sciendo

TATRA MOUNTAINS
Mathematical Publications
DOI: 10.2478/tmmp-2023-0004
Tatra Mt. Math. Publ. **83** (2023), 43–50

TWISTED EDWARDS CURVE OVER THE RING $\mathbb{F}_q[e], e^2 = 0$

Moha Ben Taleb El Hamam[1] — Abdelhakim Chillali[2] — Lhoussain El Fadil[1]

[1]Sidi Mohamed Ben Abdellah University, Fez, MOROCCO

[2]Sidi Mohamed Ben Abdellah University, Taza, MOROCCO

ABSTRACT. Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of an odd prime number. In this paper, we study the twisted Edwards curves denoted $E_{E_{a,d}}$ over the local ring $\mathbb{F}_q[e]$, where $e^2 = 0$. In the first time, we study the arithmetic of the ring $\mathbb{F}_q[e]$, $e^2 = 0$. After that we define the twisted Edwards curves $E_{E_{a,d}}$ over this ring and we give essential properties and we define the group $E_{E_{a,d}}$, these properties. Precisely, we give a bijection between the groups $E_{E_{a,d}}$ and $E_{E_{a_0,d_0}} \times \mathbb{F}_q$, where $E_{E_{a_0,d_0}}$ is the twisted Edwards curves over the finite field $\mathbb{F}_q$.

1. Introduction

In 2007, Edwards [8] introduced a new normal form of elliptic curves on a field K with a characteristic other than 2. This model has been shown to be very promising because it achieves these two objectives are the complete and faster law of addition. Bernstein et al [1], introduced twisted Edwards curves with an equation

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

For $Z \neq 0$ the homogeneous point $(X : Y : Z)$ represents the affine point $(X/Z, Y/Z)$ identified by (X, Y), with an equation: $aX^2 + Y^2 = 1 + dX^2Y^2$, and presented explicit formulas for addition and doubling over a finite field K, where $ad(a - d) \neq 0$. The addition law is defined by:

$$(X_1, Y_1) + (X_2, Y_2) = \left(\frac{X_1Y_2 + Y_1X_2}{1 + dX_1X_2Y_1Y_2}, \frac{Y_1Y_2 - aX_1X_2}{1 - dX_1X_2Y_1Y_2} \right),$$

2020 Mathematics Subject Classification: 11T71, 14G50, 94A60.
Keywords: elliptic curves, twisted Edwards curves, cryptography.

the group operations on Edwards curves were faster than those of most other elliptic curve models known at the time. In [6], Boudabra and his co-authors studied the twisted Edwards curves on the finite field $\mathbb{Z}/p\mathbb{Z}$, where $p \geq 5$ is a prime number, and on the rings $\mathbb{Z}/p^r\mathbb{Z}$ and $\mathbb{Z}/p^rq^s\mathbb{Z}$. In [2], 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 [4]).

In this work we study twisted Edwards curves over the ring $\mathbb{F}_q[e], e^2 = 0$. The motivation for this paper is the search for new groups of points of a twisted Edwards curve over a finite ring, where the complexity of the discrete logarithm calculation is good for use in cryptography. For further works in the same direction, we refer the reader to [3, 5]. Let $\mathbb{F}_q$ be a finite field of q elements, where $q = p^c$ is a power of an odd prime number p and $c \in \mathbb{N}^*$.

We started this article by studying the arithmetic of the ring $\mathbb{F}_q[e], e^2 = 0$. In Section 3, we will define the twisted Edwards curves $E_{E_{a,d}}\big(\mathbb{F}_q[e]\big)$ over this ring. Moreover, we will define the group extension

$$E_{E_{a,d}}\big(\mathbb{F}_q[e]\big) \text{ of } E_{E_{a_0,d_0}}(\mathbb{F}_q)$$

and give a bijection between the groups $E_{E_{a,d}}$ and $E_{E_{a_0,d_0}} \times \mathbb{F}_q$, where $E_{E_{a_0,d_0}}$ is the twisted Edwards curves over the finite field $\mathbb{F}_q$. Furthermore, we close this paper, by giving a link between the group $E_{E_{a,d}}$ and cryptography. We deduce that the discrete logarithm problem in $E_{E_{a,d}}$ is equivalent to the discrete logarithm problem in $E_{E_{a_0,d_0}} \times \mathbb{F}_q$ and $\#(E_{E_{a,d}}) = p^c\#(E_{E_{a_0,d_0}})$.

2. The ring $\mathbb{F}_q[e], e^2 = 0$

Let p be a prime number ≥ 3, we consider the quotient ring $A_2 = \frac{\mathbb{F}_q[X]}{X^2}$, where $\mathbb{F}_q$ is the finite field of characteristic p and q elements. The ring A_2 is identified to the ring $\mathbb{F}_q[e], e^2 = 0$. So, we have

$$A_2 := \mathbb{F}_q[e] = \{x_0 + x_1e/(x_0, x_1) \in (\mathbb{F}_q)^2\}.$$

The arithmetic operations in A_2 can be decomposed into operations in $\mathbb{F}_q$ and they are computed as follows:

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

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

A. Chillali in [7] has proved the following results:

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

Remark 1. We denote by π the canonical projection defined by

$$\begin{array}{rcll} \pi & : & A_2 & \to \mathbb{F}_q, \\ & & x_0 + x_1 e & \mapsto x_0. \end{array}$$

3. Twisted Edwards curves over the ring A_2

Let X, Y, a and d be four elements of A_2 such that $X = x_0+x_1e$, $Y = y_0+y_1e$, $a = a_0 + a_1e$ and $d = d_0 + d_1e$.

Definition 3.1. A twisted Edwards curve is defined over A_2 by the equation $aX^2 + Y^2 = 1 + dX^2Y^2$, such that $\Delta = ad(a - d)$ is invertible in A_2. We denote it by $E_{E_{a,d}}$,

$$E_{E_{a,d}} = \left\{(X, Y) \in A_2^2 \mid aX^2 + Y^2 = 1 + dX^2Y^2\right\}.$$

Lemma 3.2. *Let $\Delta_0 = a_0d_0(a_0 - d_0)$, then $\pi(\Delta) = \Delta_0$.*

Proof. Let $X, Y \in A_2$, we have

$$\pi(X + Y) = \pi(X) + \pi(Y) \quad \text{and} \quad \pi(XY) = \pi(X)\pi(Y).$$

So, $\pi(\Delta) = \Delta_0$. □

Corollary 3.3. *Δ is invertible in A_2 if and only if $\Delta_0 \neq 0$.*

Proof. Since $\pi(\Delta) = \Delta_0$, then Δ is invertible in A_2 if and only if Δ_0 is invertible in $\mathbb{F}_q$. Which is equivalent to $\Delta_0 \neq 0$. □

Using Corollary 3.3, if Δ is invertible in A_2, then $E_{E_{\pi(a),\pi(d)}}(\mathbb{F}_q)$ is twisted Edwards curves over the finite field $\mathbb{F}_q$ and we notice $E_{E_{a_0,d_0}}$, we write

$$E_{E_{a_0,d_0}} = \left\{(x_0, y_0) \in (\mathbb{F}_q)^2 \mid a_0x_0^2 + y_0^2 = 1 + d_0x_0^2y_0^2\right\}.$$

Theorem 3.4. *Let $a = a_0+a_1e$, $d = d_0+d_1e$, $X = x_0+x_1e$, and $Y = y_0+y_1e$, are elements of A_2, with*

$$aX^2 + Y^2 = 1 + dX^2Y^2, \tag{1}$$

then

$$a_0x_0^2 + y_0^2 = 1 + d_0x_0^2y_0^2 + (D + Ax_1 + By_1)e, \tag{2}$$

where

$$A = 2d_0x_0y_0^2 - 2a_0x_0, \qquad B = 2d_0x_0^2y_0 - 2y_0, \qquad D = d_1x_0^2y_0^2 - a_1x_0^2.$$

P r o o f. We have

$$\begin{aligned} aX^2+Y^2 &= (a_0+a_1e)(x_0+x_1e)^2+(y_0+y_1e)^2 \\ &= (a_0+a_1e)(x_0^2+2x_0x_1e)+y_0^2+2y_0y_1e \\ &= a_0x_0^2+2a_0x_0x_1e+a_1x_0^2e+y_0^2+2y_0y_1e \\ &= a_0x_0^2+y_0^2+(2a_0x_0x_1+a_1x_0^2+2y_0y_1)e, \end{aligned}$$

$$\begin{aligned} 1+dX^2Y^2 &= 1+(d_0+d_1e)(x_0x_1e)^2(y_0+y_1e)^2 \\ &= 1+(d_0+d_1e)(x_0^2+2x_0x_1e)(y_0^2+2y_0y_1e) \\ &= 1+d_0x_0^2y_0^2+(2d_0x_0^2y_0y_1+2d_0x_0x_1y_0^2+d_1x_0^2y_0^2)e. \end{aligned}$$

If $aX^2+Y^2=1+dX^2Y^2$, then

$$a_0x_0^2+y_0^2=1+d_0x_0^2y_0^2+[D+Ax_1+By_1]e,$$

where

$$A=2d_0x_0y_0^2-2a_0x_0, \qquad B=2d_0x_0^2y_0-2y_0, \qquad D=d_1x_0^2y_0^2-a_1x_0^2. \quad \square$$

Corollary 3.5. *If* $(X,Y)\in E_{E_{a,d}}$*, then* $(x_0,y_0)\in E_{E_{a_0,d_0}}$.

P r o o f. If $(X,Y)\in E_{E_{a,d}}$, then $aX^2+Y^2=1+dX^2Y^2$. So, by Theorem 3.4 we have

$$a_0x_0^2+y_0^2=1+d_0x_0^2y_0^2+[D+Ax_1+By_1]e.$$

Or $(1,e)$ is a basis of A_2, then $a_0x_0^2+y_0^2=1+d_0x_0^2y_0^2$. Thus $(x_0,y_0)\in E_{E_{a_0,d_0}}$. $\square$

4. The group law over $E_{E_{a,d}}$

Bernstein et al [1] also presented explicit formulas for addition and doubling on a twisted Edwards curve, these formulas are complete if a is a square and d a non-square in the underlying field.

Let (X_1,Y_1), (X_2,Y_2) two points on the twisted Edwards curve $E_{E_{a,d}}$ found by the equation

$$aX^2+Y^2=1+dX^2Y^2,$$

the sum of these points on $E_{E_{a,d}}$ is

$$(X_1,Y_1)+(X_2,Y_2)=\left(\frac{X_1Y_2+Y_1X_2}{1+dX_1X_2Y_1Y_2},\frac{Y_1Y_2-aX_1X_2}{1-dX_1X_2Y_1Y_2}\right), \ (*)$$

the neutral element is $(0,1)$ and the inverse of (X_1,Y_1) is $(-X_1,Y_1)$, these formulas are complete if a_0 is a square and d_0 a non-square in the field $\mathbb{F}_q$.

Corollary 4.1. $(E_{E_{a,d}},+)$ *is an abelian group with* $(0,1)$ *as identity element.*

Corollary 4.2. *The mapping $\tilde{\pi}$ is well defined, where is given by*

$$\begin{array}{rcl} \tilde{\pi} \; : \; E_{E_{a,d}} & \to & E_{E_{a_0,d_0}}, \\ (X,Y) & \mapsto & \big(\pi(X), \pi(Y)\big). \end{array}$$

P r o o f. From the previous theorem, we have $\big(\pi(X), \pi(Y)\big) \in E_{E_{a_0,d_0}}$ If $(X_1, Y_1) = (X_2, Y_2)$, then

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

□

Lemma 4.3. *$\tilde{\pi}$ is a surjective homomorphism of groups.*

P r o o f. Let $(x_0, y_0) \in E_{E_{a_0,d_0}}$, then there exists $(X, Y) \in E_{E_{a,d}}$, such that

$$\tilde{\pi}(X, Y) = (x_0, y_0).$$

By Theorem 3.4, we have

$$a_0x_0^2 + y_0^2 = 1 + d_0x_0^2y_0^2 + (D + Ax_1 + By_1)e,$$

or $(1, e)$ is a basis of A_2, then $D = -(Ax_1 + By_1)$.

Put $f(x, y) = a_0x^2 + y^2 - 1 - d_0x^2y^2$, we have

$$\frac{\partial f}{\partial x}(x_0, y_0) = 2a_0x_0 - 2d_0x_0y_0^2 = -A$$

and

$$\frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 - 2d_0x_0^2y_0 = -B.$$

Coefficients $-A$ and $-B$ are partial derivatives of a function $f(x, y)$ at the point (x_0, y_0), can not be all null. We can then, finally, conclude that (x_1, y_1) exists. Thus, $\tilde{\pi}$ is a surjective. □

Lemma 4.4. *The mapping*

$$\begin{array}{rcl} \theta \; : \; \mathbb{F}_q & \to & E_{E_{a,d}}, \\ x & \mapsto & (xe, 1) \end{array}$$

is an injective homomorphism.

P r o o f. Evidently, θ is well defined and injective. Let

$$x_1, x_2 \in \mathbb{F}_q, P = (x_1e, 1) \quad \text{and} \quad Q = (x_2e, 1).$$

By $(*)$ we have $P + Q = \big((x_1 + x_2)e, 1\big)$, then $\theta(x_1 + x_2) = \theta(x_1) + \theta(x_2)$, and we conclude that θ is injective homomorphism of groups. □

Corollary 4.5. *Let $H = \theta(\mathbb{F}_q)$, then $H = \ker(\tilde{\pi})$.*

P r o o f. Let $(xe, 1) \in H$, then $\tilde{\pi}(xe, 1) = (0, 1)$. We conclude that $(xe, 1) \in \ker(\tilde{\pi})$, thus $H \subset \ker(\tilde{\pi})$. Let $P = (X, Y) \in \ker(\tilde{\pi})$, then $\tilde{\pi}(X, Y) = (0, 1)$. So,

$$X = xe, \qquad Y = 1 + ye, -1ex$$

according to the equation

$$aX^2 + Y^2 = 1 + dX^2Y^2,$$

we have $y = 0$, then $(X, Y) = (xe, 1)$. Thus $\ker(\tilde{\pi}) \subset H$. Finally, $H = \ker(\tilde{\pi})$. □

Lemma 4.6. *The group H is an elementary abelian $p-$group.*

P r o o f. Let $P = (xe, 1) \in H$, we denote $2P = P + P$ and $(n+1)P = nP + P$ for all $n \geq 2$. We have from Lemma 4.4 $2P = (2xe, 1)$ and we claim that $pP = (pxe, 1) = (0, 1)$ by sum $(*)$, which completes the proof of the lemma. □

Theorem 4.7. *The sequence*

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

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

P r o o f. $\tilde{\pi}$ is a surjective homomorphism of groups, $H = \theta(\mathbb{F}_q) = \ker(\tilde{\pi})$ and θ is an injective homomorphism. We deduce the sequence

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

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

Theorem 4.8. *Let $n = \#(E_{E_{a_0,d_0}})$ the cardinality of $E_{E_{a_0,d_0}}$. If p does not divide n, then the short exact sequence*

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

is split.

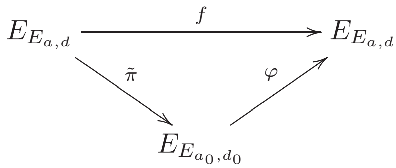
P r o o f. p doesn't divide n, then exists an integer b such that $nb = 1 \pmod{p}$. So, there is an integer m such that $1 - nb = pm$. Let f the homomorphism defined by

$$\begin{array}{rcccl} f & : & E_{E_{a,d}} & \to & E_{E_{a,d}}, \\ & & P & \mapsto & (1-nb)P\,. \end{array}$$

We have

$$\begin{array}{rcccl} \tilde{\pi} & : & E_{E_{a,d}} & \to & E_{E_{a_0,d_0}}, \\ & & (X,Y) & \mapsto & \big(\pi(X), \pi(Y)\big) \end{array}$$

is a surjective homomorphism of groups using Lemma 4.3. Then, there exists a unique morphism φ, such that the following diagram commutes:



Indeed, let $P \in \ker(\tilde{\pi}) = \theta(\mathbb{F}_q)$, then $\exists x \in \mathbb{F}_q$ such that $P = (xe, 1)$. We have from Lemma 4.6, $(1 - nb)P = pmP = (0, 1)$, then $P \in \ker(f)$. It follows that $\ker(\tilde{\pi}) \subseteq \ker(f)$, this prove the above assertion.

Now we prove that

$$\tilde{\pi} o \varphi = id_{E_{E_{a_0,d_0}}}.$$

Let $P' \in E_{E_{a_0,d_0}}$, since $\tilde{\pi}$ is surjective, then there exists a $P \in E_{E_{a,d}}$ such that $\tilde{\pi}(P) = P'$. We have

$$\varphi(P') = (1 - nb)P = P - nbP \quad \text{and} \quad nP' = (0, 1),$$

then $n\tilde{\pi}(P) = (0, 1)$ and $\tilde{\pi}(nP) = (0, 1)$ implies that $nP \in \ker(\tilde{\pi})$ and so, $nbP \in \ker(\tilde{\pi})$, therefore $\tilde{\pi}(nbP) = (0, 1)$. On the other hand,

$$\varphi(P') = (1 - nb)P = P - nbP,$$

then

$$\tilde{\pi} o \varphi(P') = \tilde{\pi}(P) - (0, 1) = P' \quad \text{and so,} \quad \tilde{\pi} \circ \varphi = id_{E_{E_{a_0,d_0}}}.$$

Hence the sequence is split. □

Corollary 4.9. *If p does not divide $\#(E_{E_{a_0,d_0}})$ then, $E_{E_{a,d}} \cong E_{E_{a_0,d_0}} \times \mathbb{F}_q$*

P r o o f. From the Theorem 4.8 the sequence

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

is split then, $E_{E_{a,d}} \cong E_{E_{a_0,d_0}} \times H$ and since $H = \ker(\tilde{\pi}) = Im\theta \cong \mathbb{F}_q$, then the corollary is proved. □

5. Conclusion

In this work, we have proved the bijection between $E_{E_{a,d}}$ and $E_{E_{a_0,d_0}} \times \mathbb{F}_q$. In cryptography applications, we deduce that the discrete logarithm problem in $E_{E_{a,d}}$ is equivalent to the discrete logarithm problem in $E_{E_{a_0,d_0}} \times \mathbb{F}_q$ and $\#(E_{E_{a,d}}) = p^c \#(E_{E_{a_0,d_0}})$, which is an important and useful factor in cryptography since it allows to obtain a huge number of points with a smaller prime p.

REFERENCES

[1] BERNSTEIN, D. J.—BIRKNER, P.—JOYE, M.—LANGE, T.—PETERS, C.: *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] ELHAMAM, M. B. T.— CHILLALI, A.—EL FADIL, L.: *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, pp. 1–4,
DOI: 10.1109/IRASET52964.2022.9738249.

[3] 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. Mat. (3s.) **40** (2022), 1–6,
DOI: https://doi.org/10.5269/bspm.51867

[4] ELHAMAM, M.B.T.— CHILLALI, A.—EL FADIL, L.: *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

[5] ELHAMAM, M.B.T.—GRINI, A.—CHILLALI, A.—EL FADIL, L.: *El Gamal cryptosystem on a Montgomery curves over non local ring*, WSEAS Trans. Math. **21** (2022), 85–89.

[6] BOUDABRA, M.—NITAJ, A.: *A new public key cryptosystem based on Edwards curves.* J. Appl. Math. Comput. **61** (2019), no. 1–2, 431–450.

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

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

Received November 1, 2022

M.B.T. EL HAMAM
L. EL FADIL
Department of Mathematics
Faculty of Sciences
Sidi Mohamed Ben Abdellah University
Fez, MOROCCO
E-mail: mohaelhomam@gmail.com
lhouelfadil2@gmail.com

A. Chillali
Department of Mathematics
Faculty of Polydisciplimary
Sidi Mohamed Ben Abdellah University
Taza, MOROCCO
E-mail: abdelhakim.chillali@usmba.ac.ma