we have :

$$2P = [1 + \alpha\varepsilon + \varepsilon : 1 + \varepsilon : 1] = 101110101$$
$$3P = [\alpha + \varepsilon : \varepsilon : 1] = 011000101$$
$$4P = [\varepsilon : 1 + \varepsilon : 1] = 001010101$$
$$5P = [\alpha + (\alpha + 1)\varepsilon : \alpha + \varepsilon : 1] = 011101101$$
$$6P = [1 + \alpha\varepsilon : \alpha\varepsilon + \varepsilon : 1] = 100100111$$
$$7P = [\alpha + 1 : \alpha\varepsilon : 1] = 110000011$$
$$8P = [\varepsilon : 1 + \alpha\varepsilon : 0] = 010010011$$
$$9P = [\alpha + 1 : \alpha + 1 + \alpha\varepsilon : 1] = 110011011$$
$$10P = [1 + \alpha\varepsilon : 1 + \varepsilon : 1] = 100111001$$
$$11P = [\alpha + (\alpha + 1)\varepsilon : \alpha\varepsilon : 1] = 011100011$$
$$12P = [\varepsilon : 1 : 1] = 010010001$$
$$13P = [\alpha + \varepsilon : \alpha : 1] = 011001001$$
$$14P = [1 + \alpha\varepsilon + \varepsilon : \alpha\varepsilon : 1] = 110100011$$
$$15P = [\alpha + 1 + \alpha\varepsilon + \varepsilon : 0 : 1] = 111100001$$
$$16P = [0 : 1 : 0] = 000010000$$

So,

$$G = \{111111111, 101110101, 011000101, 001010101, 011101101, 100100111, 110000011, 010010011\ 110011011, 100111001, 011100011, 010010001, 011001001, 110100011, 111100001, 000010000\}.$$

VI. CONCLUSION

In this work we have studed the elliptic curve over the ring $A = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$, precisely we have established the short exact sequence that defines the group extension $E_{a,b,c}(A)$ of $E_{a_0,b_0,c_0}(\mathbb{F}_{2^d})$ by $Ker(\pi_2)$, and we have given an example of coding over this ring.

REFERENCES

[1] Abdelhakim chillali, the j-invariant over $\mathbb{E}_{3^d}{}^n$.Int. j. Open problems Compt.Math.Vol.5, No.4, December 2012, ISSN 1998-6262; Copyright ICSRS Publication, WWW.i-csrc.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] W. Bosma and H. Lenstra, Complete system of two addition laws for elliptic curved, Journal of Number theory (1995).

[5] 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).

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

[7] J.H .SILVERMAN . The Arithmetic of Elliptic curves, second edition, Graduate texts in Mathematics 106.DOI 10.1007/978-0-387-09494-6-A

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

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

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

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

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