New Model of Binary Elliptic Curve

Demba Sow¹ & Djiby Sow¹

¹ Ecole Doctorale de Mathématiques et Informatique, Laboratoire d'Algèbre de Cryptologie de Géométrie Algèbrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal

Correspondence: Demba Sow, Ecole Doctorale de Mathématiques et Informatique, Laboratoire d'Algèbre de Cryptologie de Géométrie Algèbrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal. E-mail: sowdembis@yahoo.fr

Received: August 15, 2012 Accepted: September 13, 2012 Online Published: November 21, 2012 doi:10.5539/jmr.v4n6p34 URL: http://dx.doi.org/10.5539/jmr.v4n6p34

Abstract

In our paper paper we propose a new binary elliptic curve of the form $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$. If $m \ge 5$ we prove that each ordinary elliptic curve $y^2 + xy = x^3 + \alpha x^2 + \beta, \beta \ne 0$ over \mathbb{F}_{2^m} , is birationally equivalent over \mathbb{F}_{2^m} to our curve. This paper also presents the formulas for the group law.

Keywords: elliptic curves, binary Edwards curves, binary fields, binary Huff curves

1. Introduction

Recently, many papers are written about binary elliptic curves such as Binary Edwards curves (Bernstein, Lange, & Farashahi, 2008) and Binary Huff curves (Devigne & Joye, 2011). In this paper, we introduce a new binary elliptic curve.

Let *E* be a projective curve of dimension one, defined over a field \mathbb{K} . *E* is an elliptic curve if *E* is nonsingular (smooth), irreducible over $\overline{\mathbb{K}}$ (algebraic closure), with genus 1 and has at least one rational point (over \mathbb{K}).

The affine version of elliptic curve in Weierstrass form is:

$$E: y^{2} + a_{1}xy + a_{3}y = x^{3} + a_{2}x^{2} + a_{4}x + a_{6}x^{3}$$

where the coefficients a_1, a_2, a_3, a_4 and a_6 are in K; with a special element denoted by \overline{O} and called the point at infinity.

An binary non supersingular elliptic curve *E* has the classical Weierstrass equation:

$$y^2 + xy = x^3 + \alpha x^2 + \beta \qquad (\beta \neq 0).$$

The group law of a binary elliptic curve is given by the following. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be elements in *E* then we have the following:

• the neutral element is \overline{O} and the opposite of *P*, is $-P = (x_1, x_1 + y_1)$;

• if
$$Q \neq -P$$
 then $P + Q = (x_3, y_3)$:

$$- \text{ if } P \neq Q \text{ then } x_3 = \lambda^2 + \lambda + x_1 + x_2 + a \text{ and } y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \text{ with } \lambda = \frac{y_1 + y_2}{x_1 + x_2};$$

- if
$$P = Q$$
 then $x_3 = \lambda^2 + \lambda + a$ and $y_3 = x_1^2 + \lambda x_3 + x_3$ with $\lambda = x_1 + \frac{y_1}{x_1}$.

In section 2 we introduce a new binary curve and prove that it is a projective variety.

In section 3 we study the universality of the model and explain how to do the addition via a birationale equivalence.

2. A New Binary Curve

In the following, we introduce a new curve and study its properties.

Definition 2.1 (New binary curve) Suppose that k is a field such that it's characteristic is 2. Let a, b be elements of k with $ab(a + b) \neq 0$. The new binary curve with coefficients a and b is the affine curve

$$E_{a,b}: a[x^2 + y^2 + xy + 1] + (a+b)[x^2y + y^2x] = 0.$$

2.1 Varieties

Proposition 2.2 The curve $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ with $ab(a + b) \neq 0$ define over \mathbb{F}_{2^m} is absolutely irreducible in \mathbb{F}_{2^m} .

Proof. Put $H(x, y) = [a + (a+b)x]y^2 + [ax + (a+b)x^2]y + a(x^2 + 1)$ in \mathbb{F}_{2^m} . Suppose that H is reducible *i.e.* there exist four non zero functions f, f', g and g' such that $H(x, y) = [f(x) + g(x)y][f'(x) + g'(x)y] = f(x)f'(x) + (f(x)g'(x) + g(x)f'(x))y + g(x)g'(x)y^2$, by identification:

$$\begin{cases} f(x)f'(x) = a(x^2 + 1), & (1); \\ g(x)g'(x) = (a + b)x + a, & (2); \\ f(x)g'(x) + g(x)f'(x) = ax + (a + b)x^2, & (3). \end{cases}$$

• <u>1st case</u>: f = cste then $(1) \Longrightarrow f' = \frac{a(x^2 + 1)}{f}$, $(3) \Longrightarrow g = cste$ and $(2) \Longrightarrow g' = \frac{a + (a + b)x}{g}$. In (3) we have $fg' + gf' = a\frac{g}{f}x^2 + (a + b)\frac{f}{g}x + a(\frac{f}{g} + \frac{g}{f})$; by identification

$$\begin{cases} a+b = a\frac{g}{f}, & (1'); \\ a = (a+b)\frac{f}{g}, & (2'); & \text{iff.} \end{cases} \begin{cases} \frac{g}{f} = \frac{a+b}{a}, & (1''); \\ \frac{f}{g} = \frac{a}{a+b}, & (2''); \\ a(\frac{f}{g} + \frac{g}{f}) = 0, & (3'). \end{cases}$$

(3") iff. $\frac{b^2}{a+b} = 0$ iff. b = 0 impossible because $b \neq 0$.

• 2^{nd} case: f' = cste then (1) iff. $f = \frac{a(x^2 + 1)}{f'}$, (3) iff. g' = cste and (2) iff. $g = \frac{a + (a + b)x}{g'}$. In (3) we have $fg' + gf' = a\frac{g'}{f'}x^2 + (a + b)\frac{f'}{g'}x + a(\frac{f'}{g'} + \frac{g'}{f'})$; by identification

$$\begin{cases} a+b=a\frac{g'}{f'}, & (1'); \\ a=(a+b)\frac{f'}{g'}, & (2'); & \text{iff.} \end{cases} \begin{cases} \frac{g'}{f'}=\frac{a+b}{a}, & (1''); \\ \frac{f'}{g'}=\frac{a}{a+b}, & (2''); \\ a(\frac{f'}{g'}+\frac{g'}{f'})=0, & (3'). \end{cases}$$

(3") iff. $\frac{b^2}{a+b} = 0$ iff. b = 0 impossible because $b \neq 0$.

• $\frac{3^{rd} \operatorname{case:}}{g} \deg f = \deg f' = 1$ then there exists a_1 , and a_2 such that $f(x) = a_1(x+1)$ and $f'(x) = a_2(x+1)$. Equation (2) implies that g = cste or g' = cste. Suppose g = cste then $g' = \frac{a + (a+b)x}{g}$. Equation (3) implies that $fg' + gf' = a_1(x+1)\frac{[(a+b)x+a]}{g} + ga_2(x+1) = x[(a+b)x+a]$ if x = 1 then (a+b) + a = 0 impossible. 2.2 Smooth Varieties

Theorem 1.3 (Nonsingularity) Each binary curve define over \mathbb{F}_{2^m} by $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ is nonsingular.

Proof. It exists smooth variety if the following system assume solution:

$$H(x,y) = y^{2}[a + (a + b)x] + y[ax + (a + b)x^{2}] + a(x^{2} + 1) = 0, \quad (1)$$

$$\begin{cases} \frac{\partial H}{\partial x} = (a+b)y^2 + ay = 0, \tag{2}$$

$$\frac{\partial H}{\partial y} = (a+b)x^2 + ax = 0, \tag{3}$$

Equation (2) implies that y = 0 or $y = \frac{a}{a+b}$ and equation (3) implies that x = 0 or $x = \frac{a}{a+b}$.

If $x = \frac{a}{a+b}$, in (1) we have $a(\frac{a^2}{a^2+b^2}+1) = 0 \iff ab^2 = 0 \iff a = 0$ or b = 0, impossible because $ab \neq 0$. Thus *H* is nonsingular.

2.3 Projective Form

2.3.1 Homogenus Equation

If we put $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we obtain the projective form of the curve $E_{a,b}$. Thus we have the following homogenus equation:

$$a[X^{2}Z + Y^{2}Z + XYZ + Z^{3}] + (a+b)[X^{2}Y + Y^{2}X] = 0.$$

2.3.2 Infinites Points

Z = 0 implies that $(a + b)[X^2Y + Y^2X] = 0$ iff. X = 0 or Y = 0 or X = Y.

- X = 0, $\langle X : Y : 0 \rangle = \langle 0 : Y : 0 \rangle = \langle 0 : 1 : 0 \rangle$;
- Y = 0, $\langle X : Y : 0 \rangle = \langle X : 0 : 0 \rangle = \langle 1 : 0 : 0 \rangle$;
- $X = Y, \langle X : Y : 0 \rangle = \langle X : X : 0 \rangle = \langle 1 : 1 : 0 \rangle.$

We have three points at infinity.

2.3.3 Singularity of Infinites Points

• $\langle 1 : 0 : 0 \rangle$, X = 1 we have the following equation $T(Z, Y) = a[Z + Y^2Z + YZ + Z^3] + (a + b)[Y + Y^2]$. $\frac{\partial T}{\partial Y} = aZ + a + b$, $\frac{\partial T}{\partial Y}(0, 0) = a + b \neq 0$ thus the point $\langle 1 : 0 : 0 \rangle$ is a nonsingular infinite point.

• $\langle 0: 1: 0 \rangle$, Y = 1 we have the following equation $T(X, Z) = a[X^2Z + Z + XZ + Z^3] + (a + b)[X^2 + X]$. $\frac{\partial T}{\partial X} = aZ + a + b$, $\frac{\partial T}{\partial X}(0, 0) = a + b \neq 0$ thus the point $\langle 0: 1: 0 \rangle$ is a nonsingular infinite point.

• $\langle 1:1:0\rangle, X = Y = 1$ we have the following equation $T(Z) = a[Z + Z + Z + Z^3] = aZ[1 + Z^2], \frac{\partial T}{\partial Z} = a[1 + Z^2], \frac{\partial T}{\partial Z}(0,0) = a \neq 0$ thus the point $\langle 1:1:0\rangle$ is a nonsingular infinite point.

2.4 Birational Equivalence

Theorem 2.4 Suppose that k is a field such that it's characteristic is 2 and a, $b \in k$. Each curve with affine equation $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ with $ab(a + b) \neq 0$ is equivalent in a birationally way to the curve $v^2 + v\left[\frac{1+au}{a+b}\right] = u\left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2}u^2\right]$ via the map $\varphi : (x, y) \mapsto (u, v)$, with

$$u = \frac{1}{a + (a + b)x} \iff \begin{cases} x = \frac{1 + au}{(a + b)x} \\ y = \frac{y}{a + (a + b)x} \end{cases} \qquad \longleftrightarrow \qquad \begin{cases} y = \frac{v}{u} \end{cases}$$

Proof.

a) Assume that
$$v^2 + v \left[\frac{1+au}{a+b} \right] = u \left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2} u^2 \right]$$
 and prove that $a[x^2+y^2+xy+1] + (a+b)[x^2y+y^2x] = 0$
Let $H(x,y) = a[x^2+y^2+y^2+xy+1] + (a+b)[x^2y+y^2x]$. We obtain

$$H(x,y) = a \left[\frac{1+a^2u^2}{(a^2+b^2)u^2} + \frac{v^2}{u^2} + \frac{v(1+au)}{(a+b)u^2} + 1 \right] + (a+b) \left[\frac{v(1+a^2u^2)}{(a^2+b^2)u^3} + \frac{v^2(1+au)}{(a+b)u^3} \right]$$

= $a \left[(1+a^2u^2)u + uv^2(a^2+b^2) + uv(a+b)(1+au) + u^3(a^2+b^2) \right] + (a+b)[v(1+a^2u^2) + v^2(a+b)(1+au)]$
= $\frac{u(a+a^3u^2)}{a^2+b^2} + auv^2 + auv\frac{1+au}{a+b} + au^3 + v\frac{1+a^2u^2}{a+b} + v^2(1+au)$
= $v^2 + v \left[\frac{1+au}{a+b} \right] + u \left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2} \right]$
= 0

b) Suppose that
$$a[x^2+y^2+xy+1]+(a+b)[x^2y+y^2x] = 0$$
 and prove that $v^2+v\left[\frac{1+au}{a+b}\right] = u\left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2}u^2\right]$
Let $G(u,v) = v^2 + v\left[\frac{1+au}{a+b}\right] + u\left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2}u^2\right]$. We have the following
 $G(u,v) = \frac{y^2}{[a+(a+b)x]^2} + \frac{y}{a+(a+b)x}\left[\frac{1+\frac{a}{a+(a+b)x}}{a+b}\right] + \frac{1}{a+(a+b)x}\left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2} \times \frac{1}{(a+(a+b)x)^2}u^2\right]$
 $= y^2(a+(a+b)x) + y(a+(a+b)x) \times \left[\frac{a+(a+b)x+a}{a+b}\right] + \left[\frac{a(a^2+(a^2+b^2)x^2)}{a^2+b^2} + \frac{ab^2}{a^2+b^2}\right]$
 $= ay^2 + (a+b)xy^2 + axy + (a+b)x^2y + a + ax^2$
 $= a[x^2+y^2+xy+1] + (a+b)[x^2y+xy^2]$
 $= 0$

Corollary 2.5 (Projective version) Suppose that k is a field such that it's characteristic is 2 and a, $b \in k$. Each curve with projective equation $a[X^2Z + Y^2Z + XYZ + Z^3] + (a+b)[X^2Y + Y^2X] = 0$ with $ab(a+b) \neq 0$ is equivalent in a birationally way to the curve $V^2W + VW\left[\frac{W+aU}{a+b}\right] = U\left[\frac{aW^2}{a^2+b^2} + \frac{ab^2}{a^2+b^2}U^2\right]$, by

$$\left(\begin{array}{c} U = \frac{Z}{a+b} \\ V = \frac{Y}{a+b} \\ W = X + \frac{aZ}{a+b} \end{array}\right) \longleftrightarrow \left\{\begin{array}{c} X = aU + W \\ Y = (a+b)V \\ Z = (a+b)U \end{array}\right.$$

Proof. similarly to the above.

3. Universality of the Model and Addition Law

First of all let us recall the properties of trace function.

Let $\mathbb{F}_q = \mathbb{F}_{p^n}$ be a field of $q = p^n$ elements. The trace function denoted **Trace** is defined as follows: **Trace**(α) = $\alpha + \alpha^p + \dots \alpha^{pn-1}$ for $\alpha \in \mathbb{F}_q$.

Proprieties: 1 Let $\alpha, \beta \in \mathbb{F}_q$

- 1) **Trace**(α) $\in \mathbb{Z}/p\mathbb{Z}$;
- 2) **Trace**(α^p) = α ;
- 3) There exists $\gamma \in \mathbb{F}_{p^n}$, with **Trace**(γ) \neq 0;
- 4) if $a \in \mathbb{Z}/p\mathbb{Z}$, then **Trace**(a) = na;
- 5) if $a \in \mathbb{Z}/p\mathbb{Z}$, then **Trace** $(a\alpha) = a$ **Trace** (α) ;
- 6) **Trace**($\alpha + \beta$) = **Trace**(α) + **Trace**(β)
- 7) The polynomial $x^p x \alpha \in \mathbb{F}_q[x]$ is
 - (a) either irreducible;
 - (b) or a product of factors of degree 1.

8) The polynomial $x^p - x - \alpha \in \mathbb{F}_q[x]$ is product of factors of degree 1 if and only if **Trace**(α) = 0.

Corollary: Trace function for binary fields Let $\alpha, \beta \in \mathbb{F}_{2^n}$

1) **Trace**(α^2) = α ;

2) The equation $x^2 + ux + v = 0$ with $u, v \in \mathbb{F}_{2^n}[x]$, $u \neq 0$ has a solution if and only if $\operatorname{Trace}(\frac{v}{u^2}) = 0$. Furthermore, for a solution x_0 the other is $x_0 + u$.

Cardinality for elliptic curve

The cardinality of an elliptic curve E over \mathbb{F}_q is the number of \mathbb{F}_q -rational points. The theorem of HasseWeil relates the number of points to the field size.

Theorem: (Hasse-Weil) Let *E* be an elliptic curve defined over \mathbb{F}_{a} . Then

$$|E(\mathbb{F}_q)| = q + 1 - t \text{ and } |t| \le 2\sqrt{q}$$

3.1 Universality

When introducing a new form or elliptic curve, it is important to study how many "good" curve are isomorph to the new model.

Theorem 3.1 Over \mathbb{F}_{2^l} with $l \ge 5$, the curves $y^2 = x^3 + \alpha x^2 + xy + \beta$, $\beta \ne 0$ and $a[x^2 + y^2 + xy + 1] + (a+b)[x^2y + y^2x] = 0$ are birationally equivalent.

Proof.

• $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ is equivalent in a birationally way over \mathbb{F}_{2^l} to an elliptic curve in the form

$$v^{2} + v \left[\frac{1+au}{a+b} \right] = u \left[\frac{a}{a^{2}+b^{2}} + \frac{ab^{2}}{a^{2}+b^{2}}u^{2} \right]$$

via the map $\varphi_1 : (x, y) \mapsto (u, v)$, with

$$\begin{cases} u = \frac{1}{a + (a + b)x} \\ v = \frac{y}{a + (a + b)x} \end{cases} \iff \begin{cases} x = \frac{1 + au}{(a + b)u} \\ y = \frac{v}{u}. \end{cases}$$

• We have also $v^2 + v \left[\frac{1 + au}{a + b} \right] = u \left[\frac{a}{a^2 + b^2} + \frac{ab^2}{a^2 + b^2} u^2 \right]$ is equivalent in a birationally way to $v'^2 + a_1 u' v' = a_1 u' v' = a_1 u' v'$ $u'^3 + a_2u'^2 + a_4u' + a_6$ with $a_1 = \frac{a}{c(a+b)}$, $a_2 = \frac{1}{a}$, $a_4 = \frac{1}{a^2} + \frac{1}{b^2}$ and $a_6 = \frac{1}{c^2(a^2+b^2)} + \frac{1}{a^3}$ and $c^2 = \frac{ab^2}{a^2+b^2}$, via

the map $\varphi_2 : (u, v) \longmapsto (u', v')$, with

$$\begin{cases} u' = \frac{1}{a} + u \\ v' = \frac{v}{c} \end{cases} \longleftrightarrow \begin{cases} u = \frac{1}{a} + u' \\ v = cv'. \end{cases}$$

• Define change of variables, put $\begin{cases} u = \frac{1}{a} + u' \\ v = cv' \end{cases} \iff \begin{cases} u' = \frac{1}{a} + u \\ u' = \frac{1}{a} + u \\ v' = \frac{v}{c} \end{cases}$ and $c^2 = \frac{ab^2}{a^2 + b^2}$. We have $v'^2 + a_1u'v' = v''$ $u'^3 + a_2u'^2 + a_4u' + a_6$ with $a_1 = \frac{a}{c(a+b)}$, $a_2 = \frac{1}{a}$, $a_4 = \frac{1}{a^2} + \frac{1}{b^2}$ and $a_6 = \frac{1}{c^2(a^2+b^2)} + \frac{1}{a^3}$.

Define another the change of variables $\begin{cases} u' = a_1^2 T \\ v' = a_1^3 (Z + sT + \lambda) \end{cases}$ then we have

$$\begin{aligned} a_1^6(Z^2 + s^2T^2 + \lambda^2) + a_1^6t(Z + sT + \lambda) &= a_1^6T^3 + a_1^4a_2T^2 + a_1^2a_4T + a_6Z^2 + Tz \\ &= T^3 + T^2 \left[s^2 + s + \frac{a_2}{a_1^2} \right] + T \left[\lambda + \frac{a_4}{a_1^4} \right] + \lambda^2 + \frac{a_6}{a_1^6}. \end{aligned}$$

By identification: $\begin{cases} s^2 + s + \frac{a_2}{a_1^2} = a'_2 \\ \lambda + \frac{a_4}{a_1^4} = 0 \\ \lambda^2 + \frac{a_6}{a_1^6} = a'_6 \Rightarrow a'_6 = \frac{a_4^2}{a_1^8} + \frac{a_6}{a_1^6} = \frac{a_4^2 + a_1^2 a_6}{a_1^8}. \end{cases}$

Define
$$h^{-2} = \frac{a_2}{a_1^2} \Longrightarrow h = \frac{a_1}{\sqrt{a_2}}$$
. Thus we have $s^2 + s + a'_2 + h^{-2} = 0$, $h^{-2} = \frac{a_2}{a_1^2} = \frac{c^2(a^2 + b^2)}{a^3}$, $a'_6 = \left(\frac{a_4 + a_1\sqrt{a_6}}{a_1^4}\right) = \left(1 + \frac{c^2(a^2 + b^2)}{a^3} + \sqrt{1 + \frac{c^2(a^2 + b^2)}{a^3}}\right) \frac{c^2(a^2 + b^2)}{a^3} = \left(1 + h^{-2} + \sqrt{1 + h^{-2}}\right)h^{-2} \Longrightarrow h^2\sqrt{a'_6} = h^{-2} + h^{-1} \Longleftrightarrow h^{-2} + h^{-1} + h^2\sqrt{a'_6} = 0.$
Put $t = h^{-1}$ thus $t^2 + t + h^2\sqrt{a'_6} = 0$.

 $\operatorname{Thus} \begin{cases} s^{2} + s + a'_{2} + h^{-2} = 0 \\ t^{2} + t + h^{2}\sqrt{a'_{6}} = 0 \end{cases} \longleftrightarrow \begin{cases} \operatorname{Trace}(a'_{2} + h^{-2}) = 0 \\ \operatorname{Trace}(h^{2}\sqrt{a'_{6}}) = 0 \end{cases} \longleftrightarrow \begin{cases} \operatorname{Trace}(h^{-1}) = Tr(a'_{2}) \\ \operatorname{Trace}(h\sqrt[4]{a'_{6}}) = 0. \end{cases}$

For each λ , $\pi \in \mathbb{F}_2$, define

$$L_{\lambda,\pi} = \{h \in \mathbb{F}_{2^{\prime}}^* : \operatorname{Trace}(h^{-1}) = \lambda, \operatorname{Trace}(h\sqrt[4]{a_6^{\prime}}) = \pi\}$$

We define by |L| the cardinality of the set L and |E| the cardinality of E. Since $t^4 \sqrt{a'_6} + t + 1 = 0$ has at most 4 roots, we must prove that $L_{\text{Trace}(a'_6),0}$ has at least 5 elements *i.e* $|L|_{\text{Trace}(a'_6),0} \ge 5$ if $l \ge 5$.

Namely let at prove that $|L|_{0,0} \ge 5$ and $|L|_{1,0} \ge 5$ if $l \ge 4$.

We have $|L|_{0,0} + |L|_{1,0} = 2^{l-1} - 1$. Therefore, since *h* can take all values in $\mathbb{F}_{2^{l}}^{*}$, then $h\sqrt[4]{a'_{6}}$ also take all values in $\mathbb{F}_{2^{l}}^{*}$. We deduce that $|L|_{0,0} + |L|_{1,0}$ count the elements $h \in \mathbb{F}_{2^{l}}^{*}$ with **Trace**(*h*) = 0. Now, we have $|L|_{1,0} + |L|_{1,1} = 2^{l-1}$. Therefore, similarly as above $|L|_{1,0} + |L|_{1,1}$ count the elements $h \in \mathbb{F}_{2^{l}}^{*}$ with **Trace**(*h*) = 1. We have $|L|_{0,0} + |L|_{1,0} = \frac{2^{l}}{2} - 1 = 2^{l-1} - 1$, $|L|_{1,0} + |L|_{1,1} = \frac{2^{l}}{2} = 2^{l-1}$.

Let us compute $|L|_{0,0} + |L|_{1,1}$. We have the following:

 $h \in L_{0,0} \cup L_{1,1} \iff \begin{cases} \mathbf{Trace}(h^{-1}) = 0 = \mathbf{Trace}(h\sqrt[4]{a_6'}) \\ \mathbf{Trace}(h^{-1}) = 1 = \mathbf{Trace}(h\sqrt[4]{a_6'}) \end{cases} \iff \mathbf{Trace}(h^{-1}) = \mathbf{Trace}(h\sqrt[4]{a_6'}) \iff \mathbf{Trace}(h^{-1} + h\sqrt[4]{a_6'}) \end{cases} \implies \mathbf{Trace}(h^{-1}) = 0 \text{ iff we have two possibilities for } x, \text{ namely } (x \text{ and } x + 1) \text{ such that } x^2 + x + h^{-1} + h\sqrt[4]{a_6'} = 0 \iff h^2 x^2 + h^2 x + h + h^3\sqrt[4]{a_6'} = 0 \iff (hx)^2 + h(hx) = h^3\sqrt[4]{a_6'} + h \iff v^2 + uv = u^3\sqrt[4]{a_6'} + u \text{ with } v = hx \text{ and } u = h. \end{cases}$

Hasse's theorem implies that it exists $\delta = |E(\mathbb{F}_{2^l}^*)| - 2^l - 1 \in [-2\sqrt{2^l}, 2\sqrt{2^l}]$, the point (0,0) and the infinite point do not verify the above equation and two points on the curve produce one *h*.

Thus
$$|L|_{0,0} + |L|_{1,1} = (|E(\mathbb{F}_{2^{l}}^{*})| - 2)/2 = (\delta + 2^{l} + 1 - 2)/2, |L|_{0,0} + |L|_{1,1} = 2^{l-1} + \frac{\delta - 1}{2}, 4|L|_{1,0} = 2(|L|_{0,0} + |L|_{1,0}) + 2(|L|_{1,0} + |L|_{1,1}) - 2(|L|_{0,0} + |L|_{1,1}) = 2(2^{l-1} - 1) + 2(2^{l-1}) - 2(2^{l-1} - \frac{\delta - 1}{2}) = 2^{l} - (\delta + 1), 4|L|_{0,0} = 4(2^{l-1} - 1) - 4|L|_{1,0} = 4(2^{l-1} - 1) - 4|L|_{1,0} = 4(2^{l-1} - 1) - (2^{l} - (\delta - 1)) = 22^{l} - 4 - 2^{l} + \delta + 1 = 2^{l} + \delta - 3, \text{ since } \delta \in [-2\sqrt{2^{l}}, 2\sqrt{2^{l}}] \Longrightarrow \delta \ge -2\sqrt{2^{l}}, \text{ then } 4|L|_{0,0} = 2^{l} + \delta - 3 \Longrightarrow 4|L|_{0,0} \ge 2^{l} + -2\sqrt{2^{l}} - 3 \Longrightarrow |L|_{0,0} \ge \frac{2^{l} - 2\sqrt{2^{l}} - 3}{4} \text{ and } 4|L|_{1,0} \ge 2^{l} + -2\sqrt{2^{l}} - 1 \Longrightarrow |L|_{1,0} \ge \frac{2^{l} - 2\sqrt{2^{l}} - 1}{4} \ge \frac{2^{l} - 2\sqrt{2^{l}} - 3}{4} = \frac{(\sqrt{2^{l}} - 1)^{2} - 4}{4} \ge \frac{(\sqrt{2^{5}} - 1)^{2} - 4}{4} = 11.25 \ge 5.$$

As final remark, in order to transform the curve $z^2 + zt = t^3 + a'_2 t + a'_6$ to $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$, we must find *h* with **Trace** $(h^{-1}) =$ **Trace** (a'_2) and **Trace** $(h\sqrt[4]{a'_6}) = 0$, $h^{-2} = \frac{c(a^2 + b^2)}{a^3} = \frac{b^2}{a^2}$, $\frac{b}{a} = h^{-1} = t_0$ where $t_0^2 + t_0 + h^2\sqrt{a'_6} = 0$, $t_0^2 = \frac{b^2}{a^2}$, fix *b* and compute $a = \sqrt{\frac{b}{t_0}}$ and fix *a* and compute $b = \sqrt{at_0}$.

Theorem 3.2 Suppose that k is a field such that it's characteristic is 2 and a, $b \in k$. Each curve with affine equation $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ with $ab(a + b) \neq 0$ is equivalent in a birationally way to the curve $z^2 + tz = t^3 + a'_2t^2 + a'_6$ with $a'_2 = \frac{b^2}{a^2}$ and $a'_6 = \frac{a^4 + b^4}{a^8}b^4 + \frac{a^2 + b^2}{a^6}b^4$ via the map $\psi : (x, y) \mapsto (t, z)$ with

$$\begin{cases} t = \frac{b^2}{a^2} \left[\frac{(a+b)x}{a+(a+b)x} \right] \\ z = \frac{b^2}{a^2} \left[\frac{(a+b)y + \frac{a^2 + b^2}{a^2} [a+(a+b)x]}{a+(a+b)x} \right] \iff \begin{cases} x = \frac{a^3}{a+b}t \\ b^2 + a^2t \\ y = \frac{a^3}{a+b}z + \frac{a+b}{a}b^2 \\ b^2 + a^2t \end{cases}.$$

Proof.

a) Suppose that $z^2 + tz = t^3 + a'_2t^2 + a'_6$ and prove that $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$. Let $H(x, y) = a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x]$, we have the following:

$$\begin{split} H(x,y) &= a \left[\frac{\frac{a^{6}}{a^{2} + b^{2}}t^{2}}{(b^{2} + a^{2}t)^{2}} + \frac{\frac{a^{6}}{a^{2} + b^{2}}z^{2} + \frac{a^{2} + b^{2}}{a^{2}}b^{4}}{(b^{2} + a^{2}t)^{2}} + \frac{\frac{a^{3}}{a + b}t\left[\frac{a^{3}}{a + b}z + \frac{a + b}{a}b^{2}\right]}{(b^{2} + a^{2}t)^{2}} + 1 \right] \\ &+ (a + b) \left[\frac{\frac{a^{6}}{a^{2} + b^{2}}t^{2}\left[\frac{a^{3}}{a + b}z + \frac{a + b}{a}b^{2}\right]}{(b^{2} + a^{2}t)^{3}} + \frac{\frac{a^{3}}{a + b}t\left[\frac{a^{6}}{a^{2} + b^{2}}z^{2} + \frac{a^{2} + b^{2}}{a^{2}}b^{4}\right]}{(b^{2} + a^{2}t)^{3}} \right] \\ &= a[t^{2}(b^{2} + a^{2}t) + z^{2}(b^{2} + a^{2}t) + \frac{a^{4} + b^{4}}{a^{8}}b^{4}(b^{2} + a^{2}t) + zt(b^{2} + a^{2}t) + \frac{a^{2} + b^{2}}{a^{4}}b^{2}t(b^{2} + a^{2}t) \\ &+ \frac{a^{2} + b^{2}}{a^{6}}(b^{2} + a^{2}t)^{3}] + (a + b)\left[t^{2}(\frac{a^{3}}{a + b}z + \frac{a + b}{a}b^{2}) + \frac{a^{3}}{a + b}z^{2}t + \frac{b^{4}(a + b)(a^{2} + b^{2})}{a^{5}}t\right] \\ &= z^{2}[ab^{2}] + zt[ab^{2}] + t^{3}[ab^{2}] + t^{2}\left[ab^{2} + \frac{a^{2} + b^{2}}{a}b^{2}\right] + \frac{a^{4} + b^{4}}{a^{7}}b^{6} + \frac{a^{2} + b^{2}}{a^{5}}b^{6} \\ &= z^{2} + zt + t^{3} + \frac{b^{2}}{a^{2}}t^{2} + \frac{a^{4} + b^{4}}{a^{8}}b^{4} + \frac{a^{2} + b^{2}}{a^{6}}b^{4} \\ &= z^{2} + zt + t^{3} + a'_{2}t^{2} + a'_{6} \\ &= 0. \end{split}$$

b) Suppose that $a[x^2 + y^2 + xy + 1] + (a + b)[x^2y + y^2x] = 0$ and prove that $z^2 + tz = t^3 + a'_2t^2 + a'_6$. Let $G(t, z) = z^2 + tz + t^3 + a'_2t^2 + a'_6$, we have the following:

$$\begin{split} G(t,z) &= \frac{b^4}{a^4} \Biggl[\frac{(a^2+b^2)y^2 + \frac{a^4+b^4}{a^4} [a^2 + (a^2+b^2)x^2]}{(a+(a+b)x)^2} \Biggr] \\ &+ \frac{b^4}{a^4} \Biggl[\frac{(a+b)x}{a+(a+b)x} \Biggr] \Biggl[\frac{(a+b)y + dfraca^2 + b^2a^2(a+(a+b)x)}{a+(a+b)x} \Biggr] \\ &+ \frac{b^6}{a^6} \times \frac{(a^2+b^2)(a+b)x^3}{(a+(a+b)x)^3} + \frac{b^6}{a^6} \Biggl[\frac{(a^2+b^2)x^2}{(a+(a+b)x)^2} \Biggr] + \frac{b^4}{a^4} (a^2+b^2) \Biggl[\frac{a^2+b^2}{a^4} + \frac{1}{a^4} \Biggr] \\ &= y^2 [a+(a+b)x] + (a^2+b^2) \frac{a^2+(a^2+b^2)x^2}{a^4} [a+(a+b)x] + x \Biggl[y+(a+b)\frac{a+(a+b)x}{a^2} \Biggr] [a+(a+b)x] \\ &+ \frac{b^2}{a^2} (a+b)x^3 + \frac{b^2}{a^2} x^2 [a+(a+b)x] + \frac{b^2}{a^4} [a^2+(a^2+b^2)x^2] [a+(a+b)x] \\ &= ay^2 + (a+b)xy^2 + \frac{1}{a} + \frac{a+b}{a^2}x + \frac{a^2+b^2}{a^3}x^2 + \frac{(a^2+b^2)(a+b)}{a^4}x^3 + axy + (a+b)x^2y + x + \frac{a+b}{a}x^2 \\ &+ \frac{a+b}{a}x^2 + \frac{a^2+b^2}{a^2}x^3 + \frac{b^2}{a^2} (a+b)x^3 + \frac{b^2}{a}x^2 + \frac{b^2}{a^2} (a+b)x^3 \\ &+ \frac{b^2}{a^4} [a^3+a^2(a+b)x + a(a^2+b^2)x^2 + (a^2+b^2)(a+b)x^3] \\ &= a[x^2+y^2+xy+1] + (a+b)[x^2y+y^2x] \\ &= 0. \end{split}$$

Corollary 3.3 (Projective version) Suppose that k is a field such that it's characteristic is 2 and a, $b \in k$. Each curve with projective equation $a[X^2Z+Y^2Z+XYZ+Z^3]+(a+b)[X^2Y+Y^2X] = 0$ with $ab(a+b) \neq 0$ is equivalent in a birationally way to the curve $V^2W + UVW = U^3 + a'_2U^2W + a'_6W^3$ with $a'_2 = \frac{b^2}{a^2}$ and $a'_6 = \frac{a^4 + b^4}{a^8}b^4 + \frac{a^2 + b^2}{a^6}b^4$ by

$$\begin{cases} U = \frac{b^2(a+b)}{a^2}X\\ V = \frac{b^2}{a^2}\left[(a+b)Y + \frac{a^2+b^2}{a^2}(aZ+(a+b)X)\right] \iff \begin{cases} X = \frac{a^3}{a+b}U\\ Y = \frac{a^3}{a+b}V + \frac{a+b}{a}b^2W\\ Z = a^2U + b^2W \end{cases}$$

Proof. To refer to from above.

3.2 Addition Law

• Neutral element: In corollary 1.5, we have

$$\begin{cases} U = \frac{Z}{a+b} \\ V = \frac{Y}{a+b} \\ W = X + \frac{aZ}{a+b} \end{cases} \iff \begin{cases} X = aU + W \\ Y = (a+b)V \\ Z = (a+b)U \end{cases}$$

and the point at infinity is $P_{\infty} = \langle 0 : 1 : 0 \rangle$ in the elliptic curve in form $V^2W + VW\left[\frac{W+aU}{a+b}\right] = U\left[\frac{aW^2}{a^2+b^2} + \frac{ab^2}{a^2+b^2}U^2\right].$

The neutral element is the point $\varphi^{-1}(P_{\infty}) = \varphi^{-1}(0:1:0) = (0:a+b:0) = (0:1:0).$

• Symetrical element: if P = (x, y) is a point over the curve. We have $-P = \varphi^{-1}(-\varphi(P))$, and in the curve $v^2 + v \left[\frac{1+au}{a+b}\right] = u \left[\frac{a}{a^2+b^2} + \frac{ab^2}{a^2+b^2}u^2\right]$, we have $-\varphi(P) = -(u, v) = \left(u, v + \frac{1+au}{a+b}\right)$. Thus the symetrical element is -P = (x, x+y).

• Addition law: let $y = \alpha x + \beta$ denote the line (*PQ*) where $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are in the curve $\mathbf{E}_{a,b}$. We define P + Q = R where $R = (x_R, y_R)$ and $-R = (x_R, x_R + y_R)$ is third intersection point between the line and the curve.

We have $a[x^2 + (\alpha x + \beta)^2 + x(\alpha x + \beta) + 1] + (a + b)[x^2(\alpha x + \beta) + (\alpha x + \beta)^2 x] = 0$, thus $[(a + b)(\alpha + \alpha^2)]x^3 + [a(1 + \alpha + \alpha^2) + \beta(a + b)]x^2 + [a\beta + \beta^2(a + b)]x + a(\beta^2 + 1) = 0$. Thus $x_P + x_Q + x_R = \frac{a(1 + \alpha + \alpha^2) + \beta(a + b)}{(a + b)(\alpha + \alpha^2)}$

Hence we have:

$$\begin{cases} x_R = x_P + x_Q + \frac{a(1 + \alpha + \alpha^2) + \beta(a + b)}{(a + b)(\alpha + \alpha^2)} \\ y_R = \alpha x_R + \beta \end{cases}$$

with $\alpha = \frac{y_P + y_Q}{x_P + x_Q}$ and $\beta = y_P + \alpha x_P$.

4. Conclusion

We have successfully proposed a new binary elliptic curve. For further works, one must study if the addition law is unified and complete.

References

Avanzi, R., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., & Vercauteren, F. (2006). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall.

Bernstein, D. J., Birkner, P., Joye, M., Lange, T., & Peters, C. (2008). Twisted Edwards Curves.

- Bernstein, D. J., Lange, T., & Farashahi, R. R. (2008). *Binary edwards curves*. Cryptology ePrint Archive, Report 171. http://dx.doi.org/10.1007/978-3-540-85053-3
- Devigne, J., & Joye, M. (2011). Binary Huff Curves. In A. Kiayias (Ed.), Topics in Cryptology. *Lecture Notes in Computer Science*, 6558, 340-355, Springer. http://dx.doi.org/10.1007/978-3-642-19074-2_22
- Edwards, H. M. (2007). A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44, 393-422. http://dx.doi.org/10.1090/S0273-0979-07-01153-6
- Huff, G. B. (1948). Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15, 443-453. http://dx.doi.org/10.1215/S0012-7094-48-01543-9
- Joye, M., Tibouchi, M., Vergnaud, D. (2010). Huff's model for elliptic curves. In Hanrot, G., Morain, F., & Thome, E. (Eds.), Algorithmic Number Theory (ANTS-IX). *Lecture Notes in Computer Science*, *6197*, 234-250. Springer. http://dx.doi.org/10.1007/978-3-642-14518-6_20
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Math. Comp.*, 48, 203-209. http://dx.doi.org/10.1090/S0025-5718-1987-0866109-5
- Koblitz, N. (1989). Hyperelliptic cryptosystems. Journal of Cryptography. http://dx.doi.org/10.1007/BF02252872
- Miller, V. S. (1986). Short programs for functions on curves. Retrieved from http://crypto.stanford.edu/miller.pdf
- Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod *p. Mathematics of Computation*, 44(170), 483-485.
- Silvermann, J. (1986). The Arithmetique of Elliptic Curves. Springer.
- Solinas, J. (1997). An improved algorithm for arithmetic on a family of elliptic curves. Advances in Cryptology Crypto '97. *Lecture Notes in Computer Science*, *1294*, 357-371. http://dx.doi.org/10.1007/BFb0052248