# New Model of Binary Elliptic Curve 

Demba Sow ${ }^{1}$ \& Djiby Sow ${ }^{1}$<br>${ }^{1}$ Ecole Doctorale de Mathématiques et Informatique, Laboratoire d'Algèbre de Cryptologie de Géométrie Algèbrique et Applications, Université Cheikh Anta Diop de Dakar, Sénégal<br>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 $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$. If $m \geq 5$ we prove that each ordinary elliptic curve $y^{2}+x y=x^{3}+\alpha x^{2}+\beta, \beta \neq 0$ 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:

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

where the coefficients $a_{1}, a_{2}, a_{3}, a_{4}$ and $a_{6}$ are in $K$; with a special element denoted by $\bar{O}$ and called the point at infinity.

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

$$
y^{2}+x y=x^{3}+\alpha x^{2}+\beta \quad(\beta \neq 0)
$$

The group law of a binary elliptic curve is given by the following. Let $P=\left(x_{1}, y_{1}\right)$ and $Q=\left(x_{2}, y_{2}\right)$ be elements in $E$ then we have the following:

- the neutral element is $\bar{O}$ and the opposite of $P$, is $-P=\left(x_{1}, x_{1}+y_{1}\right)$;
- if $Q \neq-P$ then $P+Q=\left(x_{3}, y_{3}\right)$ :
- if $P \neq Q$ then $x_{3}=\lambda^{2}+\lambda+x_{1}+x_{2}+a$ and $y_{3}=\lambda\left(x_{1}+x_{3}\right)+x_{3}+y_{1}$ 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 $a b(a+b) \neq 0$. The new binary curve with coefficients $a$ and $b$ is the affine curve

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

### 2.1 Varieties

Proposition 2.2 The curve $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ with $a b(a+b) \neq 0$ define over $\mathbb{F}_{2^{m}}$ is absolutely irreducible in $\mathbb{F}_{2^{m}}$.
Proof. Put $H(x, y)=[a+(a+b) x] y^{2}+\left[a x+(a+b) x^{2}\right] y+a\left(x^{2}+1\right)$ in $\mathbb{F}_{2^{m}}$. Suppose that $H$ is reducible i.e. there exist four non zero functions $f, f^{\prime}, g$ and $g^{\prime}$ such that $H(x, y)=[f(x)+g(x) y]\left[f^{\prime}(x)+g^{\prime}(x) y\right]=f(x) f^{\prime}(x)+\left(f(x) g^{\prime}(x)+\right.$ $\left.g(x) f^{\prime}(x)\right) y+g(x) g^{\prime}(x) y^{2}$, by identification:

$$
\left\{\begin{array}{l}
f(x) f^{\prime}(x)=a\left(x^{2}+1\right) \\
g(x) g^{\prime}(x)=(a+b) x+a \\
f(x) g^{\prime}(x)+g(x) f^{\prime}(x)=a x+(a+b) x^{2}
\end{array}\right.
$$

- ${ }^{\text {st }}$ case $: f=$ cste then $(1) \Longrightarrow f^{\prime}=\frac{a\left(x^{2}+1\right)}{f},(3) \Longrightarrow g=$ cste and (2) $\Longrightarrow g^{\prime}=\frac{a+(a+b) x}{g}$. In (3) we have $f g^{\prime}+g f^{\prime}=a \frac{g}{f} x^{2}+(a+b) \frac{f}{g} x+a\left(\frac{f}{g}+\frac{g}{f}\right) ;$ by identification

$$
\left\{\begin{array}{ll}
a+b=a \frac{g}{f}, & \left(1^{\prime}\right) ;  \tag{1"}\\
a=(a+b) \frac{f}{g}, \\
a\left(\frac{f}{g}+\frac{g}{f}\right)=0, & \left(2^{\prime}\right) ;
\end{array} \quad \text { iff. }, \quad\left\{\begin{array}{l}
\frac{g}{f}=\frac{a+b}{a} \\
\frac{f}{g}=\frac{a}{a+b} \\
a\left(\frac{a+b}{a}+\frac{a}{a+b}\right)=0
\end{array}\right.\right.
$$

(3") iff. $\frac{b^{2}}{a+b}=0$ iff. $b=0$ impossible because $b \neq 0$.
 $f g^{\prime}+g f^{\prime}=a \frac{g^{\prime}}{f^{\prime}} x^{2}+(a+b) \frac{f^{\prime}}{g^{\prime}} x+a\left(\frac{f^{\prime}}{g^{\prime}}+\frac{g^{\prime}}{f^{\prime}}\right)$; by identification

$$
\left\{\begin{array} { l l } 
{ a + b = a \frac { g ^ { \prime } } { f ^ { \prime } } , } & { ( 1 ^ { \prime } ) ; }  \tag{1"}\\
{ a = ( a + b ) \frac { f ^ { \prime } } { g ^ { \prime } } , } & { ( 2 ^ { \prime } ) ; \quad \text { iff. } } \\
{ a ( \frac { f ^ { \prime } } { g ^ { \prime } } + \frac { g ^ { \prime } } { f ^ { \prime } } ) = 0 , } & { ( 3 ^ { \prime } ) . }
\end{array} \quad \left\{\begin{array}{l}
\frac{g^{\prime}}{f^{\prime}}=\frac{a+b}{a} \\
\frac{f^{\prime}}{g^{\prime}}=\frac{a}{a+b}, \\
a\left(\frac{a+b}{a}+\frac{a}{a+b}\right)=0
\end{array}\right.\right.
$$

(3") iff. $\frac{b^{2}}{a+b}=0$ iff. $b=0$ impossible because $b \neq 0$.
 Equation (2) implies that $g=$ cste or $g^{\prime}=$ cste. Suppose $g=$ cste then $g^{\prime}=\frac{a+(a+b) x}{g}$. Equation (3) implies that $f g^{\prime}+g f^{\prime}=a_{1}(x+1) \frac{[(a+b) x+a]}{g}+g a_{2}(x+1)=x[(a+b) x+a]$ 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 $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ is nonsingular.
Proof. It exists smooth variety if the following system assume solution:

$$
\left\{\begin{array}{l}
H(x, y)=y^{2}[a+(a+b) x]+y\left[a x+(a+b) x^{2}\right]+a\left(x^{2}+1\right)=0  \tag{1}\\
\frac{\partial H}{\partial x}=(a+b) y^{2}+a y=0 \\
\frac{\partial H}{\partial y}=(a+b) x^{2}+a x=0
\end{array}\right.
$$

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 $a\left(\frac{a^{2}}{a^{2}+b^{2}}+1\right)=0 \Longleftrightarrow a b^{2}=0 \Longleftrightarrow a=0$ or $b=0$, impossible because $a b \neq 0$.
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:

$$
a\left[X^{2} Z+Y^{2} Z+X Y Z+Z^{3}\right]+(a+b)\left[X^{2} Y+Y^{2} X\right]=0
$$

### 2.3.2 Infinites Points

$Z=0$ implies that $(a+b)\left[X^{2} Y+Y^{2} X\right]=0$ 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 $T(Z, Y)=a\left[Z+Y^{2} Z+Y Z+Z^{3}\right]+(a+b)\left[Y+Y^{2}\right]$. $\frac{\partial T}{\partial Y}=a Z+a+b, \frac{\partial T}{\partial Y}(0,0)=a+b \neq 0$ 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 $T(X, Z)=a\left[X^{2} Z+Z+X Z+Z^{3}\right]+(a+b)\left[X^{2}+X\right]$. $\frac{\partial T}{\partial X}=a Z+a+b, \frac{\partial T}{\partial X}(0,0)=a+b \neq 0$ 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 $T(Z)=a\left[Z+Z+Z+Z^{3}\right]=a Z\left[1+Z^{2}\right] \cdot \frac{\partial T}{\partial Z}=a\left[1+Z^{2}\right]$, $\frac{\partial T}{\partial Z}(0,0)=a \neq 0$ 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 $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ with $a b(a+b) \neq 0$ is equivalent in a birationally way to the curve $v^{2}+v\left[\frac{1+a u}{a+b}\right]=u\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} u^{2}\right]$ via the map $\varphi:(x, y) \longmapsto(u, v)$, with

$$
\left\{\begin{array} { l } 
{ u = \frac { 1 } { a + ( a + b ) x } } \\
{ v = \frac { y } { a + ( a + b ) x } }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
x=\frac{1+a u}{(a+b) u} \\
y=\frac{v}{u}
\end{array}\right.\right.
$$

Proof.
a) Assume that $v^{2}+v\left[\frac{1+a u}{a+b}\right]=u\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} u^{2}\right]$ and prove that $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$.

Let $H(x, y)=a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]$. We obtain

$$
\begin{aligned}
H(x, y) & =a\left[\frac{1+a^{2} u^{2}}{\left(a^{2}+b^{2}\right) u^{2}}+\frac{v^{2}}{u^{2}}+\frac{v(1+a u)}{(a+b) u^{2}}+1\right]+(a+b)\left[\frac{v\left(1+a^{2} u^{2}\right)}{\left(a^{2}+b^{2}\right) u^{3}}+\frac{v^{2}(1+a u)}{(a+b) u^{3}}\right] \\
& =a\left[\left(1+a^{2} u^{2}\right) u+u v^{2}\left(a^{2}+b^{2}\right)+u v(a+b)(1+a u)+u^{3}\left(a^{2}+b^{2}\right)\right]+(a+b)\left[v\left(1+a^{2} u^{2}\right)+v^{2}(a+b)(1+a u)\right] \\
& =\frac{u\left(a+a^{3} u^{2}\right)}{a^{2}+b^{2}}+a u v^{2}+a u v \frac{1+a u}{a+b}+a u^{3}+v \frac{1+a^{2} u^{2}}{a+b}+v^{2}(1+a u) \\
& =v^{2}+v\left[\frac{1+a u}{a+b}\right]+u\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}}\right] \\
& =0
\end{aligned}
$$

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

$$
\begin{aligned}
G(u, v) & =\frac{y^{2}}{[a+(a+b) x]^{2}}+\frac{y}{a+(a+b) x}\left[\frac{1+\frac{a}{a+(a+b) x}}{a+b}\right]+\frac{1}{a+(a+b) x}\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} \times \frac{1}{(a+(a+b) x)^{2}}\right] \\
& =y^{2}(a+(a+b) x)+y(a+(a+b) x) \times\left[\frac{a+(a+b) x+a}{a+b}\right]+\left[\frac{a\left(a^{2}+\left(a^{2}+b^{2}\right) x^{2}\right)}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}}\right] \\
& =a y^{2}+(a+b) x y^{2}+a x y+(a+b) x^{2} y+a+a x^{2} \\
& =a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+x y^{2}\right] \\
& =0
\end{aligned}
$$

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 $a\left[X^{2} Z+Y^{2} Z+X Y Z+Z^{3}\right]+(a+b)\left[X^{2} Y+Y^{2} X\right]=0$ with $a b(a+b) \neq 0$ is equivalent in a birationally way to the curve $V^{2} W+V W\left[\frac{W+a U}{a+b}\right]=U\left[\frac{a W^{2}}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} U^{2}\right]$, by

$$
\left\{\begin{array} { l } 
{ U = \frac { Z } { a + b } } \\
{ V = \frac { Y } { a + b } } \\
{ W = X + \frac { a Z } { a + b } }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
X=a U+W \\
Y=(a+b) V \\
Z=(a+b) U
\end{array}\right.\right.
$$

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 $(\alpha)=$ $\alpha+\alpha^{p}+\ldots \alpha^{p n-1}$ for $\alpha \in \mathbb{F}_{q}$.
Proprieties: 1 Let $\alpha, \beta \in \mathbb{F}_{q}$

1) $\operatorname{Trace}(\alpha) \in \mathbb{Z} / p \mathbb{Z}$;
2) $\operatorname{Trace}\left(\alpha^{p}\right)=\alpha$;
3) There exists $\gamma \in \mathbb{F}_{p^{n}}$, with $\operatorname{Trace}(\gamma) \neq 0$;
4) if $a \in \mathbb{Z} / p \mathbb{Z}$, then $\operatorname{Trace}(a)=n a$;
5) if $a \in \mathbb{Z} / p \mathbb{Z}$, then Trace $(a \alpha)=a \operatorname{Trace}(\alpha)$;
6) $\operatorname{Trace}(\alpha+\beta)=\operatorname{Trace}(\alpha)+\operatorname{Trace}(\beta)$
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 $\operatorname{Trace}(\alpha)=0$.

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

1) $\operatorname{Trace}\left(\alpha^{2}\right)=\alpha$;
2) The equation $x^{2}+u x+v=0$ with $u, v \in \mathbb{F}_{2^{n}}[x], u \neq 0$ has a solution if and only if $\operatorname{Trace}\left(\frac{v}{u^{2}}\right)=0$. 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 $\mathbb{F}_{q}$. Then

$$
\left|E\left(\mathbb{F}_{q}\right)\right|=q+1-t \text { and }|t| \leq 2 \sqrt{q} .
$$

### 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 $l \geq 5$, the curves $y^{2}=x^{3}+\alpha x^{2}+x y+\beta, \beta \neq 0$ and $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ are birationally equivalent.
Proof.

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

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

via the map $\varphi_{1}:(x, y) \longmapsto(u, v)$, with

$$
\left\{\begin{array} { l } 
{ u = \frac { 1 } { a + ( a + b ) x } } \\
{ v = \frac { y } { a + ( a + b ) x } }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
x=\frac{1+a u}{(a+b) u} \\
y=\frac{v}{u}
\end{array}\right.\right.
$$

- We have also $v^{2}+v\left[\frac{1+a u}{a+b}\right]=u\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} u^{2}\right]$ is equivalent in a birationally way to $v^{\prime 2}+a_{1} u^{\prime} v^{\prime}=$ $u^{\prime 3}+a_{2} u^{\prime 2}+a_{4} u^{\prime}+a_{6}$ with $a_{1}=\frac{a}{c(a+b)}, a_{2}=\frac{1}{a}, a_{4}=\frac{1}{a^{2}}+\frac{1}{b^{2}}$ and $a_{6}=\frac{1}{c^{2}\left(a^{2}+b^{2}\right)}+\frac{1}{a^{3}}$ and $c^{2}=\frac{a b^{2}}{a^{2}+b^{2}}$, via the map $\varphi_{2}:(u, v) \longmapsto\left(u^{\prime}, v^{\prime}\right)$, with

$$
\left\{\begin{array} { l } 
{ u ^ { \prime } = \frac { 1 } { a } + u } \\
{ v ^ { \prime } = \frac { v } { c } }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
u=\frac{1}{a}+u^{\prime} \\
v=c v^{\prime}
\end{array}\right.\right.
$$

- Define change of variables, put $\left\{\begin{array}{l}u=\frac{1}{a}+u^{\prime} \\ v=c v^{\prime}\end{array} \Longleftrightarrow\left\{\begin{array}{l}u^{\prime}=\frac{1}{a}+u \\ v^{\prime}=\frac{v}{c}\end{array}\right.\right.$ and $c^{2}=\frac{a b^{2}}{a^{2}+b^{2}}$. We have $v^{\prime 2}+a u^{\prime} u^{\prime} v^{\prime}=$ $u^{\prime 3}+a_{2} u^{\prime 2}+a_{4} u^{\prime}+a_{6}$ with $a_{1}=\frac{a}{c(a+b)}, a_{2}=\frac{1}{a}, a_{4}=\frac{1}{a^{2}}+\frac{1}{b^{2}}$ and $a_{6}=\frac{1}{c^{2}\left(a^{2}+b^{2}\right)}+\frac{1}{a^{3}}$.
Define another the change of variables $\left\{\begin{array}{l}u^{\prime}=a_{1}^{2} T \\ v^{\prime}=a_{1}^{3}(Z+s T+\lambda)\end{array}\right.$ then we have

$$
\begin{aligned}
a_{1}^{6}\left(Z^{2}+s^{2} T^{2}+\lambda^{2}\right)+a_{1}^{6} t(Z+s T+\lambda) & =a_{1}^{6} T^{3}+a_{1}^{4} a_{2} T^{2}+a_{1}^{2} a_{4} T+a_{6} Z^{2}+T z \\
& =T^{3}+T^{2}\left[s^{2}+s+\frac{a_{2}}{a_{1}^{2}}\right]+T\left[\lambda+\frac{a_{4}}{a_{1}^{4}}\right]+\lambda^{2}+\frac{a_{6}}{a_{1}^{6}}
\end{aligned}
$$

By identification: $\left\{\begin{array}{l}s^{2}+s+\frac{a_{2}}{a_{1}^{2}}=a_{2}^{\prime} \\ \lambda+\frac{a_{4}}{a_{1}^{4}}=0 \\ \lambda^{2}+\frac{a_{6}}{a_{1}^{6}}=a_{6}^{\prime} \Rightarrow a_{6}^{\prime}=\frac{a_{4}^{2}}{a_{1}^{8}}+\frac{a_{6}}{a_{1}^{6}}=\frac{a_{4}^{2}+a_{1}^{2} a_{6}}{a_{1}^{8}} .\end{array}\right.$

Define $h^{-2}=\frac{a_{2}}{a_{1}^{2}} \Longrightarrow h=\frac{a_{1}}{\sqrt{a_{2}}}$. Thus we have $s^{2}+s+a_{2}^{\prime}+h^{-2}=0, h^{-2}=\frac{a_{2}}{a_{1}^{2}}=\frac{c^{2}\left(a^{2}+b^{2}\right)}{a^{3}}, a_{6}^{\prime}=\left(\frac{a_{4}+a_{1} \sqrt{a_{6}}}{a_{1}^{4}}\right)=$ $\left(1+\frac{c^{2}\left(a^{2}+b^{2}\right)}{a^{3}}+\sqrt{1+\frac{c^{2}\left(a^{2}+b^{2}\right)}{a^{3}}}\right) \frac{c^{2}\left(a^{2}+b^{2}\right)}{a^{3}}=\left(1+h^{-2}+\sqrt{1+h^{-2}}\right) h^{-2} \Longrightarrow h^{2} \sqrt{a_{6}^{\prime}}=h^{-2}+h^{-1} \Longleftrightarrow h^{-2}+$ $h^{-1}+h^{2} \sqrt{a_{6}^{\prime}}=0$.
Put $t=h^{-1}$ thus $t^{2}+t+h^{2} \sqrt{a_{6}^{\prime}}=0$.
Thus $\left\{\begin{array}{l}s^{2}+s+a_{2}^{\prime}+h^{-2}=0 \\ t^{2}+t+h^{2} \sqrt{a_{6}^{\prime}}=0\end{array} \Longleftrightarrow\left\{\begin{array}{l}\operatorname{Trace}\left(a_{2}^{\prime}+h^{-2}\right)=0 \\ \operatorname{Trace}\left(h^{2} \sqrt{a_{6}^{\prime}}\right)=0\end{array} \Longleftrightarrow\left\{\begin{array}{l}\operatorname{Trace}\left(h^{-1}\right)=\operatorname{Tr}\left(a_{2}^{\prime}\right) \\ \operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right)=0 .\end{array}\right.\right.\right.$
For each $\lambda, \pi \in \mathbb{F}_{2}$, define

$$
L_{\lambda, \pi}=\left\{h \in \mathbb{F}_{2^{l}}^{*}: \operatorname{Trace}\left(h^{-1}\right)=\lambda, \operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right)=\pi\right\}
$$

We define by $|L|$ the cardinality of the set $L$ and $|E|$ the cardinality of $E$. Since $t^{4} \sqrt{a_{6}^{\prime}}+t+1=0$ has at most 4 roots, we must prove that $L_{\operatorname{Trace}\left(a_{6}^{\prime}\right), 0}$ has at least 5 elements i.e $\mid L_{\operatorname{Trace}\left(a_{6}^{\prime}\right), 0} \geq 5$ if $l \geq 5$.
Namely let at prove that $|L|_{0,0} \geq 5$ and $\mid L_{1,0} \geq 5$ if $l \geq 4$.
We have $|L|_{0,0}+|L|_{1,0}=2^{l-1}-1$. Therefore, since $h$ can take all values in $\mathbb{F}_{2^{2}}^{*}$, then $h \sqrt[4]{a_{6}^{\prime}}$ 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 $\operatorname{Trace}(h)=0$. Now, we have $|L|_{1,0}+|L|_{1,1}=2^{l-1}$. Therefore, similarly as above $|L|_{1,0}+\mid L_{1,1}$ count the elements $h \in \mathbb{F}_{2^{l}}^{*}$ with $\operatorname{Trace}(h)=1$. 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 $|L|_{0,0}+\mid L_{1,1}$. We have the following:
$h \in L_{0,0} \cup L_{1,1} \Longleftrightarrow\left\{\begin{array}{l}\operatorname{Trace}\left(h^{-1}\right)=0=\operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right) \\ \operatorname{Trace}\left(h^{-1}\right)=1=\operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right)\end{array} \Longleftrightarrow \operatorname{Trace}\left(h^{-1}\right)=\operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right) \Longleftrightarrow \operatorname{Trace}\left(h^{-1}+\right.\right.$ $\left.h \sqrt[4]{a_{6}^{\prime}}\right)=0$ iff we have two possibilities for $x$, namely $\left(x\right.$ and $x+1$ ) such that $x^{2}+x+h^{-1}+h \sqrt[4]{a_{6}^{\prime}}=0 \Longleftrightarrow$ $h^{2} x^{2}+h^{2} x+h+h^{3} \sqrt[4]{a_{6}^{\prime}}=0 \Longleftrightarrow(h x)^{2}+h(h x)=h^{3} \sqrt[4]{a_{6}^{\prime}}+h \Longleftrightarrow v^{2}+u v=u^{3} \sqrt[4]{a_{6}^{\prime}}+u$ with $v=h x$ and $u=h$.
Hasse's theorem implies that it exists $\delta=\left|E\left(\mathbb{F}_{2^{l}}^{*}\right)\right|-2^{l}-1 \in\left[-2 \sqrt{2^{l}}, 2 \sqrt{2^{l}}\right]$, the point $(0,0)$ and the infinite point do not verify the above equation and two points on the curve produce one $h$.
Thus $|L|_{0,0}+|L|_{1,1}=\left(\left|E\left(\mathbb{F}_{2^{l}}^{*}\right)\right|-2\right) / 2=\left(\delta+2^{l}+1-2\right) / 2,|L|_{0,0}+|L|_{1,1}=2^{l-1}+\frac{\delta-1}{2}, 4|L|_{1,0}=2\left(|L|_{0,0}+|L|_{1,0}\right)+$ $2\left(|L|_{1,0}+|L|_{1,1}\right)-2\left(|L|_{0,0}+|L|_{1,1}\right)=2\left(2^{l-1}-1\right)+2\left(2^{l-1}\right)-2\left(2^{l-1}-\frac{\delta-1}{2}\right)=2^{l}-(\delta+1), 4|L|_{0,0}=4\left(2^{l-1}-1\right)-4|L|_{1,0}=$ $4\left(2^{l-1}-1\right)-\left(2^{l}-(\delta-1)\right)=22^{l}-4-2^{l}+\delta+1=2^{l}+\delta-3$, since $\delta \in\left[-2 \sqrt{2^{l}}, 2 \sqrt{2^{l}}\right] \Longrightarrow \delta \geq-2 \sqrt{2^{l}}$, then $4|L|_{0,0}=2^{l}+\delta-3 \Longrightarrow 4|L|_{0,0} \geq 2^{l}+-2 \sqrt{2^{l}}-3 \Longrightarrow|L|_{0,0} \geq \frac{2^{l}-2 \sqrt{2^{l}}-3}{4}$ and $4|L|_{1,0} \geq 2^{l}+-2 \sqrt{2^{l}}-1 \Longrightarrow$ $|L|_{1,0} \geq \frac{2^{l}-2 \sqrt{2^{l}}-1}{4} \geq \frac{2^{l}-2 \sqrt{2^{l}}-3}{4}=\frac{\left(\sqrt{2^{l}}-1\right)^{2}-4}{4} \geq \frac{\left(\sqrt{2^{5}}-1\right)^{2}-4}{4}=11.25 \geq 5$.
As final remark, in order to transform the curve $z^{2}+z t=t^{3}+a_{2}^{\prime} t+a_{6}^{\prime}$ to $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$, we must find $h$ with $\operatorname{Trace}\left(h^{-1}\right)=\operatorname{Trace}\left(a_{2}^{\prime}\right)$ and $\operatorname{Trace}\left(h \sqrt[4]{a_{6}^{\prime}}\right)=0, h^{-2}=\frac{c\left(a^{2}+b^{2}\right)}{a^{3}}=\frac{b^{2}}{a^{2}}, \frac{b}{a}=h^{-1}=t_{0}$ where $t_{0}^{2}+t_{0}+h^{2} \sqrt{a_{6}^{\prime}}=0, t_{0}^{2}=\frac{b^{2}}{a^{2}}$, fix $b$ and compute $a=\sqrt{\frac{b}{t_{0}}}$ and fix $a$ and compute $b=\sqrt{a t_{0}}$.
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 $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ with $a b(a+b) \neq 0$ is equivalent in a birationally way to the curve $z^{2}+t z=t^{3}+a_{2}^{\prime} t^{2}+a_{6}^{\prime}$ with $a_{2}^{\prime}=\frac{b^{2}}{a^{2}}$ and $a_{6}^{\prime}=\frac{a^{4}+b^{4}}{a^{8}} b^{4}+\frac{a^{2}+b^{2}}{a^{6}} b^{4}$ via the map $\psi:(x, y) \longmapsto(t, z)$ with

Proof.
a) Suppose that $z^{2}+t z=t^{3}+a_{2}^{\prime} t^{2}+a_{6}^{\prime}$ and prove that $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$.

Let $H(x, y)=a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]$, we have the following:

$$
\begin{aligned}
H(x, y) & =a\left[\frac{\frac{a^{6}}{a^{2}+b^{2}} t^{2}}{\left(b^{2}+a^{2} t\right)^{2}}+\frac{\frac{a^{6}}{a^{2}+b^{2}} z^{2}+\frac{a^{2}+b^{2}}{a^{2}} b^{4}}{\left(b^{2}+a^{2} t\right)^{2}}+\frac{\frac{a^{3}}{a+b} t\left[\frac{a^{3}}{a+b} z+\frac{a+b}{a} b^{2}\right]}{\left(b^{2}+a^{2} t\right)^{2}}+1\right] \\
& +(a+b)\left[\frac{\frac{a^{6}}{a^{2}+b^{2}} t^{2}\left[\frac{a^{3}}{a+b} z+\frac{a+b}{a} b^{2}\right]}{\left(b^{2}+a^{2} t\right)^{3}}+\frac{\frac{a^{3}}{a+b} t\left[\frac{a^{6}}{a^{2}+b^{2}} z^{2}+\frac{a^{2}+b^{2}}{a^{2}} b^{4}\right]}{\left(b^{2}+a^{2} t\right)^{3}}\right] \\
& =a\left[t^{2}\left(b^{2}+a^{2} t\right)+z^{2}\left(b^{2}+a^{2} t\right)+\frac{a^{4}+b^{4}}{a^{8}} b^{4}\left(b^{2}+a^{2} t\right)+z t\left(b^{2}+a^{2} t\right)+\frac{a^{2}+b^{2}}{a^{4}} b^{2} t\left(b^{2}+a^{2} t\right)\right. \\
& \left.+\frac{a^{2}+b^{2}}{a^{6}}\left(b^{2}+a^{2} t\right)^{3}\right]+(a+b)\left[t^{2}\left(\frac{a^{3}}{a+b} z+\frac{a+b}{a} b^{2}\right)+\frac{a^{3}}{a+b} z^{2} t+\frac{b^{4}(a+b)\left(a^{2}+b^{2}\right)}{a^{5}} t\right] \\
& =z^{2}\left[a b^{2}\right]+z t\left[a b^{2}\right]+t^{3}\left[a b^{2}\right]+t^{2}\left[a b^{2}+\frac{a^{2}+b^{2}}{a} b^{2}\right]+\frac{a^{4}+b^{4}}{a^{7}} b^{6}+\frac{a^{2}+b^{2}}{a^{5}} b^{6} \\
& =z^{2}+z t+t^{3}+\frac{b^{2}}{a^{2}} t^{2}+\frac{a^{4}+b^{4}}{a^{8}} b^{4}+\frac{a^{2}+b^{2}}{a^{6}} b^{4} \\
& =z^{2}+z t+t^{3}+a_{2}^{\prime} t^{2}+a_{6}^{\prime} \\
& =0 .
\end{aligned}
$$

b) Suppose that $a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right]=0$ and prove that $z^{2}+t z=t^{3}+a_{2}^{\prime} t^{2}+a_{6}^{\prime}$.

Let $G(t, z)=z^{2}+t z+t^{3}+a_{2}^{\prime} t^{2}+a_{6}^{\prime}$, we have the following:

$$
\begin{aligned}
G(t, z) & =\frac{b^{4}}{a^{4}}\left[\frac{\left(a^{2}+b^{2}\right) y^{2}+\frac{a^{4}+b^{4}}{a^{4}}\left[a^{2}+\left(a^{2}+b^{2}\right) x^{2}\right]}{(a+(a+b) x)^{2}}\right] \\
& +\frac{b^{4}}{a^{4}}\left[\frac{(a+b) x}{a+(a+b) x}\right]\left[\frac{(a+b) y+d f r a c a^{2}+b^{2} a^{2}(a+(a+b) x)}{a+(a+b) x}\right] \\
& +\frac{b^{6}}{a^{6}} \times \frac{\left(a^{2}+b^{2}\right)(a+b) x^{3}}{(a+(a+b) x)^{3}}+\frac{b^{6}}{a^{6}}\left[\frac{\left(a^{2}+b^{2}\right) x^{2}}{(a+(a+b) x)^{2}}\right]+\frac{b^{4}}{a^{4}}\left(a^{2}+b^{2}\right)\left[\frac{a^{2}+b^{2}}{a^{4}}+\frac{1}{a^{4}}\right] \\
& =y^{2}[a+(a+b) x]+\left(a^{2}+b^{2}\right) \frac{a^{2}+\left(a^{2}+b^{2}\right) x^{2}}{a^{4}}[a+(a+b) x]+x\left[y+(a+b) \frac{a+(a+b) x}{a^{2}}\right][a+(a+b) x] \\
& +\frac{b^{2}}{a^{2}}(a+b) x^{3}+\frac{b^{2}}{a^{2}} x^{2}[a+(a+b) x]+\frac{b^{2}}{a^{4}}\left[a^{2}+\left(a^{2}+b^{2}\right) x^{2}\right][a+(a+b) x] \\
& =a y^{2}+(a+b) x y^{2}+\frac{1}{a}+\frac{a+b}{a^{2}} x+\frac{a^{2}+b^{2}}{a^{3}} x^{2}+\frac{\left(a^{2}+b^{2}\right)(a+b)}{a^{4}} x^{3}+a x y+(a+b) x^{2} y+x+\frac{a+b}{a} x^{2} \\
& +\frac{a+b}{a} x^{2}+\frac{a^{2}+b^{2}}{a^{2}} x^{3}+\frac{b^{2}}{a^{2}}(a+b) x^{3}+\frac{b^{2}}{a} x^{2}+\frac{b^{2}}{a^{2}}(a+b) x^{3} \\
& +\frac{b^{2}}{a^{4}}\left[a^{3}+a^{2}(a+b) x+a\left(a^{2}+b^{2}\right) x^{2}+\left(a^{2}+b^{2}\right)(a+b) x^{3}\right] \\
& =a\left[x^{2}+y^{2}+x y+1\right]+(a+b)\left[x^{2} y+y^{2} x\right] \\
& =0 .
\end{aligned}
$$

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 $a\left[X^{2} Z+Y^{2} Z+X Y Z+Z^{3}\right]+(a+b)\left[X^{2} Y+Y^{2} X\right]=0$ with $a b(a+b) \neq 0$ is equivalent in a birationally way to the curve $V^{2} W+U V W=U^{3}+a_{2}^{\prime} U^{2} W+a_{6}^{\prime} W^{3}$ with $a_{2}^{\prime}=\frac{b^{2}}{a^{2}}$ and $a_{6}^{\prime}=\frac{a^{4}+b^{4}}{a^{8}} b^{4}+\frac{a^{2}+b^{2}}{a^{6}} b^{4}$ by

$$
\left\{\begin{array} { l } 
{ U = \frac { b ^ { 2 } ( a + b ) } { a ^ { 2 } } X } \\
{ V = \frac { b ^ { 2 } } { a ^ { 2 } } [ ( a + b ) Y + \frac { a ^ { 2 } + b ^ { 2 } } { a ^ { 2 } } ( a Z + ( a + b ) X ) ] } \\
{ W = a Z + ( a + b ) X }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
X=\frac{a^{3}}{a+b} U \\
Y=\frac{a^{3}}{a+b} V+\frac{a+b}{a} b^{2} W \\
Z=a^{2} U+b^{2} W
\end{array}\right.\right.
$$

Proof. To refer to from above.

### 3.2 Addition Law

- Neutral element: In corollary 1.5, we have

$$
\left\{\begin{array} { l } 
{ U = \frac { Z } { a + b } } \\
{ V = \frac { Y } { a + b } } \\
{ W = X + \frac { a Z } { a + b } }
\end{array} \Longleftrightarrow \left\{\begin{array}{l}
X=a U+W \\
Y=(a+b) V \\
Z=(a+b) U
\end{array}\right.\right.
$$

and the point at infinity is $P_{\infty}=\langle 0: 1: 0\rangle$ in the elliptic curve in form $V^{2} W+V W\left[\frac{W+a U}{a+b}\right]=U\left[\frac{a W^{2}}{a^{2}+b^{2}}\right.$ $\left.+\frac{a b^{2}}{a^{2}+b^{2}} U^{2}\right]$.
The neutral element is the point $\varphi^{-1}\left(P_{\infty}\right)=\varphi^{-1}(0: 1: 0)=(0: a+b: 0)=(0: 1: 0)$.

- Symetrical element: if $P=(x, y)$ is a point over the curve. We have $-P=\varphi^{-1}(-\varphi(P))$, and in the curve $v^{2}+v\left[\frac{1+a u}{a+b}\right]=u\left[\frac{a}{a^{2}+b^{2}}+\frac{a b^{2}}{a^{2}+b^{2}} u^{2}\right]$, we have $-\varphi(P)=-(u, v)=\left(u, v+\frac{1+a u}{a+b}\right)$. Thus the symetrical element is $-P=(x, x+y)$.
- Addition law: let $y=\alpha x+\beta$ denote the line $(P Q)$ where $P=\left(x_{P}, y_{P}\right)$ and $Q=\left(x_{Q}, y_{Q}\right)$ are in the curve $\mathbf{E}_{a, b}$. We define $P+Q=R$ where $R=\left(x_{R}, y_{R}\right)$ and $-R=\left(x_{R}, x_{R}+y_{R}\right)$ is third intersection point between the line and the curve.
We have $a\left[x^{2}+(\alpha x+\beta)^{2}+x(\alpha x+\beta)+1\right]+(a+b)\left[x^{2}(\alpha x+\beta)+(\alpha x+\beta)^{2} x\right]=0$, thus $\left[(a+b)\left(\alpha+\alpha^{2}\right)\right] x^{3}+[a(1+$ $\left.\left.\alpha+\alpha^{2}\right)+\beta(a+b)\right] x^{2}+\left[a \beta+\beta^{2}(a+b)\right] x+a\left(\beta^{2}+1\right)=0$. Thus $x_{P}+x_{Q}+x_{R}=\frac{a\left(1+\alpha+\alpha^{2}\right)+\beta(a+b)}{(a+b)\left(\alpha+\alpha^{2}\right)}$
Hence we have:

$$
\left\{\begin{array}{l}
x_{R}=x_{P}+x_{Q}+\frac{a\left(1+\alpha+\alpha^{2}\right)+\beta(a+b)}{(a+b)\left(\alpha+\alpha^{2}\right)} \\
y_{R}=\alpha x_{R}+\beta
\end{array}\right.
$$

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, 234250. 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/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

