International Mathematical Forum, Vol. 9, 2014, no. 24, 1191 - 1196
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/imf.2014.4599

# Elliptic Curves over the Ring $\mathbb{F}_{3^d}[\varepsilon]$, $\varepsilon^4 = 0$

**My Hachem HASSIB**

Moulay Ismail University
FST Errachidia Morocco

**Abdelhakim CHILLALI**

USMBA
FP
Taza, Morocco

**Mohamed Abdou ELOMARY**

Moulay Ismail University
FST Errachidia
Morocco



**Abstract**

In [2] we defined the j-invariant of the elliptic curve over the ring $A_n = \mathbb{F}_{3^d}[\varepsilon], \varepsilon^n = 0$, in [5] we studied the elliptic curve over the ring $A_2$, and in [6] we defined the elliptic curve over the ring $A_3$. In this work we will study the elliptic curve over the ring $A_4$; and we will prove that: $0 \longrightarrow \ker \widetilde{\pi} \stackrel{i}{\longrightarrow} E^4_{a,b} \stackrel{\widetilde{\pi}}{\longrightarrow} E^1_{a_0,b_0} \longrightarrow 0$ is a short exact sequence, and is split when 3 doesn't divide $\#E^1_{a_0,b_0}$ and, deduce some cryptographic results.

**Mathematics Subject Classification:** 94A60, 11T71, 14H52,

**Keywords:** Elliptic Curves, Finite Ring, Cryptography, Short Exact Sequence.

# 1 Introduction

Let $d$ be a positive integer. We consider the quotient ring $A_n = \mathbb{F}_{3^d}[X]/(X^n)$, where $\mathbb{F}_{3^d}$ is the finite field of order $3^d$, and $n \geqslant 1$. Then the ring $A_n$ is identified to the ring $\mathbb{F}_{3^d}[\varepsilon], \varepsilon^n = 0$. So we have:

$$A_n = \{\sum_{i=0}^{n-1} x_i\varepsilon^i \mid (x_i)_{0\leqslant i\leqslant n-1} \in \mathbb{F}_{3^d}\} \text{ [2], [3].}$$

Similar as in [3] we have the following lemmas:

**Lemma 1.1.** *Let* $X = \sum_{i=0}^{n-1} x_i\varepsilon^i$. *$X$ is invertible in $A_n$ if and only if $x_0 \neq 0$.*

**Lemma 1.2.** *$A_n$ is a local ring, it's maximal ideal is $\mathfrak{M}_n = (\varepsilon)$.*

**Lemma 1.3.** *$A_n$ is a vector space over $\mathbb{F}_{3^d}$ and have $(1, \varepsilon, \ldots, \varepsilon^{n-1})$ as basis.*

**Remark 1.4.** *We denote by $\pi$ the canonical projection defined by:*

$$\begin{array}{ccc} A_n & \xrightarrow{\pi} & \mathbb{F}_{3^d} \\ \sum_{i=0}^{n-1} x_i\varepsilon^i & \longmapsto & x_0 \end{array}$$

# 2 Elliptic curves over the ring $A_4$

**Definition 2.1.** *We consider the elliptic curve over the ring $A_4$ which is given by the equation: $Y^2Z = X^3 + aX^2Z + bZ^3$, where $a, b \in A_4$ and $-a^3b$ is invertible in $A_4$, and denoted by $E^4_{a,b}$ . So we have:*

$$E^4_{a,b} = \{[X : Y : Z] \in \mathbb{P}_2(A_4) \mid Y^2Z = X^3 + aX^2Z + bZ^3\}$$

## 2.1 Classification of elements of $E^4_{a,b}$

**Proposition 2.2.** *Every element in $E^4_{a,b}$ is of the form $[X : Y : 1]$ (where $X$ or $Y \in A_4 \setminus \mathfrak{M}_4$), or $[X : 1 : Z]$ where $X, Z \in \mathfrak{M}_4$ and we write:*
$E^4_{a,b} = \{[X : Y : 1] \mid Y^2 = X^3 + aX^2 + b, \text{and } X \text{ or } Y \notin \mathfrak{M}_4\} \cup \{[X : 1 : Z] \mid Z = X^3 + aX^2Z + bZ^3, \text{and } X, Z \in \mathfrak{M}_4\}$.

***Proof.*** Let $[X : Y : Z] \in E^4_{a,b}$ , where $X, Y$ and $Z \in A_4$.

- If $Z$ is **invertible** then $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1] \sim [X : Y : 1]$. Suppose that $X, Y \in \mathfrak{M}_4$; since $Y^2 = X^3 + aX^2 + b$, then $b \in \mathfrak{M}_4$, which is absurd.

- If $Z$ is **non invertible** then $Z \in \mathfrak{M}_4$, then we will have two cases for $Y$:
  - $Y$ **invertible** then $[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}] \sim [X : 1 : Z]$.
  - $Y$ **non invertible**: we have $Y$ and $Z \in \mathfrak{M}_4$ and since $X^3 = Z(Y^2 - aX^2 - bZ^2) \in \mathfrak{M}_4$, then $X \in \mathfrak{M}_4$, we deduce that $[X : Y : Z]$ is not a projective point since $(X, Y, Z)$ is not a primitive triple [7, p.104-105].

So the proposition is proved. □

**Lemma 2.3.** *Let* $[X : 1 : Z] \in E^4_{a,b}$*, where* $X, Z \in (\varepsilon)$.
*If* $X = x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$*, then* $[X : 1 : Z] = [X : 1 : x_1^3\varepsilon^3]$

***Proof.*** Since $[X : 1 : Z] \in E^4_{a,b}$, $X = x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3$ and $Z = z_1\varepsilon + z_2\varepsilon^2 + z_3\varepsilon^3$ then, $X^3 = x_1^3\varepsilon^3$ , $aX^2Z = a_0x_1^2z_1\varepsilon^3$ and $bZ^3 = b_0z_1^3\varepsilon^3$, thus $z_1 = 0$, $z_2 = 0$ and $z_3 = x_1^3$. □

## 2.2 The group law over $E^4_{a,b}$

After classifying the elements of $E^4_{a,b}$ , we will define the group law over it. We consider firstly the mapping $\widetilde{\pi}$:

$$\begin{array}{ccc} E^4_{a,b} & \xrightarrow{\widetilde{\pi}} & E^1_{\pi(a),\pi(b)} \\ [X : Y : Z] & \longmapsto & [\pi(X) : \pi(Y) : \pi(Z)] \end{array}$$

**Theorem 2.4.** *Let* $P = [X_1 : Y_1 : Z_1]$ *and* $Q = [X_2 : Y_2 : Z_2]$ *two points in* $E^4_{a,b}$ *, and* $P + Q = [X_3 : Y_3 : Z_3]$.

- *If* $\widetilde{\pi}(P) = \widetilde{\pi}(Q)$ *then :*
  $X_3 = Y_1Y_2^2X_1 + {Y_1}^2Y_2X_2 + 2a{X_1}^2X_2Y_2 + 2aX_1{X_2}^2Y_1 + 2Z_1{Z_2}^2abY_1 + 2{Z_1}^2Z_2abY_2.$
  $Y_3 = {Y_1}^2{Y_2}^2 + 2a^2{X_1}^2{X_2}^2 + a^2bX_1Z_1{Z_2}^2 + a^2bX_2{Z_1}^2Z_2.$
  $Z_3 = aX_1X_2(Y_1Z_2 + Y_2Z_1) + a(X_1Y_2 + X_2Y_1)(X_1Z_2 + X_2Z_1) + Y_1Y_2(Y_1Z_2 + Y_2Z_1).$

- *If* $\widetilde{\pi}(P) \neq \widetilde{\pi}(Q)$ *then :*
  $X_3 = 2X_1Y_2Y_1Z_2 + X_1{Y_2}^2Z_1 + 2X_2{Y_1}^2Z_2 + X_2Y_1Y_2Z_1 + 2a{X_1}^2X_2Z_2 + aX_1{X_2}^2Z_1.$
  $Y_3 = 2{Y_1}^2Y_2Z_2 + Y_1{Y_2}^2Z_1 + 2aX_1X_2Y_1Z_2 + aX_1X_2Y_2Z_1 + 2a{X_1}^2Y_2Z_2 + a{X_2}^2Y_1Z_1.$
  $Z_3 = 2{Y_1}^2{Z_2}^2 + {Y_2}^2{Z_1}^2 + a{X_1}^2{Z_2}^2 + 2a{X_2}^2{Z_1}^2.$

***Proof.*** By using the explicit formulas in [1, p. 236—238] we prove the theorem. □

**Lemma 2.5.** $\widetilde{\pi}$ *is a surjective homomorphism of groups.*

***Proof.*** The proof of this lemma is similar to the one of lemma 5 in [4, p.13]. □

## 2.3 The $\widetilde{\pi}$ homomorphism and results

**Definition 2.6.** *We define on the set* ${\mathbb{F}_{3^d}}^3$ *the law* $*$ *by:*
$(x_1, x_2, x_3) * (x'_1, x'_2, x'_3) = \big(x_1 + x'_1, x_2 + x'_2, x_3 + x'_3 + 2a_0(x_1^2 x'_1 + x_1 {x'_1}^2)\big)$

**Lemma 2.7.** $({\mathbb{F}_{3^d}}^3, *)$ *is a group with* $(0, 0, 0)$ *as unity, and the opposite of* $(x_1, x_2, x_3)$ *is* $\big(2x_1, 2x_2, 2x_3 + a_0(x_1^2 x'_1 + x_1 {x'_1}^2)\big)$.

**Lemma 2.8.** *Let* $[X : 1 : Z]$ *and* $[X' : 1 : Z']$ *in* $E^4_{a,b}$*, where* $X, Z, X'$ *and* $Z'$ *are as in lemma 2.3, we have:*
$[X : 1 : Z] + [X' : 1 : Z'] = [X + X' + 2a(X^2 X' + X X'^2) : 1 : Z + Z']$.

***Proof.*** Since $Z = {x_1}^3 \varepsilon^3$, $Z' = {x'_1}^3 \varepsilon^3$ then $Z^2 = Z'^2 = ZZ' = 0$; and since $X, X' \in (\varepsilon)$ so, $X^2 X'^2 = 0$. Then, we conclude from theorem 2.4 . □

**Lemma 2.9.** *The subset* $G_4 = \{[X : 1 : Z] \mid X \text{ and } Y \in \mathfrak{M}_4\}$ *is a subgroup of* $E^4_{a,b}$*, and every element in* $G_4$*, not unity, is of order* $9$.

***Proof.*** Let $P = [X : 1 : Z] \in G_4$, we denote $2P = P + P$ and $(n + 1)P = nP + P$ for all $n \geqslant 2$. We have from lemma 2.8 : $2P = [2X(1 + 2aX^2) : 1 : 2Z]$, $3P = [aX^3 : 1 : 0]$ and $9P = [0 : 1 : 0]$, then the order of $G_4$ divides 9 and is not 3 since $3P \neq [0 : 1 : 0]$ when $X \neq 0$. So, the lemma is proved. □

**Lemma 2.10.** *The mapping*

$$\begin{array}{ccc} ({\mathbb{F}_{3^d}}^3, *) & \xrightarrow{\theta} & (E^4_{a,b}, +) \\ (x_1, x_2, x_3) & \longmapsto & [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3] \end{array}$$

*is an injective homomorphism of groups.*

***Proof.*** From lemma 2.3 we deduce that $\theta$ is well defined and the image of zero is zero, and from lemma 2.8 we prove that $\theta$ is an homomorphism of groups. Now let $(x_1, x_2, x_3) \in {\mathbb{F}_{3^d}}^3$ such that $\theta(x_1, x_2, x_3) = [0 : 1 : 0]$. Then, $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3] = [0 : 1 : 0]$; therefore $x_1 = x_2 = x_3 = 0$. This prove that $\theta$ is injective. □

**Lemma 2.11.** $\ker \widetilde{\pi} = Im\theta$.

***Proof.*** Let $[x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3] \in Im\theta$ then,
$\widetilde{\pi}\ ([x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3]) = [0 : 1 : 0]$ and so, $\ker \widetilde{\pi} \supseteq Im\theta$.
Conversely let $[X : Y : Z] \in \ker \widetilde{\pi}$, then $[x_0, y_0, z_0] = [0 : 1 : 0]$, so $Y$ is invertible, and from proposition 2.2: $X, Z \in \mathfrak{M}_4$ so, $[X : Y : Z] \sim [X : 1 : Z]$; and from lemma 2.3 $[X : Y : Z] \sim [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3] \in Im\theta$.
So $\ker \widetilde{\pi} \subseteq Im\theta$. Finally: $\ker \widetilde{\pi} = Im\theta$. □

From lemmas 2.5, 2.10 and 2.11, we deduce the following corollary.

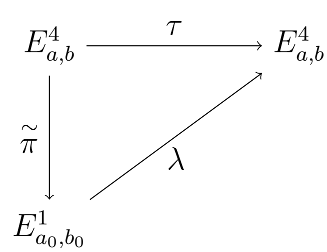
**Corollary 2.12.** *The sequence:* $0 \longrightarrow \ker(\widetilde{\pi}) \xrightarrow{\mathfrak{i}} E^4_{a,b} \xrightarrow{\widetilde{\pi}} E^1_{a_0,b_0} \longrightarrow 0$ *is exact, where* $\mathfrak{i}$ *is the canonical injection.*

**Theorem 2.13.** *Let* $N = \#E^1_{a_0,b_0}$*. If* 3 *doesn't divide* $N$*, then the short exact sequence:* $0 \longrightarrow \ker(\widetilde{\pi}) \xrightarrow{\mathfrak{i}} E^4_{a,b} \xrightarrow{\widetilde{\pi}} E^1_{a_0,b_0} \longrightarrow 0$*, is split.*

***Proof.*** 3 doesn't divide $N$, then 9 doesn't divide $N$ therefore there exists an integer $N'$ such that $NN' = 1 \bmod 9$so, $\exists m$ integer such that $1 - NN' = 9m$.
Now let $\tau$ the homomorphism defined by :

$$\begin{array}{ccc} E^4_{a,b} & \xrightarrow{\tau} & E^4_{a,b} \\ P & \longmapsto & (1 - NN')P \end{array}$$

There exists an unique morphism $\lambda$, such that the following diagram commutes:




Effectively: let $P \in \ker(\widetilde{\pi}) = \theta(\mathbb{F}^3_{3^d})$, then: $\exists (x_1, x_2, x_3) \in \mathbb{F}_{3^d}{}^3$ such that: $P = [x_1\varepsilon + x_2\varepsilon^2 + x_3\varepsilon^3 : 1 : x_1^3\varepsilon^3]$. We have from lemma 2.9: $(1 - NN')P = 9mP = [0 : 1 : 0]$, then $P \in \ker(\tau)$. It follows that $\ker(\widetilde{\pi}) \subseteq \ker(\tau)$, this prove the above assertion .
Now let us prove that $\widetilde{\pi} \circ \lambda = id_{E^1_{a_0,b_0}}$ and take $P_0 \in E^1_{a_0,b_0}$; since $\widetilde{\pi}$ is surjective then $\exists P \in E^4_{a,b}$ such that $\widetilde{\pi}\ (P) = P_0$. We have $\lambda(P_0) = (1 - NN')P = P - NN'P$ and, $NP_0 = [0 : 1 : 0]$ (since $N = \#E^1_{a_0,b_0}$), then $N\ \widetilde{\pi}\ (P) = [0 : 1 : 0]$ and $\widetilde{\pi}\ (NP) = [0 : 1 : 0]$ implies that $NP \in \ker(\widetilde{\pi})$ and so, $NN'P \in \ker(\widetilde{\pi})$; therefore $\widetilde{\pi}\ (NN'P) = [0 : 1 : 0]$ and, since $\lambda(P_0) = (1 - NN')P = P - NN'P$ then: $\widetilde{\pi} \circ \lambda(P_0) = \widetilde{\pi}\ (P) - [0 : 1 : 0] = P_0$ and so: $\widetilde{\pi} \circ \lambda = id_{E^1_{a_0,b_0}}$.
Finally the sequence is split. □

**Corollary 2.14.** *If* 3 *doesn't divide* $\#E^1_{a_0,b_0}$ *then,* $E^4_{a,b} \cong {\mathbb{F}_{3^d}}^3 \oplus E^1_{a_0,b_0}$.

***Proof.*** From the theorem 2.13 the sequence is split then, $E^4_{a,b} \cong \ker(\widetilde{\pi}) \oplus E^1_{a_0,b_0}$, and since $\ker(\widetilde{\pi}) \cong Im\theta \cong {\mathbb{F}_{3^d}}^3$ therefore, the corollary is proved. □

## 2.4 Cryptographic application

From the corollary 2.14 we deduce the following results:

- $\#E^4_{a,b} = 27^d.N$
- The Discrete Logarithm on the elliptic curve $E^4_{a,b}$ is equivalent to the one on $E^1_{a_0,b_0}$.
- If the Discrete Logarithm on $E^4_{a,b}$ is trivial then we can break it on the elliptic curve $E^1_{a_0,b_0}$ with trivial attacks.

# References


[1] W. Bosma and H.W. Lenstra, *Complete System of Two Addition Laws for Elliptic Curves*, Journal of Number Theory, (1995).

[2] A. Chillali, *The j-invariant over* $E^n_{3^d}$, Int. J. Open Problems Compt. Math.,vol.**5**, No. 4, December 2012, ISSN 1998-6262; Copyright ICSRS Publication, 106 - 111.

[3] A. Chillali, *Elliptic Curves of the Ring* $\mathbb{F}_q[\varepsilon]$ , $\varepsilon^n = 0$, International Mathematical Forum, (2011).

[4] M. H. Hassib and A. Chillali, *The* $\widetilde{\pi}$ *homomorphism of* $\mathrm{E}_{a,b}(\mathbb{F}_{3^d}[\varepsilon])$, AIP publishing, vol.**1557** , 12 - 14 (2013).

[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 , ISBN 978-1-61804-130-2, (2012), 71 - 73.

[6] M. H. Hassib, A. Chillali and Mohamed Abdou ELOMARY, *Special Ideal Ring* $\mathrm{A}_3$ *and Cryptography*, 978-1-4799-0324-5/13/$31.00 ©2013 IEEE.

[7] Lenstra, H.W, *Elliptic Curves and Number-Theoretic Algorithms*, Processing of the International Congress of Mathematicians,Berkely,California,USA, (1986).


**Received: May 19, 2014**