Finite Ring Of Characteristic 2 And Cryptography

Abdelhakim CHILLALI
FST, USMBA, FES
MORROCO
chil2007@voila.fr

Abstract— **In [1] and [2] we defined the elliptic curve over the ring $F_{3^d}[\varepsilon], \varepsilon^2 = 0$. In this work we will give some properties of the elliptic curve over the special ideal ring of characteristic 2 and an application in cryptography. Our future work will focus on the study of the general case of these rings, which seem to be beneficial and interesting in cryptography, specially the one based on the identity (IBE) [6], [7], [8]**.

Keywords— Elliptic curves; finite ring; characteristic 3; cryptography.

I. INTRODUCTION

Let d be a positive integer. We consider the quotient ring

II. THE RING

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

Lemma 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 2. A_n is a local ring, its maximal ideal is $M = (\varepsilon)$.

Lemma 3. A_n is a vector space over , and $(1, \varepsilon, \dots, \varepsilon^{n-1})$ is a basis of A_n.

Remark 1. We denote $I_j = (\varepsilon^j)$, where $j = 1, \dots, n-1$. then: $(I_j)_{1 \le j \le n-1}$ is a decreasing sequence of ideals of A_n and $I_1 = M$.

$$M = I_1 \supseteq I_2 \dots \supseteq I_{n-1}$$

III. ELLIPTIC CURVES OVER THE RING

We consider the elliptic curve over the ring A_3 which is given by the equation: where $a, b \in A_3$ and $-a^3 b$ is invertible in A_3.

A. Notations

We denote the elliptic curve over A_3 by , and we write:

B. Classification of elements of $E_{a,b}^3$

Proposition 1. Every element of $E_{a,b}^3$ is of the form $[X : Y : 1]$ or $[x\varepsilon + y\varepsilon^2 : 1 : 0]$, where $x \in F_{3^d}$ and $y \in F_{3^d}$. We write:

Proof: Let , where X, Y and $Z \in A_3$.

We have two cases for Z :

- Z **invertible**: then $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1] \sim [X : Y : 1]$.
- Z **non invertible:** so $Z \in M$ (see lemma 1), then we have two cases for Y :

  - Y **invertible**:

$[X : Y : Z] = [XY^{-1} : 1 : ZY^{-1}] \sim [X : 1 : Z]$. Since $[X : 1 : Z] \in E_{a,b}^3$, then

$X^3 = Z(1 - aX^2 - bZ^2)$, so $X^3 \in M$.

But $X^3 = \sum_{i=0}^{2} x_i^3 \varepsilon^{3i} \in M$ implies that $x_0^3 = 0$, then $x_0 = 0$, this means that $X \in M$. So $X^3 = x_0^3 = 0$, we deduce that $Z = 0$ and $X = x\varepsilon + y\varepsilon^2$, where $x \in F_{3^d}$ and $y \in F_{3^d}$.

At last, $[X : Y : Z] \sim [x\varepsilon + y\varepsilon^2 : 1 : 0]$

  - Y **non invertible**:

We have Y and $Z \in M$, since:

$X^3 = Z(Y^2 - aX^2 - bZ^2) \in M$ then $x_0^3 = 0$ and so $X \in M$.

We deduce that $[X : Y : Z]$ isn't a projective point since (X, Y, Z) isn't a primitive triple.[5,p.104-105] ∎

We consider the canonical projection π defined by:

$\pi : \mathbb{F}_{3^d}[\varepsilon] \to \mathbb{F}_{3^d}$

$x_0 + x_1\varepsilon + x_2\varepsilon^2 \to x$

We define the mapping $\tilde{\pi}$ by :

$$E^3_{a,b} \overset{\tilde{\pi}}{\to} E^1_{\pi(a),\pi(b)}$$
$$[X : Y : Z] \to [\pi(X) : \pi(Y) : \pi(Z)]$$

theorem 1. Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in $E^3_{a,b}$, and $P + Q = [X_3 : Y_3 : Z_3]$.

- If $\tilde{\pi}(P) = \tilde{\pi}(Q)$ then :

- If $\tilde{\pi}(P) \neq \tilde{\pi}(Q)$ then :

Proof : By using the explicit formulas in W.Bosma and H.W. Lenstra's article **[4, p.236-238]** we prove the theorem. ■

C. The $\tilde{\pi}_3$ homomorphism

Theorem 2. *Let $X = \tilde{X} + x_2\varepsilon^2$, $Y = \tilde{Y} + y_2\varepsilon^2$, $Z = \tilde{Z} + z_2\varepsilon^2$, $a = \tilde{a} + a_2\varepsilon^2$ and $b = \tilde{b} + b_2\varepsilon^2$ are elements in A_3.*

If $[X : Y : Z] \in E^3_{a,b}$ then:

$$\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}^2\tilde{Z} + \tilde{b}\tilde{Z}^3 - [Ax_2 + By_2 + Cz_2 + D]\varepsilon^2$$

where $A = a_0 x_0 z_0$, $B = 2y_0 z_0$ $C = y_0^2 - a_0 x_0^2$ and $D = 2a_2 x_0^2 z_0 + 2b_2 z_0^3$

Proof : Since $[X : Y : Z] \in E^2_{a,b}$ then:

$Y^2 Z = X^3 + aX^2 Z + bZ^3$, so

$$\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}^2\tilde{Z} + \tilde{b}\tilde{Z}^3 +$$
$$[\tilde{a}(x_0^2 z_2 + 2x_0 x_2 z_0) + a_2 x_0^2 z_0]\varepsilon^2 + b_2 z_0^3\varepsilon^2$$

then

$$\tilde{Y}^2\tilde{Z} = \tilde{X}^3 + \tilde{a}\tilde{X}^2\tilde{Z} + \tilde{b}\tilde{Z}^3 + [(a_2 x_0^2 z_0 + b_2 z_0^3) +$$
$$(2a_0 x_0 z_0)x_2 - (2y_0 z_0)y_2 + (a_0 x_0^2 - y_0^2)z_2]\varepsilon^2$$

Then we deduce the theorem. ■

Definition 1. We define the map π_3 as follows:

$$A_3 \overset{\pi_3}{\to} A_2$$
$$\sum_{i=0}^{2} x_i\varepsilon^i \to \sum_{i=0}^{1} x_i\delta^i$$

where $\varepsilon^3 = 0$ and $\delta^2 = 0$.

Lemma 4. π_3 is a surjective morphism of rings.

We have the following lemma

Lemma 5. The map:

is a surjective homomorphism of groups.

Proof : Let $[X : Y : Z] \in E^3_{a,b}$.

- From theorem 2, $\tilde{\pi}_3$ is well defined.

Then, let $Q = [X : Y : Z] \in E^2_{\pi_3(a),\pi_3(b)}$, where $X = x_0 + x_1\delta$, $Y = y_0 + y_1\delta$ and $Z = z_0 + z_1\delta$.

We consider in $\mathbb{F}_{3^d}$, the equation:

(1)

where A, B, C and D are as in theorem 2.

Since A , B and C are partial derivatives of the function $F(X, Y, Z) = Y^2 Z - X^3 - a_0 X^2 Z - b_0 Z^3$ at the point (x_0, y_0, z_0), and since $[x_0 : y_0 : z_0] \in E^1_{a_0,b_0}$ (the elliptic curve over A_1 which is defined by the equation: $F(X, Y, Z) = 0$); then A , B and C can't be all null, so the equation (1) has at least a solution in $\mathbb{F}_{3^d}{}^3$ which we denote (x_2, y_2, z_2) ; then:

$$P = [x_0 + x_1\varepsilon + x_2\varepsilon^2 : y_0 + y_1\varepsilon + y_2\varepsilon^2 : z_0 + z_1\varepsilon + z_2\varepsilon^2] \text{ in } E^3_{a,b}$$

and $\tilde{\pi}_3(P) = Q$. So:

- $\tilde{\pi}_3$ is surjective.

■

Lemma 6. The mapping:

$$\mathbb{F}_{3^d} \overset{\theta_3}{\to} E^3_{a,b}$$
$$x \to [x\varepsilon^2 : 1 : 0]$$

is an injective morphism of groups.

Proof : We have from the subsection II-B:

$(\forall x \in \mathrm{F}_{3^d}):[x\varepsilon^2:1:0]\in E^3_{a,b}$

Then :

- θ_3 is well defined.

And since $[l\varepsilon^2:1:0]+[h\varepsilon^2:1:0]=[(l+h)\varepsilon^2:1:0]$ then :

- θ_3 is a morphism of groups.

$l \in \mathrm{F}_{3^d}$, we have: $\theta_3(l)=[0:1:0]$, which implies that $l=0$. ie,

- θ_3 is injective.

■

Corollary 1. $ker(\tilde{\pi}_3)=\theta_3(\mathrm{F}_{3^d})$

Proof : Let $[l\varepsilon^2:1:0]\in\theta_3(\mathrm{F}_{3^d})$, then

$\tilde{\pi}_3([l\varepsilon^2:1:0])=[0:1:0]$, so:

- $ker(\tilde{\pi}_3)\supseteq\theta_3(\mathrm{F}_{3^d})$.

Now let $[X:Y:Z]\in ker(\tilde{\pi}_3)$, then

$\tilde{\pi}_3([X:Y:Z])=[0:1:0]$; and by using the same notations as in theorem 2 we obtain:

$[\tilde{X}:\tilde{Y}:\tilde{Z}]=[0:1:0]$; then

$\tilde{X}=0$, $\tilde{Z}=0$, and $\tilde{Y}$ is invertible in A_2, so

$X=x_2\varepsilon^2$, $Z=z_2\varepsilon^2$ and Y is invertible in A_3; we deduce that:

$[X:Y:Z]\sim[x_2\varepsilon^2:1:z_2\varepsilon^2]\in E^3_{a,b}$,

this means: $z_2\varepsilon^2=0$, so

$[X:Y:Z]\sim[x_2\varepsilon^2:1:0]$. ie:

- $ker(\tilde{\pi}_k)\subseteq\theta_k(\mathrm{F}_{3^d})$.

We conclude that $ker(\tilde{\pi}_k)=\theta_k(\mathrm{F}_{3^d})$. ■

From corollary 1, we deduce the following corollary:

Corollary 2. The sequence :

is a short exact sequence which defines the group extension $E^3_{a,b}$ of $E^2_{\pi_3(a),\pi_3(b)}$ by $Ker(\tilde{\pi}_3)$, where i_3 is the canonical injection.

The last corollary allows us to calculate the cardinal of $E^3_{a,b}$ depending of the cardinals of $E^2_{\pi_3(a),\pi_3(b)}$ and $ker(\tilde{\pi}_3)$.

IV. CRYPTOGRAPHIC APPLICATION

Let $E^3_{a,b}$ an elliptic curve over A_3 and $P\in E^3_{a,b}$ of order l. We will use the subgroup $\langle P\rangle$ of $E^3_{a,b}$ to encrypt messages, and we denote $G=\langle P\rangle$.

A. Coding of elements of G

We will give a code to each element $Q=mP\in G$ where $m\in\{1,\ldots,l\}$ defined as it follows:

if $Q=[x_0+x_1\varepsilon+x_2\varepsilon^2:y_0+y_1\varepsilon+y_2\varepsilon^2:z_0]$ where $x_i,y_i\in\mathrm{F}_{3^d}$ for $i=0,1$ or 2 and $z_0=0$ or 1.

We set:

$x_i=c_{0i}+c_{1i}\alpha+\ldots+c_{(d-1)i}\alpha^{d-1}$

$y_i=f_{0i}+f_{1i}\alpha+\ldots+f_{(d-1)i}\alpha^{d-1}$

where α is primitive root of an irreducible polynomial of degree d over F_3, and $c_{ij},f_{ij}\in\mathrm{F}_3$.

Then we code Q as it follows:

- If $z_0=1$, then:

- If $z_0=0$, then:

Remark 2. The security of this encryption is based on the discrete logarithm problem.

B. Example

Let $a=(2+\alpha)+\varepsilon+\varepsilon^2$, $b=1+\alpha\varepsilon+2\varepsilon^2$ in A_3, so the elliptic curve $E^3_{a,b}$ has 1134 elements, and the elliptic curve $E^2_{\tilde{a},\tilde{b}}$ has 126.

Let $P=[1:2\alpha+\alpha\varepsilon:1]$ and $G=\langle P\rangle$.

G is a subgroup of order 42 of $E^2_{\tilde{a},\tilde{b}}$.

$(\forall Q\in G)(\exists m\in\{1,\ldots,42\}):Q=mP$

C. Encryption and decryption of messages

Let the following message:

"***jns3 rabat***"

Its encryption is:

1120000101001001000100000002
1020001020011221001011 00121
0100022000111210002010011 00
0000201001120100102200110 00
000201001001100100200 1

Let the following message:

2101000110001001000100000001
1220002000012101000220001 10
0200022200100010010020012 10
1000220001001100100200100 21
0020010012101000110001210 10
0022000100110010020011000 00
0201001122100202200101120 02
200001

Its decryption is:

"***end of the talk***"

Remark 2. With this application, we can encrypt and decrypt any message of any length.
This application was implemented by Maple.

V. CONCLUSION

In this work we defined the ring A_3, given its properties, and we used the elliptic curve defined on it to encrypt and decrypt a message.

We reveal that there is enormous tasks to do about this subject, we cite:

- A generalization to the case of the ring $A_n, n..3$.
- Create new Cryptosystems.
- Discrete logarithm attack.
- Cryptography over the elliptic curve defined over the ring $A_n, n..3$.

REFERENCES

[1] Abdelhakim *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 , www.i-csrs.org, pp. 106-111 (2012).

[2] M.H. Hassib and A. Chillali, *Example of cryptography over the ring* $\mathrm{F}_{3^d}[\varepsilon], \varepsilon^2 = 0$, Latest trends in Applied Informatics and Computing, p.71-73, ISBN 978-1-61804-130-2, (2012).

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

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

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

[6] Nicolas Meloni, Arithmétique pour la Cryptographie basée sur les Courbes Elliptiques, Thèse Doctorat
Université Montpellier II, FRANCE, (2007).

[7] D. Boneh and M. Franklin, *Identity based encryption from the Weill pairing*, Advanced in Cryptography- CRYPTO 2001, Springer-Verlag LNCS 2139, 213-229, (2001).

[8] Giray Komurcu and Erkay Savas, *An efficient Hardware Implementation of the Tate Pairing in Characteristic Tree*, Third International Conference on Systems, DOI 10.109/ICONS.2008.27, IEEE (2008).