Int. J. Open Problems Compt. Math., Vol. 6, No. 2, June 2013
ISSN 1998-6262;
www.i-csrs.org

Elliptic Curve Over Special Ideal Ring

Abdelhakim Chillali

Department of Mathematic and Computer, FST, Fez
chil2007@voila.fr

Abstract

The goal of this article is to study elliptic curves over the ring $F_q[\epsilon]$, with F_q a finite field of order q and with the relation $\epsilon^5 = 0$. The motivation for this work came from search for new groups with intractable (DLP) discrete logarithm problem is therefore of great importance. The observation groups where the discrete logarithm problem (DLP) is believed to be intractable have proved to be inestimable building blocks for cryptographic applications.

Keywords: *Elliptic curves over the ring, Public key cryptography, Finite field, Ring, Special ideal ring, The discrete logarithm problem...*

1 Introduction

Let p be an odd prime number and n be an integer such that $n \geq 1$. Consider the quotient ring $A_n = F_q[X]/(X^n)$, where F_q is the finite field of characteristic p and q elements. Then the ring A_n may be identified to the ring $F_q[\epsilon]$ where $\epsilon^n = 0$. In other word [1, 2, 3]

$$A_n = \left\{ \sum_{i=0}^{n-1} a_i \epsilon^i | \ \ (a_i)_{0 \leq i \leq n-1} \in F_q^n \right\}.$$

The following result is easy to prove:

Lemma 1.1 *Let $X = \sum_{i=0}^{n-1} x_i \epsilon^i$ and $Y = \sum_{i=0}^{n-1} y_i \epsilon^i$ be two elements of A_n. Then*

$$XY = \sum_{i=0}^{n-1} z_i \epsilon^i \ \ \texttt{where} \ \ z_j = \sum_{i=0}^{j} x_i y_{j-i}.$$

Remark 1.2 *Let* $Y = \sum_{i=0}^{n-1} y_i\epsilon^i$ *be the inverse of the element* $X = \sum_{i=0}^{n-1} x_i\epsilon^i$*. Then*

$$\begin{cases} y_0 = x_0^{-1} \\ y_j = -x_0^{-1}\sum_{i=0}^{j-1} y_i x_{j-i}, \quad \forall j > 0 \end{cases}$$

We consider the canonical projection π defined by:

$$\pi : \left| \begin{array}{ccc} A_n & \longrightarrow & F_q \\ \sum_{i=0}^{n-1} x_i\epsilon^i & \longmapsto & x_0 \end{array} \right.$$

Lemma 1.3 π *is a morphism of rings.*

Proof 1 *Let* $X = \sum_{i=0}^{n-1} x_i\epsilon^i$ *and* $Y = \sum_{i=0}^{n-1} y_i\epsilon^i$*, then*

$$X + Y = \sum_{i=0}^{n-1} (x_i + y_i)\epsilon^i$$

$$XY = \sum_{i=0}^{n-1} z_i\epsilon^i \;\; \texttt{where} \;\; z_j = \sum_{i=0}^{j} x_i y_{j-i}.$$

We have:

$$\pi(X + Y) = x_0 + y_0 = \pi(X) + \pi(Y)$$

$$\pi(XY) = z_0 = x_0 y_0 = \pi(X)\pi(Y).$$

So, π *is a morphism of rings.*

2 Elliptic Curve Over A

In this section we suppose $n = 5$*. An elliptic curve over ring* $A = A_5$ *is curve that is given by such Weierstrass equation:*

$$(\star) : Y^2Z = X^3 + aXZ^2 + bZ^3$$

where $a,\ b \in\ A$ *and* $4a^3 + 27b^2$ *is invertible in* A*. We denote by* $E_{a,b}$ *the elliptic curve over* A*. The set* $E_{a,b}$ *together with a special point* $\mathcal{O}$ *-called the point infinity-, a commutative binary operation denoted by* $+$*. It is well known that the binary operation* $+$ *endows the set* $E_{a,b}$ *with an abelian group with* $\mathcal{O}$ *as identity element.*

3 The main results

Lemma 3.1 *The mapping*

$$\pi_{a,b} : \left| \begin{array}{rcl} E_{a,b} & \longrightarrow & E_{\pi(a),\pi(b)} \\ [X:Y:Z] & \longmapsto & [\pi(X):\pi(Y):\pi(Z)] \end{array} \right.$$

is a surjective homomorphism of groups.

Proof 2 *Consider $[X1:Y1:Z1]$ and $[X2:Y2:Z2]$ in $E_{a,b}$.*
We have

$$\pi_{a,b}([X1:Y1:Z1]+[X2:Y2:Z2]) = \pi_{a,b}([X1:Y1:Z1])+\pi_{a,b}([X2:Y2:Z2]).$$

So, $\pi_{a,b}$ is a homomorphism of groups.
Let $[x_0:y_0:z_0]$ in $E_{\pi(a),\pi(b)}$, then

$$a = a_0 + a_1\epsilon + a_2\epsilon^2 + a_3\epsilon^3 + a_4\epsilon^4$$

$$b = b_0 + b_1\epsilon + b_2\epsilon^2 + b_3\epsilon^3 + b_4\epsilon^4$$

$$X = x_0 + x_1\epsilon + x_2\epsilon^2 + x_3\epsilon^3 + x_4\epsilon^4$$

$$Y = y_0 + y_1\epsilon + y_2\epsilon^2 + y_3\epsilon^3 + y_4\epsilon^4$$

$$Z = z_0 + z_1\epsilon + z_2\epsilon^2 + z_3\epsilon^3 + z_4\epsilon^4$$

If $[X:Y:Z]$ in $E_{a,b}$, then

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In order to simplify this last expression, we have

$$(1) : f_0 + f_1\epsilon + f_2\epsilon^2 + f_3\epsilon^3 + f_4\epsilon^4 = 0$$

where

$$f_0 = -y_0^2z_0 + b_0z_0^3 + a_0x_0z_0^2 + x_0^3$$

$$f_1 = (z_0^2a_0 + 3x_0^2)x_1 - 2y_0z_0y_1 + (-y_0^2 + 3b_0z_0^2 + 2a_0x_0z_0)z_1 + b_1z_0^3 + z_0^2a_1x_0$$

$$f_2 = (z_0^2a_0+3x_0^2)x_2 - 2z_0y_0y_2 + (-y_0^2+3b_0z_0^2+2a_0x_0z_0)z_2 + z_0^2a_1x_1 - 2y_0y_1z_1 - z_0y_1^2 + 3x_1^2x_0 + 3b_0z_1^2z_0 + 3b_1z_0^2z_1 + b_2z_0^3 + a_0x_0z_1^2 + 2z_0z_1a_0x_1 + 2z_0z_1a_1x_0 + z_0^2a_2x_0.$$

$$(1) \Leftrightarrow f_0 = 0, f_1 = 0, f_2 = 0, f_3 = 0 \ \textbf{and} \ f_4 = 0$$

$$f_0 = 0 \Leftrightarrow [x_0:y_0:z_0] \in E_{\pi(a),\pi(b)}$$

Coefficients $z_0^2a_0 + 3x_0^2$, $2z_0y_0$ and $-y_0^2 + 3b_0z_0^2 + 2a_0x_0z_0$ are partial derivative of a function $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^3$ at the point (x_0, y_0, z_0), can not be all three null.
We can then at last conclude that $[x_1:y_1:z_1]$, $[x_2:y_2:z_2]$, $[x_3:y_3:z_3]$ and $[x_4:y_4:z_4]$.
Finally, $\pi_{a,b}$ is a surjective homomorphism of groups.

Lemma 3.2 *The mapping*

$$\theta : \left| \begin{array}{rcl} F_q^4 & \longrightarrow & E_{a,b} \\ (l,k,h,s) & \longmapsto & [l\epsilon + k\epsilon^2 + h\epsilon^3 + s\epsilon^4 : 1 : l^3\epsilon^3 + 3l^2k\epsilon^4] \end{array} \right.$$

is a injective homomorphism of groups.

Proof 3 *Evidently, θ is injective.*
Every $[l\epsilon + k\epsilon^2 + h\epsilon^3 + s\epsilon^4 : 1 : l^3\epsilon^3 + 3l^2k\epsilon^4]$ satisfies the equation of $(\star)$.
We have:
$[l\epsilon+k\epsilon^2+h\epsilon^3+s\epsilon^4 : 1 : l^3\epsilon^3+3l^2k\epsilon^4]+[l'\epsilon+k'\epsilon^2+h'\epsilon^3+s'\epsilon^4 : 1 : l'^3\epsilon^3+3l'^2k'\epsilon^4] = [(l+l')\epsilon+(k+k')\epsilon^2+(h+h')\epsilon^3+(s+s')\epsilon^4 : 1 : (l+l')^3\epsilon^3+3(l+l')^2(k+k')\epsilon^4]$

Finally

$$\theta((l,k,h,s) + (l',k',h',s')) = \theta(l,k,h,s) + \theta(l',k',h',s'),$$

and we concluded θ is injective homomorphism of groups.

Definition 3.3 *We definite G by $G = Ker(\pi_{a,b})$.*

Corollary 3.4 *The set $G = \theta(F_q^4)$.*

Proof 4 *Let*

$$[l\epsilon + k\epsilon^2 + h\epsilon^3 + s\epsilon^4 : 1 : l^3\epsilon^3 + 3l^2k\epsilon^4] \in \theta(F_q^4),$$

then

$$\pi_{a,b}([l\epsilon + k\epsilon^2 + h\epsilon^3 + s\epsilon^4 : 1 : l^3\epsilon^3 + 3l^2k\epsilon^4]) = [0:1:0],$$

we concluded

$$[l\epsilon + k\epsilon^2 + h\epsilon^3 + s\epsilon^4 : 1 : l^3\epsilon^3 + 3l^2k\epsilon^4] \in G.$$

Let

$$P = [X : Y : Z] \in G,$$

then

$$\pi_{a,b}(P) = [0:1:0].$$

We set

$$X = x_1\epsilon + x_2\epsilon^2 + x_3\epsilon^3 + x_4\epsilon^4,$$
$$Y = 1 + y_1\epsilon + y_2\epsilon^2 + y_3\epsilon^3 + y_4\epsilon^4,$$
$$Z = z_1\epsilon + z_2\epsilon^2 + z_3\epsilon^3 + z_4\epsilon^4,$$

and

$$Y^{-1} = 1 + s_1\epsilon + s_2\epsilon^2 + s_3\epsilon^3 + s_4\epsilon^4.$$

So,

$$\begin{array}{rcl} P & = & [Y^{-1}X : 1 : Y^{-1}Z] \\ & = & [x_1\epsilon + x'_2\epsilon^2 + x'_3\epsilon^3 + x'_4\epsilon^4 : 1 : z_1\epsilon + z'_2\epsilon^2 + z'_3\epsilon^3 + z'_4\epsilon^4]. \end{array}$$

We have

$$P \in E_{a,b},$$

thus

$$z_1 = 0, z'_2 = 0, z'_3 = x_1^3 \text{ and } z'_4 = 3x_1^2x'_2.$$

So,

$$P \in \theta(F_q^4).$$

Finally,

$$G = \theta(F_q^4).$$

We deduce easily the following corollaries.

Corollary 3.5 *The group G is an elementary abelian p-group, called group at infinity of $E_{a,b}$.*

Corollary 3.6 *The sequence*

$$0 \to G \xrightarrow{j} E_{a,b} \xrightarrow{\pi_{a,b}} E_{\pi(a),\pi(b)} \to 0$$

be a short exact sequence defining the group extension $E_{a,b}$ of $E_{\pi(a),\pi(b)}$ by G.

4 Open Problem

In this section you should present an open problems.

- *The cyclic subgroups of these curves.*
- *The attack on the discrete logarithm.*
- *Other crypto systems, more particular signature systems can be built From these curves and the study of these could allow to get stronger.*
- *Generic Groups.*
- *Study elliptic curves over the ring $F_q[\epsilon]$, with F_q a finite field of order q and with the relation $\epsilon^n = 0$; $n > 5$.*

ACKNOWLEDGEMENTS. *I would thank Professor M. E. Charkani for his helpful comments and suggestions.*

References

[1] *A. Chillali, "Ellipic cuvre over ring"*, International Mathematical Forum, *Vol. 6, no . 31, (2011), pp.1501-1505.*

[2] *A. Chillali, "Cryptography Over Elliptic Curve Of The Ring $F_q[\epsilon], \epsilon^4 = 0$"*, World Academy of Science, Engineering and Technology 78 2011*, (2011), pp.847-850.*

[3] *M. Virat,* Courbe elliptique sur un anneau et applications cryptographiques*, Thése Docteur en Sciences, Nice-Sophia Antipolis, (2009).*