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

(3s.) **v. 2026 (44) 6** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.81149

Binary Twisted Hessian Curve Over a Local Ring

Abdelâli Grini

ABSTRACT: Let $\mathbb{F}_{2^n}$ be a finite field, where n is a positive integer. In this article, we will study the twisted Hessian curve over the ring $A_2 = \mathbb{F}_{2^n}[e]$, where the relation $e^2 = 0$. More precisely, we will give many various explicit formulas, which describe the binary operations calculus in $HB^2_{a,d}$, where $HB^2_{a,d}$ is the binary twisted Hessian curve over A_2, and we will reduce the cost of the complexity of the calculus in $HB^2_{a,d}$. In a first time, we describe these curves over this ring. In addition, we prove that when 2 doesn't divide $\#(HB_{\pi(a),\ \pi(d)})$, then $HB^2_{a,d}$ is a direct sum of $HB_{\pi(a),\ \pi(d)}$ and $\mathbb{F}_{2^n}$, where $HB_{\pi(a),\ \pi(d)}$ is the twisted Hessian curve over $\mathbb{F}_{2^n}$. Other results are deduced from, we cite the equivalence of the discrete logarithm problem on the binary twisted Hessian curves $HB^2_{a,d}$ and $HB_{\pi(a),\ \pi(d)}$, which is beneficial for cryptography and cryptanalysis as well.

Keywords: Finite ring, Binary Twisted Hessian curve, cryptography.

Contents

1. Introduction

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 [8,10] that compute discrete logarithms for the cyclic subgroup of the elliptic curve. To 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 $\mathbb{F}_{2^n}[X]/(X^2)$ which verifies this property because it increases the time needed to solve the discrete logarithm problem, we will prove that $\#(HB^2_{a,d}) = 2^n\#(HB_{\pi(a),\ \pi(d)})$, so we may reserve up memory once we do the calculations. As a result, we can note that the time for solving the discrete logarithm problem on $HB^2_{a,d}$ is greater than that of the twisted Hessian curve on a finite field.

2020 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted December 31, 2025. Published February 17, 2026

This paper is organized as follows. In Section 2, We study the arithmetic of the ring A_2, 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 $\mathbb{F}_{2^n}[e]$ and we will classify the elements of the binary twisted Hessian curve $HB^2_{a,d}$. Afterwards, we will define the group law of $HB^2_{a,d}$ and we will show that $HB^2_{a,d}$ is a direct sum of $HB_{\pi(a),\ \pi(d)}$ and the maximal ideal of A_2, when 2 doesn't divide $\#(HB_{\pi(a),\ \pi(d)})$.
Another purpose of this paper is the application of $HB^2_{a,d}$ in cryptography. Thereby, in Section 4, we deduce some cryptographic applications.

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

Let $\mathbb{F}_{2^n}$ be a finite field. We consider the quotient ring $A_2 = \mathbb{F}_{2^n}[X]/(X^2)$. Then the ring A_2 can be identified by the ring $\mathbb{F}_{2^n}[e]$, $e^2 = 0$. In other words,

$$A_2 = \{a + be/a, b \in \mathbb{F}_{2^n}\}.$$

Now, we will give some results concerning the ring A_2, which are useful for the rest of this work.

Let two elements in A_2 represented by $X = x_0 + x_1e$ and $Y = y_0 + y_1e$ with coefficients x_i and y_i are in the field $\mathbb{F}_{2^n}$ for $(i = 0, 1)$.

The arithmetic operations in A_2 can be decomposed into operations in $\mathbb{F}_{2^n}$ and they are calculated as follows:

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

$$X.Y = (x_0y_0) + (x_0y_1 + x_1y_0 + x_1y_1)e.$$

Similar as in [2,4,5,6,7], we have the following results:

- $(A_2, +, .)$ is a finite unitary commutative ring.
- A_2 is a vector space over $\mathbb{F}_q$ and has $(1, e)$ as a basis.
- A_2 is a local ring. Its maximal ideal is $M = (e) = e\mathbb{F}_{2^n}$.
- The non-invertible elements of A_2 are those in the form xe, where $x \in \mathbb{F}_{2^n}$.
  Namely, $(x_0 + x_1e)^{-1} = x_0^{-1} + x_1x_0^{-2}e$, where $x_0, x_1 \in \mathbb{F}_{2^n}$ and $x_0 \neq 0$.

Remark 2.1 *The canonical projection π defined by:*

$$\begin{array}{cccc} \pi & A_2 & \to & \mathbb{F}_{2^n} \\ & x_0 + x_1e & \mapsto & x_0 \end{array}$$

is a surjective homomorphism of rings.

3. Binary Twisted Hessian Curves Over the Ring A_2

Definition 3.1 *We consider the binary twisted Hessian curve over the ring A_2 in the projective space $\mathbb{P}^2(A_2)$, which is given by the equation: $aX^3 + Y^3 + Z^3 = dXYZ$, where $a, d \in A_2$ and $a(a + d^3)$ is invertible in A_2, and denoted by $HB^2_{a,d}$. So we have:*

$$HB^2_{a,d} = \{[X : Y : Z] \in \mathbb{P}^2(A_2) \setminus \quad aX^3 + Y^3 + Z^3 = dXYZ\}.$$

Lemma 3.1 *Let $a = a_0 + a_1e$, $d = d_0 + d_1e$ be elements of A_2.*
If $\Delta = a(a + d^3)$ is the discriminant of $HB^2_{a,d}$ and $\Delta_0 = a_0(a_0 + d_0^3)$ is the discriminant of HB_{a_0,d_0}, where HB_{a_0,d_0} is the binary twisted Hessian curve over $\mathbb{F}_{2^n}$, then $\pi(\Delta) = \Delta_0$.

Proof. Let $a = a_0 + a_1e$, $d = d_0 + d_1e$ be elements of A_2.
So $\pi(\Delta) = \pi(a(a + d^3)) = \pi((a_0 + a_1e)^2 - (a_0 + a_1e)(d_0 + d_1e)^3)$.
Then $\pi(\Delta) = \pi((a_0^2) + (a_0 + a_1e)(d_0^3 + d_0^2d_1e))$.
So $\pi(\Delta) = \pi(a_0^2 + a_0d_0^3 + (a_0d_0^2d_1 + a_1d_0^3)e)$.
Thus $\pi(\Delta) = a_0^2 + a_0d_0^3 = a_0(a_0 + d_0^3) = \Delta_0$.

Theorem 3.1 *Let $a = a_0 + a_1e$, $d = d_0 + d_1e$, $X = x_0 + x_1e$, $Y = y_0 + y_1e$ and $Z = z_0 + z_1e$ be elements of A_2, with*

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

Then

$$a_0x_0^3 + y_0^3 + z_0^3 = d_0x_0y_0z_0 + (D + Ax_1 + By_1 + Cz_1)e,$$

where

$$D = d_1x_0y_0z_0 + a_1x_0^3,$$

$$A = d_0y_0z_0 + a_0x_0^2,$$

$$B = d_0x_0z_0 + y_0^2,$$

$$C = d_0y_0x_0 + z_0^2.$$

Proof. Let $a = a_0 + a_1e$, $d = d_0 + d_1e$, $X = x_0 + x_1e$, $Y = y_0 + y_1e$ and $Z = z_0 + z_1e$ be elements of A_2. Then

$$Y^3 = y_0^3 + y_0^2y_1e$$

$$Z^3 = z_0^3 + z_0^2z_1e$$

$$aX^3 = a_0x_0^3 + a_0x_0^2x_1e + a_1x_0^3e$$

$dXYZ = d_0x_0y_0z_0 + d_1X_0y_1z_0 + (d_0X_0y_0z_1 + d_0X_0y_1z_0 + d_0X_1y_0z_0)e$.
If $aX^3 + Y^3 + Z^3 = dXYZ$, then

$$a_0X_0^3 + y_0^3 + z_0^3 = d_0x_0y_0z_0 + (D + Ax_1 + By_1 + Cz_1)e,$$

where

$$D = d_1x_0y_0z_0 - a_1x_0^3,$$

$$A = d_0y_0z_0 + a_0x_0^2,$$

$$B = d_0x_0z_0 + y_0^2,$$

$$C = d_0y_0x_0 + z_0^2.$$

Corollary 3.1 *Let $X = x_0 + x_1e$, $Y = y_0 + y_1e$ and $Z = z_0 + z_1e$ be elements of A_2.*
If $[X : Y : Z] \in HB^2_{a,d}$, then $[x_0 : y_0 : z_0] \in HB_{a_0,d_0}$.

3.1. Classification of elements of $HB^2_{a,d}$

To have a clear idea of the binary twisted Hessian curves over the ring A_2, we can classify its elements according to their projective coordinate.

Proposition 3.1 *Every element in $HB^2_{a,d}$ is of the form $[1 : Y : Z]$ (where Y or $Z \in A_2 \setminus M$), or $[xe, 1 + d_0xe, 1]$, and we write:*
$HB^2_{a,d} = \{[1 : Y : Z] \in P_2(A_2) \mid a + Y^3 + Z^3 = dYZ$, *and* Y *or* $Z \in A_2 \setminus M\} \cup \{[xe, 1 + d_0xe, 1] \mid x \in \mathbb{F}_{2^n}$ *and* $d_0 \in \mathbb{F}_{2^n}\}$.

Proof. Let $[X : Y : Z] \in HB^2_{a,d}$, where X, Y and $Z \in A_2$.

- If X is invertible, then $[X : Y : Z] = [1 : X^{-1}Y : X^{-1}Z] \sim [1 : Y : Z]$. Suppose that Y and $Z \in M$; since $a + Y^3 + Z^3 = dYZ$ then $a \in M$, which is absurd. So, Y or $Z \in A_2 \setminus M$.
- If X is non invertible, then $X \in M$, so $X = xe$, where $x \in \mathbb{F}_{2^n}$. Let $Y = y_0 + y_1e$, $Z = z_0 + z_1e$, $d = d_0 + d_1e$ and $a = a_0 + a_1e$.
  So, $[X : Y : Z] = [xe, y_0 + y_1e, z_0 + z_1e] \in HB^2_{a,d}$. Then by Corollary 3.1: $[0, y_0, z_0] \in HB^2_{a_0,d_0}$ implies that $y_0 = 1$ and $z_0 = 1$ (see [1], Theorem 2.2).
  i.e:
$$\begin{aligned}[X : Y : Z] &= [xe, 1 + y_1e, 1 + z_1e] \\ &= [xe, (1 + y_1e)(1 + z_1e), 1] \\ &= [xe, 1 + (y_1 + z_1)e, 1].\end{aligned}$$
  Hence, $1 + (y_1 + z_1)e + 1 = d_0(xe)(1 + (y_1 + z_1)e)$. Then $y_1 + z_1 = d_0xe$.
  Thus $[X : Y : Z] = [xe, 1 + xd_0e, 1]$.

3.2. The group law over $HB^2_{a,d}$

Theorem 3.2 *Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in binary twisted Hessian curve $HB^2_{a,d}$.*

1. *Define:*
$$X_3 = X_1^2Y_2Z_2 - X_2^2Y_1Z_1,$$
$$Y_3 = Z_1^2X_2Y_2 - Z_2^2X_1Y_1,$$
$$Z_3 = Y_1^2X_2Z_2 - Y_2^2X_1Z_1.$$
   If $(\pi(X_3), \pi(Y_3), \pi(Z_3)) \neq (0, 0, 0)$, then $P + Q = [X_3 : Y_3 : Z_3]$.
2. *Define:*
$$X'_3 = Z_2^2X_1Z_1 - Y_1^2X_2Y_2,$$
$$Y'_3 = Y_2^2Y_1Z_1 - aX_1^2X_2Z_2,$$
$$Z'_3 = aX_2^2X_1Y_1 - Z_1^2Y_2Z_2.$$
   If $(\pi(X'_3), \pi(Y'_3), \pi(Z'_3)) \neq (0, 0, 0)$, then $P + Q = [X'_3 : Y'_3 : Z'_3]$.

Proof. By using [[1], Theorem 3.2 and Theorem 4.2], we prove the theorem.

Corollary 3.2 *$(HB^2_{a,d}, +)$ is a commutative group with unity $[0 : 1 : 1]$.*

Lemma 3.2 *The mapping*

$$\begin{array}{rccc} \tilde{\pi}: & HB^2_{a,d} & \to & HB_{a_0,d_0} \\ & [X:Y:Z] & \mapsto & [\pi(X):\pi(Y):\pi(Z)], \end{array}$$

is a surjective homomorphism of groups.

Proof. Let $[x_0 : y_0 : z_0] \in HB_{a_0,d_0}$, then there exists $[X : Y : Z] \in HB^2_{a,d}$ such that $\tilde{\pi}([X : Y : Z]) = [x_0 : y_0 : y_0]$.
By Theorem 3.1, we have

$$D = Ax_1 + By_1 + Cz_1$$

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 $(x_0 : y_0 : z_0)$, can not be all three null. We can then, at last, conclude that $[x_1 : y_1 : z_1]$.
Finally, $\tilde{\pi}$ is a surjective.

Lemma 3.3 *The mapping*

$$\begin{array}{rccc} \theta: & \mathbb{F}_{2^n} & \to & HB^2_{a,d} \\ & x & \mapsto & [xe, 1 + d_0xe, 1], \end{array}$$

is an injective homomorphism.

Proof. Evidently, θ is injective.
Let $x_1, x_2 \in \mathbb{F}_{2^n}$, $P = [x_1e, 1 + d_0x_1e, 1]$ and $Q = [x_2e, 1 + d_0x_2e, 1]$. By Theorem 3.2 we have:

$$P + Q = [(x_1 + x_2)e : 1 + (x_1 + x_2)d_0e : 1].$$

Then $\theta((x_1 + x_2)) = \theta(x_1) + \theta(x_2)$, and we conclude that θ is injective homomorphism of groups.

We definite G by $G = ker(\tilde{\pi})$.

Corollary 3.3 *The set G is equal to $\theta(\mathbb{F}_{2^n})$.*

Proof. Let $[xe, 1 + d_0xe, 1] \in \theta(F_{2^n})$, then $\tilde{\pi}([xe, 1 + d_0xe, 1]) = [0 : 1 : 1]$.
We conclude that $[xe, 1 + d_0xe, 1] \in G$.
Thus $\theta(F_{2^n}) \subset G$.
Let $P = [X : Y : Z] \in G$, then $\tilde{\pi}([X : Y : Z]) = [0 : 1 : 1]$.
We set,

$$X = xe,$$
$$Y = 1 + y_1e$$
$$Z = 1 + z_1e$$

and

$$Z^{-1} = 1 + z_1e$$

So, $P = [Z^{-1}X : Z^{-1}Y : 1] = [xe : 1 + (y_1 + z_1)e : 1]$. We have $P \in HB^2_{a,d}$, then $y_1 + z_1 = d_0xe$. Hence, $P = [xe, 1 + d_0xe, 1] \in \theta(F_{2^n})$.
Thus, $G \subset \theta(F_{2^n})$.
Finally, $G = \theta(\mathbb{F}_{2^n})$.

We deduce the following corollary.

Corollary 3.4 *The group G is an elementary abelian 2-group.*

Theorem 3.3 *The sequence*

$$0 \to G \to HB^2_{a,d} \to HB_{a_0,d_0} \to 0$$

is a short exact sequence which defines the group extension $HB^2_{a,d}$ of HB_{a_0,d_0} by G.

Proof. By lemma 3.2, lemma 3.3 and corollary 3.3 , we deduce that the sequence

$$0 \to G \to HB^2_{a,d} \to HB_{a_0,d_0} \to 0$$

is a short exact sequence which defines the group extension $HB^2_{a,d}$ of HB_{a_0,d_0} by G.

Theorem 3.4 *Let $N = \#(HB_{a_0,d_0})$ the cardinality of HB_{a_0,d_0}. If 2 doesn't divide N, then the short exact sequence*

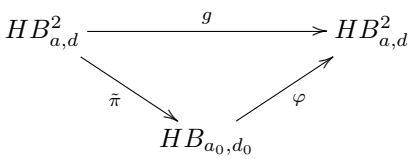
$$0 \to G \to HB^2_{a,d} \to HB_{a_0,d_0} \to 0$$

is split.

Proof. If 2 doesn't divide N, then exists an integer b such that $Nb = 1 mod 2$. So, there is an integer m such that $1 - Nb = 2m$.
Let g the homomorphism defined by:

$$\begin{array}{rccc} g: & HB^2_{a,d} & \to & HB^2_{a,d} \\ & P & \mapsto & (1-Nb)P, \end{array}$$

There exists an unique morphism φ, such that the following diagram commutes:



Indeed, let $P \in ker(\tilde{\pi}) = \theta(\mathbb{F}_{2^n})$, then: $\exists x \in \mathbb{F}_{2^n}$ such that: $P = [xe, 1 + d_0 xe, 1]$. We have: $(1 - Nb)P = 2mP = [0 : 1 : 1]$, then $P \in ker(g)$. It follows that $ker(\tilde{\pi}) \subseteq ker(g)$, this prove the above assertion.
Now we prove that $\tilde{\pi} \circ \varphi = id_{HB_{a_0,d_0}}$. Let $P' \in HB_{a_0,d_0}$, since $\tilde{\pi}$ is surjective, then there exists a $P \in HB^2_{a,d}$ such that $\tilde{\pi}(P) = P'$. We have $\varphi(P') = (1 - Nb)P = P - NbP$ and $NP' = [0 : 1 : 1]$, then $N\tilde{\pi}(P) = [0 : 1 : 1]$ and $\tilde{\pi}(NP) = [0 : 1 : 1]$ implies that $NP \in ker(\tilde{\pi})$ and so, $NbP \in ker(\tilde{\pi})$; therefore $\tilde{\pi}(NbP) = [0 : 1 : 1]$. On the other hand, $\varphi(P') = (1 - Nb)P = P - NbP$, then $\tilde{\pi} \circ \varphi(P') = \tilde{\pi}(P) - [0 : 1 : 1] = P'$ and so, $\tilde{\pi} \circ \varphi = id_{HB_{a_0,d_0}}$.
Hence the sequence is split.

Corollary 3.5 *If 2 doesn't divide $\#(HB_{a_0,d_0})$, then $HB^2_{a,d} \cong HB_{a_0,d_0} \times \mathbb{F}_{2^n}$.*

Proof. From the theorem 3.4 the sequence

$$0 \to G \to HB^2_{a,d} \to HB_{a_0,d_0} \to 0$$

is split, then $HB^2_{a,d} \cong HB_{a_0,d_0} \times G$, and since $G = ker(\tilde{\pi}) \cong Im\theta \cong \mathbb{F}_{2^n}$, so the corollary is proved.

4. Cryptographic Applications

We present some binary twisted Hessian curves $HB^2_{a,d}$ cryptography results in this section, but we will also provide more practical applications in our future work.
If 2 doesn't divide $\#(HB_{a_0,d_0})$, we deduce form the Corollary 3.5 that it allows us to acquire a large number of points, which is greatly benefited in cryptography. As a result, we can see that the time required to solve the discrete logarithm problem on $HB^2_{a,d}$ is greater than that of the binary twisted Hessian curves over a finite field.

5. Conclusion

In this article, we have studied the binary twisted Hessian curves on the ring A_2 and have showed the bijection between $HB^2_{a,d}$ and $HB_{a_0,d_0} \times \mathbb{F}_q$. For $HB^2_{a,d}$ cryptography applications, we deduce that the discrete logarithm problem on $HB^2_{a,d}$ is equivalent to the discrete logarithm problem on HB_{a_0,d_0} and $\#(HB^2_{a,d}) = 2^n \#(HB_{a_0,d_0})$.

References

1. Bernstein, D. J., Chuengsatiansup C., Kohel D., Lange T., *Twisted Hessian Curves*, Lecture Notes in Computer Science, 9230, 269-294. Springer, Cham (2015).
2. Chillali, A., *Elliptic Curves of the Ring $F_q[\epsilon]$, $e^\epsilon = 0$*. 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. 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, 18, 181-189 (2023)
5. 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).
6. 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 (2022).
7. Grini A., Chillali A., Mouanis H. , *Cryptography Over the Twisted Hessian Curve $H^3_{a,d}$*. Smart Innovation, Systems and Technologies, 237. Springer, Singapore (2022).
8. Koblitz, N., Menezes, A. & Vanstone, S., *The State of Elliptic Curve Cryptography*. Designs, Codes and Cryptography 19, 173-193 (2000).
9. Lenstra, H. W., *Eliptic Curves and Number-Theoretic Algorithms*. Processing of the International Congress of Mathematicians, Berkely, California, USA (1986).
10. Silverman, H. S., *An Introduction to the Theory of Elliptic Curves*. University of Wyoming (2006).
11. Silverman, J. H., *The Arithmetic of Elliptic Curves*. GTM, 106. Springer, New York (2009).
12. 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).

Abdelâli Grini,
Department of Mathematics,
Regional Center of Education and Professional Training, Fez-Meknes,
Morocco.
E-mail address: abdelali.grini@usmba.ac.ma