The Fundamental Mappings

Over Group $E_n^{a,b}$

Chillali Abdelhakim

FST DE FEZ
Chil2015@yahoo.fr

Abstract. In this work we study the fundamental mappings of group $E_n^{a,b}$[5], group of an elliptic curve defined over ring $A_n = \mathbb{F}_q[\varepsilon];\ \varepsilon^n = 0$, that is given by an homogeneous equation of the form $Y^2Z = X^3 + aXZ^2 + bZ^3$ where $a, b \in A_n$ and $4a^3 + 27b^2$ is invertible in A_n.

Keywords: Elliptic Curves; Cryptography; Generic Group; Finite Field.

1 Introduction:

Groups where the discrete logarithm problem (DLP) is believed to be intractable have proved to be inestimable building blocks for cryptographic applications. They are at the heart of numerous protocols such as key agreements, public-key cryptosystems, digital signatures, identification schemes [2, 3], publicly verifiable secret shaings, hash functions and bit commitments. The search for new groups with intractable DLP is therefore of great importance.

Let p be an odd prime number and n be an integer such that $n \geq 1$. Consider the quotient ring $A_n = {}^{\mathbb{F}_q[X]}\big/_{(X^n)}$ where $\mathbb{F}_q$ is the finite field of order q and characteristic p. Then $A_n = \left\{\sum_{i=0}^{n-1} a_i\, \varepsilon^i \middle| (a_i)_{0 \leq i \leq n-1} \in \mathbb{F}_q^n\right\}$, where $\boldsymbol{\varepsilon^n = 0}$. [1, 5]

Notation 1.1 We denote the canonical projections

$$\pi_k : \left| \begin{array}{c} A_k \longrightarrow A_{k-1} \\ \displaystyle\sum_{i=0}^{k-1} a_i \varepsilon^i \mapsto \sum_{i=0}^{k-2} a_i \rho^i \ ,\rho^{k-1} \end{array} \right.$$

$$k^{\pi} : \left| \begin{array}{c} A_k \longrightarrow A_1 \\ \displaystyle\sum_{i=0}^{k-1} a_i \varepsilon^i \mapsto a_0 \end{array} \right.$$

An elliptic curve over a ring A_n is a curve that is given by an equation of the form:

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \qquad (*)$$

adfa, p. 1, 2011.

where $a, b \in \ A_n$ and $4a^3 + 27b^2$ is invertible in A_n.

We denote by $E_n^{\boldsymbol{a,b}}$ the elliptic curve over A_n.

The set $E_n^{\boldsymbol{a,b}}$ is an abelian group. Its identity element is a special point O called the point at infinity. [1, 4, 5]

Notation 1.2 We denote

- $$n_\theta : \left| \begin{array}{c} \mathbb{F}_q^{n-1} \longrightarrow E_n^{\boldsymbol{a,b}} \\ (x_1, .., x_{n-1}) \mapsto [\sum_{i=1}^{n-1} x_i \varepsilon^i : 1 : Z] \end{array} \right.$$

- $n_G = n_\theta(\mathbb{F}_q^{n-1})$.[1]

2 The Fundamental Mappings Over $E_n^{\boldsymbol{a,b}}$:

Let $N = \# \ E_1^{n^{\pi(a)}, n^{\pi(b)}}$, we assume that p does not divide N.

Lemma2.1 Let $P \in E_n^{a,b}$, then $NP = [0:1:0]$ *if and only if* $P \in E_1^{n^{\pi(a)}, n^{\pi(b)}}$.

Proof:

Let $P \in E_1^{n^{\pi(a)}, n^{\pi(b)}}$, then $NP = [0:1:0]$.

Let $P = [x_0 + X : y_0 + Y : z_0 + Z] \in E_n^{a,b}$ and $Q = [x_0 : y_0 : z_0] \in E_1^{n^{\pi(a)}, n^{\pi(b)}}$.

If $NP = [0:1:0]$ then $N(P - Q) = [0:1:0]$.

Thus, $P - Q = n_\theta(l_1, l_2, .., l_{n-1})$. [1]

In deduces that $Nl_i \equiv 0 \ [p], i = 1, 2, \dots, n-1$,

or $gcd(N, p) = 1$, therefore $l_i = 0$ *and* $P = Q$.

■

Lemma2.2 Let $P \in E_n^{a,b}$, then $pNP = [0:1:0]$.

Proof:

We have $\forall P \in E_n^{a,b}, NP \in n_G$. [1]

Thus, $pNP = [0:1:0]$.

■

Lemma2.3 Let p does not divide N, then there exists a unique morphism

$$v_n : E_1^{n^{\pi(a)}, n^{\pi(b)}} \to E_n^{a,b}$$

making the following diagram (d) is commutative.

$$\begin{tikzcd}
E_n^{a,b} \arrow[r, "{[p]}"] \arrow[d, "\pi_n"'] \arrow[dr, phantom, "(d)"] & E_n^{a,b} \\
E^{n^{\pi(a)},n^{\pi(b)}} \arrow[ur, "v_n"'] &
\end{tikzcd}$$

Proof:

Let $P \in k_G$. Then $pP = [0:1:0]$.

Thus $n_G \subset \ker([p])$.

Hence, there exists a unique morphism

$$v_n : E_1^{n^{\pi(a)},n^{\pi(b)}} \to E_n^{a,b}$$

making the diagram (d) following commutative.

■

Theorem2.4 Let p does not divide N, then there exists a unique morphism

$$s_n : E_1^{n^{\pi(a)},n^{\pi(b)}} \to E_n^{a,b}$$

such as $\pi_n \circ s_n = id_{E_1^{n^{\pi(a)},n^{\pi(b)}}}$.

Proof:

Let $N' \in \mathbb{Z}$ such there exists $t \in \mathbb{Z}$ checking $1 - N'N = tp$.

Thus, $[1 - NN'] = [t] \circ [p]$.

According to lemma2.3, there exists a unique morphism

$$s_n : E_1^{n^{\pi(a)},n^{\pi(b)}} \to E_n^{a,b}$$

making the following diagram (d') is commutative.

$$\begin{tikzcd}
E_n^{a,b} \arrow[r, "{[tp]}"] \arrow[d, "\pi_n"'] \arrow[dr, phantom, "\textbf{(d')}"] & E_n^{a,b} \\
E_1^{n^{\pi(a)},n^{\pi(b)}} \arrow[ur, "s_n"'] &
\end{tikzcd}$$

Let $P \in E_1^{n^{\pi(a)},n^{\pi(b)}}$, there exists $P' \in E_n^{a,b}$ such that $\pi_n(P') = P$.

Consequently,

$$\begin{aligned}
\pi_n \circ s_n(P) &= \pi_n \circ s_n \circ \pi_n(P') \\
&= \pi_n([1 - NN'](P')) \\
&= \pi_n([P' - NN'P']) \\
&= P - NN'P
\end{aligned}$$

$$= \quad P$$

■

Theorem2.5 Let p does not divide N, then $E_n^{a,b} \cong E_1^{n^{\pi(a)},n^{\pi(b)}} \times n_G$.
Proof:

The isomorphism

$$f_n : \left| \begin{array}{c} E_1^{n^{\pi(a)},n^{\pi(b)}} \times n_G \to E_n^{a,b} \\ (P,Q) \mapsto s_n(P) + Q \end{array} \right.$$

admits an inverse isomorphism

$$F_n : \left| \begin{array}{l} E_n^{a,b} \to E_1^{n^{\pi(a)},n^{\pi(b)}} \times n_G \\ P \mapsto (\pi_n(P), NN'P) \end{array} \right.$$

- Indeed,

$$\begin{aligned} f_n \circ F_n(P) &= f_n(\pi_n(P), NN'P) \\ &= s_n \circ \pi_n(P) + NN'P \\ &= [1 - NN']P + NN'P \\ &= P \end{aligned}$$

- Similarly,

$$\begin{aligned} F_n \circ f_n(P,Q) &= F_n(s_n(P) + Q) \\ &= (\pi_n(s_n(P) + Q), NN'(s_n(P) + Q)) \end{aligned}$$

We have

$$\begin{aligned} \pi_n(s_n(P) + Q) &= \pi_n(s_n(P)) + \pi_n(Q) \\ &= P + [0:1:0] \\ &= P \end{aligned}$$

$$\begin{aligned} NN'(s_n(P) + Q) &= NN'\big((s_n(P))\big) + NN'Q \\ &= NN'(1 - NN')P' + NN'Q \\ &= N'tpNP' + NN'Q \\ &= [0:1:0] + NN'Q \\ &= NN'Q \end{aligned}$$

As $pQ = [0:1:0]$, we have

$$\begin{aligned} NN'Q &= (1 - tp)Q \\ &= Q - tpQ \\ &= Q \end{aligned}$$

We concluded, $F_n \circ f_n(P,Q) = (P,Q)$.

■

Corollary2.6 Let p does not divide N, then $E_n^{a,b} \cong E_1^{n^{\pi(a)},n^{\pi(b)}} \times \mathbb{F}_q^{n-1}$.
Proof:
We have $n_G \cong \mathbb{F}_q^{n-1}$. [1]

■

Corollary2.7 Let p does not divide N, then

$$E_n^{a,b} \quad \cong \quad C_N \times \mathbb{F}_q^{n-1}\ ;\ C_N\ is\ cyclic$$

$$or$$

$$E_n^{a,b} \quad \cong \quad \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \mathbb{F}_q^{n-1};\ \ n_2|n_1 \wedge p - 1$$

Proof:

We have

$$E_1^{n^{\pi(a)},n^{\pi(b)}} \quad \cong \quad C_N\ ;\ C_N\ is\ cyclic$$

$$or$$

$$E_1^{n^{\pi(a)},n^{\pi(b)}} \quad \cong \quad \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \frac{\mathbb{Z}}{n_2\mathbb{Z}}\ ;\ \ n_2|n_1 \wedge p - 1$$

■

Corollary2.8 Let p does not divide N, then

$$(\sqrt{q} - 1)^2 q^{n-1} \leq \# E_n^{a,b} \leq (\sqrt{q} + 1)^2 q^{n-1}$$

Proof:

Consequently Hasse's theorem [4 p127], we have $\left| q + 1 - \# E_1^{n^{\pi(a)},n^{\pi(b)}} \right| \leq 2\sqrt{q}$.

Thus,

$$(\sqrt{q} - 1)^2 q^{n-1} \leq \# E_n^{a,b} \leq (\sqrt{q} + 1)^2 q^{n-1}$$

■

References

1. A. Chillali "Ellipic cuvre over ring $\mathbb{F}_q[\varepsilon];\ \varepsilon^n = 0$ " International Mathematical Forum, Vol. 6, no . 31, 1501-1505, 2011.
2. A. Chillali, "Identification methods over $E_n^{a,b}$", In Proceedings of the 2011 international conference on Applied computational mathematics (ICACM'11), Vladimir Vasek, Yuriy Shmaliy, Denis Trcek, Nobuhiko P. Kobayashi, and Ryszard S. Choras (Eds.). World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, Wisconsin, USA, 133-138.2011.
3. A. Chillali, "Cryptography Over Elliptic Curve Of The Ring $\mathbb{F}_q[\varepsilon];\ \varepsilon^4 = 0$", World Academy of Science, Engineering and Technology 78 2011, pages 847-850, 2011.
4. Koblitz N, " Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics," Volume3. Springer, ISSN:1431-1550, 1999.
5. M. Virat, "Courbe elliptique sur un anneau et applications cryptographiques," Thèse Docteur en Sciences, Nice-Sophia Antipolis 2009.