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

(3s.) **v. 2024 (42)** : 1–8.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.62308

Classification of the elements of the twisted Hessian curves in the ring $\mathbb{F}_q[e], e^3 = e^2$

Moha Ben Taleb El Hamam , Abdelhakim Chillali and Lhoussain El Fadil

ABSTRACT: Let $\mathbb{F}_q$ denote the finite field of q elements, where q is a prime power. In this paper, we study the twisted Hessian curves denoted $H_{a,d}(\mathbb{F}_q[e])$ over the ring $\mathbb{F}_q[e]$, e is in an algebraic extension of $\mathbb{F}_q$ such that $e^3 = e^2$ and $(a, d) \in (\mathbb{F}_q[e])^2$. More precisely, we study some arithmetical properties of this ring and using the Twisted Hessian equation, we define the twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$. This work study the twisted Hessian curve helped us to define two twisted Hessian over the finite field $\mathbb{F}_q$. We end this paper by giving the classification of the elements in $H_{a,d}(\mathbb{F}_q[e])$.

Key Words: Twisted Hessian curves, Finite ring, Finite field, Local ring, Cryptography.

Contents

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. In [10], Elhamam et al. studied the binary Edwards curves on the ring $\mathbb{F}_{2^n}[e], e^2 = e$. Furthermore, they studied the twisted Edwards curves over the ring $\mathbb{F}_q[e], e^2 = e$ (see [8]) and studied the twisted Edwards curves over the ring $\mathbb{F}_q[e], e^2 = 0$ (see [9]). In [1], Bernstein and his coautors have studied the twisted Hessian curves $H_{a,d}(\mathbb{K})$ defined over a field $\mathbb{K}$. In [6], Grini et al studied the Twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$ defined over the local ring $\mathbb{F}_q[e] := \mathbb{F}_q[X]/(X^2)$, where $e^2 = 0$ and $(a, b) \in (\mathbb{F}_q[e])^2$. In [7], Elhamam et al studied the twisted Hessian curves on the ring $\mathbb{F}_q[e] := \mathbb{F}_q[X]/(X^2 - X)$, where $e^2 = e$. In the present work, we study the twisted Hessian curves on the ring $\mathbb{F}_q[X]/(X^3 - X^2)$. Our main objective is the continuation of our previous work. The motivation for this work is the search for new groups of points of a twisted Hessian curve over finite rings. The plan of this paper is as follows. In the second section, we collect some preliminaries. In Section 3, we define the twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$. The study of its discriminant and its twisted Hessian equation, allowed us to define two Twisted Hessian curves $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ defined over the finite field $\mathbb{F}_q$, where π_0 and π_1 are two surjective morphisms of rings defined by:

$$\begin{array}{rccc} \pi_0 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e + x_2 e^2 & \mapsto & x_0 \end{array}$$

and

$$\begin{array}{rccc} \pi_1 & : & \mathbb{F}_q[e] & \to & \mathbb{F}_q \\ & & x_0 + x_1 e + x_2 e^2 & \mapsto & x_0 + x_1 + x_2 \end{array}.$$

After that, in Section 4, we classified the elements of $H_{a,d}(\mathbb{F}_q[e])$.

2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted January 29, 2022. Published July 07, 2022

2. The ring $\mathbb{F}_q[e], e^3 = e^2$

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 $\mathbb{F}_q[e], e^3 = e^2$ can be constructed as an extension of the ring $\mathbb{F}_q$ by using the quotient ring of $\mathbb{F}_q[X]$ by the polynomial $X^3 - X^2$. An element $X \in \mathbb{F}_q[e]$ is represented by $X = x_0 + x_1e + x_2e^2$ where $(x_0, x_1, x_2) \in (\mathbb{F}_q)^3$. The arithmetical operations in $\mathbb{F}_q[e]$ can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

$$X + Y = (x_0 + y_0) + (x_1 + y_1)e + (x_2 + y_2)e^2,$$

$$X \cdot Y = (x_0y_0) + (x_0y_1 + x_1y_0)e + (x_2y_0 + (x_1 + x_2)y_1 + (x_0 + x_1 + x_2)y_2)e^2,$$

where $X = x_0 + x_1e + x_2e^2$ and $Y = y_0 + y_1e + y_2e^2$. We refer the reader to [3], where the authors have proved the following facts:

1. $(\mathbb{F}_q[e], +, .)$ is a finite unitary commutative ring.
2. $\mathbb{F}_q[e]$ is an $\mathbb{F}_q$-vector space of dimension 3 with $\mathbb{F}_q$-basis $\{1, e, e^2\}$.
3. $X \cdot Y = x_0y_0 + \delta_{XY}e + ((x_0 + x_1 + x_2)(y_0 + y_1 + y_2) - x_0y_0 - \delta_{XY})e^2$, where: $\delta_{XY} = (x_0 + x_1)(y_0 + y_1) - x_0y_0 - x_1y_1$.
4. $X^2 = x_0^2 + \delta_{X^2}e + ((x_0 + x_1 + x_2)^2 - (x_0 + x_1)^2 + x_1^2)e^2$, where: $\delta_{X^2} = \delta_{XX}$.
5. $X^3 = x_0^3+\delta_{X^3}e+((x_0+x_1+x_2)^3-(x_0+x_1)^3+x_1^3+3x_0x_1^2)e^2$, where: $\delta_{X^3} = (x_0+x_1)^3-x_0^3-x_1^3-3x_0x_1^2$
6. Let $X = x_0 + x_1e + x_2e^2 \in \mathbb{F}_q[e]$, then $X \in (\mathbb{F}_q[e])^\times$ if and only if $x_0 \neq 0$ and $x_0 + x_1 + x_2 \neq 0$. The inverse is given by:
$$X^{-1} = x_0^{-1} - x_1x_0^{-2}e + ((x_0 + x_1 + x_2)^{-1} + x_1x_0^{-2} - x_0^{-1})e^2.$$
7. Let $X \in \mathbb{F}_q[e]$, then X is not invertible if and only if $X = xe + ye^2$ or $X = x + ye - (x + y)e^2$, where $(x, y) \in \mathbb{F}_q^2$.
8. $\mathbb{F}_q[e]$ is a non local ring.
9. π_0 and π_1 are two surjective morphisms of rings.

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

Let X, Y, Z, a and d be in the ring $\mathbb{F}_q[e], e^3 = e^2$ such that $X = x_0 + x_1e + x_2e^2$, $Y = y_0 + y_1e + y_2e^2$, $Z = z_0+z_1e+z_2e^2$, $a = a_0+a_1e+a_2e^2$ and $d = d_0+d_1e+d_2e^2$ where $x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2, a_0, a_1, a_2$, d_0, d_1 and d_2 are in $\mathbb{F}_q$. We define a twisted Hessian 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:

$$aX^3 + Y^3 + Z^3 = dXYZ,$$

where the discriminant $\Delta = a(27a - d^3)$ is invertible in $\mathbb{F}_q[e]$. We denote these curves by: $H_{a,d}(\mathbb{F}_q[e]) = \{[X : Y : Z] \in P^2(\mathbb{F}_q[e]) : aX^3 + Y^3 + Z^3 = dXYZ\}$.

Proposition 3.1. *Let* $\Delta_0 = a_0(27a_0 - d_0^3)$ *and* $\Delta_1 = (a_0 + a_1 + a_2)(27(a_0 + a_1 + a_2) - (d_0 + d_1 + d_2)^3)$, *then*

$$\Delta = \Delta_0 + (27\delta_{a^2} - a_0\delta_{d^3} - a_1d_0^3)e + (\Delta_1 - \Delta_0 - 27\delta_{a^2} + a_0\delta_{d^3} + a_1d_0^3)e^2,$$

$\pi_0(\Delta) = \Delta_0$ *and* $\pi_1(\Delta) = \Delta_1$.

Proof. We have:

$$\begin{aligned}
\Delta &= a(27a - d^3)\\
&= 27a^2 - ad^3\\
&= 27[a_0^2 + \delta_{a^2}e + ((a_0+a_1+a_2)^2 - (a_0+a_1)^2 + a_1^2)e^2]\\
&\quad - (a_0 + a_1e + a_2e^2)[d_0^3 + \delta_{d^3}e + ((d_0+d_1+d_2)^3 - (d_0+d_1)^3 + d_1^3 + 3d_0d_1^2)e^2]\\
&= 27a_0^2 + 27\delta_{a^2}e + 27(a_0+a_1+a_2)^2e^2 - 27(a_0+a_1)^2e^2 + 27a_1^2e^2 - a_0d_0^3 - (a_0\delta_{d^3} + a_1d_0^3)e -\\
&\quad (a_0+a_1+a_2)(d_0+d_1+d_2)^3e^2 + a_0d_0^3e^2 + a_0\delta_{d^3}e^2 + a_1d_0^3e^2\\
&= 27a_0^2 - a_0d_0^3 + (27\delta_{a^2} - a_0\delta_{d^3} - a_1d_0^3)e +\\
&\quad [27(a_0+a_1+a_2)^2 - (a_0+a_1+a_2)(d_0+d_1+d_2)^3 - 27(a_0+a_1)^2\\
&\quad + 27a_1^2 + a_0d_0^3 + a_0\delta_{d^3} + a_1d_0^3]e^2\\
&= \Delta_0 + (27\delta_{a^2} - a_0\delta_{d^3} - a_1d_0^3)e + (\Delta_1 - \Delta_0 - 27\delta_{a^2} + a_0\delta_{d^3} + a_1d_0^3)e^2.
\end{aligned}$$

Which gives the results.

□

Corollary 3.2. *Δ is invertible in $\mathbb{F}_q[e]$ if and only if $\Delta_0 \neq 0$ and $\Delta_1 \neq 0$.*

Using Corollary 3.2, if Δ is invertible in $\mathbb{F}_q[e]$, then $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ and $H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ are two twisted Hessian curves over the finite field $\mathbb{F}_q$, and we notice:

$$H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) = \{[x:y:z] \in P^2(\mathbb{F}_q) \mid a_0x^3 + y^3 + z^3 = d_0xyz\},$$

$$H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) = \{[x:y:z] \in P^2(\mathbb{F}_q) \mid (a_0+a_1+a_2)x^3 + y^3 + z^3 = (d_0+d_1+d_2)xyz\}.$$

Proposition 3.3. *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 $[\pi_0(X):\pi_0(Y):\pi_0(Z)] \in P^2(\mathbb{F}_q)$ and $[\pi_1(X):\pi_1(Y):\pi_1(Z)] \in P^2(\mathbb{F}_q)$.*

Proof. Suppose that $[X:Y:Z] \in P^2(\mathbb{F}_q[e])$, then there exists $(U,V,W) \in (\mathbb{F}_q[e])^3$ 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 $x_0 + x_1 + x_2$:
a) If $x_0 + x_1 + x_2 \neq 0$, then X is invertible in $\mathbb{F}_q[e]$, so $[X:Y:Z] \in P^2(\mathbb{F}_q[e])$.
b) If $x_0 + x_1 + x_2 = 0$, then $y_0 + y_1 + y_2 \neq 0$ or $z_0 + z_1 + z_2 \neq 0$.
i) If $y_0 + y_1 + y_2 \neq 0$, then $x_0 + x_1e + (y_0 + y_1 + y_2 - x_0 - x_1)e^2 = X + e^2Y \in (\mathbb{F}_q[e])^\times$, so there exists $U \in \mathbb{F}_q[e] : UX + e^2UY = 1$, hence $[X:Y:Z] \in P^2(\mathbb{F}_q[e])$.
ii) If $z_0 + z_1 + z_2 \neq 0$ then $X + e^2Z \in (\mathbb{F}_q[e])^\times$, so $[X:Y:Z] \in P^2(\mathbb{F}_q[e])$.
In the case where $y_0 \neq 0$ or $z_0 \neq 0$, we follow the same proof.

□

Let $f_{a,d}(X,Y,Z) = aX^3 + Y^3 + Z^3 - dXYZ$.

Proposition 3.4. *Let X, Y and Z in $\mathbb{F}_q[e]$, then the point $[X:Y:Z]$ is a solution of the twisted Hessian equation in $H_{a,d}(\mathbb{F}_q[e])$ if and only if $[\pi_i(X):\pi_i(Y):\pi_i(Z)]$ is a solution of the same equation in $H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$, where $i \in \{0,1\}$ and*

$$x_1\frac{\partial f_{a_0,d_0}(x_0,y_0,z_0)}{\partial x_0} + y_1\frac{\partial f_{a_0,d_0}(x_0,y_0,z_0)}{\partial y_0} + z_1\frac{\partial f_{a_0,d_0}(x_0,y_0,z_0)}{\partial z_0} = d_1x_0y_0z_0 - a_1x_0^3.$$

Proof. We have:

$$\begin{aligned}
aX^3 &= (a_0+a_1e+a_2e^2)(x_0+x_1e+x_2e^2)^3\\
&= (a_0+a_1e+a_2e^2)[x_0^3+\delta_{X^3}e+((x_0+x_1+x_2)^3-(x_0+x_1)^3+x_1^3+3x_0x_1^2)e^2]\\
&= a_0x_0^3+(a_0\delta_{X^3}+a_1x_0^3)e+[(a_0+a_1+a_2)x_0^3+(a_0+a_1+a_2)\delta_{X^3}\\
&\quad+(a_0+a_1+a_2)(x_0+x_1+x_2)-(a_0+a_1+a_2)(x_0+x_1)^3+(a_0+a_1+a_2)x_0^3\\
&\quad+(a_0+a_1+a_2)x_0x_1^2-a_0x_0^3-a_0\delta_{X^3}-a_1x_0^3]e^2\\
&= a_0x_0^3+(a_0\delta_{X^3}+a_1x_0^3)e+[(a_0+a_1+a_2)(x_0+x_1+x_2)^3-a_0x_0^3-a_0\delta_{X^3}-a_1x_0^3]e^2,\\
Y^3 &= y_0^3+\delta_{Y^3}e+((y_0+y_1+y_2)^3-(y_0+y_1)^3+y_1^3+3y_0y_1^2)e^2,\\
Z^3 &= z_0^3+\delta_{Z^3}e+((z_0+z_1+z_2)^3-(z_0+z_1)^3+z_1^3+3z_0z_1^2)e^2,\\
dXYZ &= (d_0+d_1e+d_2e^2)(x_0+x_1e+x_2e^2)(y_0+y_1e+y_2e^2)(z_0+z_1e+z_2e^2)\\
&= d_0x_0y_0z_0+(d_0x_0y_0z_1+d_0x_0y_1z_0+d_0x_1y_0z_0+d_1x_0y_0z_0)e+\\
&\quad[(d_0+d_1+d_2)(x_0+x_1+x_2)(y_0+y_1+y_2)(z_0+z_1+z_2)-d_0x_0y_0z_0-d_0x_0y_0z_1\\
&\quad-d_0x_0y_1z_0-d_0x_1y_0z_0-d_1x_0y_0z_0]e^2,
\end{aligned}$$

so $f_{a,d}(X,Y,Z)=C+Be+Ae^2$, with:

$$\begin{aligned}
C &= a_0x_0^3+y_0^3+z_0^3-d_0x_0y_0z_0 = f_{a_0,d_0}(x_0,y_0,z_0),\\
B &= a_1x_0^3-d_1x_0y_0z_0+x_1\frac{\partial f_{a_0,d_0}}{\partial x_0}+y_1\frac{\partial f_{a_0,d_0}}{\partial y_0}+z_1\frac{\partial f_{a_0,d_0}}{\partial z_0},\\
A &= f_{a_0+a_1+a_2,d_0+d_1+d_2}(x_0+x_1+x_2,y_0+y_1+y_2,z_0+z_1+z_2)-B-C.
\end{aligned}$$

Or $\{1,e,e^2\}$ a basis of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[e]$, then: $aX^3+Y^3+Z^3=dXYZ$ if and only if
- $a_0x_0^3+y_0^3+z_0^3=d_0x_0y_0z_0$,
- $(a_0+a_1+a_2)(x_0+x_1+x_2)^3+(y_0+y_1+y_2)^3+(z_0+z_1+z_2)^3=(d_0+d_1+d_2)(x_0+x_1+x_2)(y_0+y_1+y_2)(z_0+z_1+z_2)$ and
- $x_1\frac{\partial f_{a_0,d_0}}{\partial x_0}+y_1\frac{\partial f_{a_0,d_0}}{\partial y_0}+z_1\frac{\partial f_{a_0,d_0}}{\partial z_0}=d_1x_0y_0z_0-a_1x_0^3$.

□

From the Propositions 3.1, 3.3 and 3.4, we deduce the next theorem.

Theorem 3.5. *Let X, Y and Z in $\mathbb{F}_q[e]$, then*
$[X:Y:Z]\in H_{a,d}(\mathbb{F}_q[e])$ *if and only if* $[\pi_i(X):\pi_i(Y):\pi_i(Z)]\in H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$, *for* $i\in\{0,1\}$, *and* $B=0$.

Corollary 3.6. *For $i\in\{0,1\}$, the mapping $\tilde{\pi}_i$ given by:*

$$\begin{array}{rccc}
\tilde{\pi}_i & : & H_{a,d}(\mathbb{F}_q[e]) & \to & H_{\pi_i(a),\pi_i(d)}(\mathbb{F}_q)\\
 & & [X:Y:Z] & \mapsto & [\pi_i(X):\pi_i(Y):\pi_i(Z)]
\end{array}$$

is well defined.

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

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

□

4. Classification of elements in $H_{a,d}(\mathbb{F}_q[e])$

Let $H_{a,d}(\mathbb{F}_q[e])$ be the twisted Hessian curve $aX^3 + Y^3 + Z^3 = dXYZ$ over the ring $\mathbb{F}_q[e]$. In the following, we assume that -3 is not a square in $\mathbb{F}_q$, and in this section we will classify the elements of the twisted Hessian curves, into three types, depending on whether the projective coordinate X is invertible or not. We have;

Proposition 4.1. *The elements of $H_{a,d}(\mathbb{F}_q[e])$, are of the form:*

1. $[1 : Y : Z]$,
2. $[0 : -1 : 1]$,
3. $[x_1e + x_2e^2 : 1 : -1 + z_1e + z_2e^2]$,
4. $[x_1e + x_2e^2 : -1 + y_1e + y_2e^2 : 1]$,
5. $[x_1 + x_2e - (x_1 + x_2)e^2 : 1 : -1 - z_1 - z_2 + z_1e + z_2e^2]$,
6. $[x_1 + x_2e - (x_1 + x_2)e^2 : -1 - y_1 - y_2 + y_1e + y_2e^2 : 1]$.

Proof. Let $P = [X : Y : Z] \in H_{a,d}(\mathbb{F}_q[e]))$, where $X = x_0 + x_1e + x_2e^2$, $Y = y_0 + y_1e + y_2e^2$ and $Z = z_0 + z_1e + z_2e^2$.
We have two cases of the projective coordinate X:
1) the first case; if X is invertible, then: $[X : Y : Z] \sim [1 : Y : Z]$.
2) the second case; if X is no invertible, in this case we have:
i) $X = x_1e + x_2e^2$, where $(x_1, x_2) \in \mathbb{F}_q^2$, then
• if $x_1 = x_2 = 0$, then $[X : Y : Z] = [0 : -1 : 1]$.
• if $x_1 \neq 0$ or $x_2 \neq 0$:
a) if Y invertible, then

$$[X : Y : Z] \sim [x_1e + x_2e^2 : 1 : -1 + z_1e + z_2e^2].$$

From the curve equation, Y and Z are symmetric, so we also have this types elements:

$$[X : Y : Z] \sim [x_1e + x_2e^2 : -1 + y_1e + y_2e^2 : 1].$$

b) if Y is not invertible, then we have:
Assume that: $Y = y_1e + y_2e^2$, then

$$[X : Y : Z] \sim [x_1e + x_2e^2 : y_1e + y_2e^2 : z_0 + z_1e + z_2e^2].$$

We have:

$$\tilde{\pi}_0([x_1e + x_2e^2 : y_1e + y_2e^2 : z_0 + z_1e + z_2e^2]) = [0 : 0 : z_0],$$

then $z_0 = 0$, so

$$\tilde{\pi}_0([x_1e + x_2e^2 : y_1e + y_2e^2 : z_0 + z_1e + z_2e^2]) = [0 : 0 : 0]$$

which is absurd. Therefore, $Y = y_1 + y_2e - (y_1 + y_2)e^2$ i.e:

$$[X : Y : Z] \sim [x_1e + x_2e^2 : y_1 + y_2e - (y_1 + y_2)e^2 : z_0 + z_1e + z_2e^2].$$

We have:

$$\tilde{\pi}_0([x_1e + x_2e^2 : y_1 + y_2e - (y_1 + y_2)e^2 : z_0 + z_1e + z_2e^2]) = [0 : y_1 : z_0],$$

then $y_1 = -1$ and $z_0 = 1$, so

$$[X : Y : Z] \sim [x_1e + x_2e^2 : -1 + y_2e - (-1 + y_2)e^2 : 1 + z_1e + z_2e^2].$$

According to the twisted equation, Z is not invertible which implies

$$[X : Y : Z] \sim [x_1e + x_2e^2 : -1 + y_2e - (-1 + y_2)e^2 : 1 + z_1e - (1 + z_1)e^2],$$

we have:

$$\tilde{\pi}_1([x_1e + x_2e^2 : -1 + y_2e - (-1 + y_2)e^2 : 1 + z_1e - (1 + z_1)e^2]) = [x_1 + x_2 : 0 : 0],$$

then $x_1 + x_2 = 0$ i:e:

$$\tilde{\pi}_1([x_1e + x_2e^2 : -1 + y_2e - (-1 + y_2)e^2 : 1 + z_1e - (1 + z_1)e^2]) = [0 : 0 : 0],$$

which is impossible.
ii) $X = x_1 + x_2e - (x_1 + x_2)e^2$, where $(x_1, x_2) \in \mathbb{F}_q^2$, then
• if $x_1 = x_2 = 0$, then $[X : Y : Z] = [0 : -1 : 1]$.
• if $x_1 \neq 0$ or $x_2 \neq 0$:
a) if Y invertible, then

$$[X : Y : Z] \sim [x_1 + x_2e - (x_1 + x_2)e^2 : 1 : -1 - z_1 - z_2 + z_1e + z_2e^2].$$

Likewise as Y and Z are symmetric, we have this types elements:

$$[X : Y : Z] \sim [x_1 + x_2e - (x_1 + x_2)e^2 : -1 - y_1 - y_2 + y_1e + y_2e^2 : 1].$$

b) if Y is not invertible, in this case we have
Assume that: $Y = y_1e + y_2e^2$, then

$$[X : Y : Z] \sim [x_1 + x_2e - (x_1 + x_2)e^2 : y_1e + y_2e^2 : z_0 + z_1e + z_2e^2].$$

According to twisted equation Z is not invertible which implies that:
$Z = z_1e + z_2e^2$ or $Z = z_1 + z_2e - (z_1 + z_2)e^2$ i.e:

$$\tilde{\pi}_0([x_1 + x_2e - (x_1 + x_2)e^2 : y_1e + y_2e^2 : z_1e + z_2e^2]) = [x_1 : 0 : 0]$$

or

$$\tilde{\pi}_1([x_1 + x_2e - (x_1 + x_2)e^2 : y_1e + y_2e^2 : z_1 + z_2e - (z_1 + z_2)e^2]) = [0 : y_1 + y_2 : 0],$$

which is absurd. So $Y = y_1 + y_1e - (y_1 + y_2)e^2$, then

$$[X : Y : Z] \sim [x_1 + x_2e - (x_1 + x_2)e^2 : y_1 + y_1e - (y_1 + y_2)e^2 : z_0 + z_1e + z_2e^2],$$

we have:

$$\tilde{\pi}_1([x_1 + x_2e - (x_1 + x_2)e^2 : y_1 + y_1e - (y_1 + y_2)e^2 : z_1 + z_2e + z_2e^2]) = [0 : 0 : z_1 + z_2 + z_2],$$

which is impossible.

□

From this proposition, we put:

$$\begin{aligned}
G_1 &= \{[1 : Y : Z] \mid a + Y^3 + Z^3 = dYZ\},\\
G_2 &= \{[x_1e + x_2e^2 : 1 : -1 + z_1e + z_2e^2] \mid [x_1 + x_2 : 1 : -1 + z_1 + z_2] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) \text{ and } B = 0\},\\
G_4 &= [x_1e + x_2e^2 : -1 + y_1e + y_2e^2 : 1] \mid [x_1 + x_2 : -1 + y_1 + y_2 : 1] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) \text{ and } B = 0\},\\
G_4 &= \{[x_1 + x_2e - (x_1 + x_2)e^2 : 1 : -1 - z_1 - z_2 + z_1e + z_2e^2] \mid\\
&\qquad [x_1 : 1 : -1 - z_1 - z_2] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \text{ and } B = 0\},\\
G_5 &= \{[x_1 + x_2e - (x_1 + x_2)e^2 : -1 - y_1 - y_2 + y_1e + y_2e^2 : 1] \mid\\
&\qquad [x_1 : -1 - y_1 - y_2 : 1] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \text{ and } B = 0\}.
\end{aligned}$$

We deduce the following corollaries.

Corollary 4.2. $H_{a,d}(\mathbb{F}_q[e]) = G_1 \cup G_2 \cup G_3 \cup G_4 \cup G_5 \cup \{[0:-1:1]\}$.

Corollary 4.3. *$\tilde{\pi}_0$ is a surjective mapping.*

Proof. Let $[x:y:z] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$, then
• if $x = 0$, then $[x:y:z] \sim [0:-1:1]$; hence $[0:-1:1]$ is an antecedent of $[0:-1:1]$.
• if $x \neq 0$, then $[x:y:z] \sim [1:y:z]$.
Let $P = [1 + x_1e - (1 + x_1)e^2 : y + (-1 - y + y_1)e + y_1e^2 : z + (1 - z - z_1)e + z_1e^2] \in H_{a,d}(\mathbb{F}_q[e])$,

we have: $\begin{cases} \tilde{\pi}_0(P) = [1:y:z] \in H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \\ \textit{and} \\ \tilde{\pi}_1(P) = [0:-1:1] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q) \\ \textit{and} \\ B = a_1 - d_1yz + x_1(3a_0 - d_0yz) + y_1(3y^2 - d_0z) + z_1(3z^2 - d_0y). \end{cases}$

Hence there exists $(x_1, y_1, z_1) \in (\mathbb{F}_q)^3$ such as $B = 0$. In fact, $3a_0 - d_0yz$, $3y^2 - d_0z$ and $3z^2 - d_0y$ are not all zero. Then there is an antecedent of $[1:y:z]$.

□

Corollary 4.4. *$\tilde{\pi}_1$ is a surjective mapping.*

Proof. Let $[x:y:z] \in H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$, then
• if $x = 0$, then $[x:y:z] \sim [0:-1:1]$, hence $[0:-1:1]$ is an antecedent of $[0:-1:1]$.
• if $x \neq 0$, then $[x:y:z] \sim [1:y:z]$, hence $[e^2 : -1 + e + ye^2 : 1 - e + ze^2]$ is an antecedent of $[1:y:z]$.

□

5. Conclusion

In [7], the authors found a bijection between the sets $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ over the ring $\mathbb{F}_q[e]$, where $e^2 = e$. In this work, we studied the twisted Hessian curves denoted $H_{a,d}(\mathbb{F}_q[e])$ over the ring $\mathbb{F}_q[e]$, where $e^3 = e^2$ and $(a, d) \in (\mathbb{F}_q[e])^2$. Furthermore, we gave a classification of elements in the twisted Hessian curves $H_{a,d}(\mathbb{F}_q[e])$ and we conclude that we have not a bijection between the sets $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$. Thus, we suggestion the following open question, which has relation ship with cryptography, is there a cyclic subgroup G of $H_{a,d}(\mathbb{F}_q[e])$ such that, $G \simeq H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$. Then, in this case, $H_{a,d}(\mathbb{F}_q[e])$ and $H_{\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times H_{\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ have the same discrete logarithm problem.

References

1. D.J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange, *Twisted Hessian Curves*, In: Lauter K., Rodrguez-Henrques F. (eds) Progress in Cryptology – LATINCRYPT 2015, Lecture Note in Computer Science, vol. **9230**, pp 269–294. Springer, Cham(2015).
2. D.J. Bernstein and T. Lange. *Faster addition and doubling on elliptic curves*. In Asiacrypt 2007 **37**, pages 29?50, 2007. http://cr.yp.to/newelliptic/newelliptic-20070906.pdf.
3. A. Boulbot, A. Chillali and A. Mouhib, *ELLIPTIC CURVES OVER THE RING $Fq[e]; e^3 = e^2$*, Gulf Journal of Mathematics, Vol. **4**, Issue 4, pp 123–129, (2016).
4. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic Curves Over the Ring R*, Bol. Soc. Paran(2020), v. **38** 3, pp 193–201, (2020).
5. M. Joye and J. Quisquater, *Hessian elliptic curves and sidechannel attacks* Cryptographic Hardware and Embedded Systems - CHES 2001', vol. 2162 of Lecture Notes in Computer Science, pp. 402–410, Springer-Verlag, 2001.
6. A. Grini, A. Chillali and H. Mouanis, *Twisted Hessian curves over the Ring $\mathbb{F}_q[e], e^2 = 0$*. International Journal of Computer Aided Engineering and Technology, (2020, to appear).
7. M.B.T. El Hamam, A. Chillali and L. El Fadil, *Twisted Hessian curves over the Ring $\mathbb{F}_q[e], e^2 = e$*. Bol. Soc. Paran, (3s.) v. 2022 (40) ISSN-0037-8712, (2022)
8. M.B.T. El Hamam, A. Chillali and L. El Fadil, *A New Addition Law in Twisted Edwards Curves on Non Local Ring*. In: Nitaj, A., Zkik, K. (eds) Cryptography, Codes and Cyber Security. I4CS 2022. Communications in Computer and Information Science, vol 1747. Springer, Cham. https://doi.org/10.1007/978-3-031-23201-5_3, 2022.

9. M.B.T. El Hamam, A. Chillali and L. El Fadil, *TWISTED EDWARDS CURVE OVER THE RING* $\mathbb{F}_q[e], e^2 = 0$. In: Tatra Mt. Math. Publ. 83 (2023), 43–50. DOI: 10.2478/tmmp-2023-0004, 2023.

10. M.B.T. El Hamam, A. Chillali and L. El Fadil, *Public key cryptosystem and binary Edwards curves on the ring* $\mathbb{F}_{2^n}[e], e^2 = e$ *for data management*. In: 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1-4, doi: 10.1109/IRASET52964.2022.9738249, 2022.

11. A. Grini, A. Chillali and H. Mouanis, *A new cryptosystem based on a twisted Hessian curve* $H^4_{a,d}$. J. Appl. Math. Comput, 2021.

12. C. Chuengsatianup, C. Martindale, *Pairing-Friendly Twisted Hessian curves* In: Chakraboty D., Iwata T. (eds) Progress in Cryptology INDOCRYPT 2018. Lecture Notes in Computer Science, vol **11356**. Springer, Cham (2018).

13. M. Joye, J. Quisquater, *Hessian elliptic curves and sidechannel attacks*. Cryptographic Hardware and Embedded Systems-CHES 2001, Lecture Notes in Computer Science, vol. 2162, Springer, pp. 402–410, (2001).

14. M. Joye and J.J. Quisquater, *Hessian elliptic curves and side-channel attacks*. In CHES 2001 **13**, pages 402–410, (2001). http://joye.site88.net/.

15. H.W. Lenstra, *Eliptic Curves and Number-Theoretic Algorithms* Processing of the International Congress of Mathematicians, Berkely, California, USA(1986).

16. H. M. Edwards. *A normal form for elliptic curves*. Bulletin of the American Mathematical Society, 44: pp. 393–422, (2007). http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html.

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

and

Lhoussain El Fadil,
Sidi Mohamed Ben Abdellah University,
FSDM, Fez, Morocco.
E-mail address: lhouelfadil2@gmail.com

and

Moha ben taleb El Hamam,
Sidi Mohamed Ben Abdellah University,
FSDM, Fez, Morocco.
E-mail address: mohaelhomam@gmail.com