El Gamal Cryptosystem on a Montgomery Curves Over Non Local Ring

[1]MOHA BEN TALEB ELHAMAM, [1]ABDELALI GRINI, [2]ABDELHAKIM CHILLALI,
[1]LHOUSSAIN EL FADIL

Department of Mathematics
[1]Sidi Mohamed Ben Abdellah University, Faculty of Science Dhar El Mahraz
[2]Sidi Mohamed Ben Abdellah University, FP, LSI, Taza
Atlas, Fez, postcode 1796, Fez, Morocco
MOROCCO

Abstract: Let $\mathbb{F}_q$ be the finite field of q elements, where q is a prime power. In this paper, we study the Montgomery curves over the ring $\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle}$, denoted by $M_{A,B}(\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle})$; $(A,B) \in (\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle})^2$.
Using the Montgomery equation, we define the Montgomery curves $M_{A,B}(\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle})$ and we give a bijection between this curve and product of two Montgomery curves defined on $\mathbb{F}_q$. Furthermore, we study the addition law of Montgomery curves over the ring $\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle}$. We close this paper by introducing a public key cryptosystem which is a variant of the ElGamal cryptosystem on a Montgomery curves over the same ring.

Key-Words: Montgomery curves, Finite ring, Cryptography, ElGamal.

Received: May 10, 2021. Revised: January 13, 2022. Accepted: February 8, 2022. Published: March 2, 2022.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of order $q = p^n$ where n is a positive integer and p is a prime number. The ring $\frac{\mathbb{F}_q[X]}{\langle X^2-X\rangle}$ can be identified to the finite ring $\mathbb{F}_q[e],\ e^2 = e$. The objective of this article is the search for new groups of points of a Montgomery curve on a finite ring, for use in cryptography. In [10], Montgomery introduced a new elliptic curve model what became known as Montgomery curves and the Montgomery scale as way to speed up Lenstra's elliptic-curve factorization method [8].
Boulbot et al. study the arithmetic of the ring $\mathbb{F}_q[e]$, in particular they show that this ring is not a local [2]. In section 3, we define the Montgomery curves $M_{A,B}(\mathbb{F}_q[e])$ over this ring, we study Montgomery equation which allows us to define two Montgomery curves: $M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)$ and $M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$. In the next of this section, we classify the elements of $M_{A,B}(\mathbb{F}_q[e])$ and we give a bijection between the two sets: $M_{A,B}(\mathbb{F}_q[e])$ and $M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) \times M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$, where π_0 and π_1 are two surjective morphisms of rings defined by:

$$\begin{array}{cccc} \pi_0 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e & \mapsto & x_0 \end{array}$$

and

$$\begin{array}{cccc} \pi_1 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e & \mapsto & x_0 + x_1. \end{array}$$

We study the addition law of Montgomery curves over the ring $\mathbb{F}_q[e]$. We finish this paper by introducing a new public key cryptosystem which is a variant of the ElGamal cryptosystem [3] on a Montgomery curves over the ring $\mathbb{F}_q[e]$. For more works in this direction we refer the reader to [1].

2 The ring $\mathbb{F}_q[e],\ e^2 = e$

An element in $\mathbb{F}_q[e]$ is represented by $x_0 + x_1 e$ where $(x_0, x_1) \in \mathbb{F}_q$.
The arithmetic operations in $\mathbb{F}_q[e]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e$$

$$X.Y = (x_0 y_0) + (x_0 y_1 + x_1 y_0 + x_1 y_1)e,$$

where $X = x_0 + x_1 e$ and $Y = y_0 + y_1 e$. Let us recall the following results [1, 2]:

- $(\mathbb{F}_q[e], +, .)$ is a finite unitary commutative ring.
- $\mathbb{F}_q[e]$ is an $\mathbb{F}_q$-vector space of dimension 2 with $\mathbb{F}_q$-basis $\{1, e\}$.
- $X.Y = (x_0 y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0 y_0)e$.
- $X^2 = x_0^2 + ((x_0 + x_1)^2 - x_0^2)e$.
- $X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)e$.

- Let $X = x_0 + x_1 e \in \mathbb{F}_q[e]$, then $X \in (\mathbb{F}_q[e])^\times$ (the multiplicative group of $\mathbb{F}_q[e]$) if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. The inverse is given by:

$$X^{-1} = x_0^{-1} + ((x_0 + x_1)^{-1} - x_0^{-1})e.$$

- Let $X \in \mathbb{F}_q[e]$, then X is not invertible if and only if $X = xe$ or $X = x - xe$, such that $x \in \mathbb{F}_q$.
- $\mathbb{F}_q[e]$ is a non local ring.
- π_0 and π_1 are two surjective morphisms of rings.

3 Montgomery curves over the ring $\mathbb{F}_q[e], e^2 = e$

In this section, the elements X, Y, Z, A and B are in the ring $\mathbb{F}_q[e]$ such that $X = x_0 + x_1 e$, $Y = y_0 + y_1 e$, $Z = z_0 + z_1 e$, $A = A_0 + A_1 e$ and $B = B_0 + B_1 e$ where $x_0, x_1, y_0, y_1, z_0, z_1, A_0, A_1, B_0$ and B_1 are in $\mathbb{F}_q$. We define a Montgomery curve over the ring $\mathbb{F}_q[e]$, as a curve in the projective space $P^2(\mathbb{F}_q[e])$, which is given by the equation:

$$BY^2Z = X^3 + AX^2Z + XZ^2,$$

where A and B are parameters satisfying the condition that $\Delta = B(A^2 - 4)$ is invertible in $\mathbb{F}_q[e]$.
We denote this curves by: $M_{A,B}(\mathbb{F}_q[e])$, and we write:

$$M_{A,B}(\mathbb{F}_q[e]) = \{[X : Y : Z] \in P^2(\mathbb{F}_q) \mid BY^2Z = X^3 + AX^2Z + XZ^2\},$$

there is a unique point $O = [0 : 1 : 0]$ at infnity in $M_{A,B}$: it is the only point on $M_{A,B}$ where $Z = 0$.

Proposition 1. Let $\Delta_0 = B_0(A_0^2 - 4)$ and $\Delta_1 = (B_0 + B_1)((A_0 + A_1)^2 - 4)$. Then,

$$\Delta = \Delta_0 + (\Delta_1 - \Delta_0)e.$$

Proof. We have:

$$\begin{aligned}\Delta &= B(A^2 - 4)\\ &= (B_0 + B_1 e)[(A_0 + A_1 e)^2 - 4]\\ &= \Delta_0 + (\Delta_1 - \Delta_0)e.\end{aligned}$$

□

Corollary 1. Δ is invertible in $\mathbb{F}_q[e]$ if and only if $\Delta_0 \neq 0$ and $\Delta_1 \neq 0$.

Using Corollary 1, if Δ is invertible in $\mathbb{F}_q[e]$, then $M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)$ and $M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$ are two projective Montgomery curves over the finite field $\mathbb{F}_q$, and we notice:

$$\begin{aligned}M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) &= \{[x : y : z] \in P^2(\mathbb{F}_q) \mid B_0y^2z = x^3\\ &\quad + A_0x^2z + xz^2\}\\ M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q) &= \{[x : y : z] \in P^2(\mathbb{F}_q) \mid (B_0 + B_1)\\ &\quad y^2z = x^3 + (A_0 + A_1)x^2z + xz^2\}\end{aligned}$$

In [2] Boulbot et al. have showed the following proposition:

Proposition 2. Let X, Y and Z in $\mathbb{F}_q[e]$, then $[X : Y : Z] \in P^2(\mathbb{F}_q[e])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in P^2(\mathbb{F}_q)$, where $i \in \{0, 1\}$.

Theorem 2. Let X, Y and Z be in $\mathbb{F}_q[e]$, then $[X : Y : Z] \in M_{A,B}(\mathbb{F}_q[e])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in M_{\pi_i(A),\pi_i(B)}(\mathbb{F}_q)$, for $i \in \{0, 1\}$.

Proof. We have:

$$\begin{aligned}BY^2Z &= (B_0 + B_1e)(y_0 + y_1e)^2(z_0 + z_1e)\\ &= B_0y_0^2z_0 + [(B_0 + B_1)(y_0 + y_1)^2(z_0 + z_1) - B_0\\ &\quad y_0^2z_0]e\\ X^3 &= (x_0 + x_1e)^3\\ &= x_0^3 + [(x_0 + x_1)^3 - x_0^3]e\\ AX^2Z &= (A_0 + A_1e)(x_0 + x_1e)^2(z_0 + z_1e)\\ &= A_0x_0^2z_0 + [(A_0 + B_1)(x_0 + x_1)^2(z_0 + z_1) - A_0\\ &\quad x_0^2z_0]e\\ XZ^2 &= (x_0 + x_1e)(z_0 + z_1e)^2\\ &= x_0z_0^2 + [(x_0 + x_1)(z_0 + z_1)^2 - x_0z_0^2]e.\end{aligned}$$

As $\{1, e\}$ is an $\mathbb{F}_q$-basis of the vector space $\mathbb{F}_q[e]$,
then: $BY^2Z = X^3 + AX^2Z + XZ^2$ if and only if

$$\begin{cases} B_0y_0^2z_0 = x_0^3 + A_0x_0^2z_0 + x_0z_0^2\\ and\\ (B_0 + B_0)(y_0 + y_1)^2(z_0 + z_1) = (x_0 + x_1)^3 + (A_0 + A_1)(x_0 + x_1)^2(z_0 + z_1) + (x_0 + x_1)(z_0 + z_1)^2,\end{cases}$$

so the point $[X : Y : Z]$ is a solution of the Montgomery equation in $M_{A,B}(\mathbb{F}_q[e])$ if and only if $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)]$ is a solution of the same equation in $M_{\pi_i(A),\pi_i(B)}(\mathbb{F}_q)$ where $i \in \{0, 1\}$.
From the Corollary 1 and Proposition 2 we deduce the result. □

Corollary 3. The mappings $\tilde{\pi}_0$ and $\tilde{\pi}_1$ are well defined, where $\tilde{\pi}_i$ for $i \in \{0, 1\}$ is given by:

$$\begin{array}{cccc}\tilde{\pi}_i & : & M_{A,B}(\mathbb{F}_q[e]) & \rightarrow & M_{\pi_i(A),\pi_i(B)}(\mathbb{F}_q)\\ & & [X : Y : Z] & \mapsto & [\pi_i(X) : \pi_i(Y) : \pi_i(Z)]\end{array}$$

Proof. From the previous theorem, we have $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in M_{\pi_i(A),\pi_i(B)}(\mathbb{F}_q)$
If $[X_1 : Y_1 : Z_1] = [X_2 : Y_2 : Z_2]$, then there exist $\gamma \in (\mathbb{F}_q)^\times$ such that: $X_2 = \gamma X_1$, $Y_2 = \gamma Y_1$ and $Z_2 = \gamma Z_1$, then:

$$\begin{aligned}\tilde{\pi}_i([X_2 : Y_2 : Z_2]) &= [\pi_i(X_2) : \pi_i(Y_2) : \pi_i(Z_2)]\\ &= [\pi_i(\gamma)\pi_i(X_1) : \pi_i(\gamma)\pi_i(Y_1) : \pi_i(\gamma)\\ &\quad \pi_i(Z_1)]\\ &= [\pi_i(X_1) : \pi_i(Y_1) : \pi_i(Z_1)]\\ &= \tilde{\pi}_i([X_1 : Y_1 : Z_1]).\end{aligned}$$

□

4 The classification of elements in $M_{A,B}(\mathbb{F}_q[e])$

Let $M_{A,B}(\mathbb{F}_q[e])$ be the Montgomery curve $BY^2Z = X^3 + AX^2Z + XZ^2$ over the ring $\mathbb{F}_q[e]$. In this section we will classify the elements of the Montgomery curves, into three types, depending on whether the projective coordinate Z is invertible or not. The result is in the following proposition.

Proposition 3. The set $M_{A,B}(\mathbb{F}_q[e])$ has the following form:

$$\begin{aligned}M_{A,B}(\mathbb{F}_q[e]) = &\{[X : Y : 1] \mid BY^2 = X^3 + AX^2 + X\}\\ &\cup \{[0 : 1 : 0]\}\\ &\cup \{[xe : 1 : ze] \mid [x : 1 : z] \in M_{\pi_1(A),\pi_1(B)}\\ &(\mathbb{F}_q)\} \cup \{[xe : y - ye : e] \mid [x : 0 : 1] \in\\ &M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)\} \cup \{[x - xe : 1 : z - ze] \mid\\ &[x : 1 : z] \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)\} \cup \{[x - xe :\\ &ye : 1 - e] \mid [x : 0 : 1] \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)\}.\end{aligned}$$

Proof. Let $P = [X : Y : Z] \in M_{A,B}(\mathbb{F}_q[e]))$, where $X = x_0 + x_1e$, $Y = y_0 + y_1e$ and $Z = z_0 + z_1e$.
We have two cases of the projective coordinate Z:
1) First case: Z is invertible, then: $[X : Y : Z] \sim [X : Y : 1]$, where $\sim$ is the equivalence relation of the projective space $P^2(\mathbb{F}_q[e])$ [9, p.6] (see also [1, 4, 6, 5, 7]).
2) Second case: Z is no invertible, in this case we have:
i) $Z = ze$, where $z \in \mathbb{F}_q$, then:
• If $z = 0$ then $[X : Y : Z] = [0 : 1 : 0]$, else $z \neq 0$:
We have: $\pi_0([x_0 + x_1e : y_0 + y_1e : ze]) = [x_0 : y_0 : 0] \in M_{\pi_0(A),\pi_0(B)}$, then $x_0 = 0$ and $y_0 \neq 0$, i.e:

$$[X : Y : Z] = [xe : 1 + ye : ze]$$

there are two sub-cases of $y \in \mathbb{F}_q$:
a) $y \neq -1$, then $1 + ye$ is invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] \sim [xe : 1 : ze]$, where $[x : 1 : z] \in M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$.
b) $y = 1$ then $1 - e$ is not invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] = [xe : 1 - e : ze]$, where $[x : 1 : z] \in M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$ then necessary $z \neq 0$ according to Montgomery equation, hence $[X : Y : Z] \sim [xe : y - ye : e]$, where $[x : 0 : 1] \in M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$
ii) $Z = z - ze$, where $z \in \mathbb{F}_q$.
• If $z = 0$ then $[X : Y : Z] = [0 : 1 : 0]$, else $z \neq 0$, we have $\pi_1([x_0 + x_1e : y_0 + y_1e : z - ze]) = [x_0 + x_1 : y_0 + y_1 : 0] \in M_{\pi_1(A),\pi_1(B)}$ then: $x_0 + x_1 = 0$ and $y_0 + y_1 \neq 0$, i.e:

$$[X : Y : Z] = [x - xe : y_0 + y_1e : z - ze]$$

there are two sub-cases of $y_0 \in \mathbb{F}_q$:
a) $y_0 \neq 0$ then $y_0 + y_1e$ is invertible in $\mathbb{F}_q[e]$, so we have:

$$[X : Y : Z] \sim [x - xe : 1 : z - ze]$$

b) $y_0 = 0$ then $y_0 + y_1e$ is not invertible in $\mathbb{F}_q[e]$, so we have: $[X : Y : Z] = [x - xe : ye : z - ze]$, where $[x : 0 : z] \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)$ then necessary $z \neq 0$ according to Montgomery equation, hence $[X : Y : Z] \sim [x - xe : ye : 1 - e]$, where $[x : 0 : 1] \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)$ □

Corollary 4. $\tilde{\pi}_0$ is a surjective mapping.

Proof. Let $[x : y : z] \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q)$, then:
• if $y = 0$ then $z \neq 0$ so $[x : y : z] \sim [x : 0 : 1]$; hence $[x - xe : e : 1 - e]$ is an antecedent of $[x : 0 : z]$
• if $y \neq 0$, then $[x : y : z] \sim [x : 1 : z]$; hence $[x - xe : 1 : z - ze]$ is an antecedent of $[x : 1 : z]$. □

Corollary 5. $\tilde{\pi}_1$ is a surjective mapping.

Proof. Let $[x : y : z] \in M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$, then:
• if $y = 0$ then $z \neq 0$ so $[x : y : z] \sim [x : 0 : 1]$; hence $[xe : 1 - e : e]$ is an antecedent of $[x : 0 : 1]$
• if $y \neq 0$, then $[x : y : z] \sim [x : 1 : z]$; hence $[xe : 1 : ze]$ is an antecedent of $[x : 1 : z]$. □

The next proposition gives a bijection between the two sets $M_{A,B}(\mathbb{F}_q[e])$ and $M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) \times M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$.

Proposition 4. The $\tilde{\pi}$ mapping defined by:

$$\begin{array}{rcll}\tilde{\pi} : & M_{A,B}(\mathbb{F}_q[e]) & \to & M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) \times M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)\\ & [X : Y : Z] & \mapsto & ([\pi_0(X) : \pi_0(Y) : \pi_0(Z)], [\pi_1(X) : \pi_1(Y) : \pi_1(Z)])\end{array}$$

is a bijection.

Proof. • As $\tilde{\pi}_0$ and $\tilde{\pi}_1$ are well defined, then $\tilde{\pi}$ is well defined.
• Let $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) \times$

$M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q))$, clearly:
$\tilde{\pi}([x_0+(x_1-x_0)e : y_0+(y_1-y_0)e : z_0+(z_1-z_0)e]) = ([x_0 : y_0 : z_0],[x_1 : y_1 : z_1])$, hence $\tilde{\pi}$ is a surjective mapping.

• Let $[X : Y : Z]$ and $[X' : Y' : Z']$ are elements of $M_{A,B}(\mathbb{F}_q[e])$, where $X = x_0+x_1e$, $Y = y_0+y_1e$, $Z = z_0+z_1e$, $X' = x'_0+x'_1e$, $Y' = y'_0+y'_1e$ and $Z' = z'_0+z'_1e$,
such that: $\tilde{\pi}([X : Y : Z]) = \tilde{\pi}([X' : Y' : Z'])$,
then:

$$[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0]$$

and

$$[x_0+x_1 : y_0+y_1 : z_0+z_1] = [x'_0+x'_1 : y'_0+y'_1 : z'_0+z'_1],$$

then there exist $(k,l) \in (\mathbb{F}_q^*)^2$ such that:

$$\begin{cases} x'_0 = kx_0 \\ y'_0 = ky_0 \\ z'_0 = kz_0 \end{cases} \text{ and } \begin{cases} x'_0+x'_1 = l(x_0+x_1) \\ y'_0+y'_1 = l(y_0+y_1) \\ z'_0+z'_1 = l(z_0+z_1) \end{cases}$$

So $\begin{cases} x'_1 = (l-k)x_0+x_1 \\ y'_1 = (l-k)y_0+y_1 \\ z'_1 = (l-k)z_0+z_1 \end{cases}$

Then:

$$\begin{cases} X' = kx_0+((l-k)x_0+x_1)e = (k+(l-k)e)X \\ Y' = ky_0+((l-k)y_0+y_1)e = (k+(l-k)e)Y \\ Z' = kz_0+((l-k)z_0+z_1)e = (k+(l-k)e)Z \end{cases}$$

As $k+(l-k)e$ is invertible in $\mathbb{F}_q[e]$, so $[X' : Y' : Z'] = [X : Y : Z]$, hence $\tilde{\pi}$ is an injective mapping.
We can easily show that the mapping $\tilde{\pi}^{-1}$ defined by:

$$\tilde{\pi}^{-1}([x_0 : y_0 : z_0],[x_1 : y_1 : z_1]) = [x_0+(x_1-x_0)e : y_0+ (y_1-y_0)e : z_0+(z_1-z_0)e]$$

is the inverse of $\tilde{\pi}$. □

Corollary 6. The cardinal of $M_{A,B}(\mathbb{F}_q[e])$ is equal to the cardinal of $M_{\pi_0(A),\pi_0(B)}(\mathbb{F}_q) \times M_{\pi_1(A),\pi_1(B)}(\mathbb{F}_q)$.

5 The group law

Let $P = (X_1 : Y_1 : Z_1)$ be a point on $M_{A,B}(\mathbb{F}_q[e])$ and $[n]P = (X_n : Y_n : Z_n)$. By [10], the sum $[n+m]P = [n]P \oplus [m]P$ is given by the following formulas where Y_n never appears.
Addition: $n \neq m$

$$\begin{aligned} X_{m+n} &= Z_{m-n}((X_m-Z_m)(X_n+Z_n)+(X_m+Z_m) \\ &\quad (X_n-Z_n))^2, \\ Z_{m+n} &= X_{m-n}((X_m-Z_m)(X_n+Z_n)-(X_m+Z_m) \\ &\quad (X_n-Z_n))^2. \end{aligned}$$

Doubling: $n = m$

$$\begin{aligned} 4X_nZ_n &= (X_n+Z_n)^2-(X_n-Z_n)^2, \\ X_{2n} &= (X_n+Z_n)^2(X_n-Z_n)^2, \\ Z_{2n} &= 4X_nZ_n((X_n-Z_n)^2+((A+2)/4)(4X_nZ_n)). \end{aligned}$$

6 Cryptography applications

6.1 Cryptography results

From the proposition 4, we have:

• If $card(M_{A;B}(\mathbb{F}_q[e])) := n$ is an odd number, then $n = s \times t$ is the factorization of n, where $s := card(M_{\pi_0(A);\pi_0(B)}(\mathbb{F}_q))$ and $t := card(M_{\pi_1(A);\pi_1(B)}(\mathbb{F}_q))$, hence the cardinal of $M_{A;B}(\mathbb{F}_q[e])$ is not a prime number.

• The discrete logarithm problem in $M_{A,B}(\mathbb{F}_q[e])$ is equivalent to the discrete logarithm problem in $M_{\pi_0(A);\pi_0(B)}(\mathbb{F}_q) \times M_{\pi_1(A);\pi_1(B)}(\mathbb{F}_q)$.

6.2 ElGamal cryptosystem on a Montgomery curves over this ring

ElGamal cryptosystem for $M_{A,B}(\mathbb{F}_q[e])$ consists essentially in mapping the operations customarily carried out in the multiplicative group $\mathbb{Z}_p$ to the set of points of a Montgomery curve $M_{A,B}(\mathbb{F}_q[e])$, endowed with an additive group operation. An entity chooses and publishes a prime number p (large), a Montgomery curve $M_{A,B}(\mathbb{F}_q[e])$ and a point P in $M_{A,B}(\mathbb{F}_q[e])$.

6.2.1 Key creation:

- Choose a secret integer s_A.
- Compute $Q_A = s_AP$ in $M_{A,B}(\mathbb{F}_q[e])$.
- Publish the public key Q_A.

6.2.2 Encryption:

- Choose the plain text P_m in $M_{A,B}(\mathbb{F}_q[e])$.
- Choose an ephemeral key k.
- Use Alice's public key Q_A to calculate $u = kP$ in $M_{A,B}(\mathbb{F}_q[e])$ and $v = P_m+kQ_A$ in $M_{A,B}(\mathbb{F}_q[e])$.
- Send the cipher text (u, v)

6.2.3 Decryption:

Calculate $v-s_Au$ in $M_{A,B}(\mathbb{F}_q[e])$. This value is equal to P_m.
ElGamal cryptosystem is directly based on the difficulty of solving the discrete logarithm problem over $(E,+)$ of base P. This problem requires to find n where $Q = nP$ and points P, Q belong to a set of points E of a Montgomery curve $M_{A,B}(\mathbb{F}_q[e])$. It is known to be computationally difficult and thus can be utilized to accomplish a more elevated level of security in cryptosystem.

References:

[1] Ben Taleb, E.M., Chillali, A., El Fadil, L., Twisted Hessian curves over the Ring $\mathbb{F}_q[e]$, $e^2 = e$, Bol. Soc. Paran, (3s.) v.(40), doi:10.52699/bspm.15867, (2022).

[2] Boulbot, A., Chillali, A., Mouhib, A., "Elliptic Curves Over the Ring R", Bol. Soc. Paran., Vol.38, No.3, 2020, 193-201.

[3] ElGamal, T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, In Proceedings of CRYPTO 84 on Advances in cryptology. Springer-Verlag New York, Inc, 1985, pp. 10-18.

[4] Grini, A., Chillali, A., Mouanis, H., The Binary Operations Calculus in $H^2_{a,d}$. Bol. Soc. Paran, Vol.40, 2020, 1-6.

[5] Grini, A., Chillali, A., Mouanis, H., Cryptography over twisted Hessian curves of the ring $F_q[\varepsilon]$, $\varepsilon^2 = 0$. Adv. Math.: Sci. J., vol.10 , no.1, 2021, 235-243.

[6] Grini, A., Chillali, A. & Mouanis, H. A new cryptosystem based on a twisted Hessian curve $H^4_{a,d}$. J. Appl. Math. Comput., 2021.

[7] Grini A., Chillali A., Mouanis H. Cryptography Over the Twisted Hessian Curve $H^3_{a,d}$. In: Ben Ahmed M., Teodorescu HN.L., Mazri T., Subashini P., Boudhir A.A. (eds) Networking, Intelligent Systems and Security. Smart Innovation, Systems and Technologies, vol. 237. Springer, Singapore, 2022.

[8] Hendrik, W., Lenstra Jr., Factoring integers with elliptic curves. Annals of mathe-matics, 1987, pp. 649-673.

[9] Lenstra, H. W., Eliptic Curves and Number-Theoretic Algorithms. Processing Int. Congress Math., USA, 1986.

[10] Peter L., Montgomery, Speeding the Pollard and Elliptic Curve Methods of Facorization, Mathematics of Computation., vol. 48, 1987, 243-264.