Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–15.
ISSN-0037-8712
doi:10.5269/bspm.63526

New elliptic group over a nonlocal ring $\mathbb{F}_{2^d}[\varepsilon]$, $\varepsilon^3 = \varepsilon^2$ *

Abdelhamid Tadmori

ABSTRACT: In this paper, we consider the set of elliptic curves over an extended nonlocal ring of characteristic two $A = \frac{\mathbb{F}_{2^d}[X]}{(X^3 - X^2)}$. Then by studying the arithmetic operation of this ring, and define such elliptic curves, we come to classify their elements. More precisely, we define a new group law structure on this elliptic curve by using one of the explicit bijection $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d}) \times E_{\pi_2(a),\pi_2(b)}(A_2) \simeq E_{a,b}(A)$, where $A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$ is a local ring, π_1 is a sum projection of the coordinates elements in A, and π_2 is the surjective morphism defined by:

$$\pi_2 : A \longrightarrow A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$$

$$x_0 + x_1\varepsilon + x_2\varepsilon^2 \longmapsto x_0 + x_1\sigma \quad \text{where } \sigma^2 = 0.$$

Key Words: Finite ring, finite field, elliptic curve, cryptography.

Contents

1. Introduction

Elliptic curves over (finite) fields provide a paradigm for major areas of current research in number theory, in algebraic geometry and in cryptography; see [6,8,9,12,14]. Its extension to elliptic curves over finite rings faces the difficulty of constructing such curves in an explicit way. The case of elliptic curves over rings has been studied in different aspects. In algebraic geometry, the theoretical study of these curves in the case of Dedekind domain R is exhibited in the book of Silverman; as a Neron model for E/K, which is a smooth group scheme, whose generic fiber is E/K, where K is the fraction field of ring R, giving just some examples over a discrete valuation ring $\mathbb{Z}_N$, where $N \in \mathbb{N}^*$. The existence of Neron models came from the theorem 6.1 see [13] page 325. In number theory, the study of these curves on a ring $\mathbb{Z}_{p.q}$, where p and q are distinct prime numbers, is set out in the article of Lenstra, it has allowed to factor a large integers using elliptic curves; see [10]. In cryptography, the thesis of Sebastia Martin studies the cryptographic application of the curves on a ring $\mathbb{Z}_{N'}$, where $N' = p.q$, see [11]. Marie Virat's thesis studies the properties of the elliptic curves defined on kind of local ring $\mathbb{F}_p[\varepsilon]$, $\varepsilon^2 = 0$ from a cryptographic point of view, with p is a prime number which differs from 2 and 3; see [21]. On one side, Mr A. Chillali has generalized the work on the kind of local ring $\mathbb{F}_q[\varepsilon]$, $\varepsilon^n = 0$, where q is a power of a prime number which differs from 2 and 3; see [4,5]. On the other hand, Mr Hachem Hassib has studied the elliptic curves on the local ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^n = 0$; see [7]. On our side, we have studied the elliptic curves on the local ring $\mathbb{F}_{2^d}[\varepsilon]; \varepsilon^n = 0$, see [17,18]. In the paper [2], the authors A. Boulbout, A. Chillali and A. Mouhib have defined a set of elliptic curves over the nonlocal ring $\mathbb{F}_q[e]; e^2 = e$, where q

* The work is supported by Faculty of science and Technology, Alhoceima

Submitted May 11, 2022. Published March 24, 2025
2010 *Mathematics Subject Classification:* 11T30, 14H52, 11G07, 11T71.

is the power of prime p with $p \geq 5$, and given the classification of its elements. In the work, see [19], we have studied the set of elliptic curves over the nonlocal ring $\mathbb{F}_{2^d}[\varepsilon]; \varepsilon^2 = \varepsilon$, and we have identified a group law over these curves. In this work, we will extend our study to the elliptic curves over the nonlocal ring $\mathbb{F}_{2^d}[\varepsilon]$, $\varepsilon^3 = \varepsilon^2$. More precisely, we give a classification of elements of such elliptic curves, and construct a group law over it, giving some properties.

We begin by studying the arithmetic over the ring $A = \mathbb{F}_{2^d}[\varepsilon]$, $\varepsilon^3 = \varepsilon^2$.

2. Arithmetic operations in the ring A

Let d be a positive prime integer. We consider the extension of the finite field $\mathbb{F}_{2^d}$ by using the quotient ring of the polynomial ring $\mathbb{F}_{2^d}[X]$, and the ideal generated by the polynomial $X^3 - X^2$. The ring $A = \frac{\mathbb{F}_{2^d}[X]}{(X^3 - X^2)}$ is identified to the ring $\mathbb{F}_{2^d}[\varepsilon]$; $\varepsilon^3 = \varepsilon^2$, see [1]. So, we have $A = \{x_0 + x_1\varepsilon + x_2\varepsilon^2 \mid x_0, x_1, x_2 \in \mathbb{F}_{2^d}\}$, and the following lemmas:

Lemma 2.1 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2$, $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2$, then;*

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\varepsilon + (x_2 + y_2)\varepsilon^2.$$

$$\begin{aligned} X \cdot Y &= x_0y_0 + (x_0y_1 + x_1y_0)\varepsilon + \Big(x_0y_2 + x_1y_1 + x_1y_2 + x_2y_0 + x_2y_1 + x_2y_2\Big)\varepsilon^2 \\ &= x_0y_0 + (x_0y_1 + x_1y_0)\varepsilon + \Big(x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2\Big)\varepsilon^2 \end{aligned}$$

Lemma 2.2 *A is a vector space over $\mathbb{F}_{2^d}$ of dimension 3, whose basis is $\{1, \varepsilon, \varepsilon^2\}$.*

Lemma 2.3 *We have:*

$$X \cdot Y = x_0y_0 + \omega(X \cdot Y)\varepsilon + \Big((x_0 + x_1 + x_2) \cdot (y_0 + y_1 + y_2) + x_0y_0 + \omega(X \cdot Y)\Big).\varepsilon^2$$

where $\omega(X \cdot Y) = x_0y_1 + x_1y_0$.

Proof: We know that:

$$\begin{aligned} \Big((x_0 + x_1 + x_2) \cdot (y_0 + y_1 + y_2) + x_0y_0 + \omega(X \cdot Y)\Big) &= \Big(x_0y_2 + x_1y_1 + x_1y_2 + x_2y_0 + x_2y_1 + x_2y_2\Big) \\ &= x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2. \end{aligned}$$

□

Remark 2.1

$$\begin{aligned} \omega(X \cdot Y) &= (x_0 + x_1) \cdot (y_0 + y_1) + x_0y_0 + x_1y_1 \\ \omega(X^2) &= 0 \\ \omega(X^3) &= x_0^2x_1. \end{aligned}$$

Proposition 2.1 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \in A$. We have:*

$$\begin{aligned} X^2 &= x_0^2 + \Big((x_0 + x_1 + x_2)^2 + x_0^2\Big)\varepsilon^2 \\ X^3 &= x_0^3 + x_0^2x_1\varepsilon + \Big((x_0 + x_1 + x_2)^3 + x_0^3 + x_0^2x_1\Big)\varepsilon^2 \end{aligned}$$

Proof: By using Lamma 2.3 and Remark 2.1, we have:

$$\begin{aligned} X^2 &= x_0^2+\omega(X^2)\varepsilon+\Big((x_0+x_1+x_2)^2+x_0^2+\omega(X^2)\Big)\varepsilon^2 \\ &= x_0^2+\Big((x_0+x_1+x_2)^2+x_0^2\Big)\varepsilon^2 \\ X^3 &= x_0^3+\omega(X^3)\varepsilon+\Big[\Big(x_0^2+(x_0+x_1+x_2)^2+x_0^2\Big)(x_0+x_1+x_2)+x_0^3+\omega(X^3)\Big]\varepsilon^2 \\ &= x_0^3+x_0^2x_1\varepsilon+\Big((x_0+x_1+x_2)^3+x_0^3+x_0^2x_1\Big)\varepsilon^2. \end{aligned}$$

□

Proposition 2.2 *The element $X=x_0+x_1\varepsilon+x_2\varepsilon^2\in A$, is invertible if and only if x_0 and $x_0+x_1+x_2$, are invertibles in $\mathbb{F}_{2^d}$. The inverse of X is given by:*

$$X^{-1}=x_0^{-1}+x_1x_0^{-2}\varepsilon+\Big((x_0+x_1+x_2)^{-1}+x_1x_0^{-2}+x_0^{-1}\Big)\varepsilon^2.$$

Proof: Let $Y=y_0+y_1\varepsilon+y_2\varepsilon^2$ the inverse of $X=x_0+x_1\varepsilon+x_2\varepsilon^2$. So $X\cdot Y=1$, which identically equivalent to:

$$x_0y_0+\omega(X\cdot Y)\varepsilon+\Big((x_0+x_1+x_2).(y_0+y_1+y_2)+x_0y_0+\omega(X\cdot Y)\Big)\varepsilon^2=1.$$

Thereby,

$$\begin{aligned} X\cdot Y=1 \iff & \begin{cases} x_0y_0=1 \\ \omega(X\cdot Y)=0 \\ (x_0+x_1+x_2).(y_0+y_1+y_2)+x_0y_0+\omega(X\cdot Y)=0 \end{cases} \\ \iff & \begin{cases} x_0y_0=1 \\ x_0y_1+x_1y_0=0 \\ (x_0+x_1+x_2).(y_0+y_1+y_2)=1 \end{cases} \\ \iff & \begin{cases} y_0=x_0^{-1} \\ y_1=x_1x_0^{-2} \\ y_2=(x_0+x_1+x_2)^{-1}+x_0^{-1}+x_1x_0^{-2} \end{cases} \end{aligned}$$

which gives the result. □

Remark 2.2 *An element $X=x_0+x_1\varepsilon+x_2\varepsilon^2\in A$, is invertible if and only if $x_0\neq 0$ and $x_0+x_1+x_2\neq 0$ in $\mathbb{F}_{2^d}$.*

Corollary 2.1 *An element $X=x_0+x_1\varepsilon+x_2\varepsilon^2\in A$, is non-invertible if and only if $x_0=0$ or $x_0+x_1+x_2=0$. On the other words, X is of the form $X=x\varepsilon+y\varepsilon^2$, or of the form $X=x+y\varepsilon+(x+y)\varepsilon^2$, where $(x,y)\in\mathbb{F}_{2^d}^2$.*

Lemma 2.4 *$A=\mathbb{F}_{2^d}[\varepsilon]$; $\varepsilon^3=\varepsilon^2$, is a nonlocal ring.*

Proof: Consider two ideals defined by:

$$I=\{x\varepsilon+y\varepsilon^2 \mid (x,y)\in\mathbb{F}_{2^d}^2\} \text{ and } J=\{x+y\varepsilon+(x+y)\varepsilon^2 \mid (x,y)\in\mathbb{F}_{2^d}^2\}.$$

From the previous corollary, it is clear that $I\cup J$ is the set of the no invertible elements in A. Say that;

$$\begin{aligned} x\varepsilon+y\varepsilon^2=x'+y'\varepsilon+(x'+y')\varepsilon^2 &\implies x'+(x+y')\varepsilon+(x'+y'+y)\varepsilon^2=0 \\ &\implies x'=0,\ x=y' \text{ and } y=y'=x, \end{aligned}$$

because $\{1, \varepsilon, \varepsilon^2\}$ is a basis of A as a vector space over $\mathbb{F}_{2^d}$. So, $I \cap J = \{x\varepsilon + x.\varepsilon^2 \mid x \in \mathbb{F}_{2^d}\}$, thus $I \cap J \neq I$ and $I \cap J \neq J$. As a result, we have neither $I \subset J$ nor $J \subset I$, then $I \cup J$ is no an ideal. Hence, A is nonlocal ring. □

Next, we show some relationship, and give one of the explicit formula of an isomorphism:

$$A \simeq A_1 \times A_2,$$

where $A_1 = \mathbb{F}_{2^d}$, and A_2 is the local ring $A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$, with the technique which allows us to show some explicit properties of the elliptic curve over a nonlocal ring A; $E_{a,b}(A)$. Firstly, we have the following lemma:

Lemma 2.5 *Let R be a ring and $e \in R$ be a no trivial idempotent element. Then, we have the isomorphism $R \simeq R_1 \times R_2$, where $R_1 = eR$, and $R_2 = (1-e)R$ are two nonzero rings.*

Proof: It is clear that R_1 and R_2 are nonzero, since neither e nor $1-e$ is 0. Otherwise, e is idempotent implies that $(1-e)^2 = 1-2e+e^2 = 1-e$, so $1-e$ is also idempotent. To show that R_1, and R_2 are rings it suffices to show that they have a unit of multiplicative law. For R_1; if $eX \in R_1$, then $e(eX) = e^2X = eX$, and since $e = e \cdot 1 \in R_1$, so e is the unit element of R_1. As the same $1-e$ is the unit of R_2. Furthermore, it is trivial to show that:

$$\psi_1 : R \longrightarrow R_1$$
$$X \longmapsto eX$$

and

$$\psi_2 : R \longrightarrow R_2$$
$$X \longmapsto (1-e)X$$

are surjectives morphisms. We will show that the combined morphism:

$$\psi : R \longrightarrow R_1 \times R_2$$
$$X \longmapsto (\psi_1(X),\, \psi_2(X)) = (eX,\, (1-e)X)$$

is a ring isomorphism; indeed, it is clear that ψ is a morphism of rings, since both ψ_1, and ψ_2 are morphisms. Further, if $\psi(X) = (0,0)$, then $eX = (1-e)X = 0$ hence, $X = 0$, thus ψ is injective. On the other hand, if $(eX_1, (1-e)X_2) \in R_1 \times R_2$, we get $\psi(eX_1 + (1-e)X_2) = \Big(e^2X_1 + e(1-e)X_2,\, (1-e)eX_1 + (1-e)^2X_2\Big) = (eX_1, (1-e)X_2)$. Therfore, ψ is also surjective, which gives the result. □

Corollary 2.2 *For the ring $A = \mathbb{F}_{2^d}[\varepsilon]$; $\varepsilon^3 = \varepsilon^2$, we have the isomorphism $A \simeq R_1 \times R_2$ where $R_1 = \{\varepsilon^2 X \mid X \in A\}$, and $R_2 = \{(1-\varepsilon^2)X \mid X \in A\}$.*

Proof: We take $e = \varepsilon^2$, since $e^2 = (\varepsilon^2)^2 = \varepsilon^3 \cdot \varepsilon = \varepsilon^2 \cdot \varepsilon = \varepsilon^3 = \varepsilon^2 = e$, then e is idempotent in A, so by using Lemma 2.5, we deduce the result. □

Remark 2.3 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2$, $Y = y_0 + y_1\varepsilon + y_2\varepsilon^2 \in A$.*

- *If $X' = \varepsilon^2 X$ and $Y' = \varepsilon^2 Y \in R_1$, then*

$$\begin{aligned} X' &= (x_0 + x_1 + x_2)\varepsilon^2 \\ Y' &= (y_0 + y_1 + y_2)\varepsilon^2 \\ X' + Y' &= (x_0 + y_0 + x_1 + y_1 + x_2 + y_2)\varepsilon^2, \\ X' \cdot Y' &= (x_0 + x_1 + x_2)(y_0 + y_1 + y_2)\varepsilon^2. \end{aligned}$$

- *If* $X' = (1-\varepsilon^2)X$ *and* $Y' = (1-\varepsilon^2)Y \in R_2$, *then*

$$\begin{aligned} X' &= x_0 + x_1\varepsilon + (x_0+x_1)\varepsilon^2 \\ Y' &= y_0 + y_1\varepsilon + (y_0+y_1)\varepsilon^2 \\ X'+Y' &= (x_0+y_0) + (x_1+y_1)\varepsilon + (x_0+y_0+x_1+y_1)\varepsilon^2, \\ X'\cdot Y' &= x_0.y_0 + \omega(X'\cdot Y')\varepsilon + (x_0y_0 + \omega(X'\cdot Y'))\varepsilon^2, \text{ where } \omega(X'\cdot Y') = x_0y_1 + x_1y_0. \end{aligned}$$

We denote φ_1, φ_2 these mappings:

$$\varphi_1 : R_1 \longrightarrow A_1 = \mathbb{F}_{2^d}$$

$$\varepsilon^2.X \longmapsto x_0 + x_1 + x_2$$

and

$$\varphi_2 : R_2 \longrightarrow A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$$

$$x_0 + x_1\varepsilon + (x_0+x_1)\varepsilon^2 \longmapsto x_0 + x_1\sigma$$

where $\sigma^2 = 0$.

Lemma 2.6 *The mappings* φ_1 *and* φ_2, *defined previously are the isomorphisms of rings.*

Proof:

- Let $a, b \in R_1$. So, there exists X, $Y \in A$ such that $a = \varepsilon^2 X$, and $b = \varepsilon^2 Y$, thus:

$$\begin{aligned} \varphi_1(a+b) &= \varphi_1(\varepsilon^2(X+Y)) \\ &= x_0 + y_0 + x_1 + y_1 + x_2 + y_2 \\ &= (x_0+x_1+x_2) + (y_0+y_1+y_2) \\ &= \varphi_1(\varepsilon^2 X) + \varphi_1(\varepsilon^2 Y) \\ &= \varphi_1(a) + \varphi_1(b). \end{aligned}$$

  And

$$\begin{aligned} \varphi_1(a\cdot b) &= \varphi_1(\varepsilon^2 X\cdot\varepsilon^2 Y)) \\ &= \varphi_1(\varepsilon^4(X\cdot Y)) \\ &= \varphi_1(\varepsilon^2(X\cdot Y)) \\ &= (x_0+x_1+x_2)\cdot(y_0+y_1+y_2) \\ &= \varphi_1(\varepsilon^2 X)\cdot\varphi_1(\varepsilon^2 Y) \\ &= \varphi_1(a)\cdot\varphi_1(b). \end{aligned}$$

  This proves that φ_1 is a morphism of ring. On the other hand, let $a, b \in R_1$ such that $\varphi_1(a) = \varphi_1(b)$, where $a = \varepsilon^2 X$ and $b = \varepsilon^2 Y$.

$$\begin{aligned} \varphi_1(a) = \varphi_1(b) &\Longrightarrow x_0 + x_1 + x_2 = y_0 + y_1 + y_2 \\ &\Longrightarrow \varepsilon^2(x_0+x_1+x_2) = \varepsilon^2(y_0+y_1+y_2) \\ &\Longrightarrow \varepsilon^2 X = \varepsilon^2 Y \\ &\Longrightarrow a = b. \end{aligned}$$

  So, φ_1 is injective. Finally, let $x \in \mathbb{F}_{2^d}$, there we take $X = 0 + 0.\varepsilon + x.\varepsilon^2$, and we have $\varphi_1(\varepsilon^2.X) = x$, which proves that φ_1 is surjective.

- With the same method applying Remark 2.3. Let $X,\ Y \in R_2$, thus X and Y are of the form $X = x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2$ and $Y = y_0 + y_1\varepsilon + (y_0 + y_1)\varepsilon^2$.

$$\begin{aligned}\varphi_2(X+Y) &= \varphi_2\Big((x_0+y_0)+(x_1+y_1)\varepsilon+(x_0+y_0+x_1+y_1)\varepsilon^2\Big)\\ &= x_0+y_0+(x_1+y_1)\sigma\\ &= \varphi_2(X)+\varphi_2(Y)\end{aligned}$$

And

$$\begin{aligned}\varphi_2(X\cdot Y) &= \varphi_2\Big(x_0.y_0+\omega(X\cdot Y)\varepsilon+(x_0y_0+\omega(X\cdot Y))\varepsilon^2\Big)\\ &= x_0y_0+\omega(X\cdot Y)\sigma\\ &= x_0y_0+(x_0y_1+x_1y_0)\sigma\\ &= (x_0+x_1\sigma)\cdot(y_0+y_1\sigma)\\ &= \varphi_2(X)\cdot\varphi_2(Y).\end{aligned}$$

which proves that φ_2 is a morphism of rings. Since

$$\begin{aligned}\varphi_2(X)=\varphi_2(Y) &\Longrightarrow x_0+x_1\sigma = y_0+y_1\sigma\\ &\Longrightarrow x_0=y_0 \text{ and } x_1=y_1\\ &\Longrightarrow X=Y;\end{aligned}$$

because $\{1,\sigma\}$ is the basis of the $\mathbb{F}_{2^d}$ vector space A_2. This proves that φ_2 is injective. For the surjection, let $X' \in A_2$, then $X' = x'_0 + x'_1\sigma$, so the antecedent of X' by φ_2 is $X = x'_0 + x'_1\varepsilon + (x'_0 + x'_1)\varepsilon^2$.

□

Theorem 2.1 *The mapping:*

$$\Phi : A \longrightarrow A_1 \times A_2$$

$$X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \longmapsto \Big(\varphi_1\circ\psi_1(X),\ \varphi_2\circ\psi_2(X)\Big)$$

is an isomorphism.

Proof: Using the Corollary 2.2 and Lemma 2.6, we prove the result.

□

Corollary 2.3 *The following mapping:*

$$\pi_1 : A \longrightarrow A_1 = \mathbb{F}_{2^d}$$

$$X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \longmapsto x_0 + x_1 + x_2$$

$$\pi_2 : A \longrightarrow A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$$

$$x_0 + x_1\varepsilon + x_2\varepsilon^2 \longmapsto x_0 + x_1\sigma$$

are the surjective morphisms of rings.

Proof: Since ψ_1, ψ_2, φ_1 and φ_2 are the surjective morphisms of rings, and $\pi_1 = \varphi_1\circ\psi_1$, $\pi_2 = \varphi_2\circ\psi_2$, then we have the result. □

Corollary 2.4 *Every element $X \in A$, can be written as follows:*

$$X = \varphi_2^{-1}(\pi_2(X)) + \pi_1(X).\varepsilon^2.$$

Proof: Let $X = x_0+x_1\varepsilon+x_2\varepsilon^2 \in A$. We have $\pi_2(X) = x_0+x_1\sigma$, where $\sigma^2 = 0$ and φ_2 is the isomorphism defined previously, so $\varphi_2^{-1}(\pi_2(X)) = x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2$. Hence, we have:

$$\varphi_2^{-1}(\pi_2(X)) + \pi_1(X)\varepsilon^2 = x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2 + (x_0 + x_1 + x_2)\varepsilon^2 = X.$$

□

Corollary 2.5 *An element $X = x_0 + x_1\varepsilon + x_2\varepsilon^2 \in A$ is invertible if and only if $x_0 + x_1 + x_2$ is invertible in A_1, and $x_0 + x_1\sigma$ is invertible in A_2.*

Proof: Since every element $x_0 + x_1\sigma \in A_2$ is invertible if and only if $x_0 \neq 0$, and by using Remark 2.2 we deduce the result. □

3. Properties of an elliptic curve over the ring A

This section gives a definition of an elliptic curve, and their properties on the ring $A = \mathbb{F}_{2^d}[\varepsilon]$; $\varepsilon^3 = \varepsilon^2$; noted by $E_{a,b}(A)$, where $a = a_0 + a_1\varepsilon + a_2\varepsilon^2$, $b = b_0 + b_1\varepsilon + b_2\varepsilon^2 \in A$. More precisely, we prove the bijection:

$$E_{a,b}(A) \simeq E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d}) \times E_{\pi_2(a),\pi_2(b)}(A_2).$$

Firstly, we have the following definitions; see [3,13,16].

Definition 3.1 *We define an elliptic curve over the ring A, noted $E_{a,b}(A)$ as a curve given by such Weierstrass equation:*

$$Y^2Z + XYZ = X^3 + aX^2Z + bZ^3 \tag{3.1}$$

where $a, b \in A$, that b is invertible. The discriminant $\Delta = b$, and the J-invariant is $J = b^{-1}$ noted by $\frac{1}{b}$. We write:

$$E_{a,b}(A) = \{[X : Y : Z] \in \mathbb{P}_2(A) \mid Y^2Z + XYZ = X^3 + aX^2Z + bZ^3\}$$

Definition 3.2 *We define two reductions of $E_{a,b}(A)$, one is over $\mathbb{F}_{2^d}$, as a curve given by such Weierstrass equation:*

$$Y^2Z + XYZ = X^3 + \pi_1(a)X^2Z + \pi_1(b)Z^3 \tag{3.2}$$

where $\pi_1(a) = a_0 + a_1 + a_2$, $\pi_1(b) = b_0 + b_1 + b_2 \in \mathbb{F}_{2^d}$, and $\pi_1(b) \neq 0$, which noted by $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$. The second is over $A_2 = \frac{\mathbb{F}_{2^d}[X]}{(X^2)}$ as a curve given by such Weierstrass equation:

$$Y^2Z + XYZ = X^3 + \pi_2(a)X^2Z + \pi_2(b)Z^3 \tag{3.3}$$

where $\pi_2(a) = a_0 + a_1\sigma$, $\pi_2(b) = b_0 + b_1\sigma \in A_2$, and $\pi_2(b)$ is invertible in A_2, which is noted by $E_{\pi_2(a),\pi_2(b)}(A_2)$.
The discriminants $\Delta_i = \pi_i(b)$, and the J- invariants $J_i = (\pi_i(b))^{-1}$, where $i \in \{1, 2\}$.

Proposition 3.1 *We have $\Delta = \varphi_2^{-1}(\Delta_2) + \Delta_1 \cdot \varepsilon^2$, and the discriminant Δ is invertible in the ring A if and only if Δ_1 and Δ_2 are invertible respectively in $\mathbb{F}_{2^d}$ and in A_2.*

Proof: By using Corollary 2.4 and 2.5, we prove the proposition. □

Proposition 3.2 *Let $X = x_0 + x_1\varepsilon + x_2\varepsilon^2, Y = y_0 + y_1\varepsilon + y_2\varepsilon^2$ and $Z = z_0 + z_1\varepsilon + z_2\varepsilon^2 \in A$. Then, $[X : Y : Z] \in \mathbb{P}_2(A)$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}_2(A_i)$, for all $i \in \{1, 2\}$.*

Proof: $\Longrightarrow$) Suppose that $[X : Y : Z] \in \mathbb{P}_2(A)$, so there exists $(U, V, W) \in A^3$ such that $U \cdot X + V \cdot Y + W \cdot Z = 1$, then $\pi_i(U) \cdot \pi_i(X) + \pi_i(V) \cdot \pi_i(Y) + \pi_i(W) \cdot \pi_i(Z) = 1$, which implies that $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}_2(A_i)$ for all $i \in \{1, 2\}$.
$\Longleftarrow$) Suppose that $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathbb{P}_2(A_i)$ for all $i \in \{1, 2\}$, so there exists at least one of the coordinates of the point $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ which is invertible in A_i.
• For example, if $\pi_2(X) \in A_2^*$, then we have two cases of $\pi_1(X)$:

1) If $\pi_1(X) \neq 0$, then X is invertible in the ring A; because $\pi_1(X)$, $\pi_2(X)$ are invertible. Hence, $[X : Y : Z] \in \mathbb{P}_2(A)$.

2) If $\pi_1(X) = 0$, then $[\pi_1(X) : \pi_1(Y) : \pi_1(Z)] \in \mathbb{P}_2(\mathbb{F}_{2^d})$ implies that $\pi_1(Y) \neq 0$ or $\pi_1(Z) \neq 0$.

   • If $\pi_1(Y) \neq 0$, then:

$$\varphi_2^{-1}(\pi_2(X)) + \Big(\pi_1(Y) + \varphi_2^{-1}(\pi_2(X))\Big)\varepsilon^2 =$$
$$x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2 + \Big(y_0 + y_1 + y_2 + x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2\Big)\varepsilon^2$$

$$\begin{aligned} &= x_0 + x_1\varepsilon + \Big(y_0 + y_1 + y_2 + x_0 + x_1\Big)\varepsilon^2 \\ &= X + (X + Y)\varepsilon^2 \\ &= (1 + \varepsilon^2)X + Y\varepsilon^2. \end{aligned}$$

   is invertible in A, so there exists $U \in A$ such that:

$$U \cdot (1 + \varepsilon^2)X + U \cdot Y\varepsilon^2 = 1.$$

   Hence, $[X : Y : Z] \in \mathbb{P}_2(A)$.

   • If $\pi_1(Z) \neq 0$, with similar proof, we have $[X : Y : Z] \in \mathbb{P}_2(A)$.

• If $\pi_2(X) \notin A_2^*$, we have either $\pi_2(Y) \in A_2^*$ or $\pi_2(Z) \in A_2^*$, so we follow the same proof. □

Proposition 3.3 *Let $(X, Y, Z) \in A^3$. We have $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$ if and only if $\pi_i(Y)^2\pi_i(Z) + \pi_i(X)\pi_i(Y)\pi_i(Z) = \pi_i(X)^3 + \pi_i(a)\pi_i(X)^2\pi_i(Z) + \pi_i(b)\pi_i(Z)^3$, for all $i \in \{1, 2\}$.*

Proof: By using Corollary 2.4, we have:

$$\begin{aligned} Y^2Z &= \varphi_2^{-1}(\pi_2(Y^2Z)) + \pi_1(Y^2Z).\varepsilon^2 \\ XYZ &= \varphi_2^{-1}(\pi_2(XYZ)) + \pi_1(XYZ).\varepsilon^2 \\ X^3 + aX^2Z + bZ^3 &= \varphi_2^{-1}(\pi_2(X^3 + aX^2Z + bZ^3)) + \pi_1(X^3 + aX^2Z + bZ^3).\varepsilon^2 \end{aligned}$$

Then:
$\Longrightarrow$) Assume that $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$. So, we have:

$$\begin{aligned} \pi_2(Y^2Z + XYZ) &= \pi_2(X^3 + aX^2Z + bZ^3), \\ \pi_1(Y^2Z + XYZ) &= \pi_1(X^3 + aX^2Z + bZ^3) \end{aligned}$$

Since π_2, π_1 are morphisms of rings, we obtain the result.
$\Longleftarrow$) Now, we assume that we have:

$$\begin{cases} \pi_2(Y)^2\pi_2(Z) + \pi_2(X)\pi_2(Y)\pi_2(Z) = \pi_2(X)^3 + \pi_2(a)\pi_2(X)^2\pi_2(Z) + \pi_2(b)\pi_2(Z)^3 \\ \pi_1(Y)^2\pi_1(Z) + \pi_1(X)\pi_1(Y)\pi_1(Z) = \pi_1(X)^3 + \pi_1(a)\pi_1(X)^2\pi_1(Z) + \pi_1(b)\pi_1(Z)^3. \end{cases}$$

which gives

$$\begin{cases} \pi_2(Y^2Z) + \pi_2(XYZ) = \pi_2(X^3 + aX^2Z + bZ^3) \\ \pi_1(Y^2Z) + \pi_1(XYZ) = \pi_1(X^3 + aX^2Z + bZ^3) \end{cases} \Longrightarrow$$

$$\begin{cases} \varphi_2^{-1}\Big(\pi_2(Y^2Z)\Big) + \varphi_2^{-1}\Big(\pi_2(XYZ)\Big) = \varphi_2^{-1}\Big(\pi_2(X^3 + aX^2Z + bZ^3)\Big) \\ \pi_1(Y^2Z) + \pi_1(XYZ) = \pi_1(X^3 + aX^2Z + bZ^3) \end{cases}$$

Thus, by using the above formulas, we deduce that $Y^2Z + XYZ = X^3 + aX^2Z + bZ^3$. □

Theorem 3.1 $[X : Y : Z] \in E_{a,b}(A) \Longleftrightarrow [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in E_{\pi_i(a),\pi_i(b)}(A_i)$, $\forall\, i \in \{1, 2\}$.

Proof: By using propositions 3.2 and 3.3, we prove the theorem. □

Corollary 3.1 *For all $i \in \{1, 2\}$, the correspondence $\tilde{\pi_i}$ defined by:*

$$\tilde{\pi_i} : E_{a,b}(A) \longrightarrow E_{\pi_i(a),\pi_i(b)}(A_i)$$

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

is a surjective mapping.

Proof: From the previous theorem, it is clear that $\tilde{\pi_i}$ is the correspondence. Let $[X : Y : Z]$ and $[X' : Y' : Z']$ two points in the elliptic curve $E_{a,b}(A)$ such that $[X : Y : Z] = [X' : Y' : Z']$, then there exists an invertible element $U \in A$ such that $X' = UX,\ Y' = UY$ and $Z' = UZ$, thereby:

$$\begin{aligned} \tilde{\pi_i}([X' : Y' : Z']) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\ &= [\pi_i(U)\pi_i(X) : \pi_i(U)\pi_i(Y) : \pi_i(U)\pi_i(Z)] \\ &= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)];\ \textit{because}\ \pi_i(U) \in A_i^* \\ &= \tilde{\pi_i}([X : Y : Z]) \end{aligned}$$

Therefore, $\tilde{\pi_i}$ is well defined.
Further, let $[x : y : z] \in E_{\pi_1(a),\pi_1(b)}(A_1)$. For example, we have $\tilde{\pi_1}([x\varepsilon^2 : 1 + (1 + y)\varepsilon^2 : z\varepsilon^2]) = [x : y : z]$, and for $[x_0 + x_1\sigma : y_0 + y_1\sigma : z_0 + z_1\sigma] \in E_{\pi_2(a),\pi_2(b)}(A_2)$, we have $\tilde{\pi_2}([x_0 + x_1\varepsilon + (x_0 + x_1)\varepsilon^2 : y_0 + y_1\varepsilon + (1 + y_0 + y_1)\varepsilon^2 : z_0 + z_1\varepsilon + (z_0 + z_1)\varepsilon^2]) = [x_0 + x_1\sigma : y_0 + y_1\sigma : z_0 + z_1\sigma]$. Then, for all $i \in \{1, 2\}$, $\tilde{\pi_i}$ is a surjective mapping. □

Theorem 3.2 *The mapping:*

$$\tilde{\pi} : E_{a,b}(A) \longrightarrow E_{\pi_1(a),\pi_1(b)}(A_1) \times E_{\pi_2(a),\pi_2(b)}(A_2)$$

$$[X : Y : Z] \longmapsto \Big([\pi_1(X) : \pi_1(Y) : \pi_1(Z)],\ [\pi_2(X) : \pi_2(Y) : \pi_2(Z)]\Big)$$

is a bijection. The inverse of $\tilde{\pi}$ is the mapping $\tilde{\pi}^{-1}$ such that
$\tilde{\pi}^{-1}\Big([x_2 : y_2 : z_2],\ [x_0+x_1\sigma : y_0+y_1\sigma : z_0+z_1\sigma]\Big) = [x_0+x_1\varepsilon+(x_0+x_1+x_2)\varepsilon^2 :\ y_0+y_1\varepsilon+(y_0+y_1+y_2)\varepsilon^2 :\ z_0 + z_1\varepsilon + (z_0 + z_1 + z_2)\varepsilon^2]$.

Proof:

(i) We have $\tilde{\pi}([X : Y : Z]) = \Big(\tilde{\pi_1}([X : Y : Z]),\ \tilde{\pi_2}([X : Y : Z])\Big)$, since $\tilde{\pi_1}$ and $\tilde{\pi_2}$ are well defined, so $\tilde{\pi}$ is well defined.

(ii) Let $\Big([x_2 : y_2 : z_2],\ [x_0 + x_1\sigma : y_0 + y_1\sigma : z_0 + z_1\sigma]\Big) \in E_{\pi_1(a),\pi_1(b)}(A_1) \times E_{\pi_2(a),\pi_2(b)}(A_2)$, then $[x_0+x_1\varepsilon+(x_0+x_1+x_2)\varepsilon^2 :\ y_0+y_1\varepsilon+(y_0+y_1+y_2)\varepsilon^2 :\ z_0+z_1\varepsilon+(z_0+z_1+z_2)\varepsilon^2]$ is an antecedent of $\Big([x_2 : y_2 : z_2],\ [x_0 + x_1\sigma : y_0 + y_1\sigma : z_0 + z_1\sigma]\Big)$. Thereby, $\tilde{\pi}$ is surjective.

(iii) Let $[X : Y : Z] = [x_0 + x_1\varepsilon + x_2\varepsilon^2 : y_0 + y_1\varepsilon + y_2\varepsilon^2 : z_0 + z_1\varepsilon + z_2\varepsilon^2]$, and $[X' : Y' : Z'] = [x'_0 + x'_1\varepsilon + x'_2\varepsilon^2 : y'_0 + y'_1\varepsilon + y'_2\varepsilon^2 : z'_0 + z'_1\varepsilon + z'_2\varepsilon^2]$ two elements of $E_{a,b}(A)$ such that

$$\tilde{\pi}([X : Y : Z]) = \tilde{\pi}([X' : Y' : Z'])$$

Then:

$$\Big([x_0 + x_1 + x_2 : y_0 + y_1 + y_2 : z_0 + z_1 + z_2],\ [x_0 + x_1\sigma : y_0 + y_1\sigma : z_0 + z_1\sigma]\Big) =$$
$$\Big([x'_0 + x'_1 + x'_2 : y'_0 + y'_1 + y'_2 : z'_0 + z'_1 + z'_2],\ [x'_0 + x'_1\sigma : y'_0 + y'_1\sigma : z'_0 + z'_1\sigma]\Big)$$

$\Longleftrightarrow \exists\, \alpha \in A_1^*$ and $\beta \in A_2^*$ such that;

$$\begin{aligned}
x'_0 + x'_1 + x'_2 &= \alpha(x_0 + x_1 + x_2)\\
y'_0 + y'_1 + y'_2 &= \alpha(y_0 + y_1 + y_2)\\
z'_0 + z'_1 + z'_2 &= \alpha(z_0 + z_1 + z_2)\\
x'_0 + x'_1\sigma &= \beta(x_0 + x_1\sigma) \Longleftrightarrow \varphi_2^{-1}(x'_0 + x'_1\sigma) = \varphi_2^{-1}(\beta(x_0 + x_1\sigma))\\
y'_0 + y'_1\sigma &= \beta(y_0 + y_1\sigma) \Longleftrightarrow \varphi_2^{-1}(y'_0 + y'_1\sigma) = \varphi_2^{-1}(\beta(y_0 + y_1\sigma))\\
z'_0 + z'_1\sigma &= \beta(z_0 + z_1\sigma) \Longleftrightarrow \varphi_2^{-1}(z'_0 + z'_1\sigma) = \varphi_2^{-1}(\beta(z_0 + z_1\sigma))
\end{aligned}$$

which is equivalent to:

$$\begin{aligned}
x'_2 &= \alpha(x_0 + x_1 + x_2) + (x'_0 + x'_1)\\
y'_2 &= \alpha(y_0 + y_1 + y_2) + (y'_0 + y'_1)\\
z'_2 &= \alpha(z_0 + z_1 + z_2) + (z'_0 + z'_1)\\
x'_0 + x'_1\varepsilon + (x'_0 + x'_1)\varepsilon^2 &= \beta(x_0 + x_1\varepsilon) + \beta(x_0 + x_1)\varepsilon^2\\
y'_0 + y'_1\varepsilon + (y'_0 + y'_1)\varepsilon^2 &= \beta(y_0 + y_1\varepsilon) + \beta(y_0 + y_1)\varepsilon^2\\
z'_0 + z'_1\varepsilon + (z'_0 + z'_1)\varepsilon^2 &= \beta(z_0 + z_1\varepsilon) + \beta(z_0 + z_1)\varepsilon^2
\end{aligned}$$

so, as $\{1, \varepsilon, \varepsilon^2\}$ is the basis of the ring A as a vector space over $\mathbb{F}_q$, then we have:

$$\begin{aligned}
x'_0 &= \beta x_0\\
x'_1 &= \beta x_1\\
(x'_0 + x'_1) &= \beta(x_0 + x_1)
\end{aligned}$$

Thereby, $X' = \beta(x_0 + x_1\varepsilon) + \alpha(x_0 + x_1 + x_2)\varepsilon^2 + \beta(x_0 + x_1)\varepsilon^2$. This gives that, $X' = (\beta + (\alpha + \beta)\varepsilon^2) \cdot X$, and with the same technique, we find:

$$\begin{aligned}
Y' &= (\beta + (\alpha + \beta)\varepsilon^2) \cdot Y\\
Z' &= (\beta + (\alpha + \beta)\varepsilon^2) \cdot Z.
\end{aligned}$$

Since $\beta + (\alpha + \beta)\varepsilon^2$ is invertible in A, then $[X' : Y' : Z'] = [X : Y : Z]$, so $\tilde{\pi}$ is injective. Finally, we show easily that:

$$\tilde{\pi} \circ \tilde{\pi}^{-1} = Id_{E_{\pi_1(a),\pi_1(b)}(A_1) \times E_{\pi_2(a),\pi_2(b)}(A_2)}$$

and $\tilde{\pi}^{-1} \circ \tilde{\pi} = Id_{E_{a,b}(A)}$. □

Remark 3.1 *Let P, $Q \in E_{a,b}(A)$, we have:*

$$P = Q \Longleftrightarrow \tilde{\pi}(P) = \tilde{\pi}(Q) \Longleftrightarrow \tilde{\pi_1}(P) = \tilde{\pi_1}(Q) \text{ and } \tilde{\pi_2}(P) = \tilde{\pi_2}(Q).$$

4. Classification of the elements of elliptic curve $E_{a,b}(A)$

Firstly, we describe the different expressions of the points of this curve. After, we will regroup them as a theorem.
Let $[X:Y:Z]=[x_0+x_1\varepsilon+x_2\varepsilon^2 : y_0+y_1\varepsilon+y_2\varepsilon^2 : z_0+z_1\varepsilon+z_2\varepsilon^2]\in E_{a,b}(A)$.

1) If Z is invertible in the ring A, then $[X:Y:Z]=[Z^{-1}X : Z^{-1}Y : 1]$, so it is of the form $[X:Y:1]$.

2) If Z is no invertible, then Z is either of the form $Z=z_1\varepsilon+z_2\varepsilon^2$ or of the form $Z=z_0+z_1\varepsilon+(z_0+z_1)\varepsilon^2$, we have:

   (a) If $Z=z_1\varepsilon+z_2\varepsilon^2$, where $(z_1,z_2)\in\mathbb{F}_{2^d}^2$, then $\tilde{\pi}_2([X:Y:Z])=[x_0+x_1\sigma : y_0+y_1\sigma : z_1\sigma]\in E_{\pi_2(a),\pi_2(b)}(A_2)$, and since $E_{\pi_2(a),\pi_2(b)}(A_2)=\{[X:Y:1] \mid X;Y\in A_2 : Y^2+XY=X^3+\pi_2(a)X^2+\pi_2(b)\}\cup\{[x\sigma:1:0] \mid x\in\mathbb{F}_{2^d}\}$; see [15] then $z_1=0$, $x_0=0$ and $y_0\neq 0$ in $\mathbb{F}_{2^d}$, hence $[X:Y:Z]=[x_1\varepsilon+x_2\varepsilon^2 : y_0+y_1\varepsilon+y_2\varepsilon^2 : z_2\varepsilon^2]$. Further, since $\tilde{\pi}_1([X:Y:Z])=[x_1+x_2 : y_0+y_1+y_2 : z_2]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$. Then, there are two subcases of $y_0+y_1+y_2\in\mathbb{F}_{2^d}$:
      - If $y_0+y_1+y_2\neq 0$, then $y_0+y_1\varepsilon+y_2\varepsilon^2$ is invertible in A, so $[X:Y:Z]$ is of the form $[x\varepsilon+x'\varepsilon^2:1:z\varepsilon^2]$, where $x,x',z\in\mathbb{F}_{2^d}$.
      - If $y_0+y_1+y_2=0$ *ie* : $y_2=y_0+y_1\ mod(2)$ then $y_0+y_1\varepsilon+y_2\varepsilon^2=y_0+y_1\varepsilon+(y_0+y_1)\varepsilon^2$ is no invertible in A, so we have $[X:Y:Z]=[x_1\varepsilon+x_2\varepsilon^2 : y_0+y_1\varepsilon+(y_0+y_1)\varepsilon^2 : z_2\varepsilon^2]$, where $[x_1+x_2:0:z_2]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$, so in this case $z_2\in\mathbb{F}_{2^d}^*$.

   (b) If $Z=z_0+z_1\varepsilon+(z_0+z_1)\varepsilon^2$, where $(z_0,z_1)\in\mathbb{F}_{2^d}^2$, then $\tilde{\pi}_1([X:Y:Z])=[x_0+x_1+x_2 : y_0+y_1+y_2 : 0]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$ so $x_0+x_1+x_2=0$, and $y_0+y_1+y_2\neq 0$, hence $[X:Y:Z]=[x_0+x_1\varepsilon+(x_0+x_1)\varepsilon^2 : y_0+y_1\varepsilon+y_2\varepsilon^2 : z_0+z_1\varepsilon+(z_0+z_1)\varepsilon^2]$, so we have two sub-cases of $y_0\in\mathbb{F}_{2^d}$:
      - If $y_0\neq 0$, then $y_0+y_1\varepsilon+y_2\varepsilon^2$ is invertible in A, hence $[X:Y:Z]=[x+x'\varepsilon+(x+x')\varepsilon^2 : 1:z+z'\varepsilon+(z+z')\varepsilon^2]$, where $[x+x'\sigma:1:z+z'\sigma]\in E_{\pi_2(a),\pi_2(b)}(A_2)$.
      - If $y_0=0$, then $Y=y_1\varepsilon+y_2\varepsilon^2$ is not invertible in A, so we have $[X:Y:Z]=[x_0+x_1\varepsilon+(x_0+x_1)\varepsilon^2 : y_1\varepsilon+y_2\varepsilon^2 : z_0+z_1\varepsilon+(z_0+z_1)\varepsilon^2]$, where $[x_0+x_1\sigma : y_1\sigma : z_0+z_1\sigma]\in E_{\pi_2(a),\pi_2(b)}(A_2)$, then it is necessary that $z_0\neq 0$, and $[X:Y:Z]=[x+x'\varepsilon+(x+x')\varepsilon^2 : y\varepsilon+y'\varepsilon^2 : 1+z\varepsilon+(1+z)\varepsilon^2]$, where $y+y'\neq 0$, and $[x+x'\sigma : y\sigma : 1+z\varepsilon]\in E_{\pi_2(a),\pi_2(b)}(A_2)$.

From the previous description, we have the following theorem:

Theorem 4.1 *The element of the elliptic curve $E_{a,b}(A)$ has one of these forms:*

1) $[x\varepsilon+x'\varepsilon^2:1:z\varepsilon^2]$, *where* $[x+x':1:z]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$ *such that* $x,x',z\in\mathbb{F}_{2^d}$.

2) $[x\varepsilon+x'\varepsilon^2 : y+y'\varepsilon+(y+y')\varepsilon^2 : z\varepsilon^2]$, *where* $y\neq 0$ *and* $[x+x':0:z]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$. *In this case* $z\in\mathbb{F}_{2^d}^*$.

3) $[x+x'\varepsilon+(x+x')\varepsilon^2:1:z+z'\varepsilon+(z+z')\varepsilon^2]$, *where* $[x+x'\sigma:1:z+z'\sigma]\in E_{\pi_2(a),\pi_2(b)}(A_2)$.

4) $[x+x'\varepsilon+(x+x')\varepsilon^2 : y\varepsilon+y'\varepsilon^2 : 1+z\varepsilon+(1+z)\varepsilon^2]$, *where* $y+y'\neq 0$, *and* $[x+x'\sigma : y\sigma : 1+z\varepsilon]\in E_{\pi_2(a),\pi_2(b)}(A_2)$.

5) $[X:Y:1]$, *where* $X,Y\in A$ *verify the equation:*

$$Y^2+XY=X^3+aX^2+b.$$

5. The group law over the elliptic curve $E_{a,b}(A)$

In this section, we come to construct a group law over the set $E_{a,b}(A)$, using the bijection of theorem 3.2. We know that $E_{\pi_i(a),\pi_i(b)}(A_i)$, is an abelien group for all $i\in\{1,2\}$, and has $[0:1:0]$ as a neutral element, and the opposite of $[X:Y:Z]$ is $[X:X+Y:Z]$. Moreover, if $P=[X_1:Y_1:Z_1], Q=[X_2:Y_2:Z_2]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$ are two points, we have $P+Q=[X_3:Y_3:Z_3]$, which is computed by the following theorem.

Theorem 5.1 *i) If $P = Q$, then:*

$$\begin{aligned}
X_3 &= X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + X_2^2Y_1^2 + X_1X_2^2Y_1 + \pi_1(a)X_1^2X_2Y_2 + \pi_1(a)X_1X_2^2Y_1 + \\
&\quad \pi_1(a)X_1^2X_2^2 + \pi_1(b)X_1Y_1Z_2^2 + \pi_1(b)X_2Y_2Z_1^2 + \pi_1(b)X_1^2Z_2^2 + \pi_1(b)Y_1Z_2^2Z_1 + \\
&\quad \pi_1(b)Y_2Z_1^2Z_2 + \pi_1(b)X_1Z_2^2Z_1.\\
Y_3 &= Y_1^2Y_2^2 + X_2Y_1^2Y_2 + \pi_1(a)X_1X_2^2Y_1 + \pi_1(a)^2X_1^2X_2^2 + \pi_1(b)X_1^2X_2Z_2 + \\
&\quad \pi_1(b)X_1X_2^2Z_1 + \pi_1(b)X_1Y_1Z_2^2 + \pi_1(b)X_1^2Z_2^2 + \pi_1(ab)X_2^2Z_1^2 + \pi_1(ab)X_1^2Z_2^2 + \\
&\quad \pi_1(b)Y_1Z_1Z_2^2 + \pi_1(b)X_1Z_1Z_2^2 + \pi_1(ab)X_1Z_1Z_2^2 + \pi_1(ab)X_2Z_1^2Z_2 + \\
&\quad \pi_1(b)^2Z_1^2Z_2^2.\\
Z_3 &= X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2X_2^2 + Y_1^2X_2Z_2 + X_1^2Y_2Z_2 + \\
&\quad \pi_1(a)X_1^2Y_2Z_2 + \pi_1(a)X_2^2Y_1Z_1 + X_1^2X_2Z_2 + \pi_1(a)X_1X_2^2Z_1 + \\
&\quad \pi_1(b)Y_1Z_1Z_2^2 + \pi_1(b)Y_2Z_1^2Z_2 + \pi_1(b)X_1Z_1Z_2^2.
\end{aligned}$$

ii) If $P \neq Q$, then:

$$\begin{aligned}
X_3 &= X_1Y_2^2Z_1 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + \pi_1(a)X_1^2X_2Z_2 + \\
&\quad \pi_1(a)X_1X_2^2Z_1 + \pi_1(b)X_1Z_1Z_2^2 + \pi_1(b)X_2Z_1^2Z_2.\\
Y_3 &= X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + \\
&\quad \pi_1(a)X_1^2Y_2Z_2 + \pi_1(a)X_2^2Y_1Z_1 + \pi_1(a)X_1^2X_2Z_2 + \pi_1(a)X_1X_2^2Z_1 + \\
&\quad \pi_1(b)Y_1Z_1Z_2^2 + \pi_1(b)Y_2Z_1^2Z_2 + \pi_1(b)X_1Z_1Z_2^2 + \pi_1(b)X_2Z_1^2Z_2.\\
Z_3 &= X_1^2X_2Z_2 + X_1X_2^2Z_1 + Y_1^2Z_2^2 + Y_2^2Z_1^2 + X_1Y_1Z_2^2 + X_2Y_2Z_1^2 + \pi_1(a)X_1^2Z_2^2 + \\
&\quad \pi_1(a)X_2^2Z_1^2.
\end{aligned}$$

Proof: See [3,19]. □

And for $P = [X_1 : Y_1 : Z_1], Q = [X_2 : Y_2 : Z_2] \in E_{\pi_2(a),\pi_2(b)}(A_2)$, considering the projection:

$$\pi_0 : A_2 \longrightarrow \mathbb{F}_{2^d}$$

$$x + x'\sigma \longmapsto x$$

We have $P + Q = [X_3 : Y_3 : Z_3]$, which is computed by the following theorem.

Theorem 5.2 *i) If $[\pi_0(X_1) : \pi_0(Y_1) : \pi_0(Z_1)] = [\pi_0(X_2) : \pi_0(Y_2) : \pi_0(Z_2)]$, then:*

$$\begin{aligned}
X_3 &= X_1Y_1Y_2^2 + X_2Y_1^2Y_2 + X_2^2Y_1^2 + X_1X_2^2Y_1 + \pi_2(a)X_1^2X_2Y_2 + \pi_2(a)X_1X_2^2Y_1 + \\
&\quad \pi_2(a)X_1^2X_2^2 + \pi_2(b)X_1Y_1Z_2^2 + \pi_2(b)X_2Y_2Z_1^2 + \pi_2(b)X_1^2Z_2^2 + \pi_2(b)Y_1Z_2^2Z_1 + \\
&\quad \pi_2(b)Y_2Z_1^2Z_2 + \pi_2(b)X_1Z_2^2Z_1.\\
Y_3 &= Y_1^2Y_2^2 + X_2Y_1^2Y_2 + \pi_2(a)X_1X_2^2Y_1 + \pi_2(a)^2X_1^2X_2^2 + \pi_2(b)X_1^2X_2Z_2 + \\
&\quad \pi_2(b)X_1X_2^2Z_1 + \pi_2(b)X_1Y_1Z_2^2 + \pi_2(b)X_1^2Z_2^2 + \pi_2(ab)X_2^2Z_1^2 + \pi_2(ab)X_1^2Z_2^2 + \\
&\quad \pi_2(b)Y_1Z_1Z_2^2 + \pi_2(b)X_1Z_1Z_2^2 + \pi_2(ab)X_1Z_1Z_2^2 + \pi_2(ab)X_2Z_1^2Z_2 + \\
&\quad \pi_2(b)^2Z_1^2Z_2^2.\\
Z_3 &= X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2X_2^2 + Y_1^2X_2Z_2 + X_1^2Y_2Z_2 + \\
&\quad \pi_2(a)X_1^2Y_2Z_2 + \pi_2(a)X_2^2Y_1Z_1 + X_1^2X_2Z_2 + \pi_2(a)X_1X_2^2Z_1 + \\
&\quad \pi_2(b)Y_1Z_1Z_2^2 + \pi_2(b)Y_2Z_1^2Z_2 + \pi_2(b)X_1Z_1Z_2^2.
\end{aligned}$$

ii) If $[\pi_0(X_1):\pi_0(Y_1):\pi_0(Z_1)] \neq [\pi_0(X_2):\pi_0(Y_2):\pi_0(Z_2)]$, *then:*

$$\begin{aligned}
X_3 &= X_1Y_2^2Z_1 + X_2Y_1^2Z_2 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + \pi_2(a)X_1^2X_2Z_2 + \\
&\quad \pi_2(a)X_1X_2^2Z_1 + \pi_2(b)X_1Z_1Z_2^2 + \pi_2(b)X_2Z_1^2Z_2.\\
Y_3 &= X_1^2X_2Y_2 + X_1X_2^2Y_1 + Y_1^2Y_2Z_2 + Y_1Y_2^2Z_1 + X_1^2Y_2Z_2 + X_2^2Y_1Z_1 + \\
&\quad \pi_2(a)X_1^2Y_2Z_2 + \pi_2(a)X_2^2Y_1Z_1 + \pi_2(a)X_1^2X_2Z_2 + \pi_2(a)X_1X_2^2Z_1 + \\
&\quad \pi_2(b)Y_1Z_1Z_2^2 + \pi_2(b)Y_2Z_1^2Z_2 + \pi_2(b)X_1Z_1Z_2^2 + \pi_2(b)X_2Z_1^2Z_2.\\
Z_3 &= X_1^2X_2Z_2 + X_1X_2^2Z_1 + Y_1^2Z_2^2 + Y_2^2Z_1^2 + X_1Y_1Z_2^2 + X_2Y_2Z_1^2 + \pi_2(a)X_1^2Z_2^2 + \\
&\quad \pi_2(a)X_2^2Z_1^2.
\end{aligned}$$

Proof: See [3,15]. □

Definition 5.1 *Let* $P, Q \in E_{a,b}(A)$. *We define a law over* $E_{a,b}(A)$ *as an addition law by* $P+Q = \tilde{\pi}^{-1}(\tilde{\pi}(P)+\tilde{\pi}(Q))$.

Remark 5.1 *With this definition, we have* $\tilde{\pi}(P+Q) = \tilde{\pi}(P)+\tilde{\pi}(Q)$.

Proposition 5.1 *The set* $(E_{a,b}(A), +)$ *is a commutative group with* $[0:1:0]$ *as neutral element, and the opposite of the point* $[X:Y:Z]$ *is* $[X:X+Y:Z]$.

Proof: By using the fact that $\tilde{\pi}$ is a bijection, and satisfies $\tilde{\pi}(P+Q) = \tilde{\pi}(P)+\tilde{\pi}(Q)$, it is easy to show that $(E_{a,b}(A), +)$ is a commutative group, and its neutral element is $[0:1:0]$; because $\Big(E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d}) \times E_{\pi_2(a),\pi_2(b)}(A_2), +\Big)$ is an abelian group, with neutral element is $\Big([0:1:0], [0:1:0]\Big)$.
Let $[X:Y:Z] = [x_0+x_1\varepsilon+x_2\varepsilon^2 : y_0+y_1\varepsilon+y_2\varepsilon^2 : z_0+z_1\varepsilon+z_2\varepsilon^2] \in E_{a,b}(A)$, with the same technique as [19] we have:

$$\begin{aligned}
[X:Y:Z]+[X:X+Y:Z] &= \tilde{\pi}^{-1}(\tilde{\pi}([X:Y:Z])+\tilde{\pi}([X:X+Y:Z]))\\
&= \tilde{\pi}^{-1}\Big([0:1:0],[0:1:0]\Big)\\
&= [0:1:0]
\end{aligned}$$

□

Corollary 5.1 *For this law, the bijection* $\tilde{\pi}$ *is an isomorphism of groups.*

Proposition 5.2 *Let* $P=[X_1:Y_1:Z_1]$, $Q=[X_2:Y_2:Z_2]$, *and* $P+Q=[X_3:Y_3:Z_3]$ *in* $E_{a,b}(A)$. *Notice that:*

$$[\pi_1(X_1):\pi_1(Y_1):\pi_1(Z_1)]+[\pi_1(X_2):\pi_1(Y_2):\pi_1(Z_2)] = [X_3^{(1)}:Y_3^{(1)}:Z_3^{(1)}],$$

and $[\pi_2(X_1):\pi_2(Y_1):\pi_2(Z_1)]+[\pi_2(X_2):\pi_2(Y_2):\pi_2(Z_2)] = [x_0^{(2)}+x_1^{(2)}\sigma : y_0^{(2)}+y_1^{(2)}\sigma : z_0^{(2)}+z_1^{(2)}\sigma]$. *Then,* $P+Q=[X_3:Y_3:Z_3]$ *is given by:*

$$\begin{aligned}
X_3 &= x_0^{(2)}+x_1^{(2)}\varepsilon+\Big(X_3^{(1)}+(x_0^{(2)}+x_1^{(2)})\Big)\varepsilon^2\\
Y_3 &= y_0^{(2)}+y_1^{(2)}\varepsilon+\Big(Y_3^{(1)}+(y_0^{(2)}+y_1^{(2)})\Big)\varepsilon^2\\
Z_3 &= z_0^{(2)}+z_1^{(2)}\varepsilon+\Big(Z_3^{(1)}+(z_0^{(2)}+z_1^{(2)})\Big)\varepsilon^2
\end{aligned}$$

Proof: By using the definition $P+Q=\tilde{\pi}^{-1}\Big(\tilde{\pi}(P)+\tilde{\pi}(Q)\Big)$, we have:

$$P+Q=\tilde{\pi}^{-1}\Big([X_3^{(1)}:Y_3^{(1)}:Z_3^{(1)}],\,[x_0^{(2)}+x_1^{(2)}\sigma:y_0^{(2)}+y_1^{(2)}\sigma:z_0^{(2)}+z_1^{(2)}\sigma]\Big),$$

So, with the expression of $\tilde{\pi}^{-1}$, we will get:

$$\begin{aligned} X_3 &= x_0^{(2)}+x_1^{(2)}\varepsilon+\Big(X_3^{(1)}+(x_0^{(2)}+x_1^{(2)})\Big)\varepsilon^2\\ Y_3 &= y_0^{(2)}+y_1^{(2)}\varepsilon+\Big(Y_3^{(1)}+(y_0^{(2)}+y_1^{(2)})\Big)\varepsilon^2\\ Z_3 &= z_0^{(2)}+z_1^{(2)}\varepsilon+\Big(Z_3^{(1)}+(z_0^{(2)}+z_1^{(2)})\Big)\varepsilon^2 \end{aligned}$$

□

Corollary 5.2 *The cardinal of the elliptic curve $E_{a,b}(A)$ is not a prime number, is equal to the cardinal of $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})\times E_{\pi_2(a),\pi_2(b)}(A_2)$.*

Proof: By applying the bijection of theorem 3.2, we have $|E_{a,b}(A)|=|E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})|\times|E_{\pi_2(a),\pi_2(b)}(A_2)|$. We also know that $|E_{\pi_2(a),\pi_2(b)}(A_2)| = |E_{a_0,b_0}(\mathbb{F}_{2^d})|\times|\mathbb{F}_{2^d}|$, where $a_0=\pi_0(\pi_2(a))$, $b_0=\pi_0(\pi_2(b))$; see [13,20]. On the other hand, since every element of $\mathbb{F}_{2^d}$ is a square, and one can easily verifies that the points $[0:\sqrt{\pi_1(b)}:1]\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$ and $[0:\sqrt{b_0}:1]\in E_{a_0,b_0}(\mathbb{F}_{2^d})$, then the both cardinal $|E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})|$ and $|E_{a_0,b_0}(\mathbb{F}_{2^d})|$ are not equal to 1. Hence, the both $|E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})|$ and $|E_{\pi_2(a),\pi_2(b)}(A_2)|$ are not equal to 1, which gives the result. □

We finish this work with these important remarks, which allows us to perform such cryptosystem protocol.

- By using the theorems 4.1, 5.1, 5.2 and proposition 5.2, we can give the explicit formulas of the addition law in $(E_{a,b}(A),+)$ for every case of the theorem 4.1.
- The cardinal of $E_{a,b}(A)$ is not a prime number, but contains more elements.
- The discrete logarithm problem in $E_{a,b}(A)$ is equivalent to the discrete logarithm problem in $E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})\times E_{\pi_2(a),\pi_2(b)}(A_2)$.
- Let $P\in E_{a,b}(A)$ such that $\tilde{\pi}(P)=(P_1,P_2)$, where $P_1\in E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})$ and $P_2\in E_{\pi_2(a),\pi_2(b)}(A_2)$. If l_1 is the order of P_1 and l_2 is the order of P_2, then P is of order $l=ppcm(l_1,l_2)$.

6. Conclusion

In this work, we have proved an explicit formula of the ismorphism $E_{a,b}(A)\simeq E_{\pi_1(a),\pi_1(b)}(\mathbb{F}_{2^d})\times E_{\pi_2(a),\pi_2(b)}(A_2)$, and its reciprocal like; $\tilde{\pi}^{-1}$ such that $\tilde{\pi}^{-1}\Big([x_2:y_2:z_2],\,[x_0+x_1\sigma:y_0+y_1\sigma:z_0+z_1\sigma]\Big)=[x_0+x_1\varepsilon+(x_0+x_1+x_2)\varepsilon^2:\,y_0+y_1\varepsilon+(y_0+y_1+y_2)\varepsilon^2:\,z_0+z_1\varepsilon+(z_0+z_1+z_2)\varepsilon^2]$, which allow us to define a group law algorithm on the elliptic curve $E_{a,b}(A)$, and the classification of its elements. The implementation of the algorithms can be done by using a Maple program.

Acknowledgments

The author would like to thank the Faculty of Science and Technology Al-Hoceima, the editorial and reviewing committee for their helpful suggestions.

References

1. Atiyah M. F. and Macdonald I. G, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Co, Reading Massachusetts-Menlo Park, California, 1969.
2. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic curves over the ring R^**, Boletim da Sociedade Paranaense de Matematica (3s), v.38, 3(2020), 193-201.
3. Abdelhakim Chillali and Lhoussain El Fadil, *Elliptic Curve over a Local Finite Ring R_n*, In: Open Access books Built by scientists, for scientists, pp: 1-25, Book Citation Index, Web of Science, (2020).
4. Chillali.A, *Identification Methods Over $\mathbf{E}^n_{a,b}$*, Recent Researches in Applied and Computational Mathematics, ISBN: 978-1-61804-002-2, 133-138, 2011.
5. Chillali.A, *Cryptography over elliptic curve of the ring $\mathbb{F}_q[\varepsilon], \varepsilon^4 = 0$*, World Academy of Science, Engineering and Technology, 5, 06-21, 2011.
6. Hartshorne J, *Algebraic Geometry*, Springer-Verlag, GTM 52, 1977.
7. Hassib M.H, Chillali A, Elomary M.A, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, 9, 276-287, 2015.
8. N.Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation, 48, 203-209, 1987.
9. Lawrence C. Washington, *Elliptic curves Number Theory and Cryptography*, Discrete Mathematics and Its Applications, Chapman and Hall/CRC, 2003.
10. H.W.Lenstra Jr, *Elliptic curves and number theoretic algorithms*, Proceedings of the International Congress of Mathematicians, Berkeley-California, USA-AMS, 99-120, 1986.
11. Sebastià Martin, *Corbes Elliptiques modul N i Applicacions Criptografiques*, PhD thesis, Departament de Matemàtica Aplicada i Telemática, Universitat Politècnica de Catalunya, 1998.
12. C.E.Shannon, *A Mathematical Theory of communication*, Bell system technical journal, 27, 623-656, 1948.
13. J.H.Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 1994.
14. J.H.Silverman, *the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 1986.
15. A.Tadmori, A.Chillali, M.Ziane, *The Binary Operations Calculus in $\mathbf{E}_{a,b,c}$*, International Journal of Mathematical Models and Methods in Applied Sciences, 9, 171-175, 2015.
16. A.Tadmori, A.Chillali, M. Ziane, *Normal Forme of the Elliptic Curve over the Finite Ring*, Journal of Mathematics and System Science, 4, 194-196, 2014.
17. A.Tadmori, A.Chillali, M. Ziane, *Cryptography over the elliptic curve Ea,b(A3)*, Journal of Taibah University for Science, 9, 326-331, 2015.
18. A.Tadmori, A.Chillali, M.Ziane, *Elliptic Curve over Ring $\mathbf{A_4} = \mathbb{F}_{2^d}[\varepsilon]; \varepsilon^4 = 0$*, Applied Mathematical Sciences, 9, 1721 - 1733, 2015.
19. A.Tadmori, A.Chillali, M.Ziane, *Elliptic curve over a nonlocal ring $\mathbb{F}_{2^d}[\varepsilon]; \varepsilon^2 = \varepsilon$*, Asian-European Journal of Mathematics, Vol.15, No.3(2022) 2250046 (22 pages), World Scientific Publishing Company, DOI: 10.1142/S1793557122500462.
20. Abdelhamid Tadmori, Abdelhakim Chillali, M'hamed Ziane, *Elliptic curve over SPIR of characteristic two*, Proceedings of the 2013 International Conference on Applied Mathematics and Computational Methods, AMCM 2013.
21. M.Virat, *Courbes elliptiques sur un anneau et applications cryptographiques*, Thèse pour obtenir le titre de Docteur en Sciences de l'université de Nice-Sophia Antipolis, 2009.

Abdelhamid Tadmori,

Department of Mathematics and Informatics,

Faculty of Science and Technology, Al Hoceima,

University Abdelmalek Essaadi,

Morocco.

E-mail address: atadmori@yahoo.fr or: a.tadmori@uae.ac.ma