






# A New Addition Law in Twisted Edwards Curves on Non Local Ring

Moha Ben Taleb Elhamam<sup>1</sup> , Abdelhakim Chillali<sup>2</sup> ,  
and Lhoussain El Fadil<sup>1</sup> 

<sup>1</sup> Sidi Mohamed Ben Abdellah University, FSDM, Fez, Morocco

<sup>2</sup> Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco

abdelhakim.chillali@usmba.ac.ma

**Abstract.** Let  $\mathbb{F}_q$  be a finite field of  $q$  elements with  $q = p^r$  for some odd prime integer  $p$  and a positive integer  $r$ . Let  $R = \mathbb{F}_q[e]$ , where  $e^2 = e$ . The purpose of this paper is to investigate  $E_{E,a,d}(R)$  be the twisted Edwards curves over  $R$ , with  $a, d \in R$ . In the end of the paper, we study the complexity of this new addition law in  $E_{E,a,d}(R)$  and highlight some links of our results with elliptic curves cryptosystem.

**Keywords:** Twisted Edwards curves · Addition law · Cryptography

## 1 Introduction

The use of elliptic curves in cryptography is an important tool in several cryptography going back independently to Koblitz [10] and Miller [11]. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. It allows smaller keys to provide equivalent security compared to other cryptosystem. It can also be used to encrypt images of different sizes in embedded systems such as in (cf. [12–14]). In particular, it is shown that Edwards curves and twisted Edwards curves can be very useful to improve the efficiency of protocols (cf. [1–4]). Let us quote here some interesting works that are related to the subject of our paper. In 2007, Edwards introduced a new normal form for elliptic curves on a field  $K$  with characteristic an odd prime  $p$ , containing a unified addition formula for adding and doubling points (cf. [1]). Bernstein and Lange, presented fast explicit formulas for group operations on an Edwards curve and they compared it to the different shapes of elliptic curves and different coordinate systems for base group operations. The comparison indicated that the Edwards curve is a good choice in cryptography (cf. [2]).

Thereafter, in 2008, Bernstein and his co-authors introduced the twisted Edwards curves with equation:

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2. \quad (1)$$

For  $Z \neq 0$  the homogeneous point  $(X : Y : Z)$  represents the affine point  $(X/Z, Y/Z)$  of equation:  $aX^2 + Y^2 = 1 + dX^2Y^2$ , where  $a, d \in K$  are non zero

and distinct. In addition, they introduced explicit formulas for addition and doubling over a finite field  $K$  as follows:

$$(X_1, Y_1) + (X_2, Y_2) = \left( \frac{X_1 Y_2 + Y_1 X_2}{1 + d X_1 X_2 Y_1 Y_2}, \frac{Y_1 Y_2 - a X_1 X_2}{1 - d X_1 X_2 Y_1 Y_2} \right),$$

the group operations on Edwards curves were faster than those of most other elliptic curve models known at the time. The mentioned authors gave quick explicit formulas for twisted Edwards curves in projective and inverted coordinates. Furthermore, they showed that twisted Edwards curves save more times than many other curves (cf. [3]). In the same year, Bernstein and his co-authors introduced the binary Edwards curves (cf. [5]). In 2019, Boudabra and Nitaj studied the twisted Edwards curves on the finite field  $\mathbb{F}_p$  where  $p \geq 5$  is a prime number, and they extend their study to the ring  $\mathbb{Z}/p^r\mathbb{Z}$  and  $\mathbb{Z}/p^r q^s\mathbb{Z}$ . They also proposed a new scheme and studied its efficiency and security (cf. [4]). In the current work, we study twisted Edwards curves over the ring  $R = \mathbb{F}_q[e]$ , with  $e^2 = e$  and  $\mathbb{F}_q$  the finite field of order  $q = p^n$ ,  $n$  a positive integer, and  $p$  an odd prime integer. Furthermore, we give the relation between twisted Edwards curves over a finite field  $\mathbb{F}_q$  and twisted Edwards curves over the ring  $R$ . In 2022, Elhamam and his co-authors studied the binary Edwards curves on the ring  $\mathbb{F}_{2^n}[e]$ ,  $e^2 = e$  (cf. [8]). This paper is structured as follows: In Sect. 2, we collect some known arithmetic properties of the ring  $R$  which we need to use in the remainder. In Sect. 3, we define the twisted Edwards curves  $E_{E,a,d}(R)$  over  $R$  and study the invertibility of  $ab(a - b)$  in  $R$ , which allows us to define the two twisted Edwards curves  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$  and  $E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ , where  $\pi_0$  and  $\pi_1$  are two surjective morphisms of rings defined by:

$$\begin{aligned} \pi_0 : \mathbb{F}_q[e] &\rightarrow \mathbb{F}_q & \text{and} & & \pi_1 : \mathbb{F}_q[e] &\rightarrow \mathbb{F}_q \\ x_0 + x_1 e &\mapsto x_0 & & & x_0 + x_1 e &\mapsto x_0 + x_1. \end{aligned}$$

Next, we present the elements of  $E_{a,d}(R)$  and give a bijection between the two sets;  $E_{E,a,d}(R)$  and  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ . Section 4 is dedicated to the study of the addition in twisted Edwards curves over the ring  $R$ . We define the additive law  $P \tilde{+} Q$  in  $E_{E,a,d}(R)$  by  $P \tilde{+} Q = \tilde{\pi}^{-1}(\tilde{\pi}(P) + \tilde{\pi}(Q))$ , for all points  $P$  and  $Q$  of  $E_{E,a,d}(R)$ , and we conclude that the map  $\tilde{\pi}$  is an isomorphism between the groups  $E_{E,a,d}(R)$  and  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ . Thereafter, we study the complexity of the sum law in the twisted Edwards curve  $E_{E,a,d}(R)$ . We conclude by highlighting some links of our results with cryptography. For more works in this direction we refer the reader to [7, 9].

## 2 The Ring $\mathbb{F}_q[e]$ , $e^2 = e$

Let  $\mathbb{F}_q$  be a finite field with  $q = p^r$  for some odd prime integer  $p$  and a positive integer  $r$ . Consider the quotient ring  $R = \frac{\mathbb{F}_q[X]}{X^2 - X}$ . Since  $X^2 - X$  is the minimal polynomial of  $e$  over  $\mathbb{F}_q$ , the ring  $R$  is identified to the ring  $\mathbb{F}_q[e]$ , where  $e^2 = e$ . Therefore,

$$R = \{x_0 + x_1 e \mid (x_0, x_1) \in (\mathbb{F}_q)^2\}.$$

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

$$\begin{aligned} X + Y &= (x_0 + y_0) + (x_1 + y_1)e, \\ X \cdot Y &= (x_0y_0) + (x_0y_1 + x_1y_0 + x_1y_1)e. \end{aligned}$$

Then we have the following known proprieties [6] :

1.  $(R, +, \cdot)$  is a finite unitary commutative ring.
2.  $R$  is an  $\mathbb{F}_q$ -vector space of dimension 2 with  $\mathbb{F}_q$ -basis  $\{1, e\}$ .
3.  $X \cdot Y = (x_0y_0) + ((x_0 + x_1)(y_0 + y_1) - x_0y_0)e$ .
4.  $X^2 = x_0^2 + ((x_0 + x_1)^2 - x_0^2)e$ .
5.  $X^3 = x_0^3 + ((x_0 + x_1)^3 - x_0^3)e$ .
6. Put  $X = x_0 + x_1e \in R$ . Then,  $X$  is invertible in  $R$  if and only if  $x_0 \neq 0$  and  $x_0 + x_1 \neq 0$ . In this case we have,  $X^{-1} = x_0^{-1} + ((x_0 + x_1)^{-1} - x_0^{-1})e$ .
7.  $R$  is a non local ring.
8.  $\pi_0$  and  $\pi_1$  are two surjective morphisms of rings.

In the remainder of this paper we *assume that*  $p \neq 2$ .

### 3 Twisted Edwards Curves over the Ring $R$

Let  $X, Y, a$  and  $d$  be four elements of  $R$  such that  $X = x_0 + x_1e, Y = y_0 + y_1e, a = a_0 + a_1e$  and  $d = d_0 + d_1e$ . We recall that a twisted Edwards curve is defined over finite fields. By analogous, we extend it as follows:

**Definition 1.** *A twisted Edwards curve is defined over  $R$  is defined by the equation:*

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

such that  $\Delta = ad(a - d)$  is invertible in  $R$ . We denote it by  $E_{E,a,d}(R)$ ;

$$E_{E,a,d}(R) := \{(X, Y) \in R \mid aX^2 + Y^2 = 1 + dX^2Y^2\}.$$

The following proposition allows to test the inversibility of  $\Delta$ .

**Proposition 1.** *Let  $\Delta_0 = a_0d_0(a_0 - d_0)$  and  $\Delta_1 = (a_0 + a_1)(d_0 + d_1)((a_0 + a_1) - (d_0 + d_1))$ . Then,*

$$\Delta = \Delta_0 + (\Delta_1 - \Delta_0) \text{ and } \begin{cases} \Delta_0 = \pi_0(\Delta) \\ \Delta_1 = \pi_1(\Delta). \end{cases}$$

**Proof.** We have:

$$\begin{aligned} \Delta &= ad(a - d) \\ &= (a_0 + a_1e)(d_0 + d_1e)((a_0 + a_1e) - (d_0 + d_1e)) \\ &= [a_0d_0 + (a_0d_1 + a_1d_0 + a_1d_1)e][(a_0 - d_0) + (a_1 - d_1)e] \\ &= a_0d_0(a_0 - d_0) + [a_0d_0(a_1 - d_1) + (a_0d_1 + a_1d_0 + a_1d_1)(a_0 - d_0) + (a_0d_1 + a_1d_0 + a_1d_1)(a_1 - d_1)]e \\ &= a_0d_0(a_0 - d_0) + [(a_0 + a_1)(d_0 + d_1)((a_0 + a_1) - (d_0 + d_1)) - a_0d_0(a_0 - d_0)]e \\ &= \Delta_0 + (\Delta_1 - \Delta_0)e. \end{aligned}$$

Thus,  $\Delta_0 = \pi_0(\Delta)$  and  $\Delta_1 = \pi_1(\Delta)$ . □

The following corollary is an immediate consequence of Proposition 1.

**Corollary 1.**  $\Delta$  is invertible in  $R$  if and only if  $\Delta_0 \neq 0$  and  $\Delta_1 \neq 0$ .

By Corollary 1, if  $\Delta$  is invertible in  $R$ , then  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$  and  $E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$  are two twisted Edwards curves over the finite field  $\mathbb{F}_q$ . Note that

$$E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) = \{(x, y) \in (\mathbb{F}_q)^2 \mid a_0x^2 + y^2 = 1 + d_0x^2y^2\},$$

$$E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q) = \{(x, y) \in (\mathbb{F}_q)^2 \mid (a_0 + a_1)x^2 + y^2 = 1 + (d_0 + d_1)x^2y^2\}.$$

The following theorem characterizes the points of the twisted Edwards curves.

**Theorem 1.** Let  $X$  and  $Y$  be two elements of  $R$ .  $(X, Y) \in E_{E,a,d}(R)$  if and only if  $(\pi_i(X), \pi_i(Y)) \in E_{E,\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$ , for  $i \in \{0, 1\}$ .

**Proof.** We have:

$$\begin{aligned} aX^2 + Y^2 &= (a_0 + a_1e)(x_0 + x_1e)^2 + (y_0 + y_1e)^2 \\ &= (a_0 + a_1e)(x_0^2 + ((x_0 + x_1)^2 - x_0^2)e) + y_0^2 + ((y_0 + y_1)^2 - y_0^2)e \\ &= a_0x_0^2 + y_0^2 + [(a_0 + a_1)(x_0 + x_1)^2 + (y_0 + y_1)^2 - a_0x_0^2 - y_0^2]e, \text{ and} \end{aligned}$$

$$\begin{aligned} 1 + dX^2Y^2 &= 1 + (d_0 + d_1e)(x_0 + x_1e)^2(y_0 + y_1e)^2 \\ &= 1 + (d_0 + d_1e)(x_0^2 + ((x_0 + x_1)^2 - x_0^2)e)(y_0^2 + ((y_0 + y_1)^2 - y_0^2)e) \\ &= 1 + d_0x_0^2y_0^2 + [(d_0 + d_1)(x_0 + x_1)^2(y_0 + y_1)^2 - d_0x_0^2y_0^2]e, \end{aligned}$$

As  $\{1, e\}$  is an  $\mathbb{F}_q$ -basis of the  $\mathbb{F}_q$ -vector space  $R$ , then  $aX^2 + Y^2 = 1 + dX^2Y^2$  if and only if

$$\begin{cases} a_0x_0^2 + y_0^2 = 1 + d_0x_0^2y_0^2 \\ \text{and} \\ (a_0 + a_1)(x_0 + x_1)^2 + (y_0 + y_1)^2 = 1 + (d_0 + d_1)(x_0 + x_1)^2(y_0 + y_1)^2 \end{cases}.$$

Which gives the result. □

**Corollary 2.** The mapping:

$$\begin{aligned} \tilde{\pi}_i : E_{E,a,d}(R) &\rightarrow E_{E,\pi_i(a),\pi_i(d)}(\mathbb{F}_q) \\ (X, Y) &\mapsto (\pi_i(X), \pi_i(Y)) \end{aligned}$$

is well defined,  $i \in \{0, 1\}$ .

**Proof.** By Theorem 1, we have  $(\pi_i(X), \pi_i(Y)) \in E_{E,\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$ . If  $(X_1, Y_1) = (X_2, Y_2)$ , then  $X_2 = X_1$  and  $Y_2 = Y_1$ . Therefore,

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

□

Now we classify the elements of  $E_{E,a,d}(R)$ . In fact we have:

**Proposition 2.** *The elements of  $E_{E,a,d}(R)$  are of the form:*

- $(X, Y)$  such that  $X$  is invertible,
- $(xe, \alpha + ye)$  such that  $\alpha \in \{-1, 1\}$  and  $(x, \alpha + y) \in E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ ,
- $(x - xe, y + (\alpha - y)e)$  such that  $\alpha \in \{-1, 1\}$  and  $(x, y) \in E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ .

**Proof.** Let  $P = (X, Y) \in E_{E,a,d}(R)$ , where  $X = x_0 + x_1e$  and  $Y = y_0 + y_1e$ . We distinguish two cases of  $X$ :

The First case:  $X$  is invertible.

The second case:  $X$  is not invertible. In this case we distinguish the next two sub-cases:

- i) If  $X = xe$ , where  $x \in \mathbb{F}_q$ , we have:  $\pi_0(xe, y_0 + y_1e) = (0, y_0) \in E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$  then,  $(0, y_0) = (0, 1)$  or  $(0, y_0) = (0, -1)$ , so  $(xe, Y) = (xe, \alpha + ye)$  such that  $(x, \alpha + y) \in E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ ;  $\alpha \in \{-1, 1\}$ .
- ii) If  $X = x - xe$ , where  $x \in \mathbb{F}_q$ , then we have:  $\pi_1(x - xe, y_0 + y_1e) = (0, y_0 + y_1) \in E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$  then,  $(0, y_0 + y_1) = (0, 1)$  or  $(0, y_0 + y_1) = (0, -1)$ , so  $(x - xe, Y) = (x - xe, y + (\alpha - y)e)$  such that  $(x, y) \in E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$ ;  $\alpha \in \{-1, 1\}$ .

□

**Corollary 3.** *The maps  $\tilde{\pi}_0$  and  $\tilde{\pi}_1$  are surjective.*

**Proof.** Let  $(x, y) \in E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$  (resp.  $(x', y') \in E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ ), then  $(x - xe, y + (1 - y)e)$  (resp.  $(x'e, 1 + (y' - 1)e)$ ) is an antecedent of  $(x, y)$  (resp.  $(x', y')$ ). □

The following theorem establishes a 1 - 1 correspondence between  $E_{E,a,d}(R)$  and  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ , and so it will be used to calculate the cardinal of  $E_{E,a,d}(R)$  in Corollary 4.

**Theorem 2.** *The map  $\tilde{\pi}$  defined by:*

$$\begin{aligned} \tilde{\pi} : E_{E,a,d}(R) &\rightarrow E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q) \\ (X, Y) &\mapsto ((\pi_0(X), \pi_0(Y)), (\pi_1(X), \pi_1(Y))) \end{aligned}$$

*is a bijection.*

**Proof.**

- As  $\tilde{\pi}_0$  and  $\tilde{\pi}_1$  are well defined, then  $\tilde{\pi}$  is well defined.
- Let  $((x_0, y_0), (x_1, y_1)) \in E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ , then

$$\begin{aligned} a_0x_0^2 + y_0^2 &= 1 + d_0x_0^2y_0^2, \\ (a_0 + a_1)x_1^2 + y_1^2 &= 1 + (d_0 + d_1)x_1^2y_1^2, \end{aligned}$$

Put  $X = x_0 + (x_1 - x_0)e$  and  $Y = y_0 + (y_1 - y_0)e$ . We have:

$$\begin{aligned} aX^2 + Y^2 &= a_0x_0^2 + y_0^2 + [(a_0 + a_1)x_1^2 + y_1^2 - a_0x_0^2 - y_0^2]e, \\ 1 + dX^2Y^2 &= 1 + d_0x_0^2y_0^2 + [(d_0 + d_1)x_1^2y_1^2 - d_0x_0^2y_0^2]e, \end{aligned}$$

So  $(X, Y) \in E_{E,a,d}(R)$ . Note that  $\tilde{\pi}((x_0 + (x_1 - x_0)e, y_0 + (y_1 - y_0)e)) = ((x_0, y_0), (x_1, y_1))$ . Hence  $\tilde{\pi}$  is a surjective map.

- Let  $(X, Y)$  and  $(X', Y')$  are elements of  $E_{E,a,d}(R)$ , where  $X = x_0 + x_1e$ ,  $Y = y_0 + y_1e$ ,  $X' = x'_0 + x'_1e$ ,  $Y' = y'_0 + y'_1e$ . If  $(x_0, y_0) = (x'_0, y'_0)$  and  $(x_0 + x_1, y_0 + y_1) = (x'_0 + x'_1, y'_0 + y'_1)$ , then

$$\begin{cases} x'_0 = x_0 \\ y'_0 = y_0 \end{cases} \text{ and } \begin{cases} x'_1 = x_1 \\ y'_1 = y_1. \end{cases}$$

Therefore,  $\tilde{\pi}$  is an injective application.

We can easily show that the mapping  $\tilde{\pi}^{-1}$  defined by:

$$\tilde{\pi}^{-1}((x_0, y_0), (x_1, y_1)) = (x_0 + (x_1 - x_0)e, y_0 + (y_1 - y_0)e)$$

is the converse of  $\tilde{\pi}$ .

□

**Corollary 4.** *The cardinal of  $E_{E,a,d}(R)$  equals to the cardinal of  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ .*

*Example 1.* In  $R = \mathbb{F}_5[e]$ , let  $a = 1 + 3e$  and  $d = 2 + 3e$ . We have:

$$\begin{aligned} E_{E,a,d}(R) &= \{(0, 1), (0, 4), (0, 1 + 3e), (0, 4 + 2e), (2, 2 + 3e), (2, 3 + 2e), (3, 2 + 3e), (3, 3 + 2e), \\ &\quad (2e, 1 + 4e), (2e, 4 + e), (3e, 1 + 4e), (3e, 4 + e), (1 + 4e, e), (1 + 4e, 4e), \\ &\quad (2 + e, 2 + 3e), (2 + e, 3 + 2e), (2 + 3e, 2 + 2e), (2 + 3e, 2 + 4e), (2 + 3e, 3 + 3e), \\ &\quad (2 + 3e, 3 + e), (3 + 4e, 2 + 3e), (3 + 4e, 3 + 2e), (1 + e, 0), (4 + e, e), \\ &\quad (4 + e, 4e), (1 + 2e, 0), (3 + 2e, 2 + 2e), (3 + 2e, 2 + 4e), (3 + 2e, 3 + 3e), \\ &\quad (3 + 2e, 3 + e), (4 + 3e, 0), (4 + 4e, 0)\}, \end{aligned}$$

$$E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_5) = \{(0, 1), (0, 4), (1, 0), (2, 2), (2, 3), (3, 2), (3, 3), (4, 0)\},$$

$$E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_5) = \{(0, 1), (0, 4), (2, 0), (3, 0)\}.$$

## 4 Addition in Twisted Edwards Curve $E_{E,a,d}(R)$

Let  $(x_1, y_1), (x_2, y_2)$  two points on the twisted Edwards curve  $E_{E,\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$ , for  $i \in \{0, 1\}$ .

The sum of these points on  $E_{E,\pi_i(a),\pi_i(d)}(\mathbb{F}_q)$ , for  $i \in \{0, 1\}$  is given by:

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1y_2 + y_1x_2}{1 + \pi_i(d)x_1x_2y_1y_2}, \frac{y_1y_2 - \pi_i(a)x_1x_2}{1 - \pi_i(d)x_1x_2y_1y_2} \right). \quad (2)$$

The neutral element of this law is  $(0, 1)$  and the inverse of an element  $(x_1, y_1)$  is  $(-x_1, y_1)$ . These formulas are complete if  $\pi_i(a)$  is a square and  $\pi_i(d)$  is a non-square in the field  $\mathbb{F}_q$ , for  $i \in \{0, 1\}$  (cf. [3]).

**Lemma 1.** *Let  $a = a_0 + a_1e$  be an element the  $R$ . Then,  $a$  is a square in  $R$  if and only if  $a_0$  and  $a_0 + a_1$  are squares in  $\mathbb{F}_q$ .*

**Proof.** Let us start by proving the direct implication. If  $a$  is a square in  $R$ , then there exists  $b = b_0 + b_1e \in R$ , with  $a = b^2$ . Thus,  $a_0 + a_1e = b_0^2 + ((b_0 + b_1)^2 - b_0^2)e$ . So  $a_0 = b_0^2$  and  $a_1 = (b_0 + b_1)^2 - b_0^2$ . Therefore,  $a_0 = b_0^2$  and  $a_0 + a_1 = (b_0 + b_1)^2$ , i.e.  $a_0$  and  $a_0 + a_1$  are squares in  $\mathbb{F}_q$ .

For the converse let  $a = a_0 + a_1e$  be an element of  $R$ , with  $a_0$  and  $a_0 + a_1$  are squares in  $\mathbb{F}_q$ . Then, there exists  $(b_0, b_1) \in (\mathbb{F}_q)^2$ , where  $a_0 = b_0^2$  and  $a_0 + a_1 = b_1^2$ . Therefore,  $a_0 + a_1e = b_0^2 + (b_1^2 - b_0^2)e = (b_0 + (b_1 - b_0)e)^2$ , i.e.  $a_0 + a_1e$  is a square in  $R$ . □

The following example shows that if  $a$  is not a square in  $R$ , then the addition on  $E_{E,a,d}(R)$  is not always defined as in the following example. Consider  $p = 5$ ,  $a = 2 + 3e$ ,  $d = 2 + 3e$ , then  $a$  and  $d$  are not squares and  $P = (2 + 4e, 1)$  and  $Q = (4, 4 + 2e)$  are a point on  $E_{E,a,d}(R)$ . Nevertheless,  $P + Q$  not possible since the inverse of  $1 + dX_1X_2Y_1Y_2 = e$  does not exist.

**Lemma 2.** *Let  $d_0 + d_1e$ ,  $\alpha \in \{-1, 1\}$ , and  $(X_1, Y_1), (X_2, Y_2)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$ , where  $X_1 = x_0 + x_1e$ ,  $Y_1 = y_0 + y_1e$ ,  $X_2 = x'_0 + x'_1e$  and  $Y_1 = y'_0 + y'_1e$ , then  $\alpha + dX_1X_2Y_1Y_2$  is invertible in  $R$  if and only if  $\alpha + d_0x_0x'_0y_0y'_0 \neq 0$  and  $\alpha + (d_0 + d_1)(x_0 + x_1)(x'_0 + x'_1)(y_0 + y_1)(y'_0 + y'_1) \neq 0$  in  $\mathbb{F}_q$ .*

**Proof.** We have:

$$\begin{aligned} \alpha + dX_1X_2Y_1Y_2 &= \alpha + (d_0 + d_1e)(x_0 + x_1e)(x'_0 + x'_1e)(y_0 + y_1e)(y'_0 + y'_1e) \\ &= \alpha + d_0x_0x'_0y_0y'_0 + [\alpha + (d_0 + d_1)(x_0 + x_1)(x'_0 + x'_1)(y_0 + y_1)(y'_0 + y'_1) - \\ &\quad (\alpha + d_0x_0x'_0y_0y'_0)]e, \end{aligned}$$

$\alpha + dX_1X_2Y_1Y_2$  is invertible in  $R$  if and only if  $\pi_0(\alpha + dX_1X_2Y_1Y_2) \neq 0$  and  $\pi_1(\alpha + dX_1X_2Y_1Y_2) \neq 0$  in  $\mathbb{F}_q$ , i.e.:  $\alpha + d_0x_0x'_0y_0y'_0 \neq 0$  and  $\alpha + (d_0 + d_1)(x_0 + x_1)(x'_0 + x'_1)(y_0 + y_1)(y'_0 + y'_1) \neq 0$  in  $\mathbb{F}_q$ . □

**Corollary 5.** *Let  $d_0 + d_1e$  be an element in  $R$  and  $(X_1, Y_1), (X_2, Y_2)$  two points of the twisted Edwards curve  $E_{E,a,d}(R)$ . If  $\pi_0(d)$  and  $\pi_1(d)$  are not a square in  $\mathbb{F}_q$ , then  $\alpha + dX_1X_2Y_1Y_2$  is invertible in  $R$ ,  $\alpha \in \{-1, 1\}$ .*

**Corollary 6.** *Let  $a, d$  be two elements of  $R$  and  $(X_1, Y_1), (X_2, Y_2)$  two points of the twisted Edwards curve  $E_{E,a,d}(R)$ . Assume that  $a$  is a square and  $d$  is not a square in  $R$ , then*

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

*is well defined in  $E_{E,a,d}(R)$ .*

In order to reduce the computation cost in  $E_{E,a,d}(R)$ , we introduce a new addition in  $E_{E,a,d}(R)$  in Sect. 4, and we compare the computation cost of the new law with the that law given in Corollary 6.

As  $\tilde{\pi}$  is a bijection mapping between the two sets  $E_{E,a,d}(R)$  and  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ , we can define the sum on  $E_{E,a,d}(R)$ .

**Definition 2.** Let  $P = (X_1, Y_1)$  and  $Q = (X_2, Y_2)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$ , assume that  $a$  is a square and  $d$  is not a square in  $R$ , we define the additive law  $P \tilde{+} Q$  in  $E_{E,a,d}(R)$  by:  $P \tilde{+} Q = \tilde{\pi}^{-1}(\tilde{\pi}(P) + \tilde{\pi}(Q))$ .

Keep the assumptions of the above definition during this section. The following corollaries can be easily proved:

**Corollary 7.** The set  $(E_{E,a,d}(R), \tilde{+})$  is a commutative group, which has  $(0, 1)$  as its zero element and the inverse of  $(X_1, Y_1)$  is  $(-X_1, Y_1)$ .

**Corollary 8.** The  $\tilde{\pi}$  mapping is an isomorphism of groups.

By using formula (2), Theorem 2 and Proposition 2, we shall give the explicit formula of sum of two points in the twisted Edwards curve  $E_{E,a,d}(R)$  in the next lemmas.

**Lemma 3.** Let  $P = (xe, \alpha + ye)$  and  $Q = (x'e, \beta + y'e)$  be two elements of  $E_{E,a,d}(R)$  such that  $\alpha \in \{-1, 1\}$  and  $\beta \in \{-1, 1\}$ . Then  $P \tilde{+} Q = (x_3e, \alpha\beta + (y_3 - \alpha\beta)e)$ , where

$$x_3 = \frac{x(\beta + y') + (\alpha + y)x'}{1 + \pi_1(d)xx'(\alpha + y)(\beta + y')} \text{ and } y_3 = \frac{(\alpha + y)(\beta + y') - \pi_1(a)xx'}{1 - \pi_1(d)xx'(\alpha + y)(\beta + y')}.$$

**Proof.** As  $\begin{cases} \tilde{\pi}_0(xe, \alpha + ye) = (0, \alpha) \\ \tilde{\pi}_0(x'e, \beta + y'e) = (0, \beta) \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(xe, \alpha + ye) = (x, \alpha + y) \\ \tilde{\pi}_1(x'e, \beta + y'e) = (x', \alpha + y') \end{cases}$ , according to the formula (2), we have:

$$\tilde{\pi}_0(xe, \alpha + ye) + \tilde{\pi}_0(x'e, \beta + y'e) = (0, \alpha\beta) \text{ and } \tilde{\pi}_1(xe, \alpha + ye) + \tilde{\pi}_1(x'e, \beta + y'e) = (x_3, y_3), \text{ where}$$

$$x_3 = \frac{x(\beta + y') + (\alpha + y)x'}{1 + \pi_1(d)xx'(\alpha + y)(\beta + y')} \text{ and } y_3 = \frac{(\alpha + y)(\beta + y') - \pi_1(a)xx'}{1 - \pi_1(d)xx'(\alpha + y)(\beta + y')}.$$

Therefore,

$$P \tilde{+} Q = \tilde{\pi}^{-1}((0, \alpha\beta), (x_3, y_3)) = (x_3e, \alpha\beta + (y_3 - \alpha\beta)e).$$

□

**Lemma 4.** Let  $P = (xe, \alpha + ye)$  and  $Q = (x' - x'e, y' + (\beta - y')e)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$  such that  $\alpha \in \{-1, 1\}$  and  $\beta \in \{-1, 1\}$ . Then  $P \tilde{+} Q = (\alpha x' + (\beta x - \alpha x')e, \alpha y' + (\beta(\alpha + y) - \alpha y')e)$ .



**Proof.** As  $\begin{cases} \tilde{\pi}_0(xe, \alpha + ye) = (0, \alpha) \\ \tilde{\pi}_0(x' - x'e, y' + (\beta - y')e) = (x', y') \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(xe, \alpha + ye) = (x, \alpha + y) \\ \tilde{\pi}_1(x' - x'e, y' + (\beta - y')e) = (0, \beta) \end{cases}$ ,  
According to the formula (2), we have:

$$\tilde{\pi}_0(xe, \alpha + ye) + \tilde{\pi}_0(x'e, \beta + y'e) = (\alpha x', \alpha y') \text{ and } \tilde{\pi}_1(xe, \alpha + ye) + \tilde{\pi}_1(x'e, \beta + y'e) = (\beta x, \beta(\alpha + y)).$$

Then

$$P\tilde{+}Q = \tilde{\pi}^{-1}((\alpha x', \alpha y'), (\beta x, \beta(\alpha + y))) = (\alpha x' + (\beta x - \alpha x')e, \alpha y' + (\beta(\alpha + y) - \alpha y')e).$$

□

**Lemma 5.** Let  $P = (x - xe, y + (\alpha - y)e)$  and  $Q = (x' - x'e, y' + (\beta - y')e)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$  such that  $\alpha \in \{-1, 1\}$  and  $\beta \in \{-1, 1\}$ . Then  $P\tilde{+}Q = (x_3 - x_3e, y_3 + (\alpha\beta - y_3)e)$ , where

$$x_3 = \frac{xy' + yx'}{1 + \pi_0(d)xx'yy'} \text{ and } y_3 = \frac{yy' - \pi_0(a)xx'}{1 - \pi_0(d)xx'yy'}.$$

**Proof.** As  $\begin{cases} \tilde{\pi}_0(x - xe, y + (\alpha - y)e) = (x, y) \\ \tilde{\pi}_0(x' - x'e, y' + (\beta - y')e) = (x', y') \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(x - xe, y + (\alpha - y)e) = (0, \alpha) \\ \tilde{\pi}_1(x' - x'e, y' + (\beta - y')e) = (0, \beta) \end{cases}$ ,  
According to formula (2), we have:

$$\begin{aligned} \tilde{\pi}_0(x - xe, y + (\alpha - y)e) + \tilde{\pi}_0(x' - x'e, y' + (\beta - y')e) &= (x_3, y_3) \text{ and} \\ \tilde{\pi}_1(x - xe, y + (\alpha - y)e) + \tilde{\pi}_1(x' - x'e, y' + (\beta - y')e) &= (0, \alpha\beta), \text{ where} \end{aligned}$$

$$x_3 = \frac{xy' + yx'}{1 + \pi_0(d)xx'yy'} \text{ and } y_3 = \frac{yy' - \pi_0(a)xx'}{1 - \pi_0(d)xx'yy'}.$$

Therefore,

$$P\tilde{+}Q = \tilde{\pi}^{-1}((x_3, y_3), (0, \alpha\beta)) = (x_3 - x_3e, y_3 + (\alpha\beta - y_3)e).$$

□

**Lemma 6.** Let  $P = (xe, \alpha + ye)$  and  $Q = (x_0 + x_1e, y_0 + y_1e)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$  such that  $\alpha \in \{-1, 1\}$ . Then  $P\tilde{+}Q = (\alpha x_0 + (x_3 - \alpha x_0)e, \alpha y_0 + (y_3 - \alpha y_0)e)$ , where

$$x_3 = \frac{x(y_0 + y_1) + (\alpha + y)(x_0 + x_1)}{1 + \pi_1(d)x(x_0 + x_1)(\alpha + y)(y_0 + y_1)} \text{ and } y_3 = \frac{(\alpha + y)(y_0 + y_1) - \pi_1(a)x(x_0 + x_1)}{1 - \pi_1(d)x(x_0 + x_1)(\alpha + y)(y_0 + y_1)}.$$

**Proof.** As  $\begin{cases} \tilde{\pi}_0(xe, \alpha + ye) = (0, \alpha) \\ \tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) = (x_0, y_0) \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(xe, \alpha + ye) = (x, \alpha + y) \\ \tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) = (x_0 + x_1, y_0 + y_1) \end{cases}$ ,  
According to the formula (2), we have:

$$\begin{aligned} \tilde{\pi}_0(xe, \alpha + ye) + \tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) &= (\alpha x_0, \alpha y_0) \text{ and} \\ \tilde{\pi}_1(xe, \alpha + ye) + \tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) &= (x_3, y_3), \text{ where} \end{aligned}$$

$$x_3 = \frac{x(y_0 + y_1) + (\alpha + y)(x_0 + x_1)}{1 + \pi_1(d)x(x_0 + x_1)(\alpha + y)(y_0 + y_1)} \text{ and } y_3 = \frac{(\alpha + y)(y_0 + y_1) - \pi_1(a)x(x_0 + x_1)}{1 - \pi_1(d)x(x_0 + x_1)(\alpha + y)(y_0 + y_1)}.$$

Therefore,

$$P \tilde{+} Q = \tilde{\pi}^{-1}((\alpha x_0, \alpha y_0), (x_3, y_3)) = (\alpha x_0 + (x_3 - \alpha x_0)e, \alpha y_0 + (y_3 - \alpha y_0)e).$$

□

**Lemma 7.** Let  $P = (x - xe, y + (\alpha - y)e)$  and  $Q = (x_0 + x_1e, y_0 + y_1e)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$  such that  $\alpha \in \{-1, 1\}$ . Then  $P \tilde{+} Q = (x_3 + (\alpha(x_0 + x_1) - x_3)e, y_3 + (\alpha(y_0 + y_1) - y_3)e)$ , where

$$x_3 = \frac{xy_0 + x_0y}{1 + \pi_0(d)xx_0yy_0} \text{ and } y_3 = \frac{yy_0 - \pi_1(a)xx_0}{1 - \pi_1(d)xx_0yy_0}.$$

**Proof.** As  $\begin{cases} \tilde{\pi}_0(x - xe, y + (\alpha - y)e) = (x, y) \\ \tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) = (x_0, y_0) \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(x - xe, y + (\alpha - y)e) = (0, \alpha) \\ \tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) = (x_0 + x_1, y_0 + y_1) \end{cases}$ ,

According to the formula (2), we have:

$$\tilde{\pi}_0(x - xe, y + (\alpha - y)e) + \tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) = (x_3, y_3) \text{ and}$$

$$\tilde{\pi}_1(xe, \alpha + ye) + \tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) = (\alpha(x_0 + x_1), \alpha(y_0 + y_1)), \text{ where}$$

$$x_3 = \frac{xy_0 + x_0y}{1 + \pi_0(d)xx_0yy_0} \text{ and } y_3 = \frac{yy_0 - \pi_1(a)xx_0}{1 - \pi_1(d)xx_0yy_0}.$$

Therefore,

$$P \tilde{+} Q = \tilde{\pi}^{-1}((x_3, y_3), (\alpha(x_0 + x_1), \alpha(y_0 + y_1))) = (x_3 + (\alpha(x_0 + x_1) - x_3)e, \alpha y_0 + (\alpha(y_0 + y_1) - y_3)e).$$

□

**Lemma 8.** Let  $P = (x_0 + x_1e, y_0 + y_1e)$  and  $Q = (x'_0 + x'_1e, y'_0 + y'_1e)$  be two points of the twisted Edwards curve  $E_{E,a,d}(R)$ . Then  $P \tilde{+} Q = (x_3 + (x'_3 - x_3)e, y_3 + (y'_3 - y_3)e)$ , where

$$x_3 = \frac{x_0y'_0 + x'_0y_0}{1 + \pi_0(d)x_0y'_0x'_0y_0}, y_3 = \frac{y_0y'_0 - \pi_0(a)x_0x'_0}{1 - \pi_0(d)x_0y'_0x'_0y_0},$$

$$x'_3 = \frac{(x_0 + x_1)(y'_0 + y'_1) + (y_0 + y_1)(x'_0 + x'_1)}{1 + \pi_1(d)(x_0 + x_1)(y'_0 + y'_1)(y_0 + y_1)(x'_0 + x'_1)}$$

and

$$y'_3 = \frac{(y_0 + y_1)(y'_0 + y'_1) - \pi_1(a)(x_0 + x_1)(x'_0 + x'_1)}{1 - \pi_1(d)(x_0 + x_1)(y'_0 + y'_1)(y_0 + y_1)(x'_0 + x'_1)}.$$

**Proof.** As  $\begin{cases} \tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) = (x_0, y_0) \\ \tilde{\pi}_0(x'_0 + x'_1e, y'_0 + y'_1e) = (x'_0, y'_0) \end{cases}$  and  $\begin{cases} \tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) = (x_0 + x_1, y_0 + y_1) \\ \tilde{\pi}_1(x'_0 + x'_1e, y'_0 + y'_1e) = (x'_0 + x'_1, y'_0 + y'_1) \end{cases}$ ,

According to the formula (2), we have:

$$\tilde{\pi}_0(x_0 + x_1e, y_0 + y_1e) + \tilde{\pi}_0(x'_0 + x'_1e, y'_0 + y'_1e) = (x_3, y_3) \text{ and}$$

$\tilde{\pi}_1(x_0 + x_1e, y_0 + y_1e) + \tilde{\pi}_1(x'_0 + x'_1e, y'_0 + y'_1e) = (x'_3, y'_3)$ , where

$$x_3 = \frac{x_0y'_0 + x'_0y_0}{1 + \pi_0(d)x_0y'_0x'_0y_0}, y_3 = \frac{y_0y'_0 - \pi_0(a)x_0x'_0}{1 - \pi_0(d)x_0y'_0x'_0y_0},$$

$$x'_3 = \frac{(x_0 + x_1)(y'_0 + y'_1) + (y_0 + y_1)(x'_0 + x'_1)}{1 + \pi_1(d)(x_0 + x_1)(y'_0 + y'_1)(y_0 + y_1)(x'_0 + x'_1)} \text{ and}$$

$$y'_3 = \frac{(y_0 + y_1)(y'_0 + y'_1) - \pi_1(a)(x_0 + x_1)(x'_0 + x'_1)}{1 - \pi_1(d)(x_0 + x_1)(y'_0 + y'_1)(y_0 + y_1)(x'_0 + x'_1)}.$$

Therefore,

$$P\tilde{+}Q = \tilde{\pi}^{-1}((x_3, y_3), (x'_3, y'_3)) = (x_3 + (x'_3 - x_3)e, y_3 + (y'_3 - y_3)e),$$

which completes the proof.  $\square$

Lemmas 3, 4, 5, 6, 7 and 8 can be regrouped in the next theorem which given the additive law of the twisted Edwards curve  $E_{E,a,d}(R)$ .

**Theorem 3.** *Let  $P = (X_1, Y_1)$  and  $Q = (X_2, Y_2)$  be in  $E_{E,a,d}(R)$ . Assume that  $\pi_i(a)$  is a square and  $\pi_i(d)$  is not a square in  $\mathbb{F}_q$ , where  $i \in \{0, 1\}$ . Under the law  $\tilde{+}$ ,  $(E_{E,a,d}(R), \tilde{+})$  is an Abelian group with zero element  $(0, 1)$ . More precisely for every  $\alpha, \beta \in \{-1, 1\}$ , we have  $P\tilde{+}Q = (X_3, Y_3)$  is given by:*

1) If  $\tilde{\pi}_0(P) = (0, \alpha)$ , then

$$X_3 = \alpha\pi_0(X_2) + (x_3 - \alpha\pi_0(X_2))e,$$

$$Y_3 = \alpha\pi_0(Y_2) + (y_3 - \alpha\pi_0(Y_2))e,$$

where

$$\tilde{\pi}_1(P) + \tilde{\pi}_1(Q) = (x_3, y_3).$$

2) If  $\tilde{\pi}_1(P) = (0, \alpha)$ , then

$$X_3 = x_3 + (\alpha\pi_1(X_2) - x_3)e,$$

$$Y_3 = y_3 + (\alpha\pi_1(Y_2) - y_3)e,$$

where

$$\tilde{\pi}_0(P) + \tilde{\pi}_0(Q) = (x_3, y_3).$$

3) If  $\tilde{\pi}_0(P) = (0, \alpha)$  and  $\tilde{\pi}_1(Q) = (0, \beta)$ , then

$$X_3 = \alpha\pi_0(X_2) + (\beta\pi_1(X_1) - \alpha\pi_0(X_2))e,$$

$$Y_3 = \alpha\pi_0(Y_2) + (\beta\pi_1(Y_1) - \alpha\pi_0(Y_2))e.$$

4) If  $\tilde{\pi}_0(P) \neq (0, \alpha)$  and  $\tilde{\pi}_1(P) \neq (0, \alpha)$ , then

$$\begin{aligned} X_3 &= x_3 + (x'_3 - x_3)e, \\ Y_3 &= y_3 + (y'_3 - y_3)e, \end{aligned}$$

where

$$\begin{aligned} \tilde{\pi}_0(P) + \tilde{\pi}_0(Q) &= (x_3, y_3), \\ \tilde{\pi}_1(P) + \tilde{\pi}_1(Q) &= (x'_3, y'_3). \end{aligned}$$

**Proof.** For the proof, we can easily show that the lemmas from 3 to 8 verify the cases of the theorem. □

Now we shall focus on the complexity of the sum law in the twisted Edwards curve  $E_{E,a,d}(R)$ .

Let  $S$  be the cost of the sum and  $M$  the cost of the multiplication in the field  $\mathbb{F}_q$ . The computation cost of calculating  $P + Q$  the sum that is defined in Corollary 6 and  $P \tilde{+} Q$  the sum that is defined in Definition 2 are given in the following table (Table 1):

**Table 1.** The complexity of the additions in the twisted Edwards curve  $E_{E,a,d}(R)$ .

Addition	+		$\tilde{+}$	
	Sum	Mult	Sum	Mult
Lemma 3	21S	75M	13S	13M
Lemma 4	3S	7M	2S	4M
Lemma 5	7S	27M	5S	13M
Lemma 6	41S	146M	13S	13M
Lemma 7	12S	32M	6S	13M
Lemma 8	48S	284M	26S	26M

The following graphics illustrate the above results (Fig. 1).

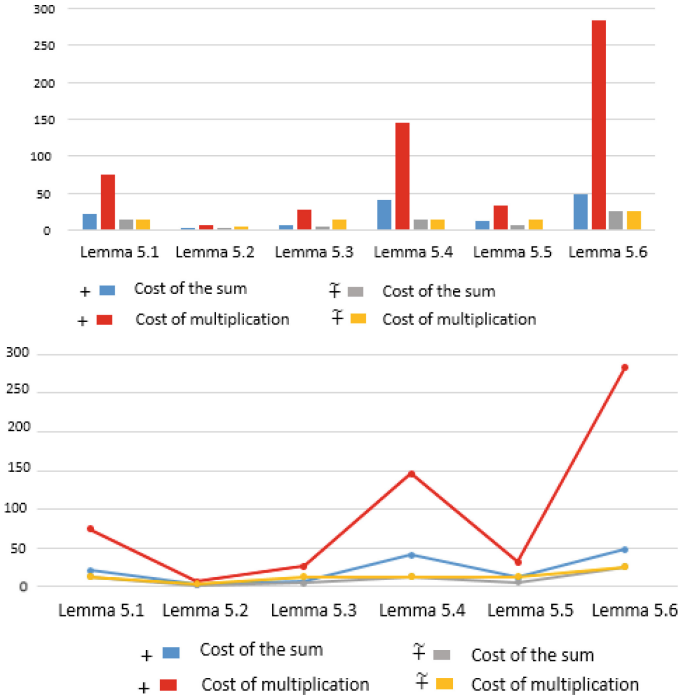


Fig. 1. The complexity of the additions in the twisted Edwards curve  $E_{E,a,d}(R)$ .

Concerning the complexity reduction of the sum law in the twisted Edwards curve  $E_{E,a,d}(R)$ , one can remark that the direct calculation of the sum  $P + Q$  is more expensive compared to the calculation of this sum  $P\tilde{+}Q$  using the isomorphism  $\tilde{\pi}$ . Which explain the need of this study.

### Links with Cryptography

Let us close this section with few applications in cryptography. We have:

- $card(E_{E,a,d}(R)) = card(E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)) \times card(E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q))$ .
- $E_{E,a,d}(R)$  and  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q) \times E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$  have the same security discrete logarithm problem.
- In cryptanalysis, break the discrete logarithm problem on  $E_{E,a,d}(R)$  is equivalent to break the discrete logarithm problem on  $E_{E,\pi_0(a),\pi_0(d)}(\mathbb{F}_q)$  and  $E_{E,\pi_1(a),\pi_1(d)}(\mathbb{F}_q)$ .

### References

1. Harold Edwards, M.: Normal form for elliptic curves. Bull. Am. Math. Soc. **44**(03), 393–423 (2007)

2. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007). [https://doi.org/10.1007/978-3-540-76900-2\\_3](https://doi.org/10.1007/978-3-540-76900-2_3)
3. Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008). [https://doi.org/10.1007/978-3-540-68164-9\\_26](https://doi.org/10.1007/978-3-540-68164-9_26)
4. Boudabra, M., Nitaj, A.: A new public key cryptosystem based on Edwards curves. *J. Appl. Math. Comput.* **61**(1), 431–450 (2019). <https://doi.org/10.1007/s12190-019-01257-y>
5. Bernstein, D.J., Lange, T., Rezaeian Farashahi, R.: Binary Edwards curves. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 244–265. Springer, Heidelberg (2008). [https://doi.org/10.1007/978-3-540-85053-3\\_16](https://doi.org/10.1007/978-3-540-85053-3_16)
6. Boulbot, A., Chillali, A., Mouhib, A.: Elliptic curves over the ring  $R$ . *Bol. Soc. Paran.* **38**(3), 193–201 (2020)
7. 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.* **40** (2022). <https://doi.org/10.52699/bspm.15867>
8. 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), pp. 1–4 (2022). <https://doi.org/10.1109/IRASET52964.2022.9738249>
9. Elhamam, M.B.T., Chillali, A., Grini, A., El Fadil, L.: El Gamal cryptosystem on a montgomery curves over non local ring. In: WSEAS Transactions on Mathematics, E-ISSN: 2224–2880, V. 21 (2022). <https://doi.org/10.37394/23206.2022.21.13>
10. Koblitz, N., Elliptic curve cryptosystems. *Math. Comput.* **48**(177), 203–209 (1987). <https://doi.org/10.2307/2007884>
11. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). [https://doi.org/10.1007/3-540-39799-X\\_31](https://doi.org/10.1007/3-540-39799-X_31)
12. Chillali, S., Oughdir, L.: ECC image encryption using matlab simulink blockset. In: Motahhir, S., Bossoufi, B. (eds.) ICDTA 2021. LNNS, vol. 211, pp. 835–846. Springer, Cham (2021). [https://doi.org/10.1007/978-3-030-73882-2\\_76](https://doi.org/10.1007/978-3-030-73882-2_76)
13. Chillali, S., Oughdir, L.: ECC Image Encryption Using System Generator. *J. Theor. Appl. Inf. Technol.* **100**(15), 5419–542515 (2022)
14. Chillali, S., Oughdir, L.: Construction of a matrix by an elliptic curve for image encryption. *Int. J. Emerg. Technol. Adv. Eng.* **12**(09), 122–129 (2022)