A New Model of Binary Elliptic Curves with Fast Arithmetic

Hongfeng Wu[1], Chunming Tang[2] and Rongquan Feng[2]
[1]College of Science, North China University of technology,
Beijing 100144, P.R. China
whfmath@gmail.com

[2]School of Mathematical Sciences, Peking University,
Beijing 100871, P.R. China
tangchunmingmath@163.com, fengrq@math.pku.edu.cn

Abstract

This paper presents a new model of ordinary elliptic curves with fast arithmetic over field of characteristic two. In addition, we propose two isomorphism maps between new curves and Weierstrass curves. This paper proposes new explicit addition law for new binary curves and prove the addition law corresponds to the usual addition law on Weierstrass curves. This paper also presents fast unified addition formulae and doubling formulae for these curves. The unified addition formulae cost $12M + 2D$, where M is the cost of a field multiplication, and D is the cost of multiplying by a curve parameter. These formulae are more efficient than other formulae in literature. Finally, this paper presents explicit formulae for w-coordinates differential addition. In a basic step of Montgomery ladder, the cost of a projective differential addition and doubling are $5M$ and $1M + 1D$ respectively, and the cost of mixed w-coordinates differential addition is $4M$.

Keywords: Elliptic curve, binary field, scalar multiplication, unified addition law, differential addition, cryptography

1 Introduction

An elliptic curve over a field K is a smooth algebraic curve of genus 1 having a specified basepoint. Every elliptic curve can be written as the locus in $\mathbb{P}^2$ of a Weierstrass cubic equation with one infinity point $(0:1:0)$. There are many other ways to represent elliptic curves such as Legendre equation, Jacobi quartic equations and intersection of two quadratic surfaces. Several forms of elliptic curves over finite fields with different coordinate systems have been studied to improve the computation efficiency of the scalar multiplications. In 2007, a family of special curve named Edwards curves introduced by Edwards in [6]. Berstein and Lange proposed a general Edwards curves in [2]. In [4], Berstein, Lange and Farashahi study the Edwards curves over binary field. Recently, Joye, Tibouchi and VergnaudIt [10] study the Huff's curve introduced by Huff in [7]. Wu and Feng in [20] present a general Huff form. One of the main operations and challenges in elliptic curve cryptosystem is the scalar multiplication. The speed of scalar multiplication plays an important role in the efficiency of the whole system. Therefore, it is an interesting problem to explore new elliptic curves form with fast group law. In this paper, we mainly talk about elliptic curves over binary fields.

For a field K with characteristic two, every ordinary elliptic curve an be written as $E : v^2 + uv = u^2 + a_2u + a_6$ with $a_6 \neq 0$. The neutral element of the general addition law is the point $(0:1:0)$ and negation is defined as $-(u_1, v_1) = (u_1, u_1+v_1)$. For point (x_1, y_1) and (x_2, y_2) on curve E, whenever defined, $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2$ and $y_3 = \lambda(x_1+x_3)+x_3+y_1$, $\lambda = (y_2+y_1)/(x_2+x_1)$ if $x_1 \neq x_2$, or $\lambda = x_1+y_1/x_1$ if $x_1 = x_2$. In [4], Bernstein et al. introduced the binary Edwards curves over field K. If $d_1, d_2 \in K$ with $d_1 \neq 0, d_2 \neq d_1^2 + d_1$, the binary Edwards curve with coefficients d_1, d_2 is the affine curve

$$E_{B,d_1.d_2} : d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2.$$

The addition law is given by $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

$$x_3 = \frac{d_1(x_1 + x_2) + d_2(x_1 + y_1)(x_2 + y_2) + (x_1 + x_1^2)(x_2(y_1 + y_2 + 1) + y_1y_2)}{d_1 + (x_1 + x_1^2)(x_2 + y_2)},$$

$$y_3 = \frac{d_1(y_1 + y_2) + d_2(x_1 + y_1)(x_2 + y_2) + (y_1 + y_1^2)(y_2(x_1 + x_2 + 1) + x_1x_2)}{d_1 + (y_1 + y_1^2)(x_2 + y_2)}.$$

This paper explore a new model of binary elliptic curves

$$S_t : x^2y + xy^2 + txy + x + y = 0.$$

Define $(1, 1, 0)$ as the neutral element, then $-(x, y) = (y, x)$. The unified addition law is defined by

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2),$$

where

$$x_3 = \frac{(x_1x_2 + y_1y_2)(y_1 + y_2) + ty_1y_2(1 + x_1x_2)}{(x_1x_2 + y_1y_2)(1 + y_1y_2)},$$

$$y_3 = \frac{(x_1x_2 + y_1y_2)(x_1 + x_2) + tx_1x_2(1 + y_1y_2)}{(x_1x_2 + y_1y_2)(1 + x_1x_2)}.$$

If we define $(0, 0, 1)$ as the neutral element, then the unified addition law is defined by

$$x_3 = \frac{(x_1x_2 + y_1y_2)(1 + y_1y_2)}{(x_1x_2 + y_1y_2)(y_1 + y_2) + ty_1y_2(1 + x_1x_2)},$$

$$y_3 = \frac{(x_1x_2 + y_1y_2)(1 + x_1x_2)}{(x_1x_2 + y_1y_2)(x_1 + x_2) + tx_1x_2(1 + y_1y_2)}.$$

Here we give some notations. The trace function Tr: $\mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by

$$\alpha \mapsto \alpha + \alpha^2 + \cdots + a^{2^{m-1}}.$$

Note that $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2)$ for all $\alpha \in \mathbb{F}_{2^m}$. The quadratic equation $x^2 + x + \alpha = 0$ has solution in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}(\alpha) = 0$.

2 Special Binary Curve

Let K denote a field of characteristic 2. Consider the set of projective points $(X : Y : Z) \in \mathbb{P}^2(K)$ satisfying the equation

$$S_t : X^2Y + XY^2 + tXYZ + XZ^2 + YZ^2 = 0 \quad (1)$$

where $t \in K$ and $t \neq 0$. The tangent line at $(1 : 1 : 0)$ is $X + Y + tZ = 0$, which intersects the curve with multiplicity 3, so that $(1 : 1 : 0)$ is an inflection point of S_t. The partial derivatives of the curve equation are $Y^2 + tYZ + Z^2, X^2 + tXZ + Z^2$ and tXY. A singular point $(X_1 : Y_1 : Z_1)$ must have $Y_1^2 + tY_1Z_1 + Z_1^2 = X_1^2 + tX_1Z_1 + Z_1^2 = tX_1Y_1 = 0$, and therefore $X_1 = Y_1 = Z_1 = 0$ since $t \neq 0$. Therefore, S_t is nonsingular. The affine form of the curve is

$$S_t : x^2y + xy^2 + txy + x + y = 0.$$

We can denote $S_t(K)$ for a field K as

$$S_t(K) = \{(x, y) \in K^2 | x^2y+xy^2+txy+x+y = 0\} \bigcup \{(1 : 0 : 0), (0 : 1 : 0), (1 : 1 : 0)\}$$

by a light abuse notation.

Note that the variant form $x^2y + xy^2 + axy + b(x + y) = 0$ is isomorphic to $x^2y + xy^2 + txy + (x + y) = 0$ via the change of variables $(x, y) \to (ax/\sqrt{b}, ay/\sqrt{b})$ with $t = a/\sqrt{b}$. The curves $x^2y + xy^2 + xy + b(x + y) = 0$ isomorphic to $x^2y + xy^2 + txy + (x + y) = 0$ by $(x, y) \to (x/\sqrt{b}, y/\sqrt{b})$ and $t = 1/\sqrt{b}$.

The curve $x^2y + xy^2 + xy + b(x + y) = 0$ look similar to binary Edwards curve $E_{B,d_1.d_2} : d_1(x+y)+d_2(x^2+y^2) = xy+xy(x+y)+x^2y^2$ without quartic item with $d_1 = b$ and $d_2 = 0$.

The generalized form $S_{a,b} : x^2y + xy^2 + axy + (x + y) + b(x^2 + y^2) = 0$ of S_t curve isomorphic to $v^2 + uv = u^3 + (b/a)u^2 + a^{-8}(1 + ab)$. We can change $S_{a,b}$ to the form $d_1(x+y)+d_2(x^2+y^2) = xy+xy(x+y)$, then it look similar is the binary Edwards curve of eliminated quartic item.

2.1 First isomorphism

Let $S_t : x^2y + xy^2 + txy + x + y = 0$ defined over finite field $\mathbb{F}_{2^m}$, then S_t is isomorphic to the Weierstrass elliptic curve

$$v^2 + uv = u^3 + \frac{1}{t^8}$$

over $\mathbb{F}_{2^m}$ via the change of variables $\varphi(x, y) = (u, v)$, where

$$u = \frac{x + y}{t^2(x + y + t)},\ v = \frac{x + y + t^2x + t}{t^4(x + y + t)}.$$

The inverse maps is $\psi(u, v) = (x, y)$, where

$$x = \frac{t^4v + 1}{t^3u + t},\ y = \frac{t^4(u + v) + 1}{t^3u + t}.$$

In projective coordinates, the correspondence projective transformations from

$$X^2Y + XY^2 + tXYZ + XZ^2 + YZ^2 = 0$$

to

$$V^2W + UVW = U^3 + \frac{1}{t^8}W^3$$

is $(X, Y, Z) \mapsto (U, V, W)$ where

$$\begin{cases} U &= t^2(X+Y), \\ V &= X+Y+t^2X+tZ, \\ W &= t^4(X+Y+tZ). \end{cases}$$

The inverse transformations is $(U, V, W) \mapsto (X, Y, Z)$ where

$$\begin{cases} X &= t^4V+W, \\ Y &= t^4(U+V)+W, \\ Z &= t^3U+tW. \end{cases}$$

The above change of variables map the element $(1, 1, 0)$ on S_t to the identity element $(0, 1, 0)$ on Weierstrass curve.

Note that curves $x^2y+xy^2+xy+b(x+y) = 0$ isomorphic to $v^2+uv = u^3+b^4$ via the change of variables

$$x = \frac{v+b^2}{u+b}, \;\; v = \frac{u+v+b^2}{u+b}.$$

Lemma 2.1. *An elliptic curve E defined over $\mathbb{F}_{2^m}$ satisfies $4|\sharp E(\mathbb{F}_{2^m})$ if and only if E isomorphic to a elliptic curve form $x^2y + xy^2 + txy + x + y = 0$.*

Proof. Since for any $a \in \mathbb{F}_{2^m}^*$, there exist a t such that $S_t : x^2y+xy^2+txy+x+y = 0$ isomorphic to $v^2 + uv = u^3 + a$. We need only to prove an elliptic curve E defined over $\mathbb{F}_{2^m}$ satisfies $4|\sharp E(\mathbb{F}_{2^m})$ if and only if E isomorphic to a elliptic curve form $W_a : v^2 + uv = u^3 + a$.

Assuming that E isomorphic to $W_a : v^2 + uv = u^3 + a$, we count the number of W_a. For any point $P = (x, y) \in S_a$ with $P \neq (0, 1, 0), (0, \sqrt{a})$, then $x \neq 0$. Therefore, $\sharp W_a(\mathbb{F}_{2^m}) = 2 + 2\sharp\{t \in \mathbb{F}_{2^m} | t^2 + t = x + \frac{a}{x^2}, x \neq 0\}$. The equation $t^2 + t = x + \frac{a}{x}$ has solution if and only if $Tr(x + \frac{a}{x^2}) = 0$, that is $\mathrm{Tr}(x) = \mathrm{Tr}(\frac{\sqrt{a}}{x})$. Note that $\sharp\{x \in \mathbb{F}_{2^m}^* | Tr(x) = Tr(\frac{\sqrt{a}}{x})\}$ is an odd since $x \mapsto \frac{\sqrt{a}}{x}$ is an involution on $\mathbb{F}_{2^m}^*$ with precisely one fixed point. Actually, point $(\sqrt[4]{a}, \sqrt{a})$ belongs W_a and has order 4, hence $4|\sharp E(\mathbb{F}_{2^m})$.

Secondly, if $4|\sharp E(\mathbb{F}_{2^m})$ then E is ordinary, it has an equation after a suitable choice of coordinates $E: y^2+xy=x^3+rx^2+a$ with $r\in\mathbb{F}_{2^m}$. We can change $v^2+uv=u^3+a$ to a standard form $E_a: y^2+xy=x^3+bx^2+a$ with some $b\in\mathbb{F}_{2^m}$. E isomorphic to E_a if and only if $Tr(r)=Tr(b)$. If E is not isomorphic to E_a, then $Tr(r)\neq Tr(b)$ and $t=a$, thus E is a quadratic twist of E_a and $\sharp E_a(\mathbb{F}_{2^m})+\sharp E(\mathbb{F}_{2^m})=2^{m+1}+2\equiv 2(\bmod 4)$. □

2.2 Second isomorphism

Let $S_t: x^2y+xy^2+txy+x+y=0$ defined over finite field $\mathbb{F}_{2^m}$, then

$$x^2y+xy^2+txy+x+y=0$$

is isomorphic to Weierstrass elliptic curve

$$v^2+uv=u^3+\frac{1}{t^8}$$

over $\mathbb{F}_{2^m}$ via the change of variables $\varphi(x,y)=(u,v)$, where

$$u=\frac{x+y}{t^2(x+y+txy)},\ v=\frac{x+y+txy+t^2y}{t^4(x+y+txy)}.$$

The inverse change is $\psi(u,v)=(x,y)$, where

$$x=\frac{t^3u+t}{t^4v+1},\ y=\frac{t^3u+t}{t^4(u+v)+1}.$$

In projective coordinates, the correspondence projective transformations from

$$X^2Y+XY^2+tXYZ+XZ^2+YZ^2=0$$

to

$$V^2W+UVW=U^3+\frac{1}{t^8}W^3$$

over $\mathbb{F}_{2^m}$ is $(X,Y,Z)\mapsto(U,V,W)$ where

$$\begin{cases} U &= (X+Y)Z, \\ V &= (X+Y)Z+tXY+t^2YZ, \\ W &= t^2(XZ+YZ+tXY). \end{cases}$$

The inverse change is $(U, V, W) \mapsto (X, Y, Z)$ where

$$\begin{cases} X &= (t^3U + tW) \cdot (t^4(U + V) + W)\,, \\ Y &= (t^3U + tW) \cdot (t^4V + W)\,, \\ Z &= (t^4(U + V) + W) \cdot (t^4V + W)\,. \end{cases}$$

The above change of variables map the element $(0, 0, 1)$ on S_t to the point $(0, 1, 0)$ on Weierstrass curve.

3 The addition law

Let C be a nonsingular cubic curve defined over a field K, and let O be a point on $C(K)$. For any two points P and Q, the line through P and Q meets the cubic curve C at one more point, denoted by PQ. With a point O as zero element and the chord-tangent composition PQ we can define the group law $P + Q$ by $P + Q = O(PQ)$ on $C(K)$ making $C(K)$ into an abelian group with O as zero element and $-P = P(OO)$. If O be an inflection point then $-P = PO$ and $OO = O$.

Note that $(1, 1, 0)$ belong to the curve and is a inflection point. The third point the line through $(1, 1, 0)$ and $(1, 0, 0)$ meets the curve is $(0, 1, 0)$. The third point the line through $(1, 1, 0)$ and $(0, 1, 0)$ meets the curve is $(1, 0, 0)$. The third point the line through $(1, 1, 0)$ and $(0, 0, 1)$ meets the curve is $(0, 0, 1)$. The third point the line through $(0, 1, 0)$ and $(0, 0, 1)$ meets the curve is $(0, 1, 0)$. The third point the line through $(1, 0, 0)$ and $(0, 0, 1)$ meets the curve is $(1, 0, 0)$.

The tangent line at $(1, 0, 0)$ is $Y = 0$. The tangent line at $(0, 1, 0)$ is $X = 0$. The tangent line at $(0, 0, 1)$ is $X + Y = 0$. The tangent line at $(1, 1, 0)$ is $X + Y + tZ = 0$.

The third point the line through (x_1, y_1) and $(0, 0)$ meets the curve is $\left(\frac{x_1(t + x_1 + y_1)}{x_1 + y_1}, \frac{y_1(t + x_1 + y_1)}{x_1 + y_1}\right)$. The third point the line tangent at (x_1, y_1) meets the curve is

$$\left(\frac{t(1 + y_1^2)}{x_1^2 + y_1^2 + x_1^2y_1^2 + t^2y_1^2 + y_1^4}, \frac{t(1 + x_1^2)}{x_1^2 + y_1^2 + x_1^2y_1^2 + t^2x_1^2 + x_1^4}\right).$$

The third point the line through (x_1, y_1) and (x_2, y_2) meets the curve is (x_3, y_3) where

$$x_3 = \frac{x_1 + y_1 + x_2 + y_2 + x_1y_2(x_2 + y_2 + t) + x_2y_1(x_1 + y_1 + t)}{(y_1 + y_2)(x_1 + y_1 + x_2 + y_2)},$$

and

$$y_3 = \frac{x_1 + y_1 + x_2 + y_2 + x_1 y_2(x_1 + y_1 + t) + x_2 y_1(x_2 + y_2 + t)}{(x_1 + x_2)(x_1 + y_1 + x_2 + y_2)}.$$

3.1 $(1, 1, 0)$ as neutral element

Let $P = (x_1, y_1)$ be a finite point on $xy^2 + yx^2 + txy + x + y = 0$, then $-P = (y_1,\ x_1)$. After some algebra, we get $2P = (x_3, y_3)$ when $x_1^2 + y_1^2 + x_1^2 y_1^2 + t^2 y_1^2 + y_1^4 \neq 0$ and $x_1^2 + y_1^2 + x_1^2 y_1^2 + t^2 x_1^2 + x_1^4 \neq 0$, where

$$\begin{aligned} x_3 &= \frac{t(1 + x_1^2)}{x_1^2 + y_1^2 + x_1^2 y_1^2 + t^2 x_1^2 + x_1^4}, \\ y_3 &= \frac{t(1 + y_1^2)}{x_1^2 + y_1^2 + x_1^2 y_1^2 + t^2 y_1^2 + y_1^4}. \end{aligned} \tag{2}$$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two finite points with $P \neq Q$. Then we can get the *dedicated point addition* formula. That is, whenever defined, we get $P + Q = (x_3, y_3)$, where

$$\begin{aligned} x_3 &= \frac{x_1 + y_1 + x_2 + y_2 + x_1 y_2(x_1 + y_1 + t) + x_2 y_1(x_2 + y_2 + t)}{(x_1 + x_2)(x_1 + y_1 + x_2 + y_2)}, \\ y_3 &= \frac{x_1 + y_1 + x_2 + y_2 + x_1 y_2(x_2 + y_2 + t) + x_2 y_1(x_1 + y_1 + t)}{(y_1 + y_2)(x_1 + y_1 + x_2 + y_2)}. \end{aligned} \tag{3}$$

In the projective coordinates, the dedicated law is $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ where

$$\begin{aligned} X_3 &= (Y_1 Z_2 + Y_2 Z_1) \cdot (Z_1 Z_2^2 (X_1 + Y_1) + Z_1^2 Z_2 (X_2 + Y_2) \\ &\quad + X_1 Y_2 Z_2 (X_1 + Y_1 + t Z_1) + X_2 Y_1 Z_1 (X_2 + Y_2 + t Z_2)), \\ Y_3 &= (X_1 Z_2 + X_2 Z_1) \cdot (Z_1 Z_2^2 (X_1 + Y_1) + Z_1^2 Z_2 (X_2 + Y_2) \\ &\quad + X_1 Y_2 Z_1 (X_2 + Y_2 + t Z_2) + X_2 Y_1 Z_2 (X_1 + Y_1 + t Z_1)), \\ Z_3 &= (X_1 Z_2 + X_2 Z_1)(Y_1 Z_2 + Y_2 Z_1)(X_1 Z_2 + Y_1 Z_2 + X_2 Z_1 + Y_2 Z_1). \end{aligned} \tag{4}$$

We can delete t from the above dedicated addition formula and get the following dedicated addition formula independence of the curve parameters.

$$
\begin{aligned}
x_3 &= \frac{(y_1+y_2)(y_1x_2+y_2x_1)}{y_1y_2(x_1+x_2)(x_1+y_1+x_2+y_2)},\\
y_3 &= \frac{(x_1+x_2)(y_1x_2+y_2x_1)}{x_1x_2(y_1+y_2)(x_1+y_1+x_2+y_2)}.
\end{aligned} \tag{5}
$$

Note that $(y_1+y_2)(y_1x_2+y_2x_1) = y_1y_2(x_1+x_2)+x_2y_1^2+x_1y_2^2$, $(x_1+x_2)(y_1x_2+y_2x_1) = x_1x_2(y_1+y_2)+x_1^2y_2+x_2^2y_1$, and $(y_1+y_2)(y_1x_2+y_2x_1)+(x_1+x_2)(y_1x_2+y_2x_1) = (x_1y_2+x_2y_1)(x_1+y_1+x_2+y_2)$.

The addition law for points $P=(X:Y:Z)$ with $XYZ=0$ are given by the following formulae.

$$
\begin{aligned}
-(0,1,0) &= (1,0,0),\\
-(1,0,0) &= (0,1,0),\\
-(0,0,1) &= (0,0,1),\\
2(0,1,0) &= (0,0,1),\\
2(1,0,0) &= (0,0,1),\\
2(0,0,1) &= (1,1,0).
\end{aligned}
$$

$$
\begin{aligned}
(0,1,0)+(1,0,0) &= (1,1,0),\\
(0,1,0)+(0,0,1) &= (0,1,0),\\
(1,0,0)+(0,0,1) &= (1,0,0),\\
(1,1,0)+(1,0,0) &= (1,0,0),\\
(1,1,0)+(0,1,0) &= (0,1,0),\\
(1,1,0)+(0,0,1) &= (0,0,1).
\end{aligned}
$$

Note that if (x_1,y_1) on $x^2y+xy^2+txy+x+y=0$ then so do $(\frac{1}{x_1},y_1)$, $(x_1,\frac{1}{y_1})$, $(\frac{1}{x_1},\frac{1}{y_1})$ whenever defined. When $x_1\neq 0$, we have $(x_1,y_1)+(\frac{1}{x_1},y_1) = (0,1,0)$. When $y_1\neq 0$, we have $(x_1,y_1)+(x_1,\frac{1}{y_1}) = (1,0,0)$.

When $P=(x_1,y_1)$ is finite and Q is at infinity or $(0,0,1)$, whenever defined, we have

$$
\left\{
\begin{aligned}
(x_1,y_1)+(1,0,0) &= (y_1,\frac{1}{x_1}),\\
(x_1,y_1)+(0,1,0) &= (\frac{1}{y_1},x_1),\\
(x_1,y_1)+(0,0,1) &= (\frac{x_1y_1+ty_1}{x_1},x_1+t).
\end{aligned}
\right.
$$

The following facts will be useful in later sections.

$$(x_1, y_1) + (\frac{1}{x_1}, \frac{1}{y_1}) = 2(y_1, \frac{1}{x_1}) = \left(\frac{(1+y_1^2)(1+x_1^2y_1^2)}{tx_1^2(1+y_1^2)}, \frac{(1+x_1^2)(1+x_1^2y_1^2)}{ty_1^2(1+x_1^2)} \right).$$

and

$$(x_1, y_1) - (\frac{1}{x_1}, \frac{1}{y_1}) = (0, 0, 1).$$

After some algebra, we can get the following *unified point addition* formula. Let $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, then

$$\begin{aligned} x_3 &= \frac{(x_1x_2 + y_1y_2)(y_1 + y_2) + ty_1y_2(1 + x_1x_2)}{(x_1x_2 + y_1y_2)(1 + y_1y_2)}, \\ y_3 &= \frac{(x_1x_2 + y_1y_2)(x_1 + x_2) + tx_1x_2(1 + y_1y_2)}{(x_1x_2 + y_1y_2)(1 + x_1x_2)}. \end{aligned} \quad (6)$$

In the projective coordinates, the unified law is $(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$ where

$$\begin{aligned} X_3 &= (X_1X_2 + Z_1Z_2) \cdot ((X_1X_2 + Y_1Y_2)(Y_1Z_2 + Y_2Z_1) + tY_1Y_2(Z_1Z_2 + X_1X_2)), \\ Y_3 &= (Y_1Y_2 + Z_1Z_2) \cdot ((X_1X_2 + Y_1Y_2)(X_1Z_2 + X_2Z_1) + tX_1X_2(Z_1Z_2 + Y_1Y_2)), \\ Z_3 &= (X_1X_2 + Y_1Y_2)(X_1X_2 + Z_1Z_2)(Y_1Y_2 + Z_1Z_2). \end{aligned} \quad (7)$$

We can prove that the addition law corresponds to the usual addition law on an elliptic curve in Weierstrass form. That is, fix $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in S_t(K)$. Assume that $(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$. Then $\varphi(x_1, y_1)+\varphi(x_2, y_2) = \varphi(x_3, y_3)$. A lengthy but straightforward calculation can show it, here is the corresponding Sage script:
Sage scrip to check $P + Q = R$.

```
R.<t,x1,y1,x2,y2>=GF(2)[ ]
S=R.quotient([
x1*y1^2+y1*x1^2+t*x1*y1+x1+y1),
x2*y2^2+y2*x2^2+t*x2*y2+x2+y2),
```

```
])
x3=(
x1*x2*(y1+y2)+y1*y2*(t+y1+y2)+t*(x1*y1*x2*y2)
)/(x1*x2+y1*y2+y1^2*y2^2+x1*y1*x2*y2)
y3=(
y1*y2*(x1+x2)+x1*x2*(t+x1+x2)+(a+b)*(x1*y1*x2*y2)
)/(x1*x2+y1*y2+x1^2*x2^2+x1*y1*x2*y2)
u1=(x1+y1)/(t^2*(x1+y1+t))
v1=(x1+y1+t^2*x1+t)/(t^4*(x1+y1+t))
u2=(x2+y2)/(t^2*(x2+y2+t))
v2=(x2+y2+t^2*x2+a+b)/(t^4*(x2+y2+t))
u3=(x3+y3)/(t^3*(x3+y3+t))
v3=(x3+y3+t^3*x3+t)/(t^4*(x3+y3+t))
lam=(v1+v2)/(u1+u2)
u4=lam^2+lam=u1+u2
v4=v1+lam*(u1+u4)+u4
0==S(numerator(u3-u4))
0==S(numerator(v3-v4))
```

Completeness of the addition law
Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, the addition law is defined when the denominators $(x_1x_2 + y_1y_2)(1 + y_1y_2)$ and $(x_1x_2 + y_1y_2)(1 + x_1x_2)$ are non-zero.

If $1+y_1y_2 = 0$, then $y_2 = \frac{1}{y_1}$, thus $Q \in \{(x_1, \frac{1}{y_1}), (\frac{1}{x_1}, \frac{1}{y_1})\}$. If $1+x_1x_2 = 0$, then $x_2 = \frac{1}{x_1}$, thus $Q \in \{(\frac{1}{x_1}, y_1), (\frac{1}{x_1}, \frac{1}{y_1})\}$.

Lemma 3.1. *Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the curves S_t. If $x_1x_2 + y_1y_2 = 0$, then $Q = (\frac{1}{x_1}, \frac{1}{y_1})$ or $Q = -P$.*

Proof. If $x_1x_2 + y_1y_2 = 0$ then $x_1x_2 = y_1y_2$. If $x_1x_2 = y_1y_2 = 1$, then $Q = (\frac{1}{x_1}, \frac{1}{y_1})$. If $x_1x_2 = y_1y_2 = a \neq 0, 1$, then $x_2 = a/x_1, y_2 = a/y_1$. Since $x_1^2y_1 + x_1y_1^2 + tx_1y_1 + x_1 + y_1 = 0$, thus

$$\frac{1}{x_1^2y_1} + \frac{1}{x_1y_1^2} + \frac{t}{x_1y_1} + \frac{1}{x_1} + \frac{1}{y_1} = 0$$

and

$$\frac{a^2}{x_1^2y_1} + \frac{a^2}{x_1y_1^2} + \frac{ta}{x_1y_1} + \frac{1}{x_1} + \frac{1}{y_1} = 0.$$

Therefore,

$$\frac{1}{x_1^2y_1} + \frac{a^2}{x_1^2y_1} + \frac{1}{x_1y_1^2} + \frac{a^2}{x_1y_1^2} + \frac{t}{x_1y_1} + \frac{ta}{x_1y_1} = 0.$$

Thus $x_1 + a^2x_1 + y_1 + a^2y_1 + tx_1y_1 + tax_1y_1 = 0$ and

$$x_1 + y_1 = \frac{tx_1y_1}{1+a}.$$

Since $x_1 + y_1 = \dfrac{tx_1y_1}{x_1y_1+1}$, therefore, $x_1y_1 = a$. From $x_1x_2 = y_1y_2 = a$ and $x_1y_1 = a$, we get $x_2 = y_1$ and $y_2 = x_1$, that is $Q = -P$. □

Note that $P = (x_1, y_1)$ and $Q \in \{(\frac{1}{x_1}, y_1), (x_1, \frac{1}{y_1}), (\frac{1}{x_1}, \frac{1}{y_1})\}$, then $P+Q = (0,1,0)$, $P+Q = (1,0,0)$ or $P-Q = (0,0,1)$. Therefore, we have the following theorem.

Theorem 3.2. *Let elliptic curve* $S_t : x^2y+xy^2+txy+x+y = 0$ *defined over* $\mathbb{F}_{2^m}$ *and let* $G \subset S_t(\mathbb{F}_{2^m})$ *be a subgroup that does not contain points* $(0,1,0)$, $(1,0,0)$ *or* $(0,0,1)$. *Then the unified addition formulae is complete.*

In particular, the addition formula is complete in a subgroup of odd order, since $(0,1,0)$, $(1,0,0)$ and $(0,0,1)$ are all of even order.

3.2 $(0,0,1)$ as neutral element

Let $P = (x_1, y_1)$ on $x^2y + xy^2 + txy + x + y = 0$, then $-P = (y_1,\ x_1)$.

After some algebra, we get $2P = (x_3, y_3)$ when $1+y_1^2 \neq 0$ and $1+x_1^2 \neq 0$, where

$$\begin{aligned} x_3 &= \frac{x_1^2 + y_1^2 + x_1^2y_1^2 + t^2x_1^2 + x_1^4}{t(1+x_1^2)}, \\ y_3 &= \frac{x_1^2 + y_1^2 + x_1^2y_1^2 + t^2y_1^2 + y_1^4}{t(1+y_1^2)}. \end{aligned} \tag{8}$$

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two finite points with $P \neq Q$. Then we can get the *dedicated point addition* formula, whenever defined,

$P+Q=(x_3,y_3)$, where where

$$\begin{aligned} x_3 &= \frac{(x_1+x_2)(x_1+y_1+x_2+y_2)}{x_1+y_1+x_2+y_2+x_1y_2(x_1+y_1+t)+x_2y_1(x_2+y_2+t)}, \\ y_3 &= \frac{(y_1+y_2)(x_1+y_1+x_2+y_2)}{x_1+y_1+x_2+y_2+x_1y_2(x_2+y_2+t)+x_2y_1(x_1+y_1+t)}. \end{aligned} \tag{9}$$

Similarly, then unified group law is defined as

$$\begin{aligned} x_3 &= \frac{(x_1x_2+y_1y_2)(1+y_1y_2)}{(x_1x_2+y_1y_2)(y_1+y_2)+ty_1y_2(1+x_1x_2)}, \\ y_3 &= \frac{(x_1x_2+y_1y_2)(1+x_1x_2)}{(x_1x_2+y_1y_2)(x_1+x_2)+tx_1x_2(1+y_1y_2)}. \end{aligned} \tag{10}$$

The addition law for points $P=(X:Y:Z)$ with $XYZ=0$ are given by the following formulae.

$$\begin{aligned} -(0,1,0) &= (0,1,0), \\ -(1,0,0) &= (1,0,0), \\ -(1,1,0) &= (1,1,0), \\ 2(0,1,0) &= (1,1,0), \\ 2(1,0,0) &= (1,1,0), \\ 2(1,1,0) &= (0,0,1). \end{aligned}$$

$$\begin{aligned} (0,1,0)+(1,0,0) &= (0,0,1), \\ (0,1,0)+(0,0,1) &= (0,1,0), \\ (1,0,0)+(0,0,1) &= (1,0,0), \\ (1,1,0)+(1,0,0) &= (0,1,0), \\ (1,1,0)+(0,1,0) &= (1,0,0), \\ (1,1,0)+(0,0,1) &= (0,0,1). \end{aligned}$$

Note that if (x_1,y_1) on $x^2y+xy^2+txy+x+y=0$ then so do $(\frac{1}{x_1},y_1)$, $(x_1,\frac{1}{y_1})$, $(\frac{1}{x_1},\frac{1}{y_1})$ whenever defined. When $x_1\neq 0$, we have $(x_1,y_1)+(\frac{1}{x_1},y_1)=(1,0,0)$. When $y_1\neq 0$, we have $(x_1,y_1)+(x_1,\frac{1}{y_1})=(0,1,0)$.

When $P=(x_1,y_1)$ is finite and Q is at infinity whenever defined, we have

$$\begin{cases} (x_1,y_1)+(1,0,0) &= \left(\dfrac{1+tx_1+x_1y_1}{x_1(1+x_1y_1)}, \dfrac{y_1(1+tx_1+x_1y_1)}{1+x_1y_1}\right), \\ (x_1,y_1)+(0,1,0) &= \left(\dfrac{x_1(1+ty_1+x_1y_1)}{1+x_1y_1}, \dfrac{1+ty_1+x_1y_1}{y_1(1+x_1y_1)}\right), \\ (x_1,y_1)+(1,1,0) &= \left(\dfrac{y_1(t+x_1+y_1)}{x_1+y_1}, \dfrac{x_1(t+x_1+y_1)}{x_1+y_1}\right), \end{cases}$$

$$(\frac{1}{x_1},\frac{1}{y_1}) = (0,1,0)+(y_1,\frac{1}{x_1}) = \left(\frac{y_1(t+x_1+y_1)}{x_1+y_1}, \frac{x_1(t+x_1+y_1)}{x_1+y_1}\right).$$

The projective coordinates law is

$$(X_3:Y_3:Z_3) = (X_1:Y_1:Z_1)+(X_2:Y_2:Z_2)$$

where

$$\begin{aligned} X_3 &= (Y_1Y_2+Z_1Z_2)(X_1X_2+Y_1Y_2) \\ &\quad \cdot((X_1X_2+Y_1Y_2)(X_1Z_2+X_2Z_1)+tX_1X_2(Z_1Z_2+Y_1Y_2)), \\ Y_3 &= (X_1X_2+Z_1Z_2)(X_1X_2+Y_1Y_2) \\ &\quad \cdot((X_1X_2+Y_1Y_2)(Y_1Z_2+Y_2Z_1)+tY_1Y_2(Z_1Z_2+X_1X_2)), \\ Z_3 &= ((X_1X_2+Y_1Y_2)(X_1Z_2+X_2Z_1)+tX_1X_2(Z_1Z_2+Y_1Y_2)) \\ &\quad \cdot((X_1X_2+Y_1Y_2)(Y_1Z_2+Y_2Z_1)+tY_1Y_2(Z_1Z_2+X_1X_2)). \end{aligned}$$

An inverted Edwards coordinates were introduced by Bernstein and Lange in [3]. For a point We use three coordinates $(X_1:Y_1:Z_1)$ on Edwards curve $x^2+y^2=1+dx^2y^2$, where $(X_1^2+Y_1^2)Z_1^2 = X_1^2+Y_1^2+dZ_1^4$ and $X_1Y_1Z_1\neq 0$, to represent the point $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve, they refer to these coordinates as inverted Edwards coordinates. It is easy to convert from standard Edwards coordinates $(X_1:Y_1:Z_1)$ to inverted Edwards coordinates, simply compute $(Y_1Z_1:X_1Z_1:X_1Y_1)$ with three multiplications. The same computation also performs the opposite conversion from inverted Edwards coordinates to standard Edwards coordinates. Using the inverted projective coordinates on $S_t: x^2y+xy^2+txy+x+y=0$, the point $(1,1,0)$ correspondence to $(0,0,1)$, and the group law use $(1,1,0)$ as neutral element correspondence to group law use $(0,0,1)$ as neutral element.

4 Explicit addition formulae

This section presents explicit formulae for affine addition, projective addition, and mixed addition on S_t curves.

4.1 $(1, 1, 0)$ as neutral element

Affine addition. The following formulae, given (x_1, y_1) and (x_2, y_2) on the curve $S_t : x^2y + xy^2 + txy + x + y = 0$, use formula (3) compute the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ if it is defined:

$$\begin{aligned}
&w_1 = x_1 + y_1 + t,\ w_2 = x_2 + y_2 + t,\ A = x_1y_2,\ B = x_2y_1,\\
&C = A \cdot w_1,\ D = B \cdot w_2,\ E = (A + B) \cdot (w_1 + w_2) + C + D,\\
&F = (x_1 + x_2) \cdot (y_1 + y_2),\ G = (x_1 + x_2)^2 + F,\ H = (y_1 + y_2)^2 + F\\
&x_3 = (w_1 + w_2 + C + D)/G,\ y_3 = (w_1 + w_2 + E)/H.
\end{aligned}$$

These formulae cost $2I + 8M + 2S$, where I is the cost of a field inversion, M is the cost of a field multiplication, S is the cost of a field squaring. We will use D denote the cost of a field squaring and of a multiplication by a curve parameter. One can replace $2I$ with $1I + 3M$ using Montgomery's inversion trick, then the affine addition use $1I + 11M$. Note that the cost of additions and squarings in $\mathbb{F}_{2^m}$ can be neglected.

The following algorithm use formula (6) compute the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ if it is defined:

$$\begin{aligned}
&A = x_1 \cdot x_2,\ B = y_1 \cdot y_2,\ C = (A + B) \cdot (y_1 + y_2),\ D = (A + B) \cdot (x_1 + x_2),\\
&E = A \cdot B,\ F = B + E,\ G = A + E,\ H = A + B + E + B^2,\\
&J = A + B + E + A^2,\ x_3 = (C + tF)/H,\ y_3 = (D + tG)/J.
\end{aligned}$$

These formulae cost $2I + 7M + 2D + 2S$ or $1I + 10M + 2D + 2S$, The $2D$ here are two multiplications by t.

Projective addition. The following formulas, given $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ on the curve S_t, use formula (4) compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ if it is defined:

$$
\begin{aligned}
&A = X_1 \cdot Z_2,\ B = X_2 \cdot Z_1,\ C = Y_1 \cdot Z_2,\ D = Y_2 \cdot Z_1,\ E = Z_1 \cdot Z_2,\\
&F = X_1 \cdot Y_2,\ G = X_2 Y_1,\ H = E(A+B+C+D),\ J = F(A+C+tE),\\
&K = G(B+D+tE),\ L = (F+G)\cdot(A+B+C+D)+J+K,\\
&X_3 = (C+D)\cdot(H+J+K),\ Y_3 = (A+B)\cdot(H+L),\\
&Z_3 = (A+B)\cdot(C+D)\cdot(A+B+C+D).
\end{aligned}
$$

These formulae cost $15M + D$. The D here is one multiplication by t.

The following algorithm use unified formula (7) compute the sum $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$ if it is defined:

$$
\begin{aligned}
&A = X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\\
&D = (X_1 + Z_1)\cdot(X_2 + Z_2) + A + C,\\
&E = (Y_1 + Z_1)\cdot(Y_2 + Z_2) + B + C,\\
&X_3 = (A+C)\cdot((A+B)\cdot E + tB\cdot(A+C)),\\
&Y_3 = (B+C)\cdot((A+B)\cdot D + tA\cdot(B+C)),\\
&Z_3 = (A+B)\cdot(A+C)\cdot(B+C).
\end{aligned}
$$

These formulae cost $13M+2D$. The $2D$ here are two multiplications by t.

Since the squarings in $\mathbb{F}_{2^m}$ can be neglected, so we have the following algorithm,

$$
\begin{aligned}
&A = X_1 \cdot X_2,\ B = Y_1 \cdot Y_2,\ C = Z_1 \cdot Z_2,\\
&D = (X_1 + Z_1)\cdot(X_2 + Z_2) + A + C,\\
&E = (Y_1 + Z_1)\cdot(Y_2 + Z_2) + B + C,\\
&F = (A+C)^2,\ G = (B+C)^2,\ H = A\cdot(B+C),\\
&I = B\cdot C,\ J = A^2,\ K = B^2,\\
&X_3 = (J+H+I)\cdot E + tB\cdot F,\\
&Y_3 = (H+K+I)\cdot D + tA\cdot G,\\
&Z_3 = (J+H+I)\cdot(B+C).
\end{aligned}
$$

These formulae cost $12M+4S+2D$. The $2D$ here are two multiplications by t.

Mixed addition. Mixed addition is compute $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (x_2, y_2)$ given $(X_1 : Y_1 : Z_1)$ and (x_2, y_2) on the curve S_t. From projective addition algorithm use formula (4) we can get the mixed addition can be computed use $12M + D$ since $Z_2 = 1$. However, use formula (7) compute mixed addition cost $11M + 2D$.

Comparison with previous work The following comparison shows that our addition formulae are more efficient than binary Edwards curve and Weierstrass curves.

The projective addition formulae of binary Edwards curves in [4] use $21M+1S+4D$, or $18M+2S+7D$ when the curve parameters are small. The fastest formulae cost $16M + 1S + 4D$ when the parameters $d_1 = d_2$ of binary Edwards curves. The best operation counts is $14M + 1S$ for Weierstrass curves with projective coordinates reported in Explicit-Formulars Database of [1]. Therefore, our formulae are more faster than the formulae in literature.

4.2 $(0, 0, 1)$ as neutral element

The similarly analysis can be done as use $(1, 1, 0)$ as neutral element, but here we neglect the details.

5 Doubling

This section presents fast doubling formulae on S_t in affine coordinates and projective coordinates.

Affine doubling. Let (x_1, y_1) be a point on S_t, and assume that the sum $2(x_1, y_1)$ is defined. From unified formula (6) with $(1, 1, 0)$ as neutral element, we get

$$2(x_1, y_1) = \left(\frac{ty_1^2(1 + x_1)^2}{(x_1^2 + y_1^2)(1 + y_1^2)}, \frac{tx_1^2(1 + y_1)^2}{(x_1^2 + y_1^2)(1 + x_1^2)} \right).$$

Note that $(x_1 + y_1)(1 + x_1)(1 + y_1) = x_1(1 + y_1^2) + y_1(1 + x_1)^2 + x_1^2 + y_1^2$, we have the following algorithm to compute $2P$:

$$A = y_1 \cdot (1 + x_1^2),\ B = x_1 \cdot (1 + y_1^2),\ D = (A + B + x_1^2 + y_1^2)^{-1},$$
$$E = tD^2,\ x_3 = E \cdot A^2,\ y_3 = E \cdot B^2.$$

These formulae cost $1I+4M+5S+D$. The $1D$ here is one multiplication by t.

From the formula (8) with $(0,0,1)$ as neutral element,

$$2(x_1,y_1) = \left(\frac{x_1^2+y_1^2+x_1^2y_1^2+t^2x_1^2+x_1^4}{t(1+x_1^2)}, \frac{x_1^2+y_1^2+x_1^2y_1^2+t^2y_1^2+y_1^4}{t(1+y_1^2)} \right).$$

We can divide $\frac{x_1^2+y_1^2+x_1^2y_1^2+t^2y_1^2+y_1^4}{t(1+y_1^2)}$ as $\frac{1}{t}(x_1+y_1+\frac{ty_1}{1+y})^2$, therefore

$$2(x_1,y_1) = \left(\frac{1}{t}(x_1+y_1+\frac{tx_1}{1+x_1})^2, \frac{1}{t}(x_1+y_1+\frac{ty_1}{1+y_1})^2 \right).$$

Note that $y_1(1+x_1) = y_1+x_1y_1, x_1(1+y_1) = x_1+x_1y_1$ and $(1+x_1)(1+y_1) = 1+x_1+y_1+x_1y_1$, we have the following algorithm to compute $2P$:

$$\begin{array}{l} A = x_1+y_1,\ B = x_1y_1,\ D = t(1+x_1+y_1+B)^{-1}, \\ x_3 = (A+(x_1+B)\cdot D)^2/t,\ y_3 = (A+(y_1+B)\cdot D)^2/t. \end{array}$$

These formulae cost $1I+3M+2S+3D$. The $3D$ here are three multiplications by t and $1/t$ twice. Julio López in [14] pointed out the following algorithm with cost $1I+3M+2S+2D$ by using $\sqrt{t}$. The same optimization applied in the first doubling formula by introduce the variable $E = tD^2$ is also due to Julio López. The $2D$ here are two multiplications by $\sqrt{t}$ and $1/\sqrt{t}$.

$$\begin{array}{l} A = x_1+y_1,\ B = x_1y_1,\ D = \sqrt{t}(1+x_1+y_1+B)^{-1}, \\ E = A/\sqrt{t},\ x_3 = (E+(x_1+B)\cdot D)^2,\ y_3 = (E+(y_1+B)\cdot D)^2. \end{array}$$

Projective doubling. Let $P = (X_1,Y_1,Z_1)$ and $2P = (X_3,Y_3,Z_3)$, From unified formula (6) with $(1,1,0)$ as neutral element, we get

$$\begin{array}{rcl} 2P &=& (tY_1^2(X_1^2+Z_1^2)^2, tX_1^2(Y_1^2+Z_1^2)^2, (X_1^2+Y_1^2)(X_1^2+Z_1^2)(Y_1^2+Z_1^2)) \\ &=& (Y_1^2(X_1^2+Z_1^2)^2, X_1^2(Y_1^2+Z_1^2)^2, (1/t)(X_1^2+Y_1^2)(X_1^2+Z_1^2)(Y_1^2+Z_1^2)). \end{array}$$

Note that

$$(X_1^2+Y_1^2)(X_1^2+Z_1^2)(Y_1^2+Z_1^2) = \left(Y_1(X_1^2+Z_1^2)+X_1(Y_1^2+Z_1^2)+Z_1(X_1^2+Y_1^2)\right)^2,$$

so we have the following algorithm

$$\begin{array}{l} A = X_1^2,\ B = Y_1^2,\ C = Z_1^2,\ D = Y_1\cdot(A+C),\ E = X_1\cdot(B+C) \\ X_3 = D^2,\ Y_3 = E^2,\ Z_3 = (1/t)(D+E+Z_1\cdot(A+B)). \end{array}$$

These formulae cost $3M + 3S + 1D$. The $1D$ here is one multiplications by $1/t$.

Comparison with previous work The following comparison shows that our doubling formulae are competitive to binary Edwards curve and Weierstrass curves.

The best projective doubling formulae on binary Edwards curves in [4] use $2M + 6S + 3D$, or $2M + 5S + 2D$ when the curve parameters $d_1 = d_2$. But in general for random curve the cost become $4M + 6S$. According to a summary in [4], The fastest inversion-free doubling formulae in Lápez-Dahab coordinates cost $4M + 4S + 1D$ introduced by Lange in [9]. In [8] Kim and Kim present doubling formulae for curves of the form $v^2 + uv = u^3 + u^2 + a_6$ needing $2M+5S+2D$. Using the extended coordinates, the improve doubling formula take $2M + 4S + 2D$ in [4]. Our projective doubling formulae cost $3M + 3S + 1D$ for general curve parameters, them are slightly slower than binary Edwards curves or Weierstrass curves. But for random curves, take $1D = 1M$ then our formulae are have more advantages.

6 Differential addition

This section presents fast explicit formulas for w-coordinate differential addition on binary curves $S_t : x^2y+xy^2+txy+x+y = 0$. We define w-function in two ways. Here $w(P) = x + y$ for $P = (x, y)$, and $\tilde{w}(P) = xy$. Note that $w(-P) = w(P)$ and $\tilde{w}(-P) = \tilde{w}(P)$, since $-(x, y) = (y, x)$. We propose explicit cost of differential addition and double for $\tilde{w}$-coordinates, and neglect the details for w-coordinates.

Differential addition means computing $Q + P$ given $P, Q, Q - P$ or computing $2P$ given P. A generally differential point addition consists in calculating $w(P + Q)$ from $w(P)$, $w(Q)$ and $w(Q - P)$ for some coordinate function w. Montgomery in [16] developed a method, called Montgomery ladder, allowing faster scalar multiplication than usual methods. Montgomery presented fast formulae for u-coordinate differential addition on non-binary elliptic curves $v^2 = u^3 + a_2u^2 + u$. The Montgomery ladder can fast compute $u(mP), u((m + 1)P)$ given $u(P)$, and is one of most important methods to compute scalar multiplication. Bernstein et al. [4] used the idea of Montgomery ladder present fast w-coordinate differential addition on binary Edwards curves.

More concretely, write $Q-P=(x_1,y_1)$, $P=(x_2,y_2)$, $Q=(x_3,y_3)$, $2P=(x_4,y_4)$ and $Q+P=(x_5,y_5)$. We will presents fast explicit formulae to compute $w(P+Q)$ and $w(2P)$ given $w(P), w(Q)$ and $w(Q-P)$, and presents fast explicit formulae to compute $\tilde{w}(P+Q)$ and $\tilde{w}(2P)$ given $\tilde{w}(P), \tilde{w}(Q)$ and $\tilde{w}(Q-P)$. Write $w_i = x_i + y_i$ and $\tilde{w}_i = x_i y_i$ for $i = 0,1,2,3,4$.

6.1 $(1,1,0)$ as neutral element

Since the doubling formula is

$$2P = 2(x,y) = \left(\frac{ty^2(1+x^2)}{(x^2+y^2)(1+y^2)}, \frac{tx^2(1+y^2)}{(x^2+y^2)(1+x^2)}\right).$$

Let $w_1 = w(P)$, then $w(2P) = \dfrac{t(1+x^2y^2)}{(1+x^2)(1+y^2)}$. Note that $xy = \dfrac{x+y}{x+y+a+b}$, thus

$$w_4 = w(2P) = \frac{t^3}{t^2 + t^2 w_2^2 + w_2^4}.$$

Similarly, we have

$$\tilde{w}_4 = \frac{1+\tilde{w}_2^4}{t^2\tilde{w}_2^2}.$$

By a lengthy but straightforward calculation, we can get, when defined,

$$\begin{aligned} w_1 + w_5 &= t + \frac{t^3}{t^2 + w_2 w_3 (t+w_2)(t+w_3)}, \\ w_1 w_5 &= \frac{t^2(w_2+w_3+t)^2}{t^2 + w_2 w_3 (t+w_2)(t+w_3)}. \end{aligned}$$

and

$$\begin{aligned} \tilde{w}_1 + \tilde{w}_5 &= \frac{t^2 \tilde{w}_2 \tilde{w}_3}{\tilde{w}_2^2 + \tilde{w}_3^2}, \\ \tilde{w}_1 \tilde{w}_5 &= \frac{1+\tilde{w}_2^2\tilde{w}_3^2}{\tilde{w}_2^2 + \tilde{w}_3^2}. \end{aligned}$$

Cost of affine $\tilde{w}$-coordinate differential addition and doubling. The explicit formulae

$$A=\tilde{w}_2^2,\ B=\tilde{w}_3^2,\ C=\tilde{w}_2\tilde{w}_3,\ D=(A+B)^{-1}$$
$$\tilde{w}_5=\tilde{w}_1+t^2C\cdot D.$$

use $1I+2M+2S+1D$, where the $1D$ is a multiplication by t^2.
Doubling: The explicit formulae

$$A=\tilde{w}_2^2,\ B=A^2,\ C=t^2A,\ D=C^{-1}$$
$$\tilde{w}_4=(1+B)\cdot D.$$

use $1I+1M+2S+1D$, where the $1D$ is a multiplication by t^2.

Cost of projective $\tilde{w}$-coordinate differential addition and doubling. Assume that $\tilde{w}_1,\tilde{w}_2,\tilde{w}_3$ are given as fractions $\tilde{W}_1/Z_1,\tilde{W}_2/Z_2,\tilde{W}_3/Z_3$ and that $\tilde{W}_4,\tilde{W}_5$ are to be output as fractions $\tilde{W}_4/Z_4,\tilde{W}_5/Z_5$.

The explicit addition formulae

$$A=\tilde{W}_2\cdot Z_3,\ B=\tilde{W}_3\cdot Z_2,\ C=(A+B)^2,$$
$$\tilde{W}_5=t^2Z_1\cdot A\cdot B+\tilde{W}_1\cdot C,\ Z_5=Z_1\cdot C.$$

use $6M+S+1D$, where the $1D$ is a multiplication by t^2.

The explicit doubling formulae

$$A=\tilde{W}_2,\ B=A^2,\ C=Z_2^2,\ D=C^2$$
$$\tilde{W}_4=B+D,\ Z_5=t^2A\cdot C.$$

use $1M+4S+1D$, where the $1D$ is a multiplication by t^2.

Here $\tilde{w}_1\tilde{w}_5$ formulas offer an interesting alternative. For example, the explicit formulae

$$A=Z_2\cdot Z_3,\ B=\tilde{W}_2\cdot\tilde{W}_3,\ C=(A+B)^2,$$
$$D=(\tilde{W}_2+Z_2)\cdot(\tilde{W}_3+Z_3)+A+B,$$
$$\tilde{W}_5=Z_1\cdot C,\ Z_5=\tilde{W}_1\cdot D^2.$$

use $5M+2S$. If $Z_2=1$ then cost of mixed w-coordinates differential addition is $4M+2S$.

6.2 $(0,0,1)$ as neutral element

Similarly, we have the following formulae.

$$w_4=w(2P)=\frac{tw_2^2(t^2+w_2^2)}{t^2+t^2w_2^2+w_2^4},$$

and

$$\tilde{w}_4 = \frac{t^2 \tilde{w}_2^2}{1 + \tilde{w}_2^4}.$$

$$\begin{aligned} w_1 + w_5 &= t + \frac{t^3}{t^2 + w_2 w_3 (t + w_2)(t + w_3)}, \\ w_1 w_5 &= \frac{t^2 (w_2 + w_3)^2}{t^2 + w_2 w_3 (t + w_2)(t + w_3)}. \end{aligned}$$

and

$$\begin{aligned} \tilde{w}_1 + \tilde{w}_5 &= \frac{t^2 \tilde{w}_2 \tilde{w}_3}{1 + \tilde{w}_2^2 \tilde{w}_3^2}, \\ \tilde{w}_1 \tilde{w}_5 &= \frac{\tilde{w}_2^2 + \tilde{w}_3^2}{1 + \tilde{w}_2^2 \tilde{w}_3^2}. \end{aligned}$$

Cost of affine $\tilde{w}$-coordinate differential addition and doubling. The explicit formulae

$$\begin{aligned} &A = \tilde{w}_2 \tilde{w}_3,\ B = A^2,\ D = (1 + B)^{-1} \\ &\tilde{w}_5 = \tilde{w}_1 + t^2 A \cdot D. \end{aligned}$$

use $1I + 2M + S + 1D$, where the $1D$ is a multiplication by t^2.
Doubling: The explicit formulae

$$\begin{aligned} &A = \tilde{w}_2^2,\ B = A^2,\ D = (1 + B)^{-1} \\ &\tilde{w}_4 = t^2 A \cdot D. \end{aligned}$$

use $1I + 1M + 2S + 1D$, where the $1D$ is a multiplication by t^2.

Cost of projective $\tilde{w}$-coordinate differential addition and doubling. Assume that $\tilde{w}_1, \tilde{w}_2, \tilde{w}_3$ are given as fractions $\tilde{W}_1/Z_1, \tilde{W}_2/Z_2, \tilde{W}_3/Z_3$ and that $\tilde{W}_4, \tilde{W}_5$ are to be output as fractions $\tilde{W}_4/Z_4, \tilde{W}_5/Z_5$.

The explicit addition formulae

$$\begin{aligned} &A = Z_2 \cdot Z_3,\ B = \tilde{W}_2 \cdot \tilde{W}_3,\ C = (A + B)^2,\ D = A \cdot B, \\ &\tilde{W}_5 = t^2 Z_1 \cdot D + \tilde{W}_1 \cdot C,\ Z_5 = Z_1 \cdot C. \end{aligned}$$

use $6M + S + 1D$, where the $1D$ is a multiplication by t^2.

The explicit doubling formulae

$$\begin{array}{l} A = \tilde{W}_2,\ B = A^2,\ C = Z_2^2,\ D = C^2 \\ \tilde{W}_4 = t^2 A \cdot C,\ Z_5 = B + D. \end{array}$$

use $1M + 4S + 1D$, where the $1D$ is a multiplication by t^2.

Here $\tilde{w}_1\tilde{w}_5$ formulas offer an interesting alternative. The explicit formulae

$$\begin{array}{l} A = Z_2 \cdot Z_3,\ B = \tilde{W}_2 \cdot \tilde{W}_3,\ C = (A+B)^2, \\ D = (\tilde{W}_2 + Z_2) \cdot (\tilde{W}_3 + Z_3) + A + B, \\ \tilde{W}_5 = Z_1 \cdot D^2,\ Z_5 = \tilde{W}_1 \cdot C. \end{array}$$

use $5M + 2S$. If $Z_2 = 1$ then cost of mixed w-coordinates differential addition is $4M + 2S$.

7 Note on binary Huff model curve

Recently, a new model of elliptic curves named binary Huff model curves by introduced in [10] without given detailed group laws. A binary Huff curve is the set of projective points $(X : Y : Z) \in P^2(\mathbb{F}_{2^m})$ satisfying the equation

$$E : aX(Y^2 + YZ + Z^2) = bY(X^2 + XZ + Z^2)$$

where $a, b \in \mathbb{F}_{2^m}$ and $a \neq b$. The affine model corresponding to the binary Huff curve is

$$ax(y^2 + y + 1) = by(x^2 + x + 1).$$

Define $(0, 0, 1)$ as the identity element, then

$$-(x_1, y_1) = \left(\frac{y_1(b + ax_1y_1)}{a + bx_1y_1}, \frac{y_1(a + bx_1y_1)}{b + ax_1y_1} \right),$$

and the unified addition formulae are defined by(whenever defined) $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

$$\begin{array}{rcl} x_3 & = & \dfrac{b(x_1 + x_2)(1 + x_1x_2y_1y_2) + (a+b)x_1x_1(1 + y_1y_2)}{b(1 + x_1x_1)(1 + x_1x_2y_1y_2)}, \\ y_3 & = & \dfrac{a(y_1 + y_2)(1 + x_1x_2y_1y_2) + (a+b)y_1y_1(1 + x_1x_2)}{a(1 + y_1y_1)(1 + x_1x_2y_1y_2)}. \end{array}$$

But upon the completion of this paper, We know(from [12]) Julien Devigne and Marc Joye [11] have independently studied binary Huff curves not only detailed group law but also differential addition, etc.. So we don't present the detail about binary Huff curves here, all interested people should see [11] for details. The special binary curve $S_t : x^2y + xy^2 + txy + x + y = 0$ studied in this paper look similar to the variant forms of binary Huff curves. But we can not get S_t curves from binary Huff curve by simple linear transformation over $\mathbb{F}_{2^m}$ otherwise some special a, b. In a word, S_t is a symmetrical cubic shapes curves with good arithmetic. Its generalized form $S_{a,b} : (x + y) + b(x^2 + y^2) = x^2y + xy^2 + axy$ look more similar to binary Edwards curves without quartic item. Note that the group law on $S_t : x^2y + xy^2 + txy + x + y = 0$ are faster than the group law on binary Huff curves. The projective doubling and projective addition formulae in [11] need $6M + 2D$ and $15M + 2D$ respectively. But we caution the reader that the generalized binary huff curve cover all ordinary curves over binary field.

Let $H_{a,b} : ax(y^2 + y + 1) = by(x^2 + x + 1)$ defined over $\mathbb{F}_{2^m}$, then

$$ax(y^2 + y + 1) = by(x^2 + x + 1)$$

is isomorphic to elliptic curve

$$v^2 + uv = u^3 + u^2 + \frac{a^4b^4}{(a + b)^8}$$

over $\mathbb{F}_{2^m}$ via the change of variables $\varphi(x, y) = (u, v)$, where

$$\begin{aligned} u &= \frac{ab(bx + ay)}{(a + b)^2(ax + by + (a + b)xy)}, \\ v &= \frac{ab(a^2bx + a^3y + ab(a + b)xy + (a + b)^3)}{(a + b)^4(ax + by + (a + b)xy)}. \end{aligned}$$

The inverse change is $\psi(u, v) = (x, y)$, where

$$x = \frac{b(a + b)^3u + a^2b(a + b)}{(a + b)^4v + a^2b^2}, \; y = \frac{a(a + b)^3u + ab^2(a + b)}{(a + b)^4(u + v) + a^2b^2}.$$

The above change of variables map the identity element $(0, 0, 1)$ on $H_{a,b}$ to the identity element $(0, 1, 0)$ on Weierstrass curve $v^2+uv = u^3+u^2+\dfrac{a^4b^4}{(a + b)^8}$.

Note that $\mathrm{Tr}(\frac{a^4b^4}{(a+b)^8}) = 0$, Hence, binary Huff elliptic curves family $ax(y^2 + y + 1) = by(x^2 + x + 1)$ isomorphic to curves family $y^2 + xy = x^3 + x^2 + t$ over $\mathbb{F}_{2^m}$ with $\mathrm{Tr}(t) = 0$.

Therefore, the binary Huff elliptic curves $ax(y^2+y+1) = by(x^2+x+1)$ only cover half of ordinary elliptic curves form $v^2+uv = u^3+u^2+t$ over $\mathbb{F}_{2^m}$ when m is odd. The elliptic curves $S_t : x^2y + xy^2 + txy + x + y$ cover all the ordinary elliptic curves form $v^2 + uv = u^3 + t$ over $\mathbb{F}_{2^m}$ when m is odd.

Let $H_{a,b,f} : ax(y^2 + fy + 1) = by(x^2 + fx + 1)$ defined over $\mathbb{F}_{2^m}$, then

$$ax(y^2 + fy + 1) = by(x^2 + fx + 1)$$

is isomorphic to elliptic curve

$$v^2 + uv = u^3 + f^{-2}u^2 + \frac{a^4b^4}{(a+b)^8f^8}$$

over $\mathbb{F}_{2^m}$ via the change of variables $\psi(u, v) = (x, y)$, where

$$x = \frac{b(a+b)^3f^3u + a^2b(a+b)f}{(a+b)^4f^4v + a^2b^2},\ y = \frac{a(a+b)^3f^3u + ab^2(a+b)f}{(a+b)^4f^4(u+v) + a^2b^2}.$$

Note that $H_{a,b,f} : ax(y^2 + fy + 1) = by(x^2 + fx + 1)$ cover all the ordinary elliptic over $\mathbb{F}_{2^m}$ [11].

Acknowledgments

We are very grateful to Marc Joye for sending their preprint [11] to us prior to publication.

References

[1] D. J. Bernstein, and T. Lange, Explicit-formulae database. URL: http://www.hyperelliptic.org/EFD.

[2] D. J. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, ASIACRYPT 2007, LNCS 4833, 29-50, Springer, 2007.

[3] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, Twisted Edwards curves, In AFRICACRYPT 2008, LNCS 5023, 389-405, Springer, 2008.

[4] D.J. Bernstein, T. Lange, R.R. Farashahi, Binary Edwards curves, In: E. Oswald, P. Rohatgi(eds.) Cryptographic Hardware and Embedded Systems, CHES 2008. LNCS vol. 5154, 244-265, Springer, 2008.

[5] É Brier,M. Joye, Weierstrass elliptic curves and side-channel attacks, in PKC 2002, LNCS 2274, 335-345, Springer, 2002.

[6] H.M. Edwards, A normal form for elliptic curves, Bulletin of the American Math- ematical Society 44, 393-422, 2007.

[7] G. B. Huff, Diophantine problems in geometry and elliptic ternary forms. Duke Math. J., 15:443-453, 1948.

[8] K.H. Kim, S.I. Kim, A new method for speeding up arithmetic on elliptic curves over binary fields (2007). URL: http://eprint.iacr.org/2007/181.

[9] T. Lange, , A note on Lápez-Dahab coordinates, Tatra Mountains Mathematical Publications 33(2006), 75-81. MR 2007f:11139. URL: http://eprint.iacr.org/2004/323.

[10] Marc Joye, M. Tibouchi, D. Vergnaud, Huff's model for elliptic curves, Algorithmic Number Theory (ANTS-IX), LNCS vol. 6197, pp. 234-250. Springer, 2010.

[11] Julien Devigne and Marc Joye, Binary Huff Curves, To appear in Cryptographers' Track at the RSA Conference 2011 (CT-RSA 2011).

[12] Marc Joye, Personal correspondence with the author, 2010.

[13] J. López, R. Dahab, Fast multiplication on elliptic curves over GF(2^m) without precomputation. Cryptographic Hardware and Embedded Systems, CHES'99. LNCS vol. 1717, 316-327. Springer, 1999.

[14] Julio López, Personal correspondence with the author, 2010.

[15] A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[16] P.L. Montgomery, Speeding the Pollard and elliptic curve methods of factor- ization, Mathematics of Computation 48(1987), 243-264.

[17] M. Stam, On Montgomery-like representations for elliptic curves over GF(2^k), PKC 2003, LNCS vol. 2567, 240-253. Springer, 2003.

[18] W.A. Stein (ed.), Sage Mathematics Software (Version 4.6), The Sage Group, 2010, http://www.sagemath.org.

[19] J.H. Silverman, The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics, Springer-Verlag, 1986.

[20] Hongfeng Wu and Rongquan Feng, Elliptic curves in Huff's model, ePrint 2010/390, URL: http://eprint.iacr.org/2010/390.