Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.75887

Huff Curve Over the Ring $\mathbb{F}_q[\epsilon], \epsilon^2 = \epsilon$ [*]

Abdelhakim Chillali, Moha Ben Taleb Elhamam and Abdelâli Grini[†]

ABSTRACT: Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of a prime number p. In this paper, we study the Huff curves over the ring $\mathbb{F}_q[\epsilon]$, where $\epsilon^2 = \epsilon$, denoted by $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$; $(a, b) \in (\mathbb{F}_q[\epsilon])^2$. Using the Huff equation, we define the Huff curves $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and we will show that $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $\mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ are two Huff curves over the field $\mathbb{F}_q$, where π_0 and π_1 are respectively the canonical projection and the sum projection of coordinates from $\mathbb{F}_q[\epsilon]$ to $\mathbb{F}_q$. Precisely, we give a bijection between the sets $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

Key Words: Cryptography, elliptic curve, finite ring, Huff curve.

Contents

1. Introduction

Elliptic curves have been widely studied in algebraic geometry and number theory since the mid-19th century. More recently, they have been used to design efficient algorithms to factor large integers [16,17], or to prove primality [1,8]. They have also proven useful in building cryptosystems [15,18]. It is known that elliptic curves can be represented in different forms. These different forms induce different arithmetic properties. To obtain fast scalar multiplications, various forms of elliptic curves have been studied in the last decades, among which Huff curve. In [14] Joye and his co-authors presented fast explicit formula for adding or doubling points on Huff curves and devised a couple of extensions and generalizations upon this model. In this work, we develop an elliptic curve model introduced by Huff in 1948 to study a diophantine problem.

In this paper, we study Huff curve over the ring $\mathbb{F}_q[\epsilon], \epsilon^2 = \epsilon$. The motivation for this paper is the search for new groups of points of a Huff curve over a finite ring, where the complexity of the discrete logarithm calculation is good for use in cryptography.

Let $\mathbb{K}$ be a finite field of order $q = p^n$ where n is a positive integer and p is a prime number. In [2], A. Boulbot et al, study the arithmetic of this ring, in particular they show that $\mathbb{F}_q[\epsilon], \epsilon^2 = \epsilon$ is not a local ring. In section 3, we define the Huff curve $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ over this ring. The study of it's discriminant and it's Huff curve equation, allows us to define two Huff curves $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $\mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$. In the next of this section, we classify the elements of $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and we give a bijection between the two sets $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, where π_0 and π_1 are two surjective morphisms of rings defined by:

$$\begin{array}{cccc} \pi_0 & : & \mathbb{F}_q[\epsilon] & \to & \mathbb{F}_q \\ & & x_0 + x_1\epsilon & \mapsto & x_0 \end{array} \text{ and } \begin{array}{cccc} \pi_1 & : & \mathbb{F}_q[\epsilon] & \to & \mathbb{F}_q \\ & & x_0 + x_1\epsilon & \mapsto & x_0 + x_1 \end{array}.$$

[*] The project is partially supported by Sidi Mohamed Ben Abdellah University, Morocco

[†] Corresponding author.

2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted February 26, 2025. Published October 30, 2025

Typeset by $\mathcal{B}^{S}\mathcal{P}_{\mathcal{M}}$ style.
© Soc. Paran. de Mat.

For more works in this direction we refer the reader to [3,4,5,6,7].

Let q be a prime power. Consider the quotient ring $R = \dfrac{\mathbb{F}_q[X]}{(X^2 - X)}$, where $\mathbb{F}_q$ is the finite field of q elements. The ring R is identified to the ring $\mathbb{F}_q[\epsilon]$, where $\epsilon^2 = \epsilon$. Therefore,

$$R = \{x_0 + x_1\epsilon | \epsilon^2 = \epsilon \text{ and } (x_0, x_1) \in (\mathbb{F}_q)^2\}.$$

The arithmetic operations in R can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\epsilon,$$
$$X \cdot Y = (x_0y_0) + (x_0y_1 + x_1y_0 + x_1y_1)\epsilon.$$

The authors of [2] proved the following facts:

1. $(R, +, \cdot)$ is a finite unitary commutative ring.
2. R is an $\mathbb{F}_q$-vector space of dimension 2 with $\mathbb{F}_q$-basis $\{1, \epsilon\}$.
3. $X \cdot Y = (x_0y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)\epsilon$.
4. $X^2 = x_0^2 + ((x_0 + x_1)^2 - x_0^2)\epsilon$.
5. $X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)\epsilon$.
6. Put $X = x_0 + x_1\epsilon \in R$. Then, X is invertible in R if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. In this case we have, $X^{-1} = x_0^{-1} + ((x_0 + x_1)^{-1} - x_0^{-1})\epsilon$.
7. R is a non local ring.
8. π_0 and π_1 are two surjective morphisms of rings.

2. Huff curve over the Ring $\mathbb{F}_q[\epsilon], \epsilon^2 = \epsilon$

In this section the elements X, Y, Z, a and b are in the ring $\mathbb{F}_q[\epsilon]$ such that $X = x_0 + x_1\epsilon$, $Y = y_0 + y_1\epsilon$, $Z = z_0 + z_1\epsilon$, $a = a_0 + a_1\epsilon$ and $b = b_0 + b_1\epsilon$ where $x_0, x_1, y_0, y_1, z_0, z_1, a_0, a_1, b_0$ and b_1 are in $\mathbb{F}_q$.

Definition 2.1 *A Huff curve over R is defined by the equation:*

$$aX(Y^2 - Z^2) = bY(X^2 - Z^2)$$

such that $\Delta = a^2 - b^2$ is invertible in R. We denote it by $\mathcal{H}_{a,b}(R)$ and we write:

$$\mathcal{H}_{a,b}(R) := \{[X : Y : Z] \in \mathbb{P}^2(R) \mid aX(Y^2 - Z^2) = bY(X^2 - Z^2)\}.$$

Remark 2.1

$$\pi_0(\Delta) = a_0^2 - b_0^2,$$
$$\pi_1(\Delta) = (a_0 + a_1)^2 - (b_0 + b_1)^2.$$

Proposition 2.1 *Let $\Delta_0 = \pi_0(\Delta)$ and $\Delta_1 = \pi_1(\Delta)$, then*

$$\Delta = \Delta_0 + (\Delta_1 - \Delta_0)\epsilon$$

Proof:

we have

$$\begin{aligned}\Delta &= a^2 - b^2\\ &= a_0^2 + ((a_0 + a_1)^2 - a_0^2)\epsilon - b_0^2 - ((b_0 + b_1)^2 - b_0^2)\epsilon\\ &= a_0^2 - b_0^2 + ((a_0 + a_1)^2 - a_0^2 - (b_0 + b_1)^2 + b_0^2)\epsilon\\ &= a_0^2 - b_0^2 + ((a_0 + a_1)^2 - (b_0 + b_1)^2 - a_0^2 + b_0^2)\epsilon\\ &= \Delta_0 + (\Delta_1 - \Delta_0)\epsilon.\end{aligned}$$

□

Corollary 2.1 *Δ is invertible in $\mathbb{F}_q[\epsilon]$ if and only if $\Delta_0 \neq 0$ and $\Delta_1 \neq 0$.*

Using Corollary 2.1, if Δ is invertible in $\mathbb{F}_q[\epsilon]$, then $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ and $\mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ are two Huff curves over the finite field $\mathbb{F}_q$, and we write:

$$\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) = \{[x:y:z] \in P^2(\mathbb{F}_q) \mid a_0 x(y^2 - z^2) = b_0 y(x^2 - z^2)\},$$

$$\mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) = \{[x:y:z] \in P^2(\mathbb{F}_q) \mid (a_0 + a_1)x(y^2 - z^2) = (b_0 + b_1)y(x^2 - z^2)\}.$$

Proposition 2.2 *Let X, Y and Z in $\mathbb{F}_q[\epsilon]$, then $[X:Y:Z] \in P^2(\mathbb{F}_q[\epsilon])$ if and only if $[\pi_0(X):\pi_0(Y):\pi_0(Z)] \in P^2(\mathbb{F}_q)$ and $[\pi_1(X):\pi_1(Y):\pi_1(Z)] \in P^2(\mathbb{F}_q)$.*

Proof:

Suppose that $[X:Y:Z] \in P^2(\mathbb{F}_q[\epsilon])$, then there exist $(U,V,W) \in (\mathbb{F}_q[\epsilon])^3$ such that $UX+VY+WZ = 1$. Hence for $i \in \{0,1\}$, we have:
$\pi_i(U)\pi_i(X) + \pi_i(V)\pi_i(Y) + \pi_i(W)\pi_i(Z) = 1$, so $(\pi_i(X), \pi_i(Y), \pi_i(Z)) \neq (0,0,0)$, which proves that $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in P^2(\mathbb{F}_q)$.
Reciprocally, let $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in P^2(\mathbb{F}_q)$ where $i \in \{0,1\}$. Suppose that $x_0 \neq 0$, then we distinguish between two case of $x_0 + x_1$:

1. $x_0 + x_1 \neq 0$: then X is invertible in $\mathbb{F}_q[\epsilon]$, so $[X:Y:Z] \in P^2(\mathbb{F}_q[\epsilon])$.
2. $x_0 + x_1 = 0$: then $y_0 + y_1 \neq 0$ or $z_0 + z_1 \neq 0$.
   (a) $y_0 + y_1 \neq 0$ then: $x_0 + (y_0 + y_1 - x_0)\epsilon = x_0 - x_0\epsilon + (y_0 + y_1)\epsilon = X + \epsilon Y \in (\mathbb{F}_q[\epsilon])^\times$, so there exist $U \in \mathbb{F}_q[\epsilon] : UX + \epsilon UY = 1$, hence $[X:Y:Z] \in P^2(\mathbb{F}_q[\epsilon])$.
   (b) $z_0 + z_1 \neq 0$ then $X + \epsilon Z \in (\mathbb{F}_q[\epsilon])^\times$, so $[X:Y:Z] \in P^2(\mathbb{F}_q[\epsilon])$.

In the case where $y_0 \neq 0$ or $z_0 \neq 0$, we follow the same proof.

□

Theorem 2.1 *Let X, Y and Z in $\mathbb{F}_q[\epsilon]$, then $[X:Y:Z] \in \mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ if and only if $[\pi_i(X):\pi_i(Y):\pi_i(Z)] \in \mathcal{H}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, where $i \in \{0,1\}$.*

Proof:

We have:

$$\begin{aligned}
aX(Y^2 - Z^2) &= (a_0 + a_1\epsilon)(x_0 + x_1\epsilon)((y_0 + y_1\epsilon)^2 - (z_0 + z_1\epsilon)^2) \\
&= [a_0x_0 + ((a_0 + a_1)(x_0 + x_1) - a_0x_0)\epsilon][y_0^2 - z_0^2 + ((y_0 + y_1)^2 - (z_0 + z_1)^2 - y_0^2 + z_0^2)\epsilon] \\
&= a_0x_0(y_0^2 - z_0^2) + [(a_0 + a_1)(x_0 + x_1)((y_0 + y_1)^2 - (z_0 + z_1)^2) - a_0x_0(y_0^2 - z_0^2)]\epsilon, \\
bY(X^2 - Z^2) &= (b_0 + b_1\epsilon)(y_0 + y_1\epsilon)((x_0 + x_1\epsilon)^2 - (z_0 + z_1\epsilon)^2) \\
&= b_0y_0(x_0^2 - z_0^2) + [(b_0 + b_1)(y_0 + y_1)((x_0 + x_1)^2 - (z_0 + z_1)^2) - b_0y_0(x_0^2 - z_0^2)]\epsilon.
\end{aligned}$$

Or $\{1, \epsilon\}$ is a basis of $\mathbb{F}_q$ vector space $\mathbb{F}_q[\epsilon]$, then $aX(Y^2 - Z^2) = bY(X^2 - Z^2)$ if and only if $a_0x_0(y_0^2 - z_0^2) = b_0y_0(x_0^2 - z_0^2)$ and $(a_0 + a_1)(x_0 + x_1)((y_0 + y_1)^2 - (z_0 + z_1)^2) = (b_0 + b_1)(y_0 + y_1)((x_0 + x_1)^2 - (z_0 + z_1)^2)$.

□

Corollary 2.2 *The mappings $\tilde{\pi}_0$ and $\tilde{\pi}_1$ are well defined, where $\tilde{\pi}_i$ for $i \in \{0,1\}$ is given by:*

$$\begin{array}{cccc}
\tilde{\pi}_i & : & \mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon]) & \rightarrow & \mathcal{H}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q) \\
 & & [X:Y:Z] & \mapsto & [\pi_i(X):\pi_i(Y):\pi_i(Z)]
\end{array}$$

Proof:

From the previous theorem, we have $[\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \in \mathcal{H}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$
If $[X : Y : Z] = [X' : Y' : Z']$, then there exists $\lambda \in (\mathbb{F}_q)^\times$ such that: $X' = \lambda X$, $Y' = \lambda Y$ and $Z' = \lambda Z$. Thus:

$$\begin{aligned}
\tilde{\pi_i}([X' : Y' : Z']) &= [\pi_i(X') : \pi_i(Y') : \pi_i(Z')] \\
&= \underbrace{[\pi_i(\lambda)\pi_i(X) : \pi_i(\lambda)\pi_i(Y) : \pi_i(\lambda)\pi_i(Z)]}_{\pi_i(\lambda)=\lambda\in(\mathbb{F}_q)^\times} \\
&= [\pi_i(X) : \pi_i(Y) : \pi_i(Z)] \\
&= \tilde{\pi_i}([X : Y : Z]).
\end{aligned}$$

□

3. Classification of elements in $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$

In this subsection we will classify the elements of the Huff curve into three types, depending on whether the third projective coordinate X is invertible or not. The result is in the following proposition.

Proposition 3.1 *Every element of $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ is of the form $[1 : Y : Z]$ or $[x\epsilon : y\epsilon : 1 - \epsilon]$ such that $[x : y : 0] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ or $[x\epsilon : y\epsilon : 1]$ such that $[x : y : 1] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ or $[x\epsilon : 1 - \epsilon : z\epsilon]$ such that $[x : 0 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ or $[x\epsilon : 1 : z\epsilon]$ such that $[x : 1 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$ or $[x - x\epsilon : y - y\epsilon : \epsilon]$ such that $[x : y : 0] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ or $[x - x\epsilon : y - y\epsilon : 1]$ such that $[x : y : 1] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ or $[x - x\epsilon : \epsilon : z - z\epsilon]$such that $[x : 0 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$ or $[x - x\epsilon : 1 : z - z\epsilon]$ such that $[x : 1 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$. We write:*

$$\begin{aligned}
\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon]) = &\left\{[1 : Y : Z] \mid a(Y^2 - Z^2) = bY(1 - Z^2)\right\} \\
&\cup \left\{[x\epsilon : y\epsilon : 1 - \epsilon] \mid [x : y : 0] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x\epsilon : y\epsilon : 1] \mid [x : y : 1] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x\epsilon : 1 - \epsilon : z\epsilon] \mid [x : 0 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x\epsilon : 1 : z\epsilon] \mid [x : 1 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x - x\epsilon : y - y\epsilon : \epsilon] \mid [x : y : 0] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x - x\epsilon : y - y\epsilon : 1] \mid [x : y : 1] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x - x\epsilon : \epsilon : z - z\epsilon] \mid [x : 0 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\} \\
&\cup \left\{[x - x\epsilon : 1 : z - z\epsilon] \mid [x : 1 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)\right\}.
\end{aligned}$$

Proof: Let $P = [X : Y : Z] \in \mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$, where $X = x_0 + x_1\epsilon$, $Y = y_0 + y_1\epsilon$ and $Z = z_0 + z_1\epsilon$. We have two cases of the third projective coordinate X:

1. First case: X is invertible, then: $[X : Y : Z] \sim [1 : Y : Z]$.

2. Second case: X is not invertible. In that case we have:

   (a) $X = x\epsilon$, where $x \in \mathbb{F}_q$, then $\tilde{\pi}_0([X : Y : Z]) = [0 : y_0 : z_0]$ so $y_0 = 0$ or $z_0 = 0$ there are two sub-cases.

   i. If $y_0 = 0$ so $z_0 \neq 0$, we have: $[0 : y_0 : z_0] \sim [0 : 0 : 1]$, hence $[X : Y : Z] \sim [x\epsilon : y\epsilon : 1 + z\epsilon]$, there are two sub-cases of z:

   A. $z = -1$ hence $[X : Y : Z] \sim [x\epsilon : y\epsilon : 1 - \epsilon]$, where $[x : y : 0] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

   B. $z \neq -1$ so Z is invertible hence $[X : Y : Z] \sim [x\epsilon : y\epsilon : 1]$, where $[x : y : 1] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

  ii. If $z_0 = 0$ so $y_0 \neq 0$, we have: $[0 : y_0 : z_0] \sim [0 : 1 : 0]$, hence $[X : Y : Z] \sim [x\epsilon : 1 + y\epsilon : z\epsilon]$, there are two sub-cases of y:

   A. $y = -1$ hence $[X : Y : Z] \sim [x\epsilon : 1 - \epsilon : z\epsilon]$, where $[x : 0 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

   B. $y \neq -1$ so Y is invertible hence $[X : Y : Z] \sim [x\epsilon : 1 : z\epsilon]$, where $[x : 1 : z] \in \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

(b) $X = x - x\epsilon$, where $x \in \mathbb{F}_q$, then $\tilde{\pi}_1([X : Y : Z]) = [0 : y_0 + y_1 : z_0 + z_1]$ so $y_0 + y_1 = 0$ or $z_0 + z_1 = 0$ there are two sub-cases.

  i. If $y_0 + y_1 = 0$ so $z_0 + z_1 \neq 0$, we have: $[0 : y_0 + y_1 : z_0 + z_1] \sim [0 : 0 : 1]$, hence $[X : Y : Z] \sim [x\epsilon : -y + y\epsilon : 1 - z + z\epsilon]$, there are two sub-cases of z:

   A. $z = 1$ hence $[X : Y : Z] \sim [x - x\epsilon : y - y\epsilon : \epsilon]$, where $[x : y : 0] \in \mathcal{H}_{\pi_0(a),\pi_0(0)}(\mathbb{F}_q)$.

   B. $z \neq 1$ so Z is invertible hence $[X : Y : Z] \sim [x - x\epsilon : y - y\epsilon : 1]$, where $[x : y : 1] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

  ii. If $z_0 + z_1 = 0$ so $y_0 + y_1 \neq 0$, we have: $[0 : y_0 + y_1 : z_0 + z_1] \sim [0 : 1 : 0]$, hence $[X : Y : Z] \sim [x\epsilon : 1 - y + y\epsilon : -z + z\epsilon]$, there are two sub-cases of y:

   A. $y = 1$ hence $[X : Y : Z] \sim [x - x\epsilon : \epsilon : z - z\epsilon]$, where $[x : 0 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

   B. $y \neq 1$ so Y is invertible hence $[X : Y : Z] \sim [x - x\epsilon : 1 : z - z\epsilon]$, where $[x : 1 : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$.

Which proves the proposition.

□

From this proposition we deduce the following corollaries.

Corollary 3.1 $\tilde{\pi}_0$ *is a surjective mapping.*

Proof: Let $[x : y : z] \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q)$, then

1. If $z \neq 0$, then $[x : y : z] \sim [x : y : 1]$, hence $[x - x\epsilon : y - y\epsilon : 1]$ is an antecedent of $[x : y : z]$.

2. If $z = 0$, then $[x : y : z] = [x : y : 0]$, hence $[x - x\epsilon : y - y\epsilon : \epsilon]$ is an antecedent of $[x : y : z]$.

□

Corollary 3.2 $\tilde{\pi}_1$ *is a surjective mapping.*

Proof: Let $[x : y : z] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$, then:

1. If $z \neq 0$, then $[x : y : z] \sim [x : y : 1]$, hence $[x\epsilon : y\epsilon : 1]$ is an antecedent of $[x : y : z]$.

2. If $z = 0$, then $[x : y : z] = [x : y : 0]$, hence $[x\epsilon : y\epsilon : 1 - \epsilon]$ is an antecedent of $[x : y : z]$.

□

Proposition 3.2 *The $\tilde{\pi}$ mapping defined by:*

$$\begin{array}{cccc} \tilde{\pi} & : & \mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon]) & \to & \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q) \\ & & [X : Y : Z] & \mapsto & ([\pi_0(X) : \pi_0(Y) : \pi_0(Z)], [\pi_1(X) : \pi_1(Y) : \pi_1(Z)]) \end{array}$$

is a bijection.

Proof:

1. As $\tilde{\pi_0}$ and $\tilde{\pi_1}$ are well defined, then $\tilde{\pi}$ is well defined.

2. Let $([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \in \mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, then $[x_0 + (x_1 - x_0)\epsilon : y_0 + (y_1 - y_0)\epsilon : z_0 + (z_1 - z_0)\epsilon] \in \mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and it is clear that
$$\tilde{\pi}([x_0 + (x_1 - x_0)\epsilon : y_0 + (y_1 - y_0)\epsilon : z_0 + (z_1 - z_0)\epsilon]) = ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]),$$
hence $\tilde{\pi}$ is a surjective mapping.

3. Lets $[X : Y : Z]$ and $[X' : Y' : Z']$ are elements of $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$, where $X = x_0 + x_1\epsilon$, $Y = y_0 + y_1\epsilon$, $Z = z_0 + z_1\epsilon$, $X' = x'_0 + x'_1\epsilon$, $Y' = y'_0 + y'_1\epsilon$ and $Z' = z'_0 + z'_1\epsilon$.
If $[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0]$ 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 exists $(k, l) \in (\mathbb{F}_q^*)^2$ such that:
$$\begin{cases} x'_0 = kx_0 \\ y'_0 = ky_0 \\ z'_0 = kz_0 \end{cases} \text{ and } \begin{cases} x'_0 + x'_1 = l(x_0 + x_1) \\ y'_0 + y'_1 = l(y_0 + y_1) \\ z'_0 + z'_1 = l(z_0 + z_1) \end{cases} \text{ so } \begin{cases} x'_1 = (l - k)x_0 + x_1 \\ y'_1 = (l - k)y_0 + y_1 \\ z'_1 = (l - k)z_0 + z_1 \end{cases}$$
then $\begin{cases} X' = kx_0 + ((l - k)x_0 + x_1)\epsilon = (k + (l - k)\epsilon)X \\ Y' = ky_0 + ((l - k)y_0 + y_1)\epsilon = (k + (l - k)\epsilon)Y \\ Z' = kz_0 + ((l - k)z_0 + z_1)\epsilon = (k + (l - k)\epsilon)Z \end{cases}$.
Or $k + (l - k)\epsilon$ is invertible in $\mathbb{F}_q[\epsilon]$, 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:
$$\tilde{\pi}^{-1}([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) = [x_0 + (x_1 - x_0)\epsilon : y_0 + (y_1 - y_0)\epsilon : z_0 + (z_1 - z_0)\epsilon]$$

is the inverse of $\tilde{\pi}$.

□

Corollary 3.3 *The cardinal of $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ is equal to the cardinal of $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.*

Cryptography applications
In cryptography applications, we have:

1. If $card(\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])) = n$ is an odd number, then $n = s \times t$ is the factorization of n, where $s = card(\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q))$ and $t = card(\mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q))$, hence the cardinal of $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ is not a prime number.

2. The discrete logarithm problem in $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ is equivalent to the discrete logarithm problem in $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

4. Addition law on Huff curve $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$

Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_2 = [X_2 : Y_2 : Z_2]$ be two points on the Huff curve $\mathcal{H}_{\pi_i(a),\pi_i(b)}(\mathbb{F}_q)$, for $i \in \{0, 1\}$ and $O = [0 : 0 : 1]$ as neutral element of the law of addition. Let $P_3 = P_1 + P_2 = [X_3 : Y_3 : Z_3]$. So,
$$\begin{aligned} X_3 &= (X_1Z_2 + X_2Z_1)(Y_1Y_2 + Z_1Z_2)^2(Z_1Z_2 - X_1X_2), \\ Y_3 &= (Y_1Z_2 + Y_2Z_1)(X_1X_2 + Z_1Z_2)^2(Z_1Z_2 - Y_1Y_2), \qquad (*) \\ Z_3 &= (Z_1^2Z_2^2 - X_1^2X_2^2)(Z_1^2Z_2^2 - Y_1^2Y_2^2). \end{aligned}$$

Theorem 4.1 *Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_2 = [X_2 : Y_2 : Z_2]$ be two points on the Huff curve over $\mathbb{F}_q$. Then the addition formula given by $(*)$ is valid provided that $X_1X_2 \neq \pm Z_1Z_2$ and $Y_1Y_2 \neq \pm Z_1Z_2$.*

In the following, we can define a new sum over $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ using the previous results.

As $\tilde{\pi}$ is a bijection mapping between the two sets $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$, we can define the sum on $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$.

Definition 4.1 *Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_2 = [X_2 : Y_2 : Z_2]$ be two points of the two points on the Huff curve $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$, we define the additive law $P_3 = P_1 \tilde{+} P_2$ in $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ by: $P_3 = P_1 \tilde{+} P_2 = \tilde{\pi}^{-1}(\tilde{\pi}(P_1) + \tilde{\pi}(P_2))$ and $O = [0 : 0 : 1]$ as neutral element of the law of addition.*

Corollary 4.1 *Let $P_1 = [X_1 : Y_1 : Z_1]$ and $P_2 = [X_2 : Y_2 : Z_2]$ be two points on the Huff curve $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ over $\mathbb{F}_q[\epsilon]$. Then the addition formula given by $(*)$ is valid provided that $\pi_i(X_1)\pi_i(X_2) \neq \pm\pi_i(Z_1)\pi_i(Z_2)$ and $\pi_i(Y_1)\pi_i(Y_2) \neq \pm\pi_i(Z_1)\pi_i(Z_2)$, for $i \in \{0, 1\}$.*

5. Conclusion

In this work, we have proved the bijection between $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ and $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$. In cryptography applications, we deduce that the discrete logarithm problem in $\mathcal{H}_{a,b}(\mathbb{F}_q[\epsilon])$ is equivalent to the discrete logarithm problem in $\mathcal{H}_{\pi_0(a),\pi_0(b)}(\mathbb{F}_q) \times \mathcal{H}_{\pi_1(a),\pi_1(b)}(\mathbb{F}_q)$.

References

1. Atkin, A. O. L. and Morain, F., *Elliptic curves and primality proving*, Math. Comp. 203 (1993) 29-68.
2. Boulbot, A., Chillali, A. and Mouhib, A., *Elliptic Curves Over the Ring R*, Bol. Soc. Paran 38 (2020) 193-201.
3. Chillali, A., Grini, A., Elhamam, M.B.T., *Twisted Hessian Curve Over a Local Ring*, Boletim da Sociedade Paranaense de Matematica 42 (2024) 1-10.
4. Elhamam, M.B.T., Chillali, A., El Fadil, L., *Twisted Hessian curves over the Ring $\mathbb{F}_q[e]$, $e^2 = e$*, Bol. Soc. Paran 40 (2022) 1-6.
5. El Hamam, M.B.T., Grini, A., Chillali, A., and El Fadil, L., *El Gamal Cryptosystem on a Montgomery Curves Over Non Local Ring*, WSEAS Transactions on Mathematics 21 (2022) 85-89.
6. El Hamam, M.B.T., Chillali, A., and El Fadil, L., *Public key cryptosystem and binary Edwards curves on the ring $\mathbb{F}_{2^n}[e]$, $e^2 = e$ for data management*, 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (2022) 1-4.
7. El Hamam, M.B.T., Chillali, A., and El Fadil, L., *A New Addition Law in Twisted Edwards Curves on Non Local Ring*, Nitaj, A., Zkik, K. (eds) Cryptography, Codes and Cyber Security. I4CS 2022 Communications in Computer and Information Science, Springer 1747 (2023).
8. Goldwasser, S. and Kilian, J., *Primality testing using elliptic curves*, In J. ACM 46 (1999) 450-472.
9. Grini, A., Chillali, A. & Mouanis, H., *The Binary Operations Calculus in $H^2_{a,d}$*, Boletim da Sociedade Paranaense de Matematica 40 (2022) 1–6.
10. Grini, A., Chillali, A., El Fadil, L. & Mouanis, H., *Twisted Hessian curves over the ring $F_q[e]$, $e^2 = 0$*, International Journal of Computer Aided Engineering and Technology 18 (2023) 181-189.
11. Grini, A., Chillali, A. & Mouanis, H., *Cryptography over twisted Hessian curves of the ring $F_q[e]$, $e^2 = 0$*, Advances in Mathematics: Scientific Journal 10 (2021) 235-243.
12. Grini, A., Chillali, A. & Mouanis, H., *A new cryptosystem based on a twisted Hessian curve $H^4_{a,d}$*, Journal of Applied Mathematics and Computing 68 (2022) 2667-2683.
13. 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, Springer 237 (2022) 351-363.
14. Joye, M., Tibouchi, M., Vergnaud, D., *Huff's model for elliptic curves*, Hanrot, G., Morain, F., Thome, E. eds. Algorithmic Number Theory (ANTS-IX) Lecture Notes in Computer Science, Springer 6197 (2010) 234-250.
15. Koblitz, N. , *Elliptic curve cryptosystems*, Math. Comp. 48 (1987) 203-209.
16. Lenstra, H. W., *Jr. Factoring integers with elliptic curves*, Ann. Math. **126** (198) 649-673.
17. Montgomery, P. L., *Speeding up the Pollard and elliptic curve methods of factorization*, Mathematics of Computation 48 (1987) 243-264.
18. Miller, V.S., *Use of elliptic curves in cryptography*, H. C. Williams, editor, Advances in Cryptology CRYPTO 85 218 of Lect. Notes Comput. Sci. Springer (1986) 417-426.

Abdelhakim Chillali,
Department of Mathematics,
Sidi Mohamed Ben Abdellah University, FP, LSI, Taza,
Morocco.
E-mail address: abdelhakim.chillali@usmba.ac.ma

and

Moha Ben Taleb El Hamam,
Department of Mathematics,
Sidi Mohamed Ben Abdellah University, Faculty of Science Dhar El Mahraz-Fez,
Morocco.
E-mail address: mohaelhomam@gmail.com

and

Abdelâli Grini,
Department of Mathematics,
Sidi Mohamed Ben Abdellah University, Faculty of Science Dhar El Mahraz-Fez,
Morocco.
E-mail address: aligrini@gmail.com