Edwards model of elliptic curves defined over any fields

Oumar Diao[1] and Emmanuel Fouotsa[2]

[1]Université de Rennes I, Laboratoire IRMAR Campus de Beaulieu
35042 Rennes Cedex, France
oumar.diao@univ-rennes1.fr
[2]Département de Mathématiques, Université de Yaoundé 1,
BP 812 Yaoundé Cameroun
emmanuelfouotsa@prmais.org *

June 18, 2012

Abstract

In this paper, we present a generalization of Edwards model for elliptic curve which is defined over any field and in particular for field of characteristic 2. This model generalize the well known Edwards model of [10] over characteristic zero field, moreover it define an ordinary elliptic curve over binary fields. For this, we use the theory of theta functions and an intermediate model embed in $\mathbb{P}^3$ that we call a level 4-theta model. We then present an arithmetic of this level 4-theta model and of our Edwards model using Riemann relations of theta functions. The group laws are complete, i.e., none exceptional case for adding a pair of points; their are also unified, i.e., formulas using for addition and for doubling are the same. Over binary fields we have very efficient arithmetics on ordinary elliptic curve, but over odd field our explicit addition laws are not competitives. Nevertheless, we give efficient differential addition laws on level 4-theta model and on Edwards model defined over any fields.

Keywords: Edwards model, elliptic curve, efficient arithmetic, complete addition law, differential addition, theta functions, Riemann relations.

1 Introduction

In [10], Edwards has described the model $Ed_c : x^2 + y^2 = c^2(1 + x^2y^2)$ for elliptic curve over field of odd characteristic $\mathbb{K}$. He gave group law formulas: let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the curve Ed_c, then the coordinates of the sum $P_3 = P_1 + P_2 = (x_3, y_3)$ are given by:

$$x_3 = \frac{x_1y_2 + x_2y_1}{c(1 + x_1x_2y_1y_2)} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)}. \quad (1)$$

The group law on Ed_c is unified, this mean that it can be used to compute the double of a point. But this group law is not complete, i.e. it does not work for every pair of inputs. In fact, notice that if $x \neq 0, y \neq 0$, and the point $(x, y) \in Ed_c$ then so are $(\pm 1/x, \pm 1/y)$. But we can not compute the sum of (x, y) and $(1/x, 1/y)$ because denominator of y_3 vanishes. Also in projective coordinates addition law 1 is not complete.

*This work was done in part when the second author visits the Laboratoire IRMAR

To fill this gap, Bernstein and Lange introduced in [3] a more general model defined by $BL_{c,d} : x^2 + y^2 = c^2(1 + dx^2y^2)$ over fields $\mathbb{K}$ of odd characteristic. Using the birational map $(\overline{x}, \overline{y}) \mapsto (x, y) = (\overline{x}\sqrt[4]{d}, \overline{y}\sqrt[4]{d})$, one can transform the classical Edwards model $Ed_c : x^2 + y^2 = c^2(1 + x^2y^2)$ to the model $BL_{c,d} : \overline{x}^2 + \overline{y}^2 = \overline{c}^2(1 + d\overline{x}^2\overline{y}^2)$, where $\overline{c} = c/\sqrt[4]{d}$. Then, one can derive the group law formulas on $BL_{c,d}$. The formulas are also unified and if d is not a square in $\mathbb{K}$ they are *complete*. But $BL_{c,d}$ and its twisted $ax^2 + y^2 = 1 + dx^2y^2$ in [4] always give singular model over binary fields.

To solve this problem over characteristic 2 field, Bernstein, Lange, and Farashahi introduced in [5] the ordinary binary Edwards model defined by $E_{B,d_1,d_2} : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2$ over a characteristic 2 field $\mathbb{K}$. The authors of [23] deduced a new Edwards model with efficient arithmetic by cancelling the quartic monome of E_{B,d_1,d_2}. But, the connection between binary Edwards curves of [5, 23] and classical Edwards model Ed_c of [10] is mysterious. To solve this problem, Diao in [9, chapter 7] introduced a new binary Edwards model which is deduced from the well known Edwards model. However model in [9] does not have an efficient arithmetic.

Contribution of this paper: A first contribution in this work is to introduce a generalization of Edwards model of elliptic curves which is valid over fields of all characteristic. For this, we use an intermediate model given by level 4-theta functions which is also defined in all characteristic. According to [10], the general Edwards model and the level 4-theta model are called *normal forms* of elliptic curves. The explicit formulas for arithmetic of these normal forms are given by Riemann theta relations. Addition and doubling can be done by same formulas, i.e., the group law is unified.

Moreover we prove that these group laws are also complete, i.e. they work for any pair of input points. More precisely let $\mathbb{F}_q$ be the field of definition of normal forms of elliptic curves. We prove that if $q \equiv 3 \bmod 4$ then addition laws on normal forms are complete. If $q \not\equiv 3 \bmod 4$, then we have a condition of completness depending of curve parameters or we can find a subgroup of odd order of normal forms where addition laws are complete.

Over binary field, the group laws of normal forms are competitives with the well known models of elliptic curve and moreover the addition on level 4-theta model is the more efficient formulas on ordinary elliptic curve in our knowledge. Indeed denote by M the multiplication, S the square and m the multiplication by constant over field $\mathbb{K}$, then addition laws cost respectively $7M + 2S + 2m$ and $12M + 2S$ for respectively level 4-theta model and Edwards model defined over binary fields.

Over fields of odd characteristic, the group laws of normal forms are not competitives. However we give the differential addition formulas for normal forms which are competitives. Indeed compute the point nP for integer n and point P on normal forms cost $4M + 3S + 4m$ and $5M + 5S + 2m$ per bits for respectively level 4-theta model and Edwards model defined over fields of odd characteristic.

Outline: This paper is divided into five sections: in Section 2, we briefly review the theory of theta functions. We give in Section 3 the equations of level 4-theta model, and we study the arithmetic and the completness of this model. We use the result of Section 3 to deduce the equation and arithmetic of our Edwards model in Section 4. In Section 5 we study the differential addition on level 4-theta model and Edwards model.

2 Theta functions

This section is dedicated to the tools we use to study normal forms of elliptic curve. Theta functions are holomorphics form over complex field $\mathbb{C}$ which give some algebraic Riemann relations. With *Lefschetz principle* [20, §6], these Riemann relations are valid over any algebraically closed field of characteristic 0. In this section we only consider elliptic curve defined over complex field $\mathbb{C}$ and for elliptic curves over finite field, we use Lefschetz principle . More precisely let $E : f(x, y) = 0$ be elliptic curve defined over finite field $\mathbb{F}_q$ of characteristic $p > 0$, we lift the coefficients of polynom $f(x, y)$ over $\mathbb{Z}_q$ the integer ring of $\mathbb{Q}_q$ an unramified extension of $\mathbb{Q}_p$. We fix an embedding $\mathbb{Q}_q \hookrightarrow \mathbb{C}$ and let $\overline{\mathbb{Q}}_q$ be the algebraic extension of $\mathbb{Q}_q$. Let $E/\mathbb{Q}_q$ be a canonical lift of E over $\mathbb{Q}_q$ (i.e. $\mathrm{End}(E/\mathbb{K}) \equiv \mathrm{End}(E/\mathbb{Q}_q)$). According to Lefschetz principle, algebraic relations defined over $\mathbb{C}$ are also valid over $\overline{\mathbb{Q}}_q$.

Let $E/\mathbb{C}$ be an elliptic curve defined over complex field $\mathbb{C}$, there exists $\omega \in \mathbb{C}$ with positive defined imaginary part such that the curve E and the torus $\mathbb{C}/(\omega\mathbb{Z}+\mathbb{Z})$ are analytically isomorphic. Theta functions are holomorphics form of $\mathbb{C}$ which are pseudo-periodic by any translation over the lattice $\omega\mathbb{Z} + \mathbb{Z}$.

2.1 General definition

Let $\mathcal{H}_1$ be the one dimensional Siegel upper-half space over $\mathbb{C}$ and let $a, b \in \mathbb{Q}$, the theta function with rational characteristics (a, b) is by definition an analytic function on $\mathbb{C} \times \mathcal{H}_1$ given by:

$$\theta_{a,b}(z,\omega) \quad = \quad \sum_{n\in\mathbb{Z}} \exp\left(i\pi(n+a)^2\omega + 2i\pi(n+a)(z+b)\right). \tag{2}$$

The classical theory of theta functions provide a projective embedding of $\mathbb{C}/(\omega\mathbb{Z}+\mathbb{Z}) = E_{\mathbb{C}}$ in projective space $\mathbb{P}^{\ell-1}$ for some integer $\ell \geq 3$ (for more details, see [19, p. 267]). To be more precise, we say that a function $f \in \mathbb{C}$ is $(\omega\mathbb{Z}+\mathbb{Z})$-quasi-periodic of level $\ell \in \mathbb{N}$ if for all $z \in \mathbb{C}$ and $m, n \in \mathbb{Z}$, we have $f(z + \omega m + n) = \exp\left(-i\ell\pi m^2\omega - 2i\ell\pi mz\right) f(z)$. For $\ell \in \mathbb{N}^\star$, the set $\mathcal{R}_{\ell,\omega}$ of $(\omega\mathbb{Z}+\mathbb{Z})-$quasi-periodic of level ℓ is a $\mathbb{C}-$vector space of dimension ℓ, whose basis can given by theta functions with characteristics $\mathcal{B}_\ell := \left\{\theta_{0,b}(z, \ell^{-1}\omega), b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right\}$. If $\ell = k^2$, then an alternative basis of $\mathcal{R}_{\ell,\Omega}$ is $\mathcal{B}_{(k,k)} := \left\{\theta_{a,b}(kz, \omega), a, b \in \frac{1}{k}\mathbb{Z}/\mathbb{Z}\right\}$. If $\ell \geq 3$, then we can consider elements of basis of $\mathcal{R}_{\ell,\omega}$ as projective coordinates of $\mathbb{P}^{\ell-1}$. And for $\ell = 2$, the image of $\mathcal{R}_{\ell,\Omega}$ in $\mathbb{P}^{\ell-1}$ is the Kummer variety associated to E, which is the quotient of E by automorphism -1. The change of basis between $\mathcal{B}_\ell$ and $\mathcal{B}_{(k,k)}$ can be obtained by formula:

$$\theta_{0,b}(z, \ell^{-1}\omega) = \sum_{\alpha\in\frac{1}{k}\mathbb{Z}/\mathbb{Z}} \theta_{\alpha,kb}(kz, \omega). \tag{3}$$

2.2 Riemann theta relations

Riemann theta relations give algebraic relations between theta functions. With these relations, one can recover the addition law on an ordinary elliptic curve. Denote by $\theta_i(z) := \theta_{0,i}(z, \ell^{-1}\omega)$, then Riemann theta relations are given by the following theorem:

Theorem 1 *Let i, j, k and l be in $\mathbb{Z}/2\ell\mathbb{Z}$. Assume that $i' = (i + j + k + l)/2, j' = (i + j - k - l)/2, k' = (i - j + k - l)/2$ and $l' = (i - j - k + l)/2$ be in $\mathbb{Z}/\ell\mathbb{Z}$. Let z_1 and z_2 be elements in*

$\mathbb{C}$. *Then, for any characters* χ *over* $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ *the theta functions of level* ℓ *satisfy:*

$$\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta)\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\right)\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0)\right)$$
$$=\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta)\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\right)\left(\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2)\right). \quad (4)$$

Proof: this is a particular case of $g=1$ of [15, Theorem 1]. □

By definition, *theta constants* are the evaluation of theta functions at 0. Formula (4) is defined when theta constants satisfy $\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta)\theta_{k+\eta}(0)\theta_{l+\eta}(0)\neq 0$ which we always assume. According to Lefschetz principle, relations (4) are also valid over $\overline{\mathbb{Q}}_q$ and then are also valid modulo odd prime $p\geq 3$. But, relations (4) are not valid in characteristic 2, because of characters. To remove characters on relations and give general relations which are valid in characteristic 2, we have the following

Corollary 2 *Consider the notation in Theorem 1, the Riemann theta relations (4) can be rewritten as follow:*

$$\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta}(0)\theta_{l+\eta}(0)$$
$$=\sum_{\eta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta}(z_2)\theta_{l'+\eta}(z_2). \quad (5)$$

Proof: The Riemann relations (4) can be rewrite as:

$$\sum_{\eta,\eta'\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta+\eta')\theta_{i+\eta}(z_1+z_2)\theta_{j+\eta}(z_1-z_2)\theta_{k+\eta'}(0)\theta_{l+\eta'}(0)$$
$$=\sum_{\eta,\eta'\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}}\chi(\eta+\eta')\theta_{i'+\eta}(z_1)\theta_{j'+\eta}(z_1)\theta_{k'+\eta'}(z_2)\theta_{l'+\eta'}(z_2). \quad (6)$$

Summing under all characters χ on the dual $\widehat{\frac{1}{2}\mathbb{Z}/\mathbb{Z}}$ gives the desired result. □

The previous theorem gives formulas (8), i.e. the addition law on level 4 theta model E_{λ_1,λ_2} defined over any field (i.e. E_{λ_1,λ_2} has a good reduction modulo p for any prime p).

3 Level 4-theta model

In this section, we define the level 4-theta model of elliptic curve which is valid over any field. In binary field, this level 4-theta model is ordinary and have a rational point of order 4. We also give the arithmetic of level 4-theta model over any field.

3.1 Model valid over any field

Model over odd characteristic. Let $\mathbb{K}$ be a field in odd characteristic. Let $\lambda\in\mathbb{K}$ be a non-zero constant. In the projective space $\mathbb{P}^3:=\mathbb{P}^3(\mathbb{K})$ with homogeneous coordinates $[X_0:$

$X_1 : X_2 : X_3]$. Taking $z_2 = 0$ and $X_i = \theta_i(z_1)$ in formula (4) we have a model of an elliptic curve over $\mathbb{P}^3$, which can be written as intersection of two quadrics (see also [17, page 352]):

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right. , \lambda_i \in \mathbb{K}^\star.$$

with the theta null point $[a_0 : a_1 : a_2 : a_3]$ given by theta constants $a_i = \theta_i(0), i = 0, 1, 2, 3$, with $a_1 = a_3$. Hence one can find a relation between λ_1, λ_2 and theta null point: $\lambda_1 = (a_0^2 + a_2^2)/(a_1^2)$ and $\lambda_2 = 2a_1^2/(a_0 a_2)$. Where

$$\lambda_1 = \lambda_2 \Longleftrightarrow a_0 a_2 (a_0^2 + a_2^2) = 2a_1^4 \tag{7}$$

is a famous *Jacobi relation* which plays a central role in this paper.

Model over even characteristic. For even characteristic, to have the level 4 theta model, it suffices to compute the $2-$adic valuation of theta constants. For this, let $\mathbb{K}$ be a finite field of characteristic 2 and let $\mathcal{W}(\mathbb{K})$ be the ring of Witt vectors with coefficients in $\mathbb{K}$. Carls in [7] prove that on canonical lift $E_{\mathcal{W}(\mathbb{K})}$ we have for all $i \in \mathbb{Z}/\ell\mathbb{Z}$ relations $a_i^2 = \alpha \sum_j \phi(a_{i+j})\phi(a_j)$ where ϕ is the lift of the Frobenius of $\mathbb{K}$ over $\mathcal{W}(\mathbb{K})$ and α is a constant. Therefore, we have $v_2(a_0) = 0$ and $v_2(a_2) = 1$, where v_2 is the $2-$adic valuation. Then, there exists c_0 and c_2 such that $a_0 = c_0$ and $a_2 = 2c_2$. Finally we have respectively $\lambda_1 = c_0^2 + 4c_2^2$ and $\lambda_2 = 1/(c_0 c_2)$. Then, the equations of level 4 theta model of elliptic curve over field $\mathbb{K}$ of even characteristic have good reductions:

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right. , \text{ where } \lambda_i \in \mathbb{K}^\star.$$

Valid model over any field. Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. Then a level 4-theta model can be define by the intersection of two equations:

$$E_{\lambda_1,\lambda_2} : \left\{ \begin{array}{rcl} X_0^2 + X_2^2 & = & \lambda_1 X_1 X_3 \\ X_1^2 + X_3^2 & = & \lambda_2 X_0 X_2 \end{array} \right. ,$$

where $\lambda_1 = c_0^2 + 4c_2^2$, $\lambda_2 = 1/(c_0 c_2) \in \mathbb{K}^\star$, and $c_0 = \theta_0(0)$ and $c_2 = \frac{1}{2}\theta_2(0)$. Jacobi relation (7) become $c_0 c_2 (c_0^2 + 4c_2^2) = 1$ and the set of points $(c_0, c_2) \in \mathbb{A}^2(\mathbb{K})$ satisfying Jacobi relation is a curve C defined over $\mathbb{K}$. The number of rationals points of C is equal to the number of level 4-theta model defined over $\mathbb{K}$. In the above definitions the condition $\lambda_1 \lambda_2 \neq 0$ ensures that the level 4-theta model E_{λ_1,λ_2} is not singular. Indeed, if we assume that $[X_0 : X_1 : X_2 : X_3]$ is a singular point, then the rank of the following matrix can not be two.

$$\begin{pmatrix} 2X_0 & -\lambda_1 X_3 & 2X_2 & -\lambda_1 X_1 \\ -\lambda_2 X_2 & 2X_1 & -\lambda_2 X_0 & 2X_3 \end{pmatrix}.$$

3.2 Addition law in level 4-theta model

Our addition law come from Riemann theta relations which are valid over all characteristic. Let $O_0 := [c_0 : 1 : 2c_2 : 1]$ be the theta null point given by $2-$adic valuation of theta constants.

Theorem 3 *Let $P_1 = [X_{1,0} : X_{1,1} : X_{1,2} : X_{1,3}]$ and $P_2 = [X_{2,0} : X_{2,1} : X_{2,2} : X_{2,3}]$ be two points on E_{λ_1,λ_2}, the coordinates of sum $P_1 + P_2 = P_3$ are given by formulas:*

$$\begin{array}{rcl} X_{3,0} & = & (X_{1,0}^2 X_{2,0}^2 + X_{1,2}^2 X_{2,2}^2) - 4(c_2/c_0) X_{1,1} X_{1,3} X_{2,1} X_{2,3} \\ X_{3,1} & = & c_0 (X_{1,0} X_{1,1} X_{2,0} X_{2,1} + X_{1,2} X_{1,3} X_{2,2} X_{2,3}) - 2c_2 (X_{1,2} X_{1,3} X_{2,0} X_{2,1} + X_{1,0} X_{1,1} X_{2,2} X_{2,3}) \\ X_{3,2} & = & (X_{1,1}^2 X_{2,1}^2 + X_{1,3}^2 X_{2,3}^2) - 4(c_2/c_0) X_{1,0} X_{1,2} X_{2,0} X_{2,2} \\ X_{3,3} & = & c_0 (X_{1,0} X_{1,3} X_{2,0} X_{2,3} + X_{1,1} X_{1,2} X_{2,1} X_{2,2}) - 2c_2 (X_{1,0} X_{1,3} X_{2,1} X_{2,2} + X_{1,1} X_{1,2} X_{2,0} X_{2,3}) \end{array} . \tag{8}$$

Proof: Let $\mathcal{B}(i,j,k,l) = \sum_{\beta\in\frac{1}{2}\mathbb{Z}/\mathbb{Z}} \theta_{i'+\beta}(z_1)\theta_{j'+\beta}(z_1)\theta_{l'+\beta}(z_2)\theta_{k'+\beta}(z_2)$, $\mathcal{Z}_{i,j} = \theta_i(z_1+z_2)\theta_j(z_1-z_2)$ and $\delta_{k,l} = \theta_k(0)\theta_l(0) = a_k a_l$. The equations (5) lead to a system of linear equations:

$$(S)\begin{cases} \delta_{k,l}\mathcal{Z}_{i,j} + \delta_{k+2,l+2}\mathcal{Z}_{i+2,j+2} &= \mathcal{B}(i,j,k,l) \\ \delta_{k+2,l}\mathcal{Z}_{i,j} + \delta_{k,l+2}\mathcal{Z}_{i+2,j+2} &= \mathcal{B}(i,j,k+2,l) \end{cases}$$

The determinant of the system (S) is $\det(S) = a_l a_{l+2}(a_k^2 - a_{k+2}^2)$. In characteristic zero, one can choose $k \notin \{1,3\}$ as $a_1 = a_3$ to have a non-vanishing determinant. Then Cramer method to resolve the system (S) gives:

$$\begin{aligned} \theta_i(z_1+z_2)\theta_j(z_1-z_2) &= \frac{\delta_{k,l+2}\mathcal{B}(i,j,k,l) - \delta_{k+2,l+2}\mathcal{B}(i,j,k+2,l)}{\delta_{k,l}\delta_{k,l+2} - \delta_{k+2,l+2}\delta_{k+2,l}} \\ &= \frac{a_k\mathcal{B}(i,j,k,l) - a_{k+2}\mathcal{B}(i,j,k+2,l)}{a_l(a_k^2 - a_{k+2}^2)}. \end{aligned} \tag{9}$$

if $k \notin \{1,3\}$, then $a_k^2 - a_{k+2}^2$ never vanishes modulo any prime p. To avoid a zero denominator in any characteristic we fix $k = 0$ and $l = i + j$. Then for $i \in \{0,1,2,3\}$ we can simplify (9) by $a_0^2 - a_2^2$ in projective coordinates to have:

$$\theta_i(z_1+z_2)\theta_j(z_1-z_2) = \frac{a_0\mathcal{B}(i,j,0,i+j) - a_2\mathcal{B}(i,j,2,i+j)}{a_{i+j}}. \tag{10}$$

In (10) we fix j equal respectively to $0,1,2$ and 3 to have 16 formulas for $i \in \{0,1,2,3\}$ (see appendix A):

$$\theta_i(z_1+z_2)\theta_0(z_1-z_2) = \frac{a_0\mathcal{B}(i,0,0,i) - a_2\mathcal{B}(i,0,2,i)}{a_i}, \tag{11}$$

$$\theta_i(z_1+z_2)\theta_1(z_1-z_2) = \frac{a_0\mathcal{B}(i,1,0,i+1) - a_2\mathcal{B}(i,1,2,i+1)}{a_{i+1}}, \tag{12}$$

$$\theta_i(z_1+z_2)\theta_2(z_1-z_2) = \frac{a_0\mathcal{B}(i,2,0,i+2) - a_2\mathcal{B}(i,2,2,i+2)}{a_{i+2}}, \tag{13}$$

$$\theta_i(z_1+z_2)\theta_3(z_1-z_2) = \frac{a_0\mathcal{B}(i,3,0,i+3) - a_2\mathcal{B}(i,3,2,i+3)}{a_{i+3}}. \tag{14}$$

Relations (11) give the addition law formulas in (8) by simplifying by $\theta_0(z_1-z_2)$. Reminding that $c_i = a_i$ if $i \neq 2$ and $2c_2 = a_2$ these relations are (see appendix A for more details):

$$\begin{aligned} \theta_0(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(0,0,0,0) - 2c_2\mathcal{B}(0,0,2,0)}{c_0}, \\ \theta_1(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(1,0,0,1) - 2c_2\mathcal{B}(1,0,2,1)}{c_1}, \\ \theta_2(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(2,0,0,2) - 2c_2\mathcal{B}(2,0,2,2)}{2c_2}, \\ \theta_3(z_1+z_2)\theta_0(z_1-z_2) &= \frac{c_0\mathcal{B}(3,0,0,3) - 2c_2\mathcal{B}(3,0,2,3)}{c_3}. \end{aligned}$$

If $l = i = 2$, the numerator and denominator of (11) are divisible by 2 such that we can simplify by 2 before reducing modulo 2. Nevertheless one can avoid a_2 in the denominator by using this alternative relation

$$\theta_i(z_1+z_2)\theta_0(z_1-z_2) = \frac{a_0\mathcal{B}(i,0,0,i+2) - a_2\mathcal{B}(i,0,2,i+2)}{a_{i+2}},$$

which gives

$$\theta_2(z_1+z_2)\theta_0(z_1-z_2) = \frac{c_0\mathcal{B}(2,0,0,0) - 2c_2\mathcal{B}(2,0,2,0)}{c_0}.$$

These relations give the theta of the sum $\theta_i(z_1+z_2)$ in term of $\theta_i(z_1)$ and $\theta_i(z_2)$, and hence the addition formulas in any fields (see appendix B for sage script verification). □

These formulas are valid modulo any prime p. In characteristic 2, the addition law formulas are given by:

$$\begin{array}{rcl} X_{3,0} &=& (X_{1,0}X_{2,0} + X_{1,2}X_{2,2})^2 \\ X_{3,1} &=& c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,1} + X_{1,2}X_{1,3}X_{2,2}X_{2,3}) \\ X_{3,2} &=& (X_{1,1}X_{2,1} + X_{1,3}X_{2,3})^2 \\ X_{3,3} &=& c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,3} + X_{1,1}X_{1,2}X_{2,1}X_{2,2}) \end{array}. \tag{15}$$

The neutral element is the theta null point: i.e. $O_0 = [c_0 : 1 : 2c_2 : 1]$ over all characteristic, which become $0_0 := [c_0 : 1 : 0 : 1]$ for characteristic 2. Over all characteristic, the opposite of 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 additions laws (8) and (15), for respectively odd and even characteristic, are also valid for doubling: they are unified additions laws. More precisely, let $[X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}]$ be a point on E_{λ_1,λ_2} the coordinates of $2[X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}] = [X_{5,0}, X_{5,1}, X_{5,2}, X_{5,3}]$ are:

$$\left\{\begin{array}{rcl} X_{5,0} &=& X_{1,0}^4 + X_{1,2}^4 - 4(c_2/c_0)X_{1,1}^2X_{1,3}^2 \\ X_{5,1} &=& c_0(X_{1,0}^2X_{1,1}^2 + X_{1,2}^2X_{1,3}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \\ X_{5,2} &=& X_{1,1}^4 + X_{1,3}^4 - (c_2/c_0)X_{1,0}^2X_{1,2}^2 \\ X_{5,3} &=& c_0(X_{1,0}^2X_{1,3}^2 + X_{1,1}^2X_{1,2}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \end{array}\right. \tag{16}$$

Observe that Kohel in [14] uses another approach as in [13] to obtain formulas (15) in characteristic 2. Denote respectively by M, S and m the cost of multiplication, square and multiplication by a constant over field $\mathbb{K}$. In characteristic 2, we have an efficient algorithm to compute point addition formulas (see §§4.3.2 for comparaison with previous work). For efficiency in odd characteristic we use a sextuplet represention to give an algorithm for point addition. The cost is given in the following corollary.

Corollary 4 (Costs of addition) *Addition of two generic points on E_{λ_1,λ_2} can be done in:*

(a) $7M + 2S + 2m$, *when $\mathbb{K}$ is a binary field;*

(b) $11M + 8S + 6m$, *when $\mathbb{K}$ is a field of odd characteristic.*

Proof: (a) Over binary field point addition formulas can by computed as:

$$A := X_{1,0}\cdot X_{2,0};\ \ B := X_{1,1}\cdot X_{2,1};\ \ C := X_{1,2}\cdot X_{2,2};\ \ D := X_{1,3}\cdot X_{2,3};\ \ X_{3,0} := (A+C)^2;$$
$$X_{3,2} := (B+D)^2;\ \ X_{3,1} := c_0(A\cdot B + C\cdot D);\ \ X_{3,2} := X_{3,1} + c_0(A+C)\cdot(B+D),$$

which cost 7 multiplications and 2 squares and 2 multiplications by constant c_0.

(b) For efficiency over fields of odd characteristic a point $[X_0 : X_1 : X_2 : X_3]$ is represented as a sextuplet $(X_0, X_1, X_2, X_3, X_0X_1, X_2X_3)$. Thus the sum $(X_{3,0}, X_{3,1}, X_{3,2}, X_{3,3}, U_3, V_3)$ of the points represented by $(X_{1,0}, X_{1,1}, X_{1,2}, X_{1,3}, U_1, V_1)$ and $(X_{2,0}, X_{2,1}, X_{2,2}, X_{2,3}, U_2, V_2)$ where $U_1 = X_{1,0}X_{1,1}$; $V_1 = X_{1,2}X_{1,3}$ and $U_2 = X_{2,0}X_{2,1}$; $V_2 = X_{2,2}X_{2,3}$ can be computed with the

algorithm:

$$A := X_{1,0}\cdot X_{2,0};\ \ B := X_{1,1}\cdot X_{2,1};\ \ C := X_{1,2}\cdot X_{2,2};\ \ D := X_{1,3}\cdot X_{2,3};\ \ E := A^2;\ \ F := B^2;$$
$$G := C^2;\ \ H := D^2;\ \ X_{3,0} := E + G + 2(c_2/c_0)((B-D)^2 - F - H);$$
$$X_{3,2} := F + H + 2(c_2/c_0)((A-C)^2 - E - G);\ \ I := ((A+B)^2 - E - F)/2;$$
$$J := ((C+D)^2 - G - H)/2;\ \ K := (U_1 + V_1)\cdot(U_2 + V_2) - I - J;$$
$$L := (A+C)\cdot(B+D) - I - J;\ \ X_{3,1} := c_0(I+J) - 2c_2K;$$
$$E := (X_{1,0} + X_{1,2})\cdot(X_{1,3} + X_{1,1}) - U_1 - V_1;\ \ F := (X_{2,0} + X_{2,2})\cdot(X_{2,3} + X_{2,1}) - U_2 - V_2;$$
$$G := E\cdot F - L;\ \ X_{3,3} := c_0L - 2c_2G;\ \ U_3 := X_{3,0}\cdot X_{3,1};\ \ V_3 := X_{3,2}\cdot X_{3,3},$$

which cost $11M + 8S + 6m$ where $6m$ equal to 2 multiplications by constant c_0 and 2 multiplications by $2c_2$ and 2 multiplications by $2c_2/c_0$. □

Lemma 5 *Let E_{λ_1,λ_2} be the level 4-theta model of an elliptic curve over field $\mathbb{K}$ of characteristic $p \geq 0$. Then:*

(1) E_{λ_1,λ_2} has a rational point of order 4.

(2) Moreover, if $p \neq 2$, then E_{λ_1,λ_2} has a rational point of order 8.

Proof: Let $\mathcal{S}_4$ be the group of permutation on $\{0,1,2,3\}$. Let $\sigma = (0,1,2,3)$ be the hull permutation of $\mathcal{S}_4$ and denote by $H_1 = \langle\sigma\rangle$ the subgroup of $\mathcal{S}_4$ generated by σ. Remark that if $P = [X_0 : X_1 : X_2 : X_3]$ is in E_{λ_1,λ_2}, then so are $[X_1 : X_2 : X_3 : X_0], [X_2 : X_3 : X_0 : X_1]$ and $[X_3 : X_0 : X_1 : X_2]$. Then, there exists an action of H_1 on points of E_{λ_1,λ_2} given by: $\sigma([X_0 : X_1 : X_2 : X_3]) = [X_{\sigma(0)} : X_{\sigma(1)} : X_{\sigma(2)} : X_{\sigma(3)}]$. Under this action, cardinal of E_{λ_1,λ_2} is divisible by 4. Moreover, if the characteristic of $\mathbb{K}$ is not 2, then we have also an action on E given by: $\tau([X_0 : X_1 : X_2 : X_3]) = [-X_0 : X_1 : -X_2 : X_3] = [X_0 : -X_1 : X_2 : -X_3]$. Under this second action, the cardinal of orbit is 2. □

Over non binary field, a part from the neutral element $O_0 = [c_0 : 1 : 2c_2 : 1]$, the level 4-theta model has 3 points of order 2 namely $\widetilde{O}_0 = [-c_0 : 1 : -2c_2 : 1], O_1 := [2c_2 : 1 : c_0 : 1]$ and $\widetilde{O}_1 := [-2c_2 : 1 : -c_0 : 1]$. The four points of order 4 are $A_1 := [1 : 2c_2 : 1 : c_0], \widetilde{A}_1 := [-1 : 2c_2 : -1, c_0], A_2 := [1 : c_0 : 1 : 2c_2]$ and $\widetilde{A}_2 := [-1 : c_0 : -1 : 2c_2]$. Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on level 4-theta model E_{λ_1,λ_2}, the actions of these rationals points of order 2 and 4 are:

$$\begin{aligned}
P + O_0 &= [X_0 : X_1 : X_2 : X_3], \quad P + \widetilde{O}_0 = [-X_0 : X_1 : -X_2 : X_3],\\
P + O_1 &= [X_2 : X_3 : X_0 : X_1], \quad P + \widetilde{O}_1 = [-X_2 : X_3 : -X_0 : X_1],\\
P + A_1 &= [X_1 : X_2 : X_3 : X_0], \quad P + \widetilde{A}_1 = [-X_1 : X_2 : -X_3 : X_0],\\
P + A_2 &= [X_3 : X_0 : X_1 : X_2], \quad P + \widetilde{A}_2 = [-X_3 : X_0 : -X_1 : X_2].
\end{aligned}$$

These formulas give: $P + \sigma^i(O_0) = \sigma^i(P)$ and $P + \tau^i(O_0) = \tau^i(P)$, which we can deduce that $\sigma(P) + \sigma(Q) = P + Q + 2\sigma(O_0)$ and $\sigma(P) - \sigma(Q) = P - Q$.

Completness of group laws. A complete group law mean that one can compute all pair of input. This propriety is used to avoid some exceptional procedure attack on elliptic curve cryptosystems [12]. Let $\mathbb{K}$ be a field of odd characteristic and let $E_{\lambda_1,\lambda_2} : X_0^2 + X_2^2 = \lambda_1 X_1 X_3, X_1^2 + X_3^2 = \lambda_2 X_0 X_2$ be a level 4-theta model defined over $\mathbb{K}$.

Lemma 6 *Let $P = [X_0 : X_1 : X_2 : X_3]$ be a point on E_{λ_1,λ_2}. If $X_i = 0$ then we can write P as of form $\sigma^j([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon])$ for some $j = 0,1,2,3$ where $\varepsilon = \sqrt{-1}$.*

Proof: Without loos of generality we can assume that $X_0 = 0$. If we have also $X_j = 0$ for $j \neq 0$ then be equations of level 4-theta model we will have $P \notin \mathbb{P}^3$. Then $X_0 = 0$ implies that $X_j \neq 0$ for $j \neq 0$. Assume also that $X_1 \neq 0$ then $X_2^2 = \lambda_1 X_1 X_3$ and $X_1^2 + X_3^2 = 0$ or equivalently $X_3 = \pm\sqrt{-1}X_1$ and $X_2^2 = \pm\sqrt{-1}\lambda_1 X_1^2$. Then over projective space we have $P = \sigma^0([0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon])$. If now we assume that $X_i = 0$ and $X_{i+1} \neq 0$, we apply a power of the permutation σ^i and use the first assumption. □

Theorem 7 (completness) *If one of these conditions hold in* $\mathbb{K}$*:*

(1) -1 *not a square in* $\mathbb{K}$*, or*

(2) $\sqrt{-1}\lambda_1$ *not a square in* $\mathbb{K}$

then addition formulas (8) are complete.

Proof: Assume that these conditions are not hold, then the addition of $P_1 = [0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \pm\varepsilon]$ and $P_2 = [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$ is not defined. Indeed let $P_1 = [0 : 1 : X_{1,2} : \varepsilon]$ be one point given by lemma 6 and let $P_2 = [X_{2,0} : X_{2,1} : X_{2,2} : X_{2,3}]$. By formulas (8) the coordinates of sum $P_1 + P_2$ are:

$$\begin{array}{rcl} X_{3,0} & = & (c_0 X_{1,2}^2 Y_{2,2}^2 - 4c_2 X_{1,3} X_{2,1} X_{2,3})/c_0 \\ X_{3,1} & = & X_{1,3} X_{1,2} (c_0 X_{2,2} Y_{2,3} - 2c_2 X_{2,0} X_{2,1}) \\ X_{3,2} & = & \varepsilon^2 X_{2,3}^2 + X_{2,1}^2 \\ X_{3,3} & = & X_{1,2} (c_0 X_{2,1} X_{2,2} - 2c_2 X_{2,0} X_{2,3}) \end{array} .$$

If $X_{3,2} = 0$ then $X_{2,3} = \pm X_{2,1}$ and if $X_{3,0} = 0$ then $X_{2,2} = \pm 2c_2\sqrt{\pm 1}X_{2,1}$. Since $P_2 \in E_{\lambda_1,\lambda_2}$ then $X_{2,0} = \pm c_0\sqrt{\pm 1}X_{2,1}$ and then we have $P_2 = [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$. According to lemma 6 the addition of point of form $P_1 = [0 : 1 : \pm\sqrt{\pm\varepsilon\lambda_1} : \varepsilon]$ and point of form $P_2 = [\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1]$ never give an element of $\mathbb{P}^3(\mathbb{K})$ then is not defined by formulas (8). □

The first sufficient condition of Theorem 7 hold when $\mathbb{K}$ is a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$ such that $q \equiv 3 \bmod 4$. Notice that all points of form $\sigma^i([\pm c_0\varepsilon : 1 : \pm 2c_2\varepsilon : \pm 1])$ given by theorem 7 have an even order, since its coordinates are given by theta constants. This implies that over any fields (including binary fields) addition law on level 4-theta model E_{λ_1,λ_2} is complete in a subgroup of odd order.

Geometric interpretation of group law on E_{λ_1,λ_2}. Let P_1 and P_2 be two points on the level 4-theta model E_{λ_1,λ_2}. Denote by $\mathcal{P}(O_0, P_1, P_2)$ the plane passing through O_0, P_1 and P_2. Then this plane intersects E_{λ_1,λ_2} at a fourth point $Q = -(P_1 + P_2)$. Denote also by $\mathcal{P}(O_0, Q)$ the tangent plane to the curve at O_0 and passing through Q. Then this plane intersects E_{λ_1,λ_2} at a fourth point which is exactly the inverse of Q.

4 Edwards model of elliptic curve

In [10], Edwards gave a normal form for elliptic curve defined over an algebraic closed field, which is valid for non-binary field and has an unified addition law. From the level 4-theta model E_{λ_1,λ_2} elliptic curve, we derive an Edwards model which is defined over any field and which extends the well known Edwards model.

4.1 Equation of Edwards model of elliptic curve

Theorem 8 *Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. The level 4-theta model E_{λ_1,λ_2} gives a normal form with equation: $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$, where $\lambda = \lambda_1\lambda_2 \in \mathbb{K}^\star$.*

Proof: Divide the first equation of E_{λ_1,λ_2} by X_0^2 and the second by X_1^2 and consider the following change of variables: $[X_0 : X_1 : X_2 : X_3] \longmapsto (x, y) = (X_2/X_0, X_3/X_1)$, we have:

$$1 + x^2 = \lambda_1 \frac{X_1X_3}{X_0^2} \quad \text{and} \quad y^2 + 1 = \lambda_2 \frac{X_0X_2}{X_1^2}.$$

Multiply the two above equations to have $(x^2 + 1)(1 + y^2) = \lambda_1\lambda_2 xy$, which can be written as $1+x^2+y^2+x^2y^2 = \lambda_1\lambda_2 xy$. The change of variables gives the neutral element $O_0 := (2c_2/c_0, 1)$ which becomes $(0, 1)$ over binary field. □

Theorem 9 *Let $\mathbb{K}$ be a non-binary field, then the normal model $\mathcal{E}_\lambda$, with the neutral element $O_0 := (2c_2/c_0, 1)$ is isomorphic to the well known Edwards model.*

Proof: As our new Edwards come from basis $\mathcal{B}_\ell := \left\{\theta_{0,b}(z, \ell^{-1}\omega), b \in \frac{1}{\ell}\mathbb{Z}/\mathbb{Z}\right\}$. Consider the alternative basis $\mathcal{B}_{(k,k)} := \left\{\theta_{a,b}(kz, \omega), a, b \in \frac{1}{k}\mathbb{Z}/\mathbb{Z}\right\}$. The formula (3) gives a change of basis:

$$\left\{\begin{array}{lcl} X_0 &=& \theta_{00}(z) + \theta_{10}(z) \\ X_1 &=& \theta_{01}(z) + \theta_{11}(z) \\ X_2 &=& \theta_{00}(z) - \theta_{10}(z) \\ X_3 &=& \theta_{01}(z) - \theta_{11}(z) \end{array}\right. \iff \left\{\begin{array}{lcl} \theta_{00}(z) &=& X_0 + X_2 \\ \theta_{01}(z) &=& X_1 + X_3 \\ \theta_{10}(z) &=& X_0 - X_2 \\ \theta_{11}(z) &=& X_1 - X_3 \end{array}\right. , \text{ where } X_i = \theta_i(z).$$

This change of basis $\mathcal{B}_{(k,k)}$ gives an alternative level 4-theta model of elliptic curve defined over non binary fields (see [18, p. 23] for more details):

$$\left\{\begin{array}{lcl} \theta_{00}^2(0)T_{00}^2 &=& \theta_{01}^2(0)T_{01}^2 + \theta_{10}^2(0)T_{10}^2 \\ \theta_{00}^2(0)T_{11}^2 &=& \theta_{10}^2(0)T_{01}^2 - \theta_{01}^2(0)T_{10}^2 \end{array}\right. , \text{ where } T_{ij} = \theta_{ij}(z) \tag{17}$$

Setting $x' = T_2/T_0, y' = T_3/T_1$ and $c = \theta_{10}(0)/\theta_{00}(0)$, the curve (17) is isomorphic to the well known Edwards model, for more details see [9, Section 7.1.1], which completes the proof. □

According to Theorems 8 and 9, we have this definition:

Definition 1 Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. An Edwards model of elliptic curves can be given by the equation:

$$\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy, \text{ where } \lambda \in \mathbb{K}^\star.$$

Theorem 10 *Let $\mathbb{K}$ be a field of characteristic $p \geq 0$ and let $\lambda \in \mathbb{K}^\star$. Then the Edwards model defined over $\mathbb{K}$ is non-singular.*

Proof: Our Edwards model is isomorphic to the Edwards model $Ed_c : X^2 + Y^2 = c^2(1 + X^2Y^2)$ where $c = \theta_{10}(0)/\theta_{00}(0)$. The model Ed_c is non singular if and only if $c^4 \neq 1$ (see [10]), i.e $(c_0 - 2c_2)^4 \neq (c_0 + 2c_2)^4$. This condition is equivalent to $c_0c_2(c_0^2 + 4c_2^2) \neq 0$ which is always true according to Jacobi relation (7). □

A part from the neutral element $O_0 := (2c_2/c_0, 1)$, the Edwards model $\mathcal{E}_\lambda : 1+x^2+y^2+x^2y^2 = \lambda xy$ has three 2−torsion rationals 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

$\mathbb{K}$: $Q_1 = (1,\gamma), Q_2 = (1,1/\gamma), Q_3 = (-1,-\gamma)$ and $Q_4 = (-1,-1/\gamma)$. The actions of rationals points of order 2 and 4 are:

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

Remark 11 If $\mathbb{K}$ is a binary field, then $P_3 = O$, $P_4 = P_2$, $Q_3 = Q_1$ and $Q_4 = Q_2$. The number of rationals points of $\mathcal{E}_\lambda$ is then divisible by 4.

4.2 Birational equivalence with Weierstraß model

Theorem 12 *Let $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ be the Edwards model of elliptic curve defined over field $\mathbb{K}$ of characteristic $p \geq 0$.*

(1) if $p \neq 2$, then $\mathcal{E}_\lambda$ is equivalent to a cubic Weierstraß model;

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

Proof: Theorem 9 gives the birational equivalence between $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ and the well known Edwards model $X^2 + Y^2 = c^2(1 + X^2Y^2)$. This well known Edwards model is 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 birational 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 Edwards model and Weierstraß model are

$$\begin{aligned} (u,v) &\longmapsto (x,y) = \left(\frac{1}{\lambda u}, \frac{\lambda^2 v + 1}{\lambda^2 u + \lambda^2 v + 1}\right) \text{ and } (0,1) \mapsto [0:1:0] \\ (x,y) &\longmapsto (u,v) = \left(\frac{1}{\lambda x}, \frac{\lambda y + x(y+1)}{\lambda^2 x(y+1)}\right) \text{ and } [0:1:0] \mapsto (0,1). \end{aligned}$$

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

Corollary 13 ($j-$Invariant) *Let $\mathbb{K}$ be a field of any characteristic and let $\mathcal{E}_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ be Edwards model over $\mathbb{K}$. The $j-$Invariant of $\mathcal{E}_\lambda$ is*

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

Over field of characteristic 2 the $j-$Invariant is $\lambda^4 = j \bmod 2$.

Proof: Let $\mathbb{K}$ be field of characteristic zero, the $j-$Invariant of Weierstraß model $v^2 = u^3 - (1 + c^4)u^2 - 4c^4u + 4c^4(1 + c^4)$ over $\mathbb{K}$ 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 $c = \theta_{10}(0)/\theta_{00}(0) = (c_0 - 2c_2)/(c_0 + 2c_2)$ then a straightforward calculation gives the desired result. Notice that the expression of j is defined modulo any prime p then j is defined over field of any characteristic. Over field 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 12. □

4.3 Addition on Edwards model

In [9] Diao uses formulas (1) on the well known Edwards model [10] to deduce an addition on binary Edwards model. Over binary field addition law in [9, Theorem 7.4] is not unified and not efficient. However to have an unified and more efficient addition law formulas we use the addition law on the level 4-theta model. More precisely we have:

Theorem 14 *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:*

$$(x_3, y_3) = \left(\frac{c_0(x_1 + y_1x_2y_2) - 2c_2(y_1 + x_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)}, \frac{c_0(x_1x_2 + y_1y_2) - 2c_2(x_1y_2 + y_1x_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)} \right). \quad (18)$$

The opposite of the point is $-(x_1, y_1) = (x_1, 1/y_1)$ and the neutral element is $O_0 := (2c_2/c_0, 1)$.

One can verify addition law on new Edwards model $\mathcal{E}_\lambda$ by this sage script [22]:

```
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 characteristic 2 fields the coordinates of sum are obtained by reducing modulo 2:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 + y_1x_2y_2}{y_2 + x_1y_1x_2}, \frac{x_1x_2 + y_1y_2}{1 + x_1y_1x_2y_2} \right). \quad (19)$$

Remark 15 Addition group law is unified over any fields, i.e. addition formulas are also valid for point doubling. The point doubling formulas can be written as follow:

$$2(x_1, y_1) = \left(\frac{c_0x_1(1 + y_1^2) - 2c_2y_1(1 + x_1^2)}{c_0y_1(1 + x_1^2) - 2c_2x_1(1 + y_1^2)}, \frac{c_0(x_1^2 + y_1^2) - 4c_2x_1y_1}{c_0(1 + x_1^2y_1^2) - 4c_2x_1y_1} \right). \quad (20)$$

Over characteristic 2 fields, the formulas (19) or (20) give the binary doubling formulas:

$$2(x_1, y_1) = \left(\frac{x_1(1 + y_1)^2}{y_1(1 + x_1)^2}, \frac{(x_1 + y_1)^2}{(1 + x_1y_1)^2} \right). \quad (21)$$

Since Theorem 7 addition law on Edwards model $\mathcal{E}_\lambda$ defined over field $\mathbb{K}$ is complete over any subgroup of $\mathcal{E}_\lambda$ of odd order.

Remark 16 One can describe geometrically the group law on Edwards model $\mathcal{E}_\lambda$ using a conic as the method in [1].

4.3.1 Explicit formulas

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

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

These formulas cost $2I + 9M + 8m$ over odd fields and $2I + 5M$ over binary fields, where I is a field inversion, M is a field multiplication, S is a field squaring, and m a multiplication by a constant. One can replace $2I$ by $1I + 3M$ using Montgomerry's inversion trick.

Remark that the negation of point cost 1 inversion which is too expensive. Nevertheless the sum and the difference of two generics points (x_1, y_1) and (x_2, y_2) have the same complexity. Indeed these following formulas compute the difference $(x_5, y_5) = (x_1, y_1) - (x_2, y_2)$ if it is defined:

$$(x_5, y_5) = \left(\frac{c_0(x_1y_2 + y_1x_2) - 2c_2(x_1x_2 + y_1y_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)}, \frac{c_0(y_1 + x_1x_2y_2) - 2c_2(x_1 + y_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)} \right). \quad (22)$$

We retrieve the eight polynoms used to compute the sum, i.e. $F_1 = x_1 + y_1x_2y_2, F_2 = y_1 + x_1x_2y_2, F_3 = y_2 + x_1y_1x_2, F_4 = x_2 + x_1y_1y_2, F_5 = x_1x_2 + y_1y_2, F_6 = x_1y_2 + y_1x_2, F_7 = 1 + x_1y_1x_2y_2$ and $F_8 = x_1y_1 + x_2y_2$. Indeed, formula (18) and formula (22) can be computed as:

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

Projective coordinates. Since over binary fields we have competitives formulas for addition law we only give projective coordinates over finite fields $\mathbb{K}$ of characteristic 2. To avoid inversions we can work in projective space $\mathbb{P}^3(\mathbb{K})$ or in $\mathbb{P}^2(\mathbb{K})$. The addition formulas in $\mathbb{P}^3(\mathbb{K})$ are given in corollary 4 and are the best known addition formulas of elliptic curves. In this section we give an alternative addition formulas in $\mathbb{P}^2(\mathbb{K})$ which are more expensives than formulas (15). Let $x = X/Z$ and $y = Y/Z$ then the coordinates of sum $[X_3 : Y_3 : Z_3] = [X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]$ can be computed as:

$$\begin{array}{l} A = X_1 \cdot X_2;\quad B = Y_1 \cdot Y_2;\quad C = A \cdot B; \\ D = X_1 \cdot Z_2;\quad E = Y_2 \cdot Z_1;\quad Z = Z_1 \cdot Z_2 \\ F = E \cdot (C + D^2);\quad G = D \cdot (C + E^2); \\ H = Z \cdot (A + B);\quad I = C + Z^2; \\ X_3 = F \cdot I;\quad Y_3 = H \cdot G;\quad Z_3 = G \cdot I \end{array} .$$

The coordinates of double $[X_4 : Y_4 : Z_4] = 2[X_1 : Y_1 : Z_1]$ can be computed as:

$$\begin{array}{l} A = (Y_1 + Z_1)^2;\quad B = (X_1 + Z_1)^2;\quad C = (Z_1 \cdot (X_1 + Y_1))^2; \\ D = A \cdot B + C;\quad E = X_1 \cdot A;\quad F = Y_1 \cdot B \\ X_4 = E \cdot D;\quad Y_4 = F \cdot C;\quad Z_4 = F \cdot D \end{array} .$$

Projective addition costs $12M + 3S$ and projective doubling costs $7M + 3S$ of field elements.

4.3.2 Comparisons of addition formulas with previous works

In this section we compare our addition formulas of normal forms in binary field with other models of elliptic curves. As Theorems 8 and 12 we choose models that are birationally equivalent to ordinary Weierstraß model $v^2+uv = u^3+b_2u^2+b_6$ where $b_2 = 0$ of Explicit-Formulas Database [2]. Recall that M, S and m are respectively the cost of multiplication, square and multiplication by a constant over field $\mathbb{K}$.

Models	Doubling	Addition
Weierstraß	$7M + 3S$	$14M + 1S$
Binary Edwards of [5]	$4M + 4S + 1m$	$16M + 1S + 4m$
Hessian	$6M + 3S$	$12M + 6S$
Huff of [8]	$6M + 5S + 2m$	$13M + 2S + 2m$
Edwards model of [23]	$3M + 3S + 1m$	$12M + 4S + 2m$
Level 4-theta model	$3M + 6S + 2m$	$7M + 2S + 2m$
Our Edwards model	$7M + 3S$	$12M + 3S$

Table 1: Comparisons of points operations in binary fields

We can observe that addition law on level 4-theta model costs only $7M + 2S + 2m$, which is the fastest addition formulas for ordinary elliptic curves.

5 Differential addition on Kummer line

As addition law on level 4-theta model is not competitive, we study in this section differential additions. Let $w(P)$ be a coordinate function of point P on normal forms, if $w(-P) = w(P)$, one can compute the coordinate function $w(nP)$ for exponentiation nP. For level 4-theta model, if $P = [X_0 : X_1 : X_2 : X_3] \in E_{\lambda_1,\lambda_2}$ we choose $w(P) \in \{X_0, X_2\}$, see subsection 5.1. For Edwards model, if $P = (x, y) \in \mathcal{E}_\lambda$ we choose $w(P) = x$, see subsection 5.2.

Our differential additions are defined over any characteristic and are very competitives to other differential addition in our knowledge. Indeed, our differential addition-doubling cost $4M + 3S + 4m$ for level 4-theta model and $5M + 5S + 2m$ for Edwards model defined over odd fields, and cost $4M + 3S + 2m$ for level 4-theta model and $5M + 4S + 2m$ for Edwards model defined over binary fields. The tables 2 and 3 show that our formula for level 4-theta model is the most efficient formula of existing formulas.

5.1 Differential addition on level 4-theta model

This section is devoted to differential addition on Kummer line of elliptic curve. Let $\mathbb{K}$ be a field of characteristic $p \geq 0$ and let E_{λ_1,λ_2} be the level 4-theta model of ordinary elliptic curve defined over $\mathbb{K}$. Let $[X_i] := [X_0 : X_1 : X_2 : X_3]$ be a point on E_{λ_1,λ_2}, the opposite of $[X_i]$ is $[X_0 : X_3 : X_2 : X_1]$. The set $\{X_0, X_2, X_1+X_3\}$ is invariant under the action of opposite. Denote $W = X_1 + X_3$, an equation of Kummer line can be written as

$$\mathcal{K}_{E_{\lambda_1,\lambda_2}} : W^2 = \frac{2}{\lambda_1}(X_0^2 + X_2^2) + \lambda_2 X_0 X_2,$$

which become $W^2 = \lambda_2 X_0 X_2$ over binary field. The addition on E_{λ_1,λ_2} do not induce an addition on corresponding Kummer line, but one can defined a differential addition on Kummer line. Let $[X_{1,i}] = [X_{1,0} : X_{1,1} : X_{1,2} : X_{1,3}]$ and $[X_{2,i}] = [X_{2,0} : X_{2,1} : X_{2,2} : X_{2,3}]$ be two points on

E_{λ_1,λ_2} and let $[X_{3,i}] = [X_{1,i}] + [X_{2,i}], [X_{4,i}] = [X_{1,i}] - [X_{2,i}]$ and $[X_{5,i}] = 2[X_{1,i}]$. For differential addition and differential doubling we express respectively the coordinates $X_{3,0}, X_{3,2}, X_{3,1} + X_{3,3}$ and $X_{5,0}, X_{5,2}, X_{5,1} + X_{5,3}$ in term of coordinates of $X_{1,i}, X_{2,i}$ and $X_{4,i}$. We have:

$$\begin{cases} X_{3,0} &= (X_{1,0}^2X_{2,0}^2 + X_{1,2}^2X_{2,2}^2) - 4(c_2/c_0)X_{1,1}X_{1,3}X_{2,1}X_{2,3} \\ X_{3,1} &= c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,1} + X_{1,2}X_{1,3}X_{2,2}X_{2,3}) - 2c_2(X_{1,0}X_{1,1}X_{2,2}X_{2,3} + X_{1,2}X_{1,3}X_{2,0}X_{2,1}) \\ X_{3,2} &= (X_{1,1}^2X_{2,1}^2 + X_{1,3}^2X_{2,3}^2) - 4(c2/c0)X_{1,0}X_{2,0}X_{1,2}X_{2,2} \\ X_{3,3} &= c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,3} + X_{1,1}X_{1,2}X_{2,1}X_{2,2}) - 2c_2(X_{1,0}X_{1,3}X_{2,1}X_{2,2} + X_{1,1}X_{1,2}X_{2,0}X_{2,3}) \end{cases}$$

$$\begin{cases} X_{4,0} &= (X_{1,0}^2X_{2,0}^2 + X_{1,2}^2X_{2,2}^2) - 4(c_2/c_0)X_{1,1}X_{1,3}X_{2,1}X_{2,3} \\ X_{4,1} &= c_0(X_{1,0}X_{1,1}X_{2,0}X_{2,3} + X_{1,2}X_{1,3}X_{2,1}X_{2,2}) - 2c_2(X_{1,0}X_{1,1}X_{2,1}X_{2,2} + X_{1,2}X_{1,3}X_{2,0}X_{2,3}) \\ X_{4,2} &= (X_{1,3}^2X_{2,1}^2 + X_{1,1}^2X_{2,3}^2) - 4(c_2/c_0)X_{1,0}X_{1,2}X_{2,0}X_{2,2} \\ X_{4,3} &= c_0(X_{1,0}X_{1,3}X_{2,0}X_{2,1} + X_{1,1}X_{1,2}X_{2,2}X_{2,3}) - 2c_2(X_{1,0}X_{1,3}X_{2,2}X_{2,3} + X_{1,1}X_{1,2}X_{2,0}X_{2,1}) \end{cases}$$

$$\begin{cases} X_{5,0} &= X_{1,0}^4 + X_{1,2}^4 - 4(c_2/c_0)X_{1,1}^2X_{1,3}^2 \\ X_{5,1} &= c_0(X_{1,0}^2X_{1,1}^2 + X_{1,2}^2X_{1,3}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \\ X_{5,2} &= X_{1,1}^4 + X_{1,3}^4 - (c_2/c_0)X_{1,0}^2X_{1,2}^2 \\ X_{5,3} &= c_0(X_{1,0}^2X_{1,3}^2 + X_{1,1}^2X_{1,2}^2) - 4c_2X_{1,0}X_{1,1}X_{1,2}X_{1,3} \end{cases}$$

A straightforward and easy calculation shows that:

$$\begin{cases} X_{3,0} &= X_{4,0} \\ X_{3,2} &= \dfrac{c_0^2 - 4c_2^2}{c_0c_2}X_{1,0}X_{2,0}\cdot X_{1,2}X_{2,2} - X_{4,2} \end{cases}, \tag{23}$$

$$\begin{cases} X_{5,0} &= \mu c_0(X_{1,0}^2 + X_{1,2}^2)^2 - 2X_{1,0}^2X_{1,2}^2 \\ X_{5,2} &= (c_2/c_0)X_{1,0}^2\cdot X_{1,2}^2 - 2\mu c_2(X_{1,0}^2 + X_{1,2}^2)^2 \end{cases}, \tag{24}$$

where $\mu = c_0/(c_0^2+4c_2^2)$. The cost of differential addition and doubling are respectively $3M+1m$ and $1M+3S+3m$ operations over fields of odd characteristic. Over binary fields differential addition and doubling cost respectively $3M+1m$ and $1M+3S+1m$ operations.

Notice that, moreover, we can also focus to the computation of coordinates functions $W_i = X_{i,1} + X_{i,3}$ for $i = 1, 2, 3, 4, 5$ which give addition law on Kummer line $\mathcal{K}_{E_{\lambda_1,\lambda_2}} : W^2 = \dfrac{2}{\lambda_1}(X_0^2 + X_2^2) + \lambda_2X_0X_2$,. We then have

$$\begin{aligned} W_3 &= W_1\cdot W_2\cdot\Big(c_0(X_{1,0}\cdot X_{2,0} + X_{1,2}\cdot X_{2,2}) - 2c_2(X_{1,0}X_{2,2} + X_{1,2}X_{2,0})\Big) - W_4 \\ W_5 &= \mu(c_0^2 - 4c_2^2)(X_{1,0}^2 + X_{1,2}^2)\cdot(W_1^2 - 2c_0c_2(X_{1,0}^2 + X_{1,2}^2)) \end{aligned}$$

Then computations cost respectively $6M+3m$ and $2M+4S+5m$ operations for respectively differentials addition and doubling over field of odd characteristic. Over binary fields these cost are respectively $5M + 2m$ operations and $2M + 4S + 2m$ for respectively differentials addition and doubling.

5.2 Differential addition on Edwards model over any fields

Let $\mathcal{E}_\lambda$ be Edwards model over any field $\mathbb{K}$ and let (x, y) be a point on $\mathcal{E}_\lambda$. The first coordinate of (x, y) is invariant under negation action. For $i = 1, 2, 3, 4$ let (x_i, y_i) be point on $\mathcal{E}_\lambda$ such that $(x_3, y_3) = (x_1, y_1) + (x_2, y_2), (x_4, y_4) = (x_1, y_1) - (x_2, y_2)$ and $(x_5, y_5) = 2(x_1, y_1)$. As in previous §5.1, our goal is to express x_3 and x_5 in term of x_1, x_2 and x_4. As in previous 5.1 we

have $x_i = X_{i,2}/X_{i,0}$ for $i = 1, 2, 3, 4, 5$ where $[X_{i,0} : X_{i,1} : X_{i,2} : X_{i,3}]$ are points on level 4-theta model. From equations (23) and (24) we have these following relations, if they are defined:

$$x_3 + x_4 = \frac{(c_0^2 - 4c_2^2)x_1x_2}{c_0c_2(1 + x_1^2x_2^2)}, \tag{25}$$

$$x_5 = \frac{(c_2/c_0)x_1^2 - 2\mu c_2(1 + x_1^2)^2}{\mu c_0(1 + x_1^2)^2 - 2x_1^2}, \tag{26}$$

where $\mu = c_0/(c_0^2+4c_2^2)$. The computation of x_3 and x_5 cost respectively $1I+1M+1S+1m$ and $1I + 2S + 3m$ operations over any field $\mathbb{K}$. To avoid inversions let $x_i = X_i/Z_i$ for $i = 1, 2, 3, 4, 5$ where $[X : Z]$ parametrize projective space $\mathbb{P}^1(\mathbb{K})$. Over any fields, formulas (25) and (26) become:

$$\begin{cases} X_3 = \frac{c_0^2-4c_2^2}{c_0c_2} Z_4X_1X_2Z_1Z_2 - X_4(X_1^2X_2^2 + Z_1^2Z_2^2) \\ Z_3 = Z_4(X_1^2X_2^2 + Z_1^2Z_2^2) \end{cases}, \tag{27}$$

$$\begin{cases} X_5 = (c_2/c_0)Z_1^2 \cdot X_1^2 - 2\mu c_2(Z_1^2 + X_1^2)^2 \\ Z_5 = \mu c_0(Z_1^2 + X_1^2)^2 - 2Z_1^2X_1^2 \end{cases}. \tag{28}$$

The computation of $[X_3 : Z_3]$ and $[X_5 : Z_5]$ cost respectively $6M + 2S + 1m$ and $1M + 3S + 3m$ operations over fields $\mathbb{K}$ of odd characteristic. The cost of computation of differential addition can be reduced to $4M + 2S + 1m$ operations if $Z_4 = 1$. At same over fields of characteristic 2 formulas (25) and (26) become:

$$\begin{cases} X_3 = (c_0/c_2)Z_4X_1X_2Z_1Z_2 + X_4(X_1X_2 + Z_1Z_2)^2 \\ Z_3 = Z_4(X_1X_2 + Z_1Z_2)^2 \end{cases}, \tag{29}$$

$$\begin{cases} X_5 = (c_2/c_0)(Z_1 \cdot X_1)^2 \\ Z_5 = (Z_1 + X_1)^4 \end{cases}. \tag{30}$$

The formulas (29) and (30) cost respectively $6M + 1S + 1m$ and $1M + 3S + 1m$ operations over fields of even characteristic. If $Z_4 = 1$ formulas (29) can be reduced to $4M + 1S + 1m$ operations over binary fields. Formulas (29) correspond to Stam [21] formulas and formulas (30) correspond to Gaudry and Lubicz formulas [11].

5.3 Comparisons with previous work on differential addition

Recall that M, S and m denote respectively the cost of field multiplication, field squaring and multiplication by constant.

Over fields of odd characteristic, Brier and Joye [6] generalize the idea of Montgomerry [16] on general Weierstraß model $v^2 = u^3 + b_2u^2 + b_6$. The method of [6] use $6M + 2S + 2m$ per bits to compute exponentiation, i.e. multiply a point on Kummer line by a scalar. The best known formula, see table 2, for computing exponentiation uses $3M + 6S + 3m$ per bits and is due by Gaudry and Lubicz in [11] on Kummer model of Legendre form $v^2 = u(u - 1)(u - b)$. Our formula for computing exponentiation costs $4M + 3S + 4m$ on level 4-theta model and $5M + 5S + 2m$ on Edwards model. Over odd fields, we can assume that $S = M$ and then our formula use $7M + 4m$ which is beter than formula in [11] which use $9M + 3m$, moreover if we assume that $m = M$ then our method save one multiplication.

model	differential doubling	differential addition	Total
Montgomerry [16]	$2M + 2S + 1m$	$3M + 2S$	$5M + 4S + 1m$
Weierstraß	$4M + 3S + 2m$	$6M + 2S + 2m$	$10M + 5S + 4m$
Gaudry and Lubicz [11]	$4S + 2m$	$3M + 2S + 1m$	$3M + 6S + 3m$
Level 4-theta model	$1M + 3S + 3m$	$3M + 1m$	$\mathbf{4M + 3S + 4m}$
Our Edwards model	$1M + 3S + 1m$	$4M + 2S + 1m$	$5M + 5S + 2m$

Table 2: Comparisons of differential addition over non-binary fields

Over binary fields, the best known formula, see table 3, due by Gaudry and Lubicz [11] to compute exponentiation uses $5M + 5S + 1m$ on Kummer model of ordinary elliptic curve $v^2 + uv = u^3 + b_6$. Our formulas to compute exponentiation use $4M + 3S + 2m$ over level 4-theta model and $5M + 4S + 2m$ over Edwards model. Our formulas on level 4-theta are the best formulas to compute on Kummer line over binary fields.

model	differential doubling	differential addition	Total
Weierstraß of [21]	$1M + 3S + 1m$	$4M + 1S$	$5M + 4S + 1m$
Binary Edwards of [5]	$1M + 3S + 1m$	$4M + 1S + 1m$	$5M + 4S + 2m$
Huff of [8]	$1M + 3S + 1m$	$4M + 2S$	$5M + 5S + 1m$
Edwards model of [23]	$1M + 4S + 1m$	$4M + 2S$	$5M + 6S + 1m$
Gaudry and Lubicz [11]	$1M + 3S + 1m$	$4M + 2S$	$5M + 5S + 1m$
Level 4-theta model	$1M + 3S + 1m$	$3M + 1m$	$\mathbf{4M + 3S + 2m}$
Our Edwards model	$1M + 3S + 1m$	$4M + 1S + 1m$	$5M + 4S + 2m$

Table 3: Comparisons of differential addition over binary fields

6 Conclusion

We successfully introduced an Edwards model of elliptic curves defined over fields of all characteristic. We used a model of elliptic curve called level 4-theta model come from theta functions of level 4. We have shown that this theta model has a nice geometric interpretation of the group law which is complete and is the fastest in characteristic two among common curves as Weierstraß, Edwards, Huff and Hessian curves.

As futur work, one must compare pairings computation using theta function and Miller algorithm over any fields where only pairings using theta function over odd fields are published by [15]. It would also be interesting to look for supersingular Edwards model of supersingular elliptic curve.

7 Acknowledgements

The authors are grateful to David Lubicz and Marc Joye for their helpful comments.

References

[1] C. Arène, T. Lange, M. Naehrig, and C. Ritzenthaler. "Faster computation of the Tate pairing". In: *Journal of number theory* vol. 131(5), pp. 842-857 (2011). (Cit. on p. 12).

[2] D. Bernstein and T. Lange. "Explicit-formulae database". In: *http://www.hyperelliptic.org/EFD* (). (Cit. on p. 14).

[3] D. Bernstein and T. Lange. "Faster Addition and Doubling on Elliptic Curves". In: *Springer Berlin / Heidelberg. vol. 4833 of LNCS – pp. 29-50* (2008). (Cit. on p. 2).

[4] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and Peters C. "Twisted Edwards curves". In: *AFRICACRYPT 2008, Vol. 5023 of LNCS, Springer, pp. 389–405* (2008). (Cit. on p. 2).

[5] D.J. Bernstein, T. Lange, and R.R. Farashahi. "Binary Edwards curves". In: *CHES 2008, Vol. 5154 of LNCS, Springer, pp. 244-265* (2008). (Cit. on pp. 2, 14, 17).

[6] E. Brier and M. Joye. "Weierstraß elliptic curves and side-channel attacks". In: *Public Key Cryptography*. Ed. by D. Naccache and P. Paillier. Vol. 2274. LNCS. Springer-Verlag, 2002, pp. 335–345. (Cit. on p. 16).

[7] R. Carls. "Theta null points of 2-adic canonical lifts". In: *A preprint is available at http://arxiv.org/math.NT/0509092* (2005). (Cit. on p. 5).

[8] J. Devigne and M. Joye. "Binary Huff curves". In: *A. Kiayias, Ed., Topics in Cryptology – CT-RSA 2011, vol. 6558 of LNCS pp. 340-355, Springer* (2011). (Cit. on pp. 14, 17).

[9] 0. Diao. "Quelques aspects de l'arithmétique des courbes hyperelliptique de genre 2". PhD thesis. Université de Rennes 1 - France, 2010. (Cit. on pp. 2, 10–12).

[10] H. M. Edwards. "A normal form for elliptic curves". In: *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). (Cit. on pp. 1, 2, 9, 10, 12).

[11] P. Gaudry and D. Lubicz. "The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines". In: *Finite Fields and Their Applications* (2009). (Cit. on pp. 16, 17).

[12] T. Izu and T. Takagi. "Exceptional procedure attack on elliptic curve cryptosystems". In: (2002). (Cit. on p. 8).

[13] D. Kohel. "Addition law structure of elliptic curves". In: *Journal of Number Theory, 131 pp 894-919* (2011). (Cit. on p. 7).

[14] D. Kohel. "Normal forms and efficient arithmetic for elliptic curves in characteristic 2". In: *to be published* (2012). (Cit. on p. 7).

[15] D. Lubicz and D. Robert. "Efficient Pairing Computation With Theta Functions". In: *preprint available at http://perso.univ-rennes1.fr/david.lubicz/articles/pairing.pdf* (2010). (Cit. on pp. 4, 17).

[16] P.L. Montgomery. "Speeding up the Pollard and elliptic curve methods of factorization". In: *Mathematics of Computation 48(177) pp:243-264* (1987). (Cit. on pp. 16, 17).

[17] D. Mumford. "On the equations defining abelian varieties I". In: *Invent. Math., pp 1:287–354* (1966). (Cit. on p. 5).

[18] D. Mumford. *Tata lectures on theta I*. Birkhäuser Boston Inc., Boston, MA, 1983. (Cit. on p. 10).

[19] D. Mumford. *The red book of varieties and schemes*. Springer-verlag, 2004. (Cit. on p. 3).

[20] J. Silvermann. *The Arithmetic of Elliptic Curves*. Springer, 1986. (Cit. on p. 3).

[21] M. Stam. "On Montgomery-like representations for elliptic curves over $GF(2^k)$". In: *PKC 2003 pp. 240-254* (2002). (Cit. on pp. 16, 17).

[22] W. Stein. "Sage Mathematics Software (Version 4.8)". In: *The Sage Group* (2012). http://www.sagemath.org. (Cit. on pp. 12, 20).

[23] H. Wu, C. Tang, and R. Feng. "A New Model of Binary Elliptic Curves with Fast Arithmetic". In: *Cryptology ePrint Archive, Report 2010/608* (2010). http://eprint.iacr.org/. (Cit. on pp. 2, 14, 17).

A Addition laws formulas over level 4-theta function

The Riemann theta formulas give 16 relations that are classified according to j. Remind that $c_0 = a_0, c_2 = a_2/2 = \theta_2(0)/2$ and $a_3 = a_1 = 1$. Let $\mathbb{K}$ be field of characteristic $p \geq 0$ and let $c_0, c_2 \in \mathbb{K}^\star$ and let $E_{\lambda_1,\lambda_2} : X_0^2 + X_2^2 = \lambda_1 X_1 X_3, X_1^2 + X_3^2 = \lambda_2 X_0 X_2$ be the level 4-theta model defined over field $\mathbb{K}$. The arithmetic (addition and doubling) on E_{λ_1,λ_2} is given by following theta formula:

$$\theta_i(z_1+z_2)\theta_j(z_1-z_2) = \frac{a_k\mathcal{B}(i,j,k,l) - a_{k+2}\mathcal{B}(i,j,k+2,l)}{a_l}.$$

This formula give 4×4 formulas that give 4 equivalent group laws on E_{λ_1,λ_2}. The 4 group laws formulas are:

$$\begin{aligned}
\theta_i(z_1+z_2)\theta_0(z_1-z_2) &= \frac{a_0\mathcal{B}(i,0,0,i) - a_2\mathcal{B}(i,0,2,i)}{a_i},\\
\theta_i(z_1+z_2)\theta_1(z_1-z_2) &= \frac{a_0\mathcal{B}(i,1,0,i+1) - a_2\mathcal{B}(i,1,2,i+1)}{a_{i+1}},\\
\theta_i(z_1+z_2)\theta_2(z_1-z_2) &= \frac{a_0\mathcal{B}(i,2,0,i+2) - a_2\mathcal{B}(i,2,2,i+2)}{a_{i+2}},\\
\theta_i(z_1+z_2)\theta_3(z_1-z_2) &= \frac{a_0\mathcal{B}(i,3,0,i+3) - a_2\mathcal{B}(i,3,2,i+3)}{a_{i+3}}.
\end{aligned}$$

$$\text{①}\begin{cases}
\theta_0(z_1+z_2)\theta_0(z_1-z_2) = \dfrac{c_0\Big(\theta_0^2(z_1)\theta_0^2(z_2) + \theta_2^2(z_1)\theta_2^2(z_2)\Big) - 4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0},\\
\theta_1(z_1+z_2)\theta_0(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big)\\
\qquad\qquad -2c_2\Big(\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2) + \theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)\Big),\\
\theta_2(z_1+z_2)\theta_0(z_1-z_2) = \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_0(z_2)\theta_2(z_2) - c_2\Big(\theta_1^2(z_1)\theta_3^2(z_2) + \theta_3^2(z_1)\theta_1^2(z_2)\Big)}{c_2},\\
\theta_3(z_1+z_2)\theta_0(z_1-z_2) = c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big)\\
\qquad\qquad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2) + \theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big).
\end{cases}$$

$$
② \begin{cases}
\theta_0(z_1+z_2)\theta_1(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big), \\
\theta_1(z_1+z_2)\theta_1(z_1-z_2) &= \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2)-c_2\Big(\theta_3^2(z_1)\theta_0^2(z_2)+\theta_2^2(z_1)\theta_1^2(z_2)\Big)}{c_2}, \\
\theta_2(z_1+z_2)\theta_1(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_1(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_2(z_2)\theta_3(z_2)\Big), \\
\theta_3(z_1+z_2)\theta_1(z_1-z_2) &= \dfrac{c_0\Big(\theta_0^2(z_1)\theta_3^2(z_2)+\theta_2^2(z_1)\theta_1^2(z_2)\Big)-4c_2\theta_1(z_1)\theta_3(z_1)\theta_0(z_2)\theta_2(z_2)}{c_0}.
\end{cases}
$$

$$
③ \begin{cases}
\theta_0(z_1+z_2)\theta_2(z_1-z_2) &= \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2)-c_2\Big(\theta_1^2(z_1)\theta_1^2(z_2)+\theta_3^2(z_1)\theta_3^2(z_2)\Big)}{c_2}, \\
\theta_1(z_1+z_2)\theta_2(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_3(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_2)\theta_0(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_1(z_2)\theta_2(z_2)\Big), \\
\theta_2(z_1+z_2)\theta_2(z_1-z_2) &= \dfrac{c_0\Big(\theta_0^2(z_1)\theta_2^2(z_2)+\theta_2^2(z_1)\theta_0^2(z_2)\Big)-4c_2\theta_1(z_1)\theta_3(z_1)\theta_1(z_2)\theta_3(z_2)}{c_0}, \\
\theta_3(z_1+z_2)\theta_2(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)\Big).
\end{cases}
$$

$$
④ \begin{cases}
\theta_0(z_1+z_2)\theta_3(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_3(z_1)\theta_0(z_2)\theta_1(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_2(z_2)\theta_3(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_3(z_1)\theta_2(z_2)\theta_3(z_2)+\theta_1(z_1)\theta_2(z_1)\theta_0(z_2)\theta_1(z_2)\Big), \\
\theta_1(z_1+z_2)\theta_3(z_1-z_2) &= \dfrac{c_0\Big(\theta_0^2(z_1)\theta_1^2(z_2)+\theta_2^2(z_1)\theta_3^2(z_2)\Big)-4c_2\theta_1(z_1)\theta_3(z_1)\theta_0(z_2)\theta_2(z_2)}{c_0}, \\
\theta_2(z_1+z_2)\theta_3(z_1-z_2) &= c_0\Big(\theta_0(z_1)\theta_1(z_1)\theta_1(z_1)\theta_2(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_0(z_2)\theta_3(z_2)\Big) \\
&\quad -2c_2\Big(\theta_0(z_1)\theta_1(z_1)\theta_0(z_2)\theta_3(z_2)+\theta_2(z_1)\theta_3(z_1)\theta_1(z_2)\theta_2(z_2)\Big), \\
\theta_3(z_1+z_2)\theta_3(z_1-z_2) &= \dfrac{c_0\theta_0(z_1)\theta_2(z_1)\theta_1(z_2)\theta_3(z_2)-c_2\Big(\theta_1^2(z_1)\theta_0^2(z_2)+\theta_3^2(z_1)\theta_2^2(z_2)\Big)}{c_2}.
\end{cases}
$$

B Sage verification

This sage script [22] verify that addition formulas (8) are valid.

```
R.<c0,c2,X0,X1,X2,X3,Y0,Y1,Y2,Y3> = QQ[]
lbd1 = c0^2 + 4*c2^2; lbd2 = 1/(c0*c2)
LB = numerator(lbd1 - lbd2)

E1 = numerator(X0^2 + X2^2 - lbd1*X1*X3); E2 = numerator(X1^2 + X3^2 - lbd2*X0*X2)
F1 = numerator(Y0^2 + Y2^2 - lbd1*Y1*Y3); F2 = numerator(Y1^2 + Y3^2 - lbd2*Y0*Y2)

S = R.quo([E1,E2,F1,F2,LB])

Z0 = (X0^2*Y0^2 + X2^2*Y2^2) - 4*(c2/c0)*X1*X3*Y1*Y3
Z1 = c0*(X0*X1*Y0*Y1 + X2*X3*Y2*Y3) - 2*c2*(X2*X3*Y0*Y1 + X0*X1*Y2*Y3)
Z2 = (X1^2*Y1^2 + X3^2*Y3^2) - 4*(c2/c0)*X0*Y0*X2*Y2
Z3 = c0*(X0*X3*Y0*Y3 + X1*X2*Y1*Y2) - 2*c2*(X0*X3*Y1*Y2 + X1*X2*Y0*Y3)

G1 = Z0^2 + Z2^2 - lbd1*Z1*Z3; G2 = Z1^2 + Z3^2 - lbd2*Z0*Z2
S(numerator(G1)) == 0; S(numerator(G2)) == 0
```