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

(3s.) v. ???? (??) : 1–10.
ISSN-0037-8712 in press
doi:10.5269/bspm.62583

Twisted Hessian Curve Over a Local Ring [*]

Abdelhakim Chillali, Abdelâli Grini and Moha Ben Taleb Elhamam

ABSTRACT: In this paper, we study the twisted Hessian curve denoted $H^n_{a,d}$ over the ring $R_n = \mathbb{F}_q[X]/(X^n)$, where $\mathbb{F}_q$ is a finite field of q elements, with q is a power of a prime number $p \geq 5$ and $n \geq 5$. In a first time, we describe these curves over this ring. In addition, we prove that when p doesn't divide $\#(H_{\pi(a),\ \pi(d)})$, then $H^n_{a,d}$ is a direct sum of $H_{\pi(a),\ \pi(d)}$ and the maximal ideal of R_n, where $H_{\pi(a),\ \pi(d)}$ is the twisted Hessian curve over $\mathbb{F}_q$. Other results are deduced from, we cite the equivalence of the discrete logarithm problem on the twisted Hessian curves $H^n_{a,d}$ and $H_{\pi(a),\ \pi(d)}$, which is beneficial for cryptography and cryptanalysis as well.

Key Words: Discrete logarithm problem, elliptic curve, twisted Hessian curve, finite ring, cryptography.

Contents

1. Introduction

In 2001, Smart [15] introduced a new normal form of elliptic curves over a field $\mathbb{F}_q$ with $q \in 2+3\mathbb{Z}$. He showed that any elliptic curve over $\mathbb{F}_q$ which has a $\mathbb{F}_q$-rational point of order 3 is birationally equivalent over some extension of $\mathbb{F}_q$ to a curve with an equation of the form $X^3 + Y^3 + Z^3 = DXYZ$. Recently, Bernstein and al [1] introduced the twisted Hessian curves with an equation

$$H_{a,d} : aX^3 + Y^3 + Z^3 = dXYZ,$$

where $a, d \in \mathbb{F}_q$ and $a(27a - d^3) \neq 0$.

Elliptic curves are often used in cryptography, and this is where twisted Hessian curves have their advantages: addition, doubling and tripling can be performed faster on twisted Hessian curves than on curves given by a Weierstrass equation. This is because the addition law on twisted Hessian curves has no exceptions, whereas the addition on Weierstrass curves. The normal form proposed by Bernstein and al [1] has very desirable cryptographic properties that allow to fight against the leakage of side-channel information from the beginning, because the group law is complete and unified. Moreover, in many cases, the group law involves fewer operations, which means that the safer calculations involved can also be faster. So, the twisted Hessian curve helps to efficiently foil side-channel attacks in the context of elliptic curve cryptography. Furthermore, the operations on twisted Hessian curves are more efficient than the Weierstrass form of elliptic curves and the discrete logarithm problem is hard to solve. This makes twisted Hessian curves suitable for cryptographic applications. However, there are exponential time algorithms [10,13] that compute discrete logarithms for the cyclic subgroup of the elliptic curve. To

---

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

2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted February 19, 2022. Published October 04, 2022

ensure maximum security of the cryptographic system, the elliptic curve must be properly chosen. For this objective, we present in this paper the twisted Hessian curve over the ring $\mathbb{F}_q[X]/(X^n)$ which verifies this property because it increases the time needed to solve the discrete logarithm problem, we will prove that $\#(H^n_{a,d}) = p^{b(n-1)}\#(H_{\pi(a),\ \pi(d)})$. As a result, we can note that the time for solving the discrete logarithm problem on $H^n_{a,d}$ is greater than that of the twisted Hessian curve on a finite field.

In [5,6], we introduced these curves over the ring R_2, and in [7] we presented the cryptography over twisted Hessian curves over the same ring. In [9] we defined the twisted Hessian curve over the ring R_3 and we presented its application in cryptography, then in [8] we introduced a new cryptosystem based on a twisted Hessian curve $H^4_{a,d}$. In this article, our contribution is an extension of the twisted Hessian curve on the local ring $\mathbb{F}_q[X]/(X^n)$ for all integers $n \geq 5$. The novelty of this approach is to get a huge number of points with a smaller prime p, because we will prove that the cardinal of this twisted Hessian curve $H^n_{a,d}$ is greater than that of $H_{\pi(a),\ \pi(d)}$ and it is equal to $p^{b(n-1)} \times H_{\pi(a),\ \pi(d)}$, so we may reserve up memory once we do the calculations. Moreover, the time required to solve the discrete logarithm problem on $H^n_{a,d}$ is greater than that of the twisted Hessian curve on a finite field.

This paper is organized as follows. In Section 2, We study the arithmetic of the ring R_n, where we establish some useful results which are necessary for the rest of this paper. In the third section, we will define the twisted Hessian curves over $\mathbb{F}_q[\epsilon]$ and we will classify the elements of the twisted Hessian curve $H^n_{a,d}$. Afterwards, we will define the group law of $H^n_{a,d}$ and we will show that $H^n_{a,d}$ is a direct sum of $H_{\pi(a),\ \pi(d)}$ and the maximal ideal of R_n, when p doesn't divide $\#(H_{\pi(a),\ \pi(d)})$.
Another purpose of this paper is the application of $H^n_{a,d}$ in cryptography. Thereby, in Section 4, we deduce some cryptographic applications.

2. Arithmetic Over the Ring $\mathbb{F}_q[X]/(X^n)$

Let p be a prime number ≥ 5 such that -3 is not a square in $\mathbb{F}_p$. We consider the quotient ring $R_n = \mathbb{F}_q[X]/(X^n)$, where $\mathbb{F}_q$ is the finite field of characteristic p and q elements. Then the ring R_n can be identified by the ring $\mathbb{F}_q[\epsilon]$, $\epsilon^n = 0$. In other words,

$$R_n = \{\sum_{j=0}^{n-1} x_j\epsilon^j / x_j \in \mathbb{F}_q \ for\ j = 0...(n-1)\}.$$

Now, we will give some results concerning the ring R_n, which are useful for the rest of this work.

Let two elements in R_n represented by $X = \sum_{j=0}^{n-1} x_j\epsilon^j$ and $Y = \sum_{j=0}^{n-1} y_j\epsilon^j$ with coefficients x_j and y_j are in the field $\mathbb{F}_q$ for $(j = 0...(n-1))$.

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

$$X + Y = \sum_{j=0}^{n-1}(x_j + y_j)\epsilon^j$$

$$X.Y = \sum_{j=0}^{n-1} Z_j\epsilon^j \ where\ Z_j = \sum_{i=0}^{j} x_i y_{j-i}$$

Similar as in [2] we have the following results:

- $(R_n, +, .)$ is a finite unitary commutative ring.
- R_n is a vector space over $\mathbb{F}_q$ and has $(1, \epsilon, \epsilon^2, ...\epsilon^{n-1})$ as a basis.
- R_n is a local ring. Its maximal ideal is $M = (\epsilon) = \epsilon\mathbb{F}_q$.
- Let $Y = \sum_{j=0}^{n-1} y_j\epsilon^j$, be the inverse of the element $X = \sum_{j=0}^{n-1} x_j\epsilon^j$, then

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

Remark 2.1. *The canonical projection* π *defined by:*

$$\begin{array}{cccc} \pi & R_n & \to & \mathbb{F}_q \\ & \sum_{j=0}^{n-1} x_j \epsilon^j & \mapsto & x_0 \end{array}$$

is a surjective homomorphism of rings.

3. Twisted Hessian Curves Over the Ring R_n

Definition 3.1. *We consider the twisted Hessian curve over the ring* R_n *in the projective space* $\mathbb{P}^2(R_n)$*, which is given by the equation:* $aX^3 + Y^3 + Z^3 = dXYZ$*, where* $a, d \in R_n$ *and* $a(27a - d^3)$ *is invertible in* R_n*, and denoted by* $H^n_{a,d}$*. So we have:*

$$H^n_{a,d} = \{[X : Y : Z] \in \mathbb{P}^2(R_n) \setminus \quad aX^3 + Y^3 + Z^3 = dXYZ\}.$$

3.1. Classification of Elements of $H^n_{a,d}$

To have a clear idea of the twisted Hessian curves over the ring R_n, we can classify its elements according to their projective coordinate. This is the subject of the following proposition.

Proposition 3.2. *Every element in* $H^n_{a,d}$ *is of the form* $[1 : Y : Z]$ *(where* Y *or* $Z \in R_n \setminus M$*) or* $[X : Y : 1]$ *(where* $X \in M$*), and we write:*
$H^n_{a,d} = \{[1 : Y : Z] \in \mathbb{P}^2(R_n) \setminus a+Y^3+Z^3 = dYZ$, *and* Y *or* $Z \in R_n \setminus M\} \cup \{[X : Y : 1] \setminus aX^3+Y^3+1 = dXY$, *and* $X \in M\}$.

Proof. Let $[X : Y : Z] \in H^n_{a,d}$, where X, Y and $Z \in R_n$.

- If X is invertible, $[X : Y : Z] = [1 : X^{-1}Y : X^{-1}Z] \sim [1 : Y : Z]$. Suppose that Y and $Z \in M$; since $a + Y^3 + Z^3 = dYZ$ then $a \in M$, which is absurd. So, Y or $Z \in R_n \setminus M$.
- If X is non invertible, then $X \in M$, so $X = \sum_{j=1}^{n-1} x_j \epsilon^j$, where $x_j \in \mathbb{F}_q$. So we have two cases for Z:
  1. Z invertible : $[X : Y : Z] = [XZ^{-1} : YZ^{-1} : 1] \sim [X : Y : 1]$.
  2. Z non invertible: We have X and $Z \in M$, since $aX^3+Y^3+Z^3 = dXYZ$, then $Y^3 \in M$ and so $Y \in M$. We deduce that $[X : Y : Z]$ isn't a projective point because (X, Y, Z) isn't a primitive triple [[11], pp. 104-105].

□

In the following lemma, we show that the elements of $H^n_{a,d}$ of the form $[X : Y : 1]$ are entirely determined by their first projective coordinate X:

Lemma 3.3. *Let* $[X : Y : 1] \in H^n_{a,d}$*, where* $X \in M$*.*
If $X = \sum_{j=1}^{n-1} x_j \epsilon^j$*, then* $Y = -1 + \sum_{j=1}^{n-1} x'_j \epsilon^j$*, where* x'_j *are function of* $x_1, ..., x_{n-1}$*, and is denoted by* Y_X*.*

Proof. Let $[X : Y : 1] \in H^n_{a,d}$, where $X = \sum_{j=1}^{n-1} x_j \epsilon^j$, $Y = \sum_{j=0}^{n-1} y_j \epsilon^j$, $a = \sum_{j=0}^{n-1} a_j \epsilon^j$ and $d = \sum_{j=0}^{n-1} d_j \epsilon^j$ then,

$$X^3 = \sum_{|\overrightarrow{k}|=3} C_3^{|\overrightarrow{k}|} \prod_{j=1}^{n-1} (x_j \epsilon^j)^{k_j}$$

such that $|\overrightarrow{k}| = \sum_{j=1}^{n-1} k_j$

$$Y^3 = \sum_{|\overrightarrow{t}|=3} C_3^{|\overrightarrow{t}|} \prod_{j=0}^{n-1} (y_j \epsilon^j)^{t_j}$$

such that $\mid \overrightarrow{t} \mid = \sum_{j=0}^{n-1} t_j$

$$XY = \sum_{j=0}^{n-1} \sum_{i=0}^{j} x_i y_{j-i} \epsilon^j$$

$$dXY = \sum_{t=0}^{n-1} \sum_{k=0}^{t} d_k \sum_{i=0}^{t-k} x_i y_{t-k-i} \epsilon^t$$

So, $aX^3 + Y^3 + Z^3 = dXYZ \Leftrightarrow$

$$\sum_{j=0}^{n-1} a_j \epsilon^j \sum_{\mid \overrightarrow{k} \mid = 3} C_3^{\mid \overrightarrow{k} \mid} \prod_{i=1}^{n-1} (x_i \epsilon^i)^{k_i} + \sum_{\mid \overrightarrow{t} \mid = 3} C_3^{\mid \overrightarrow{t} \mid} \prod_{i=0}^{n-1} (y_i \epsilon^i)^{t_i} + 1 = \sum_{t=0}^{n-1} \sum_{k=0}^{t} d_k \sum_{i=0}^{t-k} x_i y_{t-k-i} \epsilon^t$$

By multiplying both sides of the last equation by ϵ^{n-2} we find $y_0 = -1$ and $y_1 = -\frac{1}{3} d_0 x_1$. And the same we are multiplying both sides of the equation by ϵ^{n-k-1} we find by identification of the coefficients of ϵ^{n-1} in both sides that y_k is a function of $x_1, ..., x_{n-1}$.

□

Corollary 3.4. *Let $X \in M$, then there exists a unique $Y \in M$ such that $[X : -1 + Y : 1] \in H_{a,d}^n$.*

From lemma 3.3, we deduce that Y exists such that $[X : -1 + Y : 1] \in H_{a,d}^n$.
Let prove that Y is unique.
Suppose that there exist $Y, Y' \in M$, such that: $[X : -1 + Y : 1] \in H_{a,d}^n$ and $[X : -1 + Y' : 1] \in H_{a,d}^n$.
We have :

$$\begin{cases} aX^3 + (Y-1)^3 + 1 = dX(Y-1) \\ aX^3 + (Y'-1)^3 + 1 = dX(Y'-1), \end{cases}$$

this implies that,

$$(Y-1)^3 - (Y'-1)^3 = dX(Y - Y')$$

then,

$$(Y - Y')(3 + Y^2 - 2Y + YY' - Y - Y' + Y'^2 - 2Y' - dX) = 0$$

Or $Y^2 - 2Y + YY' - Y - Y' + Y'^2 - 2Y' - dX \in M$ thus, $Y = Y'$.

3.2. Group Law Over $H_{a,d}^n$

After classifying the elements of twisted Hessian curve $H_{a,d}^n$ we will define the group law on it. We firstly consider the mapping defined by:

$$\begin{array}{cccc} \tilde{\pi} : & H_{a,d}^n & \rightarrow & H_{\pi(a),\ \pi(d)} \\ & [X : Y : Z] & \mapsto & [\pi(X) : \pi(Y) : \pi(Z)] \end{array}$$

where $H_{\pi(a),\ \pi(d)}$ is the twisted Hessian curve over $\mathbb{F}_q$.

Then, we are ready to define the group law on $H_{a,d}^n$ by the following theorem:

Theorem 3.5. *Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in $H_{a,d}^n$.*

1. *Define:*

$$X_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1,$$

$$Y_3 = Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1,$$

$$Z_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1.$$

If $\tilde{\pi}([X_3 : Y_3 : Z_3]) \neq [0 : 0 : 0]$ then $P + Q = [X_3 : Y_3 : Z_3]$.

2. Define:

$$X_3' = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2,$$
$$Y_3' = Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2,$$
$$Z_3' = a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2.$$

If $\tilde{\pi}([X_3' : Y_3' : Z_3']) \neq [0:0:0]$ *then* $P + Q = [X_3' : Y_3' : Z_3']$.

Proof. We can prove the theorem by using [[1], Theorem 3.2 and 4.2]. ☐

Corollary 3.6. $(H^n_{a,d}, +)$ *is a commutative group with unity* $[0 : -1 : 1]$.

Corollary 3.7. *Let* $[X_1 : Y_{X_1} : 1]$ *and* $[X_2 : Y_{X_2} : 1]$ *two points in* $H^n_{a,d}$, *then:*

$$[X_1 : Y_{X_1} : 1] + [X_2 : Y_{X_2} : 1] = [X_3 : Y_{X_3} : 1]$$

such that:

$$X_3 = \frac{X_1 - Y_{X_1}^2 X_2 Y_{X_2}}{a X_2^2 X_1 Y_{X_1} - Y_{X_2}}$$

$$Y_{X_3} = \frac{Y_{X_2}^2 Y_{X_1} - a X_1^2 X_2}{a X_2^2 X_1 Y_{X_1} - Y_{X_2}}$$

Proof. By theorem 3.5, we deduce:

$$[X_1 : Y_{X_1} : 1] + [X_2 : Y_{X_2} : 1] = [A : B : C]$$

such that:

$$A = X_1 - Y_{X_1}^2 X_2 Y_{X_2}$$

$$B = Y_{X_2}^2 Y_{X_1} - a X_1^2 X_2$$

$$C = a X_2^2 X_1 Y_{X_1} - Y_{X_2}$$

so C is invertible, then the results. ☐

The group law is now defined on $H^n_{a,d}$, we will give some of its properties and homomorphisms defined on it.

Theorem 3.8. *Let* $a = \tilde{a} + a_{n-1}\epsilon^{n-1}$, $d = \tilde{d} + d_{n-1}\epsilon^{n-1}$, $X = \tilde{X} + X_{n-1}\epsilon^{n-1}$, $Y = \tilde{Y} + Y_{n-1}\epsilon^{n-1}$ *and* $Z = \tilde{Z} + Z_{n-1}\epsilon^{n-1}$ *be elements of* R_n, *which verified the equation:*

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

Then

$$\tilde{a}\tilde{X}^3 + \tilde{Y}^3 + \tilde{Z}^3 = \tilde{d}\tilde{X}\tilde{Y}\tilde{Z} + (D + AX_{n-1} + BY_{n-1} + CZ_{n-1})\epsilon^{n-1},$$

where

$$\begin{aligned} D &= d_{n-1}X_0Y_0Z_0 - a_{n-1}X_0^3, \\ A &= d_0Y_0Z_0 - 3a_0X_0^2, \\ B &= d_0X_0Z_0 - 3Y_0^2, \\ C &= d_0Y_0X_0 - 3Z_0^2. \end{aligned}$$

Proof. Let $a = \tilde{a} + a_{n-1}\epsilon^{n-1}$, $d = \tilde{d} + d_{n-1}\epsilon^{n-1}$, $X = \tilde{X} + X_{n-1}\epsilon^{n-1}$, $Y = \tilde{Y} + Y_{n-1}\epsilon^{n-1}$ and $Z = \tilde{Z} + Z_{n-1}\epsilon^{n-1}$ be elements of R_n. Then:

$$\begin{array}{rcl} Y^3 & = & \tilde{Y}^3 + 3\tilde{Y}^2 Y_{n-1}\epsilon^{n-1} \\ Z^3 & = & \tilde{Z}^3 + 3\tilde{Z}^2 Z_{n-1}\epsilon^{n-1} \\ aX^3 & = & \tilde{a}\tilde{X}^3 + 3\tilde{a}\tilde{X}^2 X_{n-1}\epsilon^{n-1} + a_{n-1}\tilde{X}^3\epsilon^{n-1} \\ dXYZ & = & \tilde{d}\tilde{X}\tilde{Y}\tilde{Z} + (d_{n-1}\tilde{X}\tilde{Y}\tilde{Z} + \tilde{d}\tilde{X}\tilde{Y}Z_{n-1} + \tilde{d}\tilde{X}Y_{n-1}\tilde{Z} + \tilde{d}\tilde{Y}\tilde{Z}X_{n-1})\epsilon^{n-1}. \end{array}$$

If $[X : Y : Z] \in H^n_{a,d}$, then

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

so,

$$\begin{array}{rcl} \tilde{a}\tilde{X}^3 + \tilde{Y}^3 + \tilde{Z}^3 & = & \tilde{d}\tilde{X}\tilde{Y}\tilde{Z} + (d_{n-1}X_0Y_0Z_0 - a_{n-1}X_0^3 + (d_0Y_0Z_0 - 3a_0X_0^2)X_{n-1} + \\ & & (d_0X_0Z_0 - 3Y_0^2)Y_{n-1} + (d_0Y_0X_0 - 3Z_0^2)Z_{n-1})\epsilon^{n-1}, \end{array}$$

thus,

$$\tilde{a}\tilde{X}^3 + \tilde{Y}^3 + \tilde{Z}^3 = \tilde{d}\tilde{X}\tilde{Y}\tilde{Z} + (D + AX_{n-1} + BY_{n-1} + CZ_{n-1})\epsilon^{n-1},$$

where,

$$\begin{array}{rcl} D & = & d_{n-1}X_0Y_0Z_0 - a_{n-1}X_0^3, \\ A & = & d_0Y_0Z_0 - 3a_0X_0^2, \\ B & = & d_0X_0Z_0 - 3Y_0^2, \\ C & = & d_0Y_0X_0 - 3Z_0^2. \end{array}$$

□

Lemma 3.9. *The mapping*

$$\begin{array}{rccl} \tilde{\pi} : & H^n_{a,d} & \rightarrow & H_{\pi(a),\pi(d)} \\ & [X : Y : Z] & \mapsto & [\pi(X) : \pi(Y) : \pi(Z)] \end{array}$$

is a surjective homomorphism of groups.

Proof. From Theorem 3.8; $\tilde{\pi}$ is well defined, and from Theorem 3.5 we prove that $\tilde{\pi}$ is a homomorphism. Let $[X_0 : Y_0 : Z_0] \in H_{\pi(a),\pi(d)}$, then there exists $[X : Y : Z] \in H^n_{a,d}$ such that $\tilde{\pi}([X : Y : Z]) = [X_0 : Y_0 : Z_0]$.

Indeed, by Theorem 3.8, we have

$$D = -(AX_{n-1} + BY_{n-1} + CZ_{n-1})$$

Coefficients $-A$, $-B$ and $-C$ are partial derivative of a function

$$F(X, Y, Z) = aX^3 + Y^3 + Z^3 - dXYZ$$

at the point (X_0, Y_0, Z_0), cannot be all three null. At last, we will then conclude that $[X_{n-1} : Y_{n-1} : Z_{n-1}]$. Finally, $\tilde{\pi}$ is a surjective.

□

Since $[X : Y_X : 1]$ is entirely determined by its first projective coordinate X. So, we have to define another law on M by the following definition:

Definition 3.10. *We define on the set M the law $*$ by:*

$$X_1 * X_2 \quad = \quad \frac{X_1 - Y_{X_1}^2 X_2 Y_{X_2}}{aX_2^2 X_1 Y_{X_1} - Y_{X_2}}$$

$*$ is well defined, so from the corollary 3.4 we have for $X \in M$, then there exists a unique $Y \in M$ such that $[X : -1 + Y : 1] \in H_{a,d}^n$.

Lemma 3.11. *$(M, *)$ is an abelian group with 0 as unity.*

From Theorem 3.5, we deduce the following lemma:

Corollary 3.12. *Let $X_1, X_2 \in M$ we have :*

$$Y_{X_1 * X_2} \quad = \quad \frac{Y_{X_2}^2 Y_{X_1} - aX_1^2 X_2}{aX_2^2 X_1 Y_{X_1} - Y_{X_2}}$$

Lemma 3.13. *The mapping*

$$\begin{array}{rccc} \psi : & (M, *) & \rightarrow & (H_{a,d}^n, +) \\ & X & \mapsto & [X : Y_X : 1] \end{array}$$

is an injective homomorphism of groups.

Proof. From Lemma 3.3, we deduce that ψ is well defined.
We have $\psi(0) = [0 : -1 : 1]$ and for all X_1 and $X_2 \in M$:

$$\psi(X_1 * X_2) \quad = \quad [X_1 * X_2 : Y_{X_1 * X_2} : 1]$$

From corollary 3.7 and corollary 3.12 we deduce that:

$$[X_1 * X_2 : Y_{X_1 * X_2} : 1] = [X_1 : Y_{X_1} : 1] + [X_2 : Y_{X_2} : 1],$$

then ψ is a group homomorphism.

It remains to prove that ψ is injective. Let $X \in ker(\psi)$, then $\psi(X) = [X : Y_X : 1] = [0 : -1 : 1]$ therefore $X = 0$. This proves that ψ is injective. ☐

From Proposition 3.2 and Lemma 3.3 we deduce the following lemma:

Lemma 3.14. *$Ker\ (\tilde{\pi}) = Im\ (\psi)$.*

Proof. Let $[X : Y_X : 1] \in Im(\psi)$, then

$$\tilde{\pi}([X : Y_X : 1]) = [0 : -1 : 1]$$

and so, $Im\psi \subset Ker\ \tilde{\pi}$.
Conversely, let $[X : Y : Z] \in Ker\ \tilde{\pi}$, then

$$[x_0 : y_0 : z_0] = [0 : -1 : 1],$$

so Z is invertible, and from Proposition 3.2: $X \in M$ so, $[X : Y : Z] \sim [X : Y : 1]$; and from Lemma 3.3

$$[X : Y : Z] \sim [X : Y_X : 1] \in Im\ \psi.$$

So $Ker\ \tilde{\pi} \subset Im\psi$.
Finally, $Ker\ \tilde{\pi} = Im\psi$. ☐

Corollary 3.15. *The subset* $G = ker(\tilde{\pi})$ *is a subgroup of* $H^n_{a,d}$ *and every element* P *in* G *there exists an integer* k *such that* $p^k P = [0:\ -1:\ 1]$.

Proof. Since ψ is injective, then $M \simeq Im\ (\psi) = Ker\ (\tilde{\pi})$, and $\#(M) = (p^b)^{n-1}$ this prove the corollary. □

From Lemmas 3.9, 3.13 and 3.14, we deduce the following corollary:

Corollary 3.16. *The short sequence*

$$\begin{tikzcd} O \arrow[r] & Ker\tilde{\pi} \arrow[r, "j"] & H^n_{a,d} \arrow[r, "\tilde{\pi}"] & H_{\pi(a),\ \pi(d)} \arrow[r] & 0 \end{tikzcd}$$

is exact, where j *is the canonical injection.*

Now, we prove that when p doesn't divide the cardinality of $H_{\pi(a),\ \pi(d)}$, then $H_{\pi(a),\ \pi(d)}$ is a direct factor of $H^n_{a,d}$, and we deduce from there some useful results.

Theorem 3.17. *Let* $N = \#(H_{\pi(a),\ \pi(d)})$ *the cardinality of* $H_{\pi(a),\ \pi(d)}$. *If* p *doesn't divide* N, *then the short exact sequence:*

$$\begin{tikzcd} O \arrow[r] & Ker\tilde{\pi} \arrow[r, "i"] & H^n_{a,d} \arrow[r, "\tilde{\pi}"] & H_{\pi(a),\ \pi(d)} \arrow[r] & 0 \end{tikzcd}$$

is split.

Proof. Suppose that p doesn't divide N, then p^k doesn't divide N (where k is defined in Corollary 3.15), so there exists an integer λ such that $N\lambda = 1\ mod\ p^k$. Therefore, there exists an integer α such that $1 - N\lambda = p^k\ \alpha$.
Let f the homomorphism defined by:

$$\begin{array}{rccc} f: & H^n_{a,d} & \to & H^n_{a,d} \\ & P & \mapsto & (1-N\lambda)P \end{array}$$

Then, there exists a unique morphism g, such that the following diagram commutes:

$$\begin{tikzcd} H^n_{a,d} \arrow[rr, "f"] \arrow[dr, "\tilde{\pi}"'] & & H^n_{a,d} \\ & H_{\pi(a),\ \pi(d)} \arrow[ur, "g"'] & \end{tikzcd}$$

Indeed, let $P \in ker(\tilde{\pi}) = Im\ \phi$, then by Corollary 3.15:

$$(1-N\lambda)P = p^k\alpha P = [0:-1:1],$$

so $P \in ker(f)$. It follows that $ker(\tilde{\pi}) \subseteq ker(f)$, this proves the above assertion.
Now we prove that $\tilde{\pi} \circ g = id_{H_{\pi(a),\ \pi(d)}}$. Let $Q \in H_{\pi(a),\ \pi(d)}$, since $\tilde{\pi}$ is surjective, then there exists a $P \in H^n_{a,d}$ such that $\tilde{\pi}(P) = Q$. We have $NQ = [0:-1:1]$, then

$$N\tilde{\pi}(P) = [0:-1:1]\ and\ \tilde{\pi}(NP) = [0:-1:1],$$

implies that $NP \in ker(\tilde{\pi})$ and so, $N\lambda P \in ker(\tilde{\pi})$; therefore, $\tilde{\pi}(N\lambda P) = [0:-1:1]$. Moreover,

$$g(Q) = (1-N\lambda)P = P - N\lambda P,$$

then

$$\tilde{\pi} \circ g(Q) = \tilde{\pi}(P) - [0:-1:1] = Q$$

and so, $\tilde{\pi} \circ g = id_{H_{\pi(a),\ \pi(d)}}$.
Thus the sequence is split. □

Corollary 3.18. *If p doesn't divide $\#(H_{\pi(a),\ \pi(d)})$ then, $H^n_{a,d}$ is isomorphic to $H_{\pi(a),\ \pi(d)} \times M$.*

Proof. From the Theorem 3.17 the sequence

$$\begin{tikzcd} O \arrow[r] & Ker\tilde{\pi} \arrow[r, "j"] & H^n_{a,d} \arrow[r, "\tilde{\pi}"] & H_{\pi(a),\ \pi(d)} \arrow[r] & 0 \end{tikzcd}$$

is split then, $H^n_{a,d} \cong H_{\pi(a),\ \pi(d)} \times ker(\tilde{\pi})$, and since $ker(\tilde{\pi}) \cong Im\ \phi \cong M$, then the corollary is proved. ☐

4. Cryptographic Applications

In this section, we give some cryptography results, other more practical applications are going to be given in our future works.
If p doesn't divide the cardinality of $H_{\pi(a),\ \pi(d)}$ then, form Corollary 3.18 we deduce the following results:

- The discrete logarithm problem in $H^n_{a,d}$ is equivalent to that in $H_{\pi(a),\ \pi(d)}$.
- $\#(H^n_{a,d}) = p^{b(n-1)} \times \#(H_{\pi(a),\ \pi(d)})$

This is an important and useful factor in cryptography since it allows to obtain a huge number of points with a smaller prime number p. As a consequence, we can notice that the time needed to solve the discrete logarithm problem on $H^n_{a,d}$ is larger than that of the twisted Hessian curve on a finite field.

5. Conclusion

In this paper, we have studied the twisted Hessian curves over R_n and we have proved the bijection between $H^n_{a,d}$ and $H_{\pi(a),\ \pi(d)} \times M$. For cryptography applications, we deduce that the discrete logarithm problem on $H^n_{a,d}$ is equivalent to the on on $H_{\pi(a),\ \pi(d)}$ and $\#(H^n_{a,d}) = p^{b(n-1)}\#(H_{\pi(a),\ \pi(d)})$.

References

1. Bernstein, D. J., Chuengsatiansup C., Kohel D., Lange T., *Twisted Hessian Curves.* In: Lauter K., Rodríguez-Henríquez F. (eds) Progress in Cryptology – LATINCRYPT 2015. Lecture Notes in Computer Science, 9230, 269-294. Springer, Cham (2015).
2. Chillali, A., *Elliptic Curves of the Ring $F_q[\epsilon]$, $\epsilon^n = 0$.* International Mathematical Forum, 6, 1501-1505 (2011).
3. Chuengsatiansup, C., Martindale, C., *Pairing-Friendly Twisted Hessian Curves.* In: Chakraborty D., Iwata T. (eds) Progress in Cryptology – INDOCRYPT 2018. Lecture Notes in Computer Science, 11356. Springer, Cham (2018).
4. Ben Taleb, E.M., Grini, A., Chillali, A., and Lhoussain, E. F. . *El Gamal Cryptosystem on a Montgomery Curves Over Non Local Ring.* WSEAS Transactions on Mathematics, 21, 85-89 (2022).
5. Grini, A., Chillali, A., Mouanis, H., , *The Binary Operations Calculus in $H^2_{a,d}$.* Boletim da Sociedade Paranaense de Matematica, 40, 1-6 (2020).
6. Grini, A., Chillali, A., ElFadil, L., Mouanis, H., *Twisted Hessian curves over the ring $F_q[e]$, $e^2 = 0$.* International Journal of Computer Aided Engineering and Technology(2020, to appear) Available at https://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijcaet
7. Grini, A., Chillali, A., Mouanis, H., *Cryptography over twisted Hessian curves of the ring $F_q[\epsilon]$, $\epsilon^2 = 0$.* Advances in Mathematics: Scientific Journal, 10, 235-243 (2021).
8. 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(4), 2667-2683 (2021).
9. 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, 237. Springer, Singapore (2022).
10. Koblitz, N., Menezes, A. & Vanstone, S., *The State of Elliptic Curve Cryptography.* Designs, Codes and Cryptography 19, 173-193 (2000).
11. Lenstra, H. W., *Eliptic Curves and Number-Theoretic Algorithms.* Processing of the International Congress of Mathematicians, Berkely, California, USA (1986).
12. Sahmoudi, M., Chillali,A., *Key Exchange over Particular Algebraic Closure Ring.* Tatra Mountains Mathematical Publications, 70, 151-162 (2017).

13. Silverman, H. S., *An Introduction to the Theory of Elliptic Curves*. University of Wyoming (2006).

14. Silverman, J. H., *The Arithmetic of Elliptic Curves*. GTM, 106. Springer, New York (2009).

15. Smart, N., *The Hessian form of an elliptic curve*. Cryptographic hardware and embedded systems-CHES 2001 (Paris), Lecture Notes in Computer Science, 2162, Springer, Berlin (2001).

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

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`

and

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