Palestine Journal of Mathematics

Vol 14(2)(2025) , 259–264

Binary Edwards curves over a local ring

Moha Ben Taleb El Hamam

Communicated by Ayman Badawi

MSC 2010 Classifications: 11T71, 14G50, 94A60.

Keywords and phrases: Elliptic curves, Binary Edwards curves, Cryptography.

The author would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of this paper.

Corresponding Author: Moha Ben Taleb El Hamam

Abstract. *Let n be a positive integer and consider $\mathbb{F}_{2^n}[\varepsilon]$ to be a finite ring of characteristic 2. The main goal of this paper is to investigate the binary Edwards curves, which is denoted by $E_{B_{a,d}}$, over the local ring $\mathbb{F}_{2^n}[\varepsilon]$, where $\varepsilon^2 = 0$. Furthermore, we give some links with the cryptography.*

1 Introduction

The Edwards curve is an elliptic curve discovered in 2007, by mathematician Harold Edwards [4], This model has been shown to be very promising because it has a complete group structure and faster law of addition. Bernstein et al. introduced twisted Edwards curves and mentioned several advantages of these curves compared to the Weierstrass elliptic functions [1]. In [10], Boudabra et al. studied the twisted Edwards curves on the finite field Z/pZ, where $p \geq 5$ is a prime number, and on the rings Z/p^rZ and Z/p^rq^sZ. In [7, 8] El Hamam et al. studied the twisted Edwards curves over the ring $\mathbb{F}_q[e], e^2 = e$ and $\mathbb{F}_q[e], e^2 = 0$. Bernstein et al. introduced a new shape for ordinary elliptic curves on the fields of characteristic 2, with equation $a(X+Y)+d(X^2+Y^2) = XY + XY(X+Y) + X^2Y^2$ [6]. In [5], El Hamam et al. studied the binary Edwards curves on the ring $\mathbb{F}_{2^n}[e], e^2 = e$.

In this work, we study binary Edwards curves over the ring $\mathbb{F}_{2^n}[\varepsilon], \varepsilon^2 = 0$. The motivation of this article is the research of the properties of the binary Edwards curves on a finite ring, for use in cryptography.

Let $\mathbb{F}_{2^n}$ be a finite field and n is a positive integer. The plan of this paper is the following: In Section 2, we study the arithmetic of the ring $\mathbb{F}_{2^n}[\varepsilon], \varepsilon^2 = 0$. In Section 3, we define the binary Edwards curves $E_{B_{a,d}}(\mathbb{F}_{2^n}[\varepsilon])$ over this ring. Moreover, we will define the group extension $E_{B_{a,d}}(\mathbb{F}_{2^n}[\varepsilon])$ of $E_{B_{a_0,d_0}}(\mathbb{F}_{2^n})$ and give a bijection between the groups $E_{B_{a,d}}$ and $\mathbb{F}_{2^n} \times E_{B_{a_0,d_0}}$, where $E_{B_{a_0,d_0}}$ is the binary Edwards curves over the finite field $\mathbb{F}_{2^n}$. Furthermore, we close this paper, by giving a link between the group $E_{B_{a,d}}$ and cryptography. We deduce that the discrete logarithm problem in $E_{B_{a,d}}$ is equivalent to the discrete logarithm problem in $E_{B_{a_0,d_0}} \times \mathbb{F}_{2^n}$ and $\#(E_{B_{a,d}}) = 2^n \#(E_{B_{a_0,d_0}})$.

2 Arithmetic over the ring $\mathbb{F}_{2^n}[\varepsilon], \varepsilon^2 = 0$

Let n be a positive integer, we consider the quotient ring $B_2 = \dfrac{\mathbb{F}_{2^n}[X]}{(X^2)}$, where $\mathbb{F}_{2^n}$ is the finite field of order 2^n. The ring B_2 is identified to the ring $\mathbb{F}_{2^n}[\varepsilon], \varepsilon^2 = 0$. Hence,

$$B_2 = \{x_0 + x_1\varepsilon \mid (x_0, x_1) \in \mathbb{F}_{2^n}^2\}.$$

The arithmetic operations in B_2 can be decomposed into operations in $\mathbb{F}_{2^n}$ and they are computed as follows: $X+Y=(x_0+y_0)+(x_1+y_1)\varepsilon$ and $X\cdot Y=(x_0y_0)+(x_0y_1+x_1y_0)\varepsilon$, where X and Y are two elements in B_2 represented by $X=x_0+x_1\varepsilon$ and $Y=y_0+y_1\varepsilon$ with coefficients x_0, x_1, y_0 and $y_1\in\mathbb{F}_{2^n}$. The following results can easily be verified (see [3, 6, 9, 11, 12]).

- *Let $X=x_0+x_1\varepsilon\in B_2$, X is invertible if and only if $x_0\not\equiv 0 \pmod 2$, and its inverse is $X^{-1}=x_0^{-1}-x_1x_0^{-2}\varepsilon$.*
- *B_2 is a local ring, its maximal ideal is $M=\varepsilon B_2$.*
- *B_2 is an $\mathbb{F}_{2^n}$-vector space of dimension 2 and of basis $\{1,\varepsilon\}$.*
- *We consider the canonical projection τ defined by*

$$\begin{array}{rccc}\tau & : & B_2 & \longrightarrow & \mathbb{F}_{2^n},\\ & & X & \longmapsto & x_0\end{array}$$

is a surjective morphism of rings.

3 Binary Edwards curves over the ring B_2

Let X,Y, a and d be four elements of B_2 such that $X=x_0+x_1\varepsilon$, $Y=y_0+y_1\varepsilon$, $a=a_0+a_1\varepsilon$ and $d=d_0+d_1\varepsilon$.

Definition 3.1. A binary Edwards curve is defined over B_2 by the equation $a(X+Y)+d(X^2+Y^2)=XY+XY(X+Y)+X^2Y^2$, such that a and $d+a^2+a$ are invertible in B_2. We denote it by $E_{B_{a,d}}$ and we write: $E_{B_{a,d}}=\left\{(X,Y)\in B_2^2 \mid a(X+Y)+d(X^2+Y^2)=XY+XY(X+Y)+X^2Y^2\right\}$.

Lemma 3.2. *Let a and d be in the ring B_2, then $d+a^2+a$ is invertible if and only if $d_0+a_0^2+a_0\not\equiv 0 \pmod 2$.*

Proof. We have:

$$\begin{aligned}d+a^2+a&=d_0+d_1\varepsilon+(a_0+a_1\varepsilon)^2+a_0+a_1\varepsilon\\&=d_0+d_1\varepsilon+a_0^2+a_0+a_1\varepsilon\\&=d_0+a_0^2+a_0+(d_1+a_1)\varepsilon.\end{aligned}$$

Since $\tau(d+a^2+a)=d_0+a_0^2+a_0$, then $d+a^2+a$ is invertible if and only if $d_0+a_0^2+a_0\not\equiv 0 \pmod 2$. □

Using Lemma 3.2, if a and $d+a^2+a$ are invertible in B_2, then $E_{B_{\tau(a),\tau(d)}}(\mathbb{F}_{2^n})$ is binary Edwards curve over the finite field $\mathbb{F}_{2^n}$ and we notice $E_{B_{a_0,d_0}}$. We write:

$$E_{B_{a_0,d_0}}=\left\{(x,y)\in\mathbb{F}_{2^n}^2 \mid a_0(x+y)+d_0(x^2+y^2)=xy+xy(x+y)+x^2y^2\right\}.$$

Theorem 3.3. *Let $a=a_0+a_1\varepsilon$, $d=d_0+d_1\varepsilon$, $X=x_0+x_1\varepsilon$ and $Y=y_0+y_1\varepsilon$ be elements of B_2 such that $a(X+Y)+d(X^2+Y^2)=XY+XY(X+Y)+X^2Y^2$, then*
$a_0(x_0+y_0)+d_0(x_0^2+y_0^2)=x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2+(E+Fx_1+Gy_1)\varepsilon$, where $E=-a_1(x_0+y_0)-d_1(x_0^2+y_0^2)$, $F=-a_0+y_0+y_0^2$ and $G=-a_0+x_0+x_0^2$.

Proof. We have:

$$\begin{aligned}
a(X+Y) &= (a_0+a_1\varepsilon)(x_0+x_1\varepsilon+y_0+y_1\varepsilon)\\
&= a_0(x_0+y_0)+[a_0(x_1+y_1)+a_1(x_0+y_0)]\varepsilon,\\
d(X^2+Y^2) &= (d_0+d_1\varepsilon)((x_0+x_1\varepsilon)^2+(y_0+y_1\varepsilon)^2)\\
&= d_0(x_0^2+y_0^2)+d_1(x_0^2+y_0^2)\varepsilon,\\
XY &= (x_0+x_1\varepsilon)+(y_0+y_1\varepsilon)\\
&= x_0y_0+(x_0y_1+x_1y_0)\varepsilon,\\
XY(X+Y) &= (x_0+x_1\varepsilon)(y_0+y_1\varepsilon)((x_0+x_1\varepsilon)+(y_0+y_1\varepsilon))\\
&= x_0y_0(x_0+y_0)+(x_0^2y_1+x_1y_0^2)\varepsilon,\\
X^2Y^2 &= (x_0+x_1\varepsilon)^2(y_0+y_1\varepsilon)^2\\
&= x_0^2y_0^2.
\end{aligned}$$

If $a(X+Y)+d(X^2+Y^2)=XY+XY(X+Y)+X^2Y^2$, then
$a_0(x_0+y_0)+d_0(x_0^2+y_0^2)=x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2+(E+Fx_1+Gy_1)\varepsilon$, where
$E=-a_1(x_0+y_0)-d_1(x_0^2+y_0^2)$, $F=-a_0+y_0+y_0^2$ and $G=-a_0+x_0+x_0^2$.

□

Corollary 3.4. *If $(X,Y)\in E_{B_{a,d}}$, then $(x_0,y_0)\in E_{B_{a_0,d_0}}$.*

Proof. If $(X,Y)\in E_{B_{a,d}}$, then $a(X+Y)+d(X^2+Y^2)=XY+XY(X+Y)+X^2Y^2$. So, by Theorem 3.3, we have $a_0(x_0+y_0)+d_0(x_0^2+y_0^2)=x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2+(E+Fx_1+Gy_1)\varepsilon$. As $(1,\varepsilon)$ is a basis of B_2, then $a_0(x_0+y_0)+d_0(x_0^2+y_0^2)=x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2$. Thus $(x_0,y_0)\in E_{B_{a_0,d_0}}$. □

4 The group law of the binary Edwards curve $E_{B_{a,d}}$

The authors in [2] presented an addition law for the binary Edwards curve $E_{B,a_0,d_0}(\mathbb{F}_{2^n})$. This addition law on $E_{B,a_0,d_0}(\mathbb{F}_{2^n})$ is strongly unified: it can be used with two identical inputs, i.e., to double. Given two points (X_1,Y_1) and (X_2,Y_2) in the binary Edwards curve $E_{B,a,d}$, compute the sum $(X_3,Y_3)=(X_1,Y_1)+(X_2,Y_2)$ if it is defined:

$$X_3=\frac{a(X_1+X_2)+d(X_1+Y_1)(X_2+Y_2)+(X_1+X_1^2)(X_2(Y_1+Y_2+1)+Y_1Y_2)}{a+(X_1+X_1^2)(X_2+Y_2)}, \quad (4.1)$$

$$Y_3=\frac{a(Y_1+Y_2)+d(X_1+Y_1)(X_2+Y_2)+(Y_1+Y_1^2)(Y_2(X_1+X_2+1)+X_1X_2)}{a+(Y_1+Y_1^2)(X_2+Y_2)}. \quad (4.2)$$

If the denominators $a+(X_1+X_1^2)(X_2+Y_2)$ and $a+(Y_1+Y_1^2)(X_2+Y_2)$ are invertible in B_2, then the sum (X_3,Y_3) is a point on $E_{B,a,d}$, with $(0,0)$ is the neutral element and $-(X_1,Y_1)=(Y_1,X_1)$.

Corollary 4.1. *The following mapping is well defined:*

$$\begin{aligned}
\tilde{\tau} \;:\; E_{B_{a,d}} &\to E_{B_{a_0,d_0}},\\
(X,Y) &\mapsto (\tau(X),\tau(Y)).
\end{aligned}$$

Proof. From the previous theorem, we have $(\tau(X), \tau(Y)) \in E_{B_{a_0,d_0}}$.

If $(X_1, Y_1) = (X_2, Y_2)$, then

$$\begin{aligned}\tilde{\tau}(X_2, Y_2) &= (\tau(X_2), \tau(Y_2)) \\ &= (\tau(X_1), \tau(Y_1)) \\ &= \tilde{\tau}(X_1, Y_1).\end{aligned}$$

□

Lemma 4.2. *$\tilde{\tau}$ is a surjective morphism of groups.*

Proof. Let $(x_0, y_0) \in E_{B_{a_0,d_0}}$, then there exists $(X, Y) \in E_{B_{a,d}}$ such that $\tilde{\tau}(X, Y) = (x_0, y_0)$. By Theorem 3.3, we have: $a_0(x_0+y_0)+d_0(x_0^2+y_0^2) = x_0y_0+x_0y_0(x_0+y_0)+x_0^2y_0^2+(E+Fx_1+Gy_1)\varepsilon$. As $(1, \varepsilon)$ is a basis of B_2, then $E = -(Fx_1 + Gy_1)$.

Put $f(x, y) = a_0(x + y) + d_0(x^2 + y^2) - xy - xy(x + y) - x^2y^2$, we have:

$\frac{\partial f}{\partial x}(x_0, y_0) = a_0 - y_0 - y_0^2 = -F$ and $\frac{\partial f}{\partial y}(x_0, y_0) = a_0 - x_0 - x_0^2 = -G$.

The coefficients $-F$ and $-G$ are partial derivatives of a function $f(x, y)$ at the point (x_0, y_0), can not be all zero. We can then conclude that (x_1, y_1) exists. Thus, $\tilde{\tau}$ is a surjective. □

Lemma 4.3. *The mapping*

$$\begin{array}{rccc}\vartheta & : & \mathbb{F}_{2^n} & \to & E_{B_{a,d}}, \\ & & x & \mapsto & (x\varepsilon, x\varepsilon)\end{array}$$

is an injective morphism of groups.

Proof. It is obvious that ϑ is well defined and injective. Let $x_1, x_2 \in \mathbb{F}_{2^n}$ such that $P = (x_1\varepsilon, x_1\varepsilon)$ and $Q = (x_2\varepsilon, x_2\varepsilon)$. By (4.1) and (4.2), we have $P + Q = ((x_1 + x_2)\varepsilon, (x_1 + x_2)\varepsilon)$, then $\vartheta(x_1 + x_2) = \vartheta(x_1) + \vartheta(x_2)$ and we conclude that ϑ is an injective morphism of groups. □

Corollary 4.4. *Let $S = \vartheta(\mathbb{F}_{2^n})$, then $S = \ker(\tilde{\tau})$.*

Proof. Let $(x\varepsilon, x\varepsilon) \in S$, then $\tilde{\tau}(x\varepsilon, x\varepsilon) = (0, 0)$. We conclude that $(x\varepsilon, x\varepsilon) \in \ker(\tilde{\tau})$, thus $S \subset \ker(\tilde{\tau})$. Let $P = (X, Y) \in \ker(\tilde{\tau})$, then $\tilde{\tau}(X, Y) = (0, 0)$. Therefore, $X = x\varepsilon$ and $Y = y\varepsilon$, then $(X, Y) = (x\varepsilon, y\varepsilon)$. Thus $\ker(\tilde{\tau}) \subset S$. Finally, $S = \ker(\tilde{\tau})$. □

Remark 4.5. As $\vartheta(\mathbb{F}_{2^n})$ is isomorphic to $\mathbb{F}_{2^n}$, so $S \cong \mathbb{F}_{2^n}$. Therefore, S is an abelian 2-group of order 2^n.

Theorem 4.6. *The sequence*

$$0 \longrightarrow S \longrightarrow E_{B_{a,d}} \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$$

is a short exact sequence which defines the group extension $E_{B_{a,d}}$ of $E_{B_{a_0,d_0}}$ by S.

Proof. $\tilde{\tau}$ is a surjective morphism of groups, $S = \vartheta(\mathbb{F}_{2^n}) = \ker(\tilde{\tau})$ and ϑ is an injective morphism of groups. We deduce the sequence $0 \longrightarrow S \longrightarrow E_{B_{a,d}} \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$ is a short exact sequence which defines the group extension $E_{B_{a,d}}$ of $E_{B_{a_0,d_0}}$ by S. □

Theorem 4.7. *Let $n' = \#(E_{B_{a_0,d_0}})$ the cardinality of $E_{B_{a_0,d_0}}$. If 2 does not divide n', then the short exact sequence $0 \longrightarrow S \longrightarrow E_{B_{a,d}} \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$ is split.*

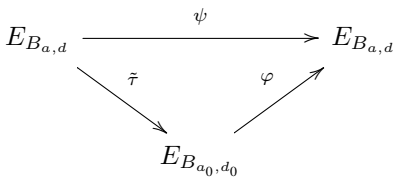
Proof. Since 2 does not divide n', then there exists an integer b such that $n'b = 1 \pmod 2$. So, there is an integer c such that $1 - n'b = 2c$. Let ψ the morphism defined by

$$\begin{array}{rccc}\psi & : & E_{B_{a,d}} & \to & E_{B_{a,d}}, \\ & & P & \mapsto & (1 - n'b)P\,.\end{array}$$

We have:

$$\begin{array}{rccc}\tilde{\tau} & : & E_{B_{a,d}} & \to & E_{B_{a_0,d_0}}, \\ & & (X, Y) & \mapsto & (\tau(X), \tau(Y))\end{array}$$

is a surjective morphism of groups by Lemma 4.2. Then, there exists a unique morphism φ, such that the following diagram commutes:



Indeed, let $P \in \ker(\tilde{\tau}) = \vartheta(\mathbb{F}_{2^n})$, then $\exists x \in \mathbb{F}_{2^n}$ such that $P = (x\varepsilon, x\varepsilon)$. We have $(1 - n'b)P = 2cP = (0,0)$, then $P \in \ker(\psi)$. It follows that $\ker(\tilde{\tau}) \subseteq \ker(\psi)$, this prove the above assertion.

Now, let us prove that $\tilde{\tau} o \varphi = id_{E_{B_{a_0,d_0}}}$. Let $Q \in E_{B_{a_0,d_0}}$, since $\tilde{\tau}$ is surjective, there exists $P \in E_{B_{a,d}}$ such that $\tilde{\tau}(P) = Q$. We have $\varphi(Q) = (1 - n'b)P = P - n'bP$ and $n'Q = (0,0)$, then $n'\tilde{\tau}(P) = (0,0)$ and $\tilde{\tau}(n'P) = (0,0)$ implies that $n'P \in \ker(\tilde{\tau})$ and so, $n'bP \in \ker(\tilde{\tau})$. Therefore, $\tilde{\tau}(nbP) = (0,0)$. On the other hand, $\varphi(Q) = (1 - n'b)P = P - n'bP$, then $\tilde{\tau} o \varphi(Q) = \tilde{\tau}(P) - (0,0) = Q$ and so, $\tilde{\tau} \circ \varphi = id_{E_{B_{a_0,d_0}}}$. Therefore, the sequence is split. □

Corollary 4.8. *If* 2 *does not divide* $\#(E_{B_{a_0,d_0}})$*, then* $E_{B_{a,d}} \cong E_{B_{a_0,d_0}} \times \mathbb{F}_{2^n}$

Proof. From the Theorem 4.7, the sequence

$$0 \longrightarrow S \longrightarrow E_{B_{a,d}} \longrightarrow E_{B_{a_0,d_0}} \longrightarrow 0$$

is split, then $E_{B_{a,d}} \cong E_{B_{a_0,d_0}} \times S$ and since $S = \ker(\tilde{\tau}) = Im\vartheta \cong \mathbb{F}_{2^n}$, then the corollary is proved. □

Links with Cryptography

In this work, we have proved the bijection between $E_{B_{a,d}}$ *and* $E_{B_{a_0,d_0}} \times \mathbb{F}_{2^n}$*. In cryptography applications, we deduce that the discrete logarithm problem in* $E_{B_{a,d}}$ *is equivalent to the discrete logarithm problem in* $E_{B_{a_0,d_0}} \times \mathbb{F}_{2^n}$ *and* $\#(E_{B_{a,d}}) = 2^n \#(E_{B_{a_0,d_0}})$*, which is an important and useful factor in cryptography.*

References

[1] *D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, Twisted Edwards curves. In: First International Conference on Cryptology in Africa, Casablanca, Morocco, Progress in Cryptology — AFRICACRYPT, Lecture Notes in Comput. Sci. Vol. 5023, Springer-Verlag, Berlin, (2008), pp. 389–405.*

[2] *D. J. Bernstein, T. Lange, and R. Rezaeian Farashahi, Binary Edwards Curves, In Oswald E., Rohatgi P. (eds) Cryptographic Hardware and Embedded Systems - CHES (2008). Lecture Notes in Computer Science, vol 5154. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85053-3-16.*

[3] *A. Chillali, Elliptic curves of the ring* $F_q[\epsilon]$*,* $\epsilon^n = 0$*, Int. Math. Forum,* ***6****, (2011) no. 29–31, 1501–1505.*

[4] *H. Edwards, Normal form for elliptic curves, Bull. Amer. Math. Soc. (N.S.)* ***44*** *(2007) no. 03, 393–423.*

[5] *M. B. T. El Hamam, A. Chillali, 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), (2022), doi: 10.1109/IRASET52964.2022.9738249.*

[6] *M. B. T. El Hamam, A. Chillali, L. El Fadil, Twisted Hessian curves over the ring* $\mathbb{F}_q[e], e^2 = e$*. Bol. Soc. Paran. Mat. (3s.)* ***40*** *(2022), doi: https://doi.org/10.5269/bspm.51867.*

[7] *M. B. T. El Hamam, A. Chillali, 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.*

[8] *M. B. T. El Hamam, A. Chillali, L. El Fadil, TWISTED EDWARDS CURVE OVER THE RING* $\mathbb{F}_q[e], e^2 = 0$*. Tatra Mt. Math. Publ.(2023) 83, 43-50.*

[9] *M. B. T. El Hamam, A. Grini, A. Chillali, L. El Fadil, El Gamal cryptosystem on a Montgomery curves over non local ring, WSEAS Trans. Math.* ***21*** *(2022), 85–89.*

[10] M. Boudabra, A. Nitaj, A new public key cryptosystem based on Edwards curves, J. Appl. Math. Comput. **61** (2019), no. 1–2, 431–450.

[11] M. B. T. El Hamam, A. Chillali, L. El Fadil, Classification of the elements of the twisted Hessian curves in the ring $\mathbb{F}_q[e], e^3 = e^2$. Bol. Soc. Paran. Mat. (3s.) **42** (2024), doi: https://doi.10.5269/bspm.62308.

[12] A. Chillali, M. B. T. El Hamam, A. Grini, Twisted Hessian curve over a local ring.Bol. Soc. Paran. Mat. (3s.) **42** (2024), doi: https://doi.10.5269/bspm.62583.

Author information

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

Received: 2024-06-08
Accepted: 2024-11-03