A new model of elliptic curves

Emmanuel FOUOTSA[1] and Oumar Diao[2]

(1) Department of Mathematics, Higher Teacher Training College
University of Bamenda, P.O.Box 39 Bambili, Cameroon
emmanuelfouotsa@yahoo.fr
(2) Laboratory Sec-ManPro, Rennes - France
diawkob@gmail.com

Abstract. In this paper, we introduce a new model of elliptic curve. We use an isogeny of order two to the level four theta model defined in [10] to obtain the new model which is defined over any finite field. We present unified addition formulas in all characteristics and study birational equivalences between this model and the Edward model and Weierstrass model of elliptic curves. We also provide the geometric interpretation of the group law in term of rational fractions which enable the computation of bilinear maps on elliptic curves, useful for the constructions of cryptographic protocols.
Key words: Elliptic curves, Group law, Divisor, Isogeny, Level four theta model.

1 Introduction

Elliptic curves are curves of genus one having a specified base point. Each elliptic curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at infinity. The must common used elliptic curve is the Weierstrass model defined over a field $\mathbb{K}$ given by the homogeneous equation $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ with $a_i \in \mathbb{K}$, $i = 1, 2, 3, 4, 6$. The base point in this case is $O = [0, 1, 0]$. On the set of points of an elliptic curve it is possible to define a structure of abelian group. When the elliptic curve is defined over a finite field $\mathbb{F}_q$, the resulting group denoted by $E(\mathbb{F}_q)$ presents many interesting applications in cryptography. Indeed, thanks to the efficient arithmetic and the fact that the Discrete Logarithm Problem (search for a solution m to the equation $[m]P = Q$ for given points $P, Q \in E(\mathbb{F}_q)$ is considered difficult to solve on that group [14, Chapter 2], cryptography based on elliptic curves has experienced an important development during the recent decades. This development led to the discovery of many other models of elliptic curves such as the Edwards model [12, 3, 4], Hessian curves [16], Huff curves [8] and the Jacobi curves [5, 7]. Recently, Diao et al. used Riemann theta functions to obtain a new model called the level four theta model [10]. In this work, we present another model of elliptic curve, from the level four theta model. More precisely, we use an isogeny of order two to obtain the new model. We present the addition formulas on that new model. The formulas obtained are unified (can be used both for addition and doubling) and valid over any finite field. We also study the completeness of our formulas. Moreover, we completely describe the geometric interpretation of the group law by rational functions which can enable the computation of some bilinear maps called pairings, that have been shown recently to be very useful in the construction of many cryptographic protocols [11], [6, Chapter X]. The rest of this paper is organised as follows: Section 2 the concept of divisor on an elliptic curve which will enable us to show that the group law on the new model is given by rational functions. In Section 3, we use an isogeny of order two to obtain our new model of elliptic curve from the level four theta model. We study the arithmetic of the new model and its "connection" with other well known models such as Weierstrass model and Edwards model [12, 3, 4]. In Section 4 we succeed to explicitly describe the rational functions that give the group law on the new model of elliptic curve. Section 5 concludes our work and presents some questions for further work.

2 The level four theta model of elliptic curve and divisors of functions

In this section, we recall the definition of the level four theta model of elliptic curve from [10]. Also, In order to easy the understanding of the geometric interpretation of the group law of the new model in section 4, we recall in this section the concepts of divisors on elliptic curves.

Definition 1. *[10] Let $\mathbb{F}_q$ be a finite field. Then the level four theta model is defined by the intersection of two equations:*

$$E_\lambda : \begin{cases} X_0^2 + X_2^2 = \lambda X_1 X_3 \\ X_1^2 + X_3^2 = \lambda X_0 X_2 \end{cases}, \text{ where } \lambda = c_0^2 + 4c_2^2$$

The base point is $[c_0 : 1 : 2c_2 : 1]$. The coefficients $c_0, c_2 \in \mathbb{F}_q^\star$ satisfy the relation $c_0 c_2 (c_0^2 + 4c_2^2) = 1$. the condition $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$ ensures that the level four theta model E_λ is non singular.

The following theorem gives the unified addition formulas on the level four theta model. These formulas are used both for addition of two different points and for the doubling of point. Another feature of these formulas is that they can be used not only in odd characteristics but are also valid for binary fields.

Theorem 1. *[10] Let $P_1 = [X_0, X_1, X_2, X_3]$ and $P_2 = [Y_0, Y_1, Y_2, Y_3]$ be two points on E_λ defined over a finite field $\mathbb{F}_q$. The coordinates $[Z_0, Z_1, Z_2, Z_3]$ of the point P_3 such that $P_1 + P_2 = P_3$ are given by :*

$$\begin{aligned} Z_0 &= (X_0^2 Y_0^2 + X_2^2 Y_2^2) - 4(c_2/c_0) X_1 X_3 Y_1 Y_3 \\ Z_1 &= a_0(X_0 X_1 Y_0 Y_1 + X_2 X_3 Y_2 Y_3) - 2c_2(X_2 X_3 Y_0 Y_1 + X_0 X_1 Y_2 Y_3) \\ Z_2 &= (X_1^2 Y_1^2 + X_3^2 Y_3^2) - 4(c_2/c_0) X_0 X_2 Y_0 Y_2 \\ Z_3 &= a_0(X_0 X_3 Y_0 Y_3 + X_1 X_2 Y_1 Y_2) - 2c_2(X_0 X_3 Y_1 Y_2 + X_1 X_2 Y_0 Y_3) \end{aligned} . \quad (1)$$

In any finite field, the opposite of the point $P = [X_0, X_1, X_2, X_3]$ is $-P = [X_0, X_3, X_2, X_1]$ (the second coordinate and the fourth coordinate are permuted). The base point is $O_0 := [c_0, 1, 2c_2, 1]$.

2.1 Note on divisors and isogeny

A divisor D on an elliptic curve E defined over a field $\mathbb{K}$ is a formal sum $D = \sum_{P \in E(\overline{\mathbb{K}})} a_P(P)$ where $a_P \in \mathbb{Z}$ and all but finitely many a_P are zero. The *degree* of D is the sum of its coefficients and the *support* of D is the set $\text{supp}(D) = \{P \in E(\overline{\mathbb{K}}) : a_P \neq 0\}$. The divisor D is defined over $\mathbb{K}$ if $D^\sigma = D$ for all Galois automorphism σ of $\mathbb{K}$. The divisor of a rational function f is $\text{Div}(f) = \sum_{P \in E(\overline{\mathbb{K}})} ord_P(f)(P)$ where $ord_P(f)$ is the order of the zero or the pole of f at P. If f has no zero or pole at P, then $\text{Div}(f) = 0$, the null divisor. A divisor D is called a principal divisor if there exists a function $f \in \overline{\mathbb{K}}(E)$ such that $D = \text{Div}(f)$. The degree of the divisor of a function is always 0 [13, Section 2]. Two divisors are said linearly equivalent if they differ by a principal divisor It follows that $\text{Princ}(E)$, the set of principal divisors is a subgroup of $\text{Div}^0(E)$, the set of zero's degree divisors. The subset $\text{Pic}^0(E)$, quotient of $\text{Div}^0(E)$ by the subgroup $\text{Princ}(E)$ is exactly isomorphic to $E(\mathbb{F}_q)$ and this justify the group structure that one has on elliptic curves.

3 The New model of elliptic curve

In this section, we derive from the level 4 theta model E_λ elliptic curve another model which is defined over any finite field. We give the birational equivalence between this model and the Weierstrass model and the Edwards model [12] over non-binary fields.

3.1 Equation of the New Model of Elliptic Curves

Theorem 2. *The level 4 theta model E_λ defined over a finite field $\mathbb{F}_q$ is 2-isogenous to the elliptic curve with equation: $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ with the neutral element $O_0 := (2c_2/c_0, 1)$, and $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$.*

Proof. Consider the map

$$\begin{array}{rccc} \phi : & E_\lambda & \to & \mathcal{E}_\lambda \\ & [X_0, X_1, X_2, X_3] & \longmapsto & (x, y) = (X_2/X_0, X_3/X_1). \end{array}$$

Then we can easily see that

$$1 + x^2 = \lambda \frac{X_1 X_3}{X_0^2} \quad \text{and} \quad y^2 + 1 = \lambda \frac{X_0 X_2}{X_1^2}.$$

Multiply the above two equations to have $(x^2+1)(1+y^2) = \lambda^2 xy$, which can be written as $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$. ϕ maps $[c_0 : 1 : 2c_2 : 1]$ to $O_0 := (2c_2/c_0, 1)$ which becomes $(0, 1)$ over binary fields.

Definition 2. *The new model of elliptic curves defined over a finite field $\mathbb{F}_q$ is given by the equation:*

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy.$$

with the neutral element $O_0 := (2c_2/c_0, 1)$ and where $\lambda = c_0^2 + 4c_2^2$ satisfies $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$

Remark 1. The elliptic curve $\mathcal{E}_\lambda$ enjoys the following property of symmetry like the Edwards model in [12]: If the point (x, y) is an element of $\mathcal{E}_\lambda$, then so is (y, x).

Theorem 3. *The elliptic curve $\mathcal{E}_\lambda$, with the neutral element $O_0 := (2c_2/c_0, 1)$ defined over a non-binary field is birationally equivalent to the Edwards model $E_c : x^2 + y^2 = c^2(1 + x^2y^2)$ in [12].*

Proof. : Consider the map:

$$\begin{array}{rccc} \varphi : & \mathcal{E}_\lambda & \to & Ec \\ & (x, y) & \longmapsto & \left(\dfrac{x+1}{x-1}, \dfrac{1+y}{1-y}\right) \\ & (2c_2/c_0, 1) & \longmapsto & (0, 1) \\ & (1, 2c_2/c_0) & \longmapsto & (1, 0) \end{array}$$

φ maps the curve $\mathcal{E}_\lambda$ to the Edwards model $E_c : x^2 + y^2 = c^2(1 + x^2y^2)$, where $c = \dfrac{c_0 - 2c_2}{c_0 + 2c_2}$. The following Sage script helps for verification:

```
R.<c0,c2,x,y>=QQ[]
E1=c0*c2*(x^2+y^2+1+x^2*y^2)-(c0^2+4*c2^2)*x*y
S=R.quo([E1])
X=(x+1)/(x-1)
Y=(1+y)/(1-y)
c=(c0-2*c2)/(c0+2*c2)
F=X^2+Y^2-c^2*(1+X^2*Y^2)
S(numerator(F))==0
```

Apart from the neutral element $O_0 := (2c_2/c_0, 1)$, the elliptic curve $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ has three 2−torsion rational points: $P_2 = (1/\gamma, 1), P_3 = (-\gamma, -1)$ and $P_4 = (-1/\gamma, -1)$, where $\gamma = 2c_2/c_0$.

The Edwards model $\mathcal{E}_\lambda$ also has four 4-torsion points which are rationals over $\mathbb{F}_q$: $Q_1 = (1,\gamma), Q_2 = (1,1/\gamma), Q_3 = (-1,-\gamma)$ and $Q_4 = (-1,-1/\gamma)$. The actions of rational points of order 2 and 4 are:

$$\begin{array}{ll} (x,y)+O_0=(x,y), & (x,y)+P_2=(1/x,1/y) \\ (x,y)+P_3=(-x,-y), & (x,y)+P_4=(-1/x,-1/y) \\ (x,y)+Q_1=(1/y,x), & (x,y)+Q_2=(y,1/x) \\ (x,y)+Q_3=(-1/y,-x), & (x,y)+Q_4=(-y,-1/x) \end{array},$$

Remark 2. If $\mathbb{F}_q$ is a binary field, then $P_3 = O_0$, $P_4 = P_2$, $Q_3 = Q_1$ and $Q_4 = Q_2$. The number of rational points of $\mathcal{E}_\lambda$ is then divisible by 4.

3.2 Birational equivalence with Weierstrass models

Theorem 4. *Let $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ be the elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic $p \geq 0$.*

(1) if $p \neq 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to a cubic Weierstrass model;
(2) if $p = 2$, then $\mathcal{E}_\lambda$ is birationally equivalent to the Weierstrass model $v^2 + uv = u^3 + 1/\lambda^4$.

Proof. : Theorem 3 gives the birational equivalence between $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ and the Edwards model $X^2 + Y^2 = c^2(1 + X^2Y^2)$. This Edwards model is birationally equivalent to the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$. Setting $X = 2c(u - c^4 - 1)/v$ and $Z = -c + uX^2/(2c)$, the quartic $Z^2 = c^2X^4 - (c^4 + 1)X^2 + c^2$ is birationally equivalent to the cubic Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$. This proves (1).
For fields of characteristic 2, the birational map and its inverse between $\mathcal{E}_\lambda$ model and Weierstrass model are

$$\begin{aligned} (u,v) &\longmapsto (x,y) = \left(\frac{1}{\lambda u}, \frac{\lambda^2 v + 1}{\lambda^2 u + \lambda^2 v + 1}\right) \\ (x,y) &\longmapsto (u,v) = \left(\frac{1}{\lambda x}, \frac{\lambda y + x(y+1)}{\lambda^2 x(y+1)}\right) \end{aligned}$$

which ends the proof (see also [9, p. 65]).

Corollary 1 ($j-$Invariant). *The $j-$ invariant of the elliptic curve $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ over a non binary field $\mathbb{F}_q$ is*

$$j = \frac{\left((c_0^4 - 4c_0^3c_2 + 8c_0^2c_2^2 + 16c_0c_2^3 + 16c_2^4)(c_0^4 + 4c_0^3c_2 + 8c_0^2c_2^2 - 16c_0c_2^3 + 16c_2^4)\right)^3}{\left(c_2c_0(c_0 - 2c_2)(c_0 + 2c_2)(c_0^2 + 4c_2^2)\right)^4}.$$

When $\mathbb{F}_q$ is a binary field then the $j-$Invariant is $j = \lambda^4$.

Proof. Suppose that $\mathbb{F}_q$ is a non-binary field. The $j-$Invariant of the Weierstrass model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$ over $\mathbb{F}_q$ is:

$$j_W = 2^4 \frac{\left((c^4 - 2c^3 + 2c^2 + 2c + 1)(c^4 + 2c^3 + 2c^2 - 2c + 1)\right)^3}{\left(c(c-1)(c+1)(c^2+1)\right)^4}.$$

Since $c = (c_0 - 2c_2)/(c_0 + 2c_2)$, a straightforward calculation gives the desired result. Notice that the expression of j is defined modulo any prime p, then j is defined over fields of any characteristic. Over fields of characteristic 2, we have $j \bmod 2 = (c_0/c_2)^4 = \lambda^4$ which is the $j-$Invariant of Weierstrass model $v^2 + uv = u^3 + 1/\lambda^4$ in theorem 4.

3.3 Addition Formulas on the new model

In this section, we use the addition law on the level 4 theta model to obtain the addition formulas on $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$.

Theorem 5. *Let (x_1, y_1) and (x_2, y_2) be two points of $\mathcal{E}_\lambda$. The coordinates of the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ are given by:*

$$(x_3, y_3) = \left(\frac{c_0(x_1 + y_1x_2y_2) - 2c_2(y_1 + x_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)}, \frac{c_0(x_1x_2 + y_1y_2) - 2c_2(x_1y_2 + y_1x_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)} \right). \tag{2}$$

The opposite of the point is $-(x_1, y_1) = (x_1, 1/y_1)$.

One can verify the correctness of the above addition formulas on $\mathcal{E}_\lambda$ using the following sage script [17]:

```
R.<c0,c2,x1,y1,x2,y2> = QQ[]
E1 = c0*c2*(x1^2 + y1^2 + 1 + x1^2*y1^2) -
     (c0^2 + 4*c2^2)*x1*y1
E2 = c0*c2*(x2^2 + y2^2 + 1 + x2^2*y2^2) -
     (c0^2 + 4*c2^2)*x2*y2
S = R.quo([E1,E2])
Nx3 = c0*(x1 + y1*x2*y2) - 2*c2*(y1 + x1*x2*y2)
Dx3 = c0*(y2 + x1*y1*x2) - 2*c2*(x2 + x1*y1*y2)
Ny3 = c0*(x1*x2 + y1*y2) - 2*c2*(x1*y2 + y1*x2)
Dy3 = c0*(1 + x1*x2*y1*y2) - 2*c2*(x1*y1 + x2*y2)
x3 = Nx3/Dx3; y3 = Ny3/Dy3

E3 = c0*c2*(x3^2 + y3^2 + 1 + x3^2*y3^2) -
     (c0^2 + 4*c2^2)*x3*y3
S(numerator(E3)) == 0
```

Over fields of characteristic 2, the coordinates of the sum of two points are obtained by a reduction modulo 2:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1y_1x_2y_2} \right). \tag{3}$$

Remark 3. The addition formulas defined above are unified over any fields, i.e. addition formulas are also valid for point doubling. The point doubling formulas can then be written as follows while replacing x_2 by x_1 and y_2 by y_1:

$$2(x_1, y_1) = \left(\frac{c_0x_1(1 + y_1^2) - 2c_2y_1(1 + x_1^2)}{c_0y_1(1 + x_1^2) - 2c_2x_1(1 + y_1^2)}, \frac{c_0(x_1^2 + y_1^2) - 4c_2x_1y_1}{c_0(1 + x_1^2y_1^2) - 4c_2x_1y_1} \right). \tag{4}$$

Over binary fields, formulas (3) or (4) give the doubling formulas:

$$2(x_1, y_1) = \left(\frac{x_1(1 + y_1)^2}{y_1(1 + x_1)^2}, \frac{(x_1 + y_1)^2}{(1 + x_1y_1)^2} \right). \tag{5}$$

Cost of the addition formulas In this section we find the cost of the addition formulas both in affine and projective coordinates. We denote I, m_1, s_1 and mc are the cost of an inversion, a multiplication, a squaring and multiplication by a constant, respectively, in a finite field.

Affine coordinates. Let (x_1, y_1) and (x_2, y_2) be two points on the elliptic curve $\mathcal{E}_\lambda : 1+x^2+y^2+x^2y^2 = \lambda^2 xy$ defined over the field $\mathbb{F}_q$. The following formulas compute the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, when it is defined:

$$A = x_1 \cdot y_1; B = x_2 \cdot y_2; C = x_1 + y_1 \cdot B; D = y_1 + x_1 \cdot B; E = y_2 + x_2 \cdot A;$$
$$F = x_2 + y_2 \cdot A; G = A + B; H = (x_1 + y_2) \cdot (x_2 + y_1) - G;$$
$$I = (x_1 + y_1) \cdot (x_2 + y_2) - H; J = 1 + A \cdot B; x_3 = (c_0 \cdot C - 2c_2 \cdot D)/(c_0 \cdot E - 2c_2 \cdot F);$$
$$y_3 = (c_0 \cdot H - 2c_2 \cdot I)/(c_0 \cdot J - 2c_2 \cdot G)$$

These formulas cost $2I + 9m_1 + 8mc$ over non-binary fields and $2I + 5m_1$ over binary fields. Remark that, the opposite of a point costs 1 inversion which is too expensive. Nevertheless the sum and the difference of two points (x_1, y_1) and (x_2, y_2) have the same complexity. Indeed, the following formula computes the difference $(x_4, y_4) = (x_1, y_1) - (x_2, y_2)$, if it is defined:

$$(x_4, y_4) = \left(\frac{c_0(x_1y_2 + y_1x_2) - 2c_2(x_1x_2 + y_1y_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)}, \frac{c_0(y_1 + x_1x_2y_2) - 2c_2(x_1 + y_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)} \right). \quad (6)$$

We retrieve the eight polynomials used to compute the sum: $F_1 = x_1 + y_1x_2y_2, F_2 = y_1 + x_1x_2y_2, F_3 = y_2 + x_1y_1x_2, F_4 = x_2 + x_1y_1y_2, F_5 = x_1x_2 + y_1y_2, F_6 = x_1y_2 + y_1x_2, F_7 = 1 + x_1y_1x_2y_2$ and $F_8 = x_1y_1 + x_2y_2$. Therefore formulas (2) and (6) can be rewritten as follows:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{c_0F_1 - 2c_2F_2}{c_0F_3 - 2c_2F_4}, \frac{c_0F_5 - 2c_2F_6}{c_0F_7 - 2c_2F_8} \right),$$
$$(x_1, y_1) - (x_2, y_2) = \left(\frac{c_0F_6 - 2c_2F_5}{c_0F_7 - 2c_2F_8}, \frac{c_0F_2 - 2c_2F_1}{c_0F_3 - 2c_2F_4} \right).$$

Projective coordinates. In this paragraph, we embeds the curve $\mathcal{E}_\lambda$ in the projective space $\mathbb{P}^2$ by setting the new coordinate $t = xy$. For efficiency reason in the computation of the sum and doubling of point, we follow the approach of Hisil et al. in [**?**] by using the extended projective coordinates $[X, Y, Z, T]$ in $\mathbb{P}^3$ where $x = X/Z, y = Y/Z, t = T/Z, T = XY/Z$ and $Z \neq 0$. The projective closure of the curve in $\mathbb{P}^3$ is then $Z^2 + X^2 + Y^2 + T^2 = \lambda^2 TZ$.

Addition of points The coordinates of the sum $[X_3, Y_3, Z_3, T_3] = [X_1, Y_1, Z_1, T_1] + [X_2, Y_2, Z_2, T_2]$ are:

$$X_3 = (X_1Z_2 + Y_1T_2)(Z_1Z_2 + T_1T_2)$$
$$Y_3 = (X_1X_2 + Y_1Y_2)(Z_1Y_2 + X_2T_1)$$
$$Z_3 = (Z_1Z_2 + T_1T_2)(Z_1Y_2 + X_2T_1)$$
$$T_3 = (X_1Z_2 + Y_1T_2)(X_1X_2 + Y_1Y_2)$$

The computation of X_3 costs $5m_1$:$X_1 \cdot Z_2, Y_1 \cdot T_2, Z_1 \cdot Z_2$ and $T_1 \cdot T_2$. The same argument follows for Y_3. This enables the cost of Z_3 and T_3 to be $1m_1$ each, since their factors are already computed in X_3 and Y_3. The total cost of the addition of two points is $12m_1$

Doubling of point The coordinates of the doubling $[X_3, Y_3, Z_3, T_3] = 2[X_1, Y_1, Z_1, T_1]$ are:

$$X_3 = (X_1Z_1 + Y_1T_1)(Z_1 + T_1)^2$$
$$Y_3 = (Y_1Z_1 + X_1T_1)(X_1 + Y_1)^2$$
$$Z_3 = (Y_1Z_1 + X_1T_1)(Z_1 + T_1)^2$$
$$T_3 = (X_1Z_1 + Y_1T_1)(X_1 + Y_1)^2$$

The computation of X_3 costs $3m_1 + 1s_1$:$X_1 \cdot Z_1, T_1 \cdot Y_1, (X_1 + Y_1)^2$ and the main product. The same argument follows for Y_3. This enables the cost of Z_3 and T_3 to be $1m_1$ each, since their factors are already computed in X_3 and Y_3. The total cost of the doubling is $8m_1 + 2s_1$.

Comparison of costs of addition formulas on the new model with other models In this section, we compare our addition formulas in binary fields with other models of elliptic curves based on the fastest results of Explicit-Formulas Database [2]. Recall that m_1, s_1 and mc are the cost of multiplication, square and multiplication by a constant, respectively, over a finite field. We can observe that, in the case where

Table 1. Comparison of points operations in binary fields

Models	Doubling	Addition
Huff of [8]	$6m_1 + 5s_1 + 2mc$	$13m_1 + 2s_1 + 2mc$
Weierstrass	$7m_1 + 3s_1$	$14m_1 + 1s_1$
The new model (This work)	$8m_1 + 2s_1$	$12m_1$
$\mathbb{Z}/4\mathbb{Z}$-normal form [15]	$7m_1 + 2s_1$	$12m_1$
Hessian [16]	$6m_1 + 3s_1$	$12m_1 + 6s_1$
Level 4 theta model[10]	$3m_1 + 6s_1 + 2mc$	$7m_1 + 2s_1 + 2mc$
Binary Edwards	$2m_1 + 5s_1 + 2mc$	$16m_1 + 1s_1 + 4mc$
μ_4-normal form [15]	$2m_1 + 5s_1 + 2mc$	$7m_1 + 2s_1$

a multiplication by a constant is free, the addition of points on the new model $\mathcal{E}_\lambda$ presents a competitive addition formulas among well known models of elliptic curves. This also means that the level 4 theta model offers good performances in scalar multiplication algorithms that perform many additions: For example the Montgomery's ladder, addition chain method and fixed base point methods such as Yao's method and Euclidean method. see [1, Chapter 13] for more details about these algorithms.

4 Geometric interpretation of the group law on $\mathcal{E}_\lambda$

In this section we describe the group law on the elliptic curves with rational functions. Especially, we study the intersection of the planes curves such as lines and conics. We will show that, considering the points $O_0 := (2c_2/c_0, 1)$, $O_0' := (1, 2c_2/c_0)$ and the points at infinity $O_1 = (1, 0, 0)$ and $O_2 = (0, 1, 0)$ and given two arbitrary points P_1, P_2 of $\mathcal{E}_\lambda$, the point $P_3 = P_1 + P_2$ is obtained as the reflection image with respect to the x-axis of the eight intersection point of $\mathcal{E}_\lambda$ and the conic (C) passing through O_1, O_2, O_0', P_1 and P_2.

Lemma 1. *1. The projective line passing through a point $P(X_0, Y_0, Z_0)$ and the point O_1 has the equation $l_1 = 0$ where : $l_1 = Z_0Y - Y_0Z$*

2. The projective line through $P(X_0, Y_0, Z_0)$ and the point O_2 has the equation $l_2 = 0$ where $l_2 = Z_0X - X_0Z = 0$

3. The divisors of the functions l_1 and l_2 are given as follows

$$div(l_1) = (P) + (Q) - 2(O_1)$$
$$div(l_2) = (P) + (-P) - 2(O_2)$$

where $Q \in E$ has the same $y-$coordinate as P.

Proof. The general equation of a line is of the form $l(X, Y, Z) = 0$ where $l(X, Y, Z) = c_XX + c_YY + c_ZZ$ and $(c_X, c_Y, c_Z) \in \mathbb{P}^2$. The proof is divided in two parts

1. The fact that the line $l_1 = 0$ passes through O_1 implies that $c_X = 0$ and the equation then follows from P being a point on the line. The same argument also applies for the line defined by l_2.
2. The line $l_1 = 0$ passing through P *and* O_1 is the horizontal line, so it also passes through some point Q which has the same $y-$coordinate with P. Since $Div(l_1)$ is a principal divisor we have :

$$\begin{aligned} Div(l_1) &= \sum_{P \in E} ord_P(l_1)(P) \\ &= (P) + (Q) - 2(O_1) \end{aligned}$$

The same argument applies for the vertical line $l2 = 0$ that must pass through the other point with the same abscise $-P$. Then

$$\begin{aligned} Div(l_2) &= \sum_{P \in E} ord_P(l_2)(P) \\ &= (P) + (-P) - 2(O_2) \end{aligned}$$

In the following we are going to find the equation of a conic $\phi(X, Y, Z) = 0$ where $\phi(X, Y, Z) = c_{X^2}X^2 + c_{Y^2}Y^2 + c_{Z^2}Z^2 + c_{XY}XY + c_{XZ}XZ + c_{YZ}YZ$ which passes through both points at infinity O_1 *and* O_2 , the point O'_0 and two arbitrary points P_1 *and* P_2 on the elliptic curve $\mathcal{E}_\lambda$.

Lemma 2. *If the conic C passes through the points O_1, O_2 and O'_0, then*

$$\phi(X, Y, Z) = c_{Z^2}(Z^2 - YZ) + c_{XY}(XY - \frac{1}{\gamma}YZ) + c_{XZ}(XZ - \frac{1}{\gamma}YZ) \tag{7}$$

where $\gamma = \frac{2c_2}{c_0}$ and $(c_{Z^2}, c_{XY}, c_{XZ}) \in \mathbb{P}^2(K)$

Proof. The evaluation of $\phi(X, Y, Z)$ at the three points O_1, O_2 *and* O'_0 gives :

$$\begin{cases} \phi(O_1) = 0 \\ \phi(O_2) = 0 \\ \phi(O') = 0 \end{cases} \iff \begin{cases} c_{X^2} = 0 \\ c_{Y^2} = 0 \\ c_{Z^2} + \frac{1}{\gamma}c_{XY} + \frac{1}{\gamma}c_{XZ} + c_{YZ} = 0 \end{cases} \tag{8}$$

From the third line of equation 8 we have :

$$\begin{aligned} c_{YZ} &= -\left(c_{Z^2} + \frac{1}{\gamma}c_{XY} + \frac{1}{\gamma}c_{XZ}\right) \\ \text{or } c_{YZ} &= -c_{Z^2} - \frac{1}{\gamma}c_{XY} - \frac{1}{\gamma}c_{XZ} \end{aligned}$$

It follows that

$$\begin{aligned} \phi(X, Y, Z) = 0 &\iff c_{Z^2}Z^2 + c_{XY}XY + c_{XZ}XZ + c_{YZ}YZ = 0 \\ &\iff c_{Z^2}Z^2 + c_{XY}XY + c_{XZ}XZ + (-c_{Z^2} - \frac{1}{\gamma}c_{XY} - \frac{1}{\gamma}c_{XZ})YZ = 0 \\ &\iff c_{Z^2}(Z^2 - YZ) + c_{XY}(XY - \frac{1}{\gamma}YZ) + c_{XZ}(XZ - \frac{1}{\gamma}YZ) = 0 \ . \end{aligned}$$

Theorem 6. *Let $P_1 = (X_1, Y_1, Z_1)$ and $P_2 = (X_2, Y_2, Z_2)$ be two points on the elliptic curve $\mathcal{E}_\lambda$. Let C be the conic passing through O_1, O_2, O'_0, P_1 and P_2. The coefficients of the equation $\phi(X, Y, Z) = c_{Z^2}(Z^2 - YZ) + c_{XY}(XY - \frac{1}{\gamma}YZ) + c_{XZ}(XZ - \frac{1}{\gamma}YZ) = 0$ of the conic C are determined as follows.*

1. *if* $P_1 \neq P_2, P_1 \neq O'_0$ *and* $P_2 \neq O'_0$, *then*

$$\begin{aligned}
c_{Z^2} &= (\gamma X_1Y_1 - Y_1Z_1)(\gamma X_2Z_2 - Y_2Z_2) - (\gamma X_2Y_2 - Y_2Z_2)(\gamma X_1Z_1 - Y_1Z_1) \\
c_{XY} &= \gamma\left[(Z_2^2 - Y_2Z_2)(\gamma X_1Z_1 - Y_1Z_1) - (Z_1^2 - Y_1Z_1)(\gamma X_2Z_2 - Y_2Z_2)\right] \\
c_{XZ} &= \gamma\left[(Z_1^2 - Y_1Z_1)(\gamma X_2Y_2 - Y_2Z_2) - (Z_2^2 - Y_2Z_2)(\gamma X_1Y_1 - Y_1Z_1)\right]
\end{aligned}$$

2. *If* $P_1 = P_2 \neq O'_0$, *then*

$$\begin{aligned}
c_{Z^2} &= 2\left(X_1^3Z_1^2 + Y_1^3Z_1^2 + Z_1^5\right) + X_1Y_1\left[2X_1Y_1\left(\frac{1}{\gamma}Y_1 - X_1 - \frac{1}{\gamma}Z_1\right) - \lambda^2X_1Z_1^2 - \frac{\lambda^2}{\gamma}Z_1^3\right] \\
c_{XY} &= 2X_1Y_1Z_1\left(X_1Y_1 - X_1Z_1 - \frac{1}{\gamma}Y_1Z_1\right) + \frac{\lambda^2\gamma - 2}{\gamma}X_1Z_1^4 + \frac{\lambda^2 - 2\gamma}{\gamma}Y_1Z_1^4 - 2Z_1^5 \\
c_{XZ} &= X_1Y_1^2\left(\frac{\lambda^2\gamma + 2}{\gamma}Z_1^2 - 2X_1Y_1\right) + 2\left(Y_1^2Z_1^3 - Y_1^3Z_1^2 - X_1^2Z_1^3 + \frac{1}{\gamma}X_1Z_1^4\right) - \frac{\lambda^2}{\gamma}Y_1Z_1^4
\end{aligned}$$

Proof. 1. The evaluation of the equation$\phi(X, Y, Z) = 0$ at the points P_1 *and* P_2 give two linear equations in c_{Z^2}, c_{XY} *and* c_{XZ}.

$$\begin{cases}
{}_{Z^2}(Z_1^2 - Y_1Z_1) + c_{XY}(X_1Y_1 - \frac{1}{\gamma}Y_1Z_1) + c_{XZ}(X_1Z_1 - \frac{1}{\gamma}Y_1Z_1) = 0 \\
c_{Z^2}(Z_2^2 - Y_2Z_2) + c_{XY}(X_2Y_2 - \frac{1}{\gamma}Y_2Z_2) + c_{XZ}(X_2Z_2 - \frac{1}{\gamma}Y_2Z_2) = 0
\end{cases}$$

Which is equivalent to

$$\begin{cases}
{}_{Z^2}\gamma(Z_1^2 - Y_1Z_1) + c_{XY}(\gamma X_1Y_1 - Y_1Z_1) + c_{XZ}(\gamma X_1Z_1 - Y_1Z_1) = 0 \\
c_{Z^2}\gamma(Z_2^2 - Y_2Z_2) + c_{XY}(\gamma X_2Y_2 - Y_2Z_2) + c_{XZ}(\gamma X_2Z_2 - Y_2Z_2) = 0
\end{cases}$$

From the projective solutions we have :

$$c_{Z^2} = \begin{vmatrix} \gamma X_1Y_1 - Y_1Z_1 & \gamma X_1Z_1 - Y_1Z_1 \\ \gamma X_2Y_2 - Y_2Z_2 & \gamma X_2Z_2 - Y_2Z_2 \end{vmatrix}$$

,

$$c_{XY} = \begin{vmatrix} \gamma X_1Z_1 - Y_1Z_1 & \gamma(Z_1^2 - Y_1Z_1) \\ \gamma X_2Z_2 - Y_2Z_2 & \gamma(Z_2^2 - Y_2Z_2) \end{vmatrix}$$

,

$$c_{XZ} = \begin{vmatrix} \gamma(Z_1^2 - Y_1Z_1) & \gamma X_1Y_1 - Y_1Z_1 \\ \gamma(Z_2^2 - Y_2Z_2) & \gamma X_2Y_2 - Y_2Z_2 \end{vmatrix}$$

then we have

$$\begin{aligned}
c_{Z^2} &= (\gamma X_1Y_1 - Y_1Z_1)(\gamma X_2Z_2 - Y_2Z_2) - (\gamma X_2Y_2 - Y_2Z_2)(\gamma X_1Z_1 - Y_1Z_1) \\
c_{XY} &= \gamma\left[(Z_2^2 - Y_2Z_2)(\gamma X_1Z_1 - Y_1Z_1) - (Z_1^2 - Y_1Z_1)(\gamma X_2Z_2 - Y_2Z_2)\right] \\
c_{XZ} &= \gamma\left[(Z_1^2 - Y_1Z_1)(\gamma X_2Y_2 - Y_2Z_2) - (Z_2^2 - Y_2Z_2)(\gamma X_1Y_1 - Y_1Z_1)\right]
\end{aligned}$$

Furthermore

2. If $P_1 = P_2 \neq 0$ we set $Z = 1$ in the equations. The tangent vector at the non singular point $P_1 = (X, Y, 1) = (x, y)$ of $\mathcal{E}_\lambda$ and the conic C are :

$$\begin{pmatrix} \lambda^2 x_1 - 2x_1^2 x_1 - 2x_1 \\ 2x_1 + 2x_1 y_1^2 - \lambda^2 y_1 \end{pmatrix} \quad , \quad \begin{pmatrix} c_{Z^2} - c_{XY}(x_1 - \frac{1}{\gamma}) + \frac{1}{\gamma} c_{XZ} \\ c_{XY} y_1 + c_{XZ} \end{pmatrix}$$

These vectors are collinear if their determinant is zero i.e

$$\begin{vmatrix} \lambda^2 x_1 - 2x_1^2 y_1 - 2y_1 & c_{Z^2} - c_{XY}(x_1 - \frac{1}{\gamma}) + \frac{1}{\gamma} c_{XZ} \\ 2x_1 + 2x_1 y_1^2 - \lambda^2 y_1 & c_{XY} y_1 + c_{XZ} \end{vmatrix} = 0$$

which is equivalent to

$$\begin{aligned} & c_{Z^2}\left[-2x_1 - 2x_1 y_1^2 + \lambda^2 y_1\right] + c_{XY}[\lambda^2 x_1 y_1 - 2x_1^2 y_1^2 - 2y_1^2 + 2x_1(x_1 - \frac{1}{\gamma}) + 2x_1 Y_1^2 (x_1 - \frac{1}{\gamma}) \\ & - \lambda^2 y_1 (x_1 - \frac{1}{\gamma})] + c_{XZ}[\lambda^2 x_1 - 2x_1^2 y_1 - 2y_1 - \frac{2}{\gamma} x_1 \\ & - \frac{2}{\gamma} x_1 y_1^2 + \frac{\lambda^2}{\gamma} y_1] = 0. \end{aligned} \tag{9}$$

By using the fact that $\phi(X_1, Y_1, 1) = \phi(x_1, y_1) = 0$ i.e

$$c_{Z^2}(1 - y_1) + c_{XY}(x_1 y_1 - \frac{1}{\gamma} y_1) + c_{XZ}(x_1 - \frac{1}{\gamma} y_1) = 0. \tag{10}$$

We have the system formed by equations 9 and 10. The resolution of the linear system give the projective solutions.

$$c_{Z^2} = \begin{vmatrix} \alpha & \beta \\ x_1 y_1 - \frac{1}{\gamma} y_1 & x_1 - \frac{1}{\gamma} y_1 \end{vmatrix}$$

$$c_{XY} = \begin{vmatrix} \beta & -2x_1 - 2x_1 y_1^2 + \lambda^2 y_1 \\ x_1 - \frac{1}{\gamma} y_1 & 1 - y_1 \end{vmatrix}$$

$$c_{XZ} = \begin{vmatrix} -2x_1 - 2x_1 y_1^2 + \lambda^2 y_1 & \alpha \\ 1 - y_1 & x_1 y_1 - \frac{1}{\gamma} y_1 \end{vmatrix}$$

where the numbers α *and* β are given below

$$\alpha = \lambda^2 x_1 y_1 - 2x_1^2 y_1^2 - 2y_1^2 + 2x_1(x_1 - \frac{1}{\gamma}) + 2x_1 y_1^2 (x_1 - \frac{1}{\gamma}) - \lambda^2 y_1 (x_1 - \frac{1}{\gamma})$$

$$\beta = \lambda^2 x_1 - 2x_1^2 y_1 - 2y_1 - \frac{2}{\gamma} x_1 - \frac{2}{\gamma} x_1 y_1^2 + \frac{\lambda^2}{\gamma} y_1$$

We then obtain

$$\begin{aligned}
c_{Z^2} &= (x_1 - \frac{1}{\gamma}y_1)\alpha - (x_1y_1 - \frac{1}{\gamma}y_1)\beta \\
&= 2x_1^3 + \frac{2}{\gamma}y_1^3 + \frac{2}{\gamma} + x_1y_1\left[2x_1y_1\left(\frac{1}{\gamma}y_1 + x_1 - \frac{1}{\gamma}\right) - \lambda^2 x_1 - \frac{\lambda^2}{\gamma}\right] \\
c_{XY} &= (1-y_1)\beta - \left(x_1 - \frac{1}{\gamma}y_1\right)(-2x_1 - 2x_1y_1^2 + \lambda^2 y_1) \\
&= 2x_1y_1\left(x_1y_1 - x_1 - \frac{1}{\gamma}y_1\right) + \frac{\lambda^2\gamma - 2}{\gamma}x_1 + \frac{\lambda^2 - 2\gamma}{\gamma}y_1 - 2 \\
c_{XZ} &= \left(x_1y_1 - \frac{1}{\gamma}y_1\right)(-2x_1 - 2x_1y_1^2 + \lambda^2 y_1) - (1-y_1)\alpha \\
&= x_1y_1\left(\frac{\lambda^2\gamma + 2}{\gamma}y_1 - 2x_1y_1^2\right) + 2y_1^2 - 2y_1^3 - 2x_1^2 + \frac{2}{\gamma}x_1 - \frac{\lambda^2}{\gamma}y_1
\end{aligned}$$

These formulas are expressed in affine coordinates, now we homogenize to obtain them in projective coordinates. We have:

$$\begin{aligned}
c_{Z^2} &= \frac{2\left(X_1^3Z_1^2 + Y_1^3Z_1^2 + Z_1^5\right) + X_1Y_1\left[2X_1Y_1\left(\frac{1}{\gamma}Y_1 - X_1 - \frac{1}{\gamma}Z_1\right) - \lambda^2X_1Z_1^2 - \frac{\lambda^2}{\gamma}Z_1^3\right]}{Z_1^5} \\
c_{XY} &= \frac{2X_1Y_1Z_1\left(X_1Y_1 - X_1Z_1 - \frac{1}{\gamma}Y_1Z_1\right) + \frac{\lambda^2\gamma - 2}{\gamma}X_1Z_1^4 + \frac{\lambda^2 - 2\gamma}{\gamma}Y_1Z_1^4 - 2Z_1^5}{Z_1^5} \\
c_{XZ} &= \frac{X_1Y_1^2\left(\frac{\lambda^2\gamma + 2}{\gamma}Z_1^2 - 2X_1Y_1\right) + 2\left(Y_1^2Z_1^3 - Y_1^3Z_1^2 - X_1^2Z_1^3 + \frac{1}{\gamma}X_1Z_1^4\right) - \frac{\lambda^2}{\gamma}Y_1Z_1^4}{Z_1^5}
\end{aligned}$$

Hence we have

$$\begin{aligned}
c_{Z^2} &= 2\left(X_1^3Z_1^2 + Y_1^3Z_1^2 + Z_1^5\right) + X_1Y_1\left[2X_1Y_1\left(\frac{1}{\gamma}Y_1 - X_1 - \frac{1}{\gamma}Z_1\right) - \lambda^2X_1Z_1^2 - \frac{\lambda^2}{\gamma}Z_1^3\right] \\
c_{XY} &= 2X_1Y_1Z_1\left(X_1Y_1 - X_1Z_1 - \frac{1}{\gamma}Y_1Z_1\right) + \frac{\lambda^2\gamma - 2}{\gamma}X_1Z_1^4 + \frac{\lambda^2 - 2\gamma}{\gamma}Y_1Z_1^4 - 2Z_1^5 \\
c_{XZ} &= X_1Y_1^2\left(\frac{\lambda^2\gamma + 2}{\gamma}Z_1^2 - 2X_1Y_1\right) + 2\left(Y_1^2Z_1^3 - Y_1^3Z_1^2 - X_1^2Z_1^3 + \frac{1}{\gamma}X_1Z_1^4\right) - \frac{\lambda^2}{\gamma}Y_1Z_1^4 \quad \square
\end{aligned}$$

Remark 4. The divisor of the conic C passing through $P_1, P_2, -P_3, O_0', O_1, O_2$ is

$$Div(C) \;=\; (P_1) + (P_2) + (-P_3) + (O_0') - 2(O_1) - 2(O_2)$$

Indeed, from Bezout's theorem the intersection of the conic $C : \phi = 0$ and the curve $\mathcal{E}_\lambda$ should have $2.4 = 8$ points counting multiplicities over $\mathbb{K}$. Note that the two points at infinity O_1 and O_2 are singular points of multiplicities 2. Moreover from the definition of the conic, the points of intersection of $\mathcal{E}_\lambda$ and (C) are $P_1, P_2, -P_3 = P_1 + P_2, O_0'$. Then we have: $Div(C) = (P_1) + (P_2) + (-P_3) + (O_0') - 2(O_1) - 2(O_2)$.

Theorem 7. *Let P_1, P_2 be two points of the elliptic curve $\mathcal{E}_\lambda$. Let $P_1, P_2 \in \mathcal{E}_\lambda$. Let $P_3 = P_1 + P_2$ and let $l_1 = Y - Z$, $l_2 = Z_3X - X_3Z$ be the functions defined in the lemma 1 at the points O_0 and $-P_3$ respectively. let $\phi = c_{Z^2}(Z^2 - YZ) + c_{XY}(XY - \frac{1}{\gamma}YZ) + c_{XZ}(XZ - \frac{1}{\gamma}YZ)$ be the unique polynomial defined by theorem 6 then we have*

$$Div\left(\frac{\phi}{l_1l_2}\right) \;\sim\; (P_1) + (P_2) - (P_3) - (O). \tag{11}$$

Proof. We know that $Div\left(\frac{\phi}{l_1 l_2}\right) \sim Div(\phi) - Div(l_1 l_2)$ *and* $Div(l_1 l_2) \sim Div(l_1) + Div(l_2)$. We have

$$\begin{aligned} Div\left(\frac{\phi}{l_1 l_2}\right) &\sim Div(\phi) - Div(l_1 l_2) \\ &\sim Div(\phi) - Div(l_1) - Div(l_2) \\ &\sim (P_1) + (P_2) + (-P_3) + (O_0') - 2(O_1) - 2(O_2) - (O_0) \\ &\quad - (O_0') + 2(O_1) - (P_3) - (-P_3) + 2(O_2) \\ &\sim (P_1) + (P_2) - (P_3) - (O_0) \end{aligned}$$

From what has been done in this section, we summarize that the point $P_3 = P_1 + P_2$ is obtained as follows given two arbitrary points P_1 *and* P_2 on the curve $\mathcal{E}_\lambda$:

1. Construct the curve $\mathcal{E}_\lambda$ and choose two arbitrary points P_1 *and* P_2 on $\mathcal{E}_\lambda$
2. Construct the conic (C) passing through the points P_1, P_2 and O_0' as defined in theorem 6
3. From the Bezout's theorem, the curve $\mathcal{E}_\lambda$ intersects the conic (C) at P_1, P_2, O_0' and at another fourth point which must be $-P_3$. Plot $-P_3$ on the curve.
4. Draw the vertical line passing through $-P_3$. This vertical line intersects the curve at P_3 which is the sum of the two points P_1 *and* P_2

We give here one example to illustrate the geometric interpretation of the group law that we have described. We assume that the curve is defined on the set of real numbers.

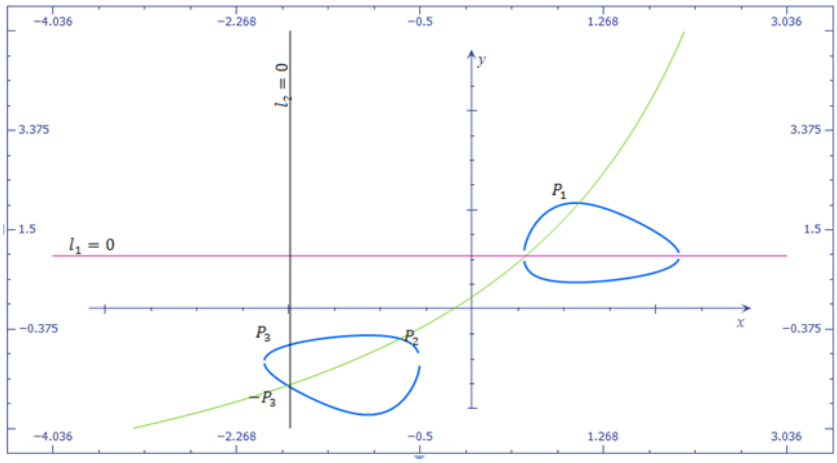

Fig. 1. Geometric interpretation of the Edwards group law on $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2 y^2 = 5xy$ over $\mathbb{R}$.$(P_3 = P_1 + P_2)$

5 Conclusion and Futur Work

In this work we successfully introduced a new model of elliptic curve. We gave a complete and unified addition formulas. We also succeed to describe the group law on this curve with rational functions, which can enable the computation of pairings for cryptographic purposes. As future work, one may try to improve the cost of the addition formulas and study the features of this curve in cryptography.

References

1. R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography. *Discrete Math. Aplli. Chapman and Hall*, 2006.
2. D. Bernstein and T. Lange. Explicit-formulae database. *http://www.hyperelliptic.org/EFD*.
3. D. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. *ASIACRYPT 2007, Springer Berlin / Heidelberg.*, vol. 4833 , pp. 29-50, 2007.
4. D.J. Bernstein, T. Lange, and R.R. Farashahi. Binary Edwards curves. *CHES 2008, LNCS, Springer,*, Vol. 5154 , pp. 244-265,, 2008.
5. O. Billet and M. Joye. The jacobi model of an elliptic curve and side-channel analysis. *AAECC 2003, LNCS*, vol. 2643, pp. 34-42, 2003.
6. I.F. Blake, G. Seroussi, and N.P. Smart. Advances in elliptic curves in cryptography. *London Mathematic Society, Cambridge University Press*, (2005).
7. D. V Chudnovsky and G. V. Chudnovky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests,. *Advances in Applied Mathematics*, vol. 7(4), pp. 385-434, 1986.
8. J. Devigne and M. Joye. Binary Huff curves. *Topics in Cryptology CT-RSA 2011, vol. 6558 of LNCS pp. 340-355, Springer*, 2011.
9. 0. Diao. Quelques aspects de l'arithmtique des courbes hyperelliptique de genre 2. *Universit de Rennes 1 - France*, 2010.
10. O. Diao and E. Fouotsa. Arithmetic of the level four theta model of elliptic curves. *Afrika Mathematica. (DOI) 10.1007/s13370-013-0203-1 (Springer)*, vol. , pp., 2013.
11. R. Dutta, R. Barua, and P. Sarkar. Pairing-based cryptography : A survey. *Cryptology ePrint Archive*, Report 2004/064, 2004.
12. H. M. Edwards. A normal form for elliptic curves. *Bulletin of the AMS 44(2007), pp. 393-422, URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html*, 2007.
13. R. Hartshorne. Algebraic curves. *Springer-Verlag, Graduate Texts in Mathematics*, vol. 52, 1977.
14. J. Hoffstein, J. Pipher, and J.H. Silvermann. An introduction to mathematical cryptography. *Undergraduate texts in Mathematic, Springer*, 2008.
15. D. Kohel. Efficient arithmetic on elliptic curves in characteristic 2. *LNCS, To appear, INDOCRYPT 2012*, 2012.
16. P. Smart, N. The hessian form of an elliptic curve. *CHES 2001, LNCS, Springer-Verlag Berlin Heidelberg*, vol. 2162, pp. 118-125, 2001.
17. W. Stein. Sage mathematics software (version 4.8). *The Sage Group*, 2012. http://www.sagemath.org.