Notes on Elliptic Curve Operation

1 Introduction

which

2 Twisted Edwards Curves

The *characteristic* of a field F is the smallest positive integer m such that

$$\underbrace{1+1+...+1}_{m}$$

denoted as $char(F) = m$ If no such m exists then the field is said to have characteristic 0. The characteristic of any field is either 0 or a prime p.

If F is a finite field of characteristic p, then the *order* of F is a prime power $q = p^r$ for some positive integer r, and we write $F = \mathbb{F}_{p^r}$ or $F = \mathbb{F}_q$.

Fix a field k with $\mathrm{char}(k) \neq 2$ [1]. Fix distinct nonzero elements $a, d \in k$. The twisted Edwards curve with coefficients a and d is the curve

$$E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

The elliptic curve has j-invariant $16(a^2 + 14ad + d^2)^3/ad(a-d)^4$.

Addition formulae. Let $(x_1, y_1), (x_2, y_2)$ be points on the twisted Edwards curve $E_{E,a,d} : ax^2 + y^2 = 1 + dx^2y^2$. The sum of these points on $E_{E,a,d}$ is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right).$$

The neutral element is $(0, 1)$, and the negative of (x_1, y_1) is $(-x_1, y_1)$.

Doubling formulae. Doublinh can be performed with exactly the same formula as addition. Doublong of a point (x_1, y_1) on the curve $E_{E,a,d}$ is:

$$(x_3, y_3) = \left(\frac{2x_1y_1}{ax_1^2 + y_1^2}, \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2}\right)$$

[1] The *characteristic* of a field is the smallest positive integer m such that $\underbrace{1+1+...+1}_{m} = 0$

3 Projective Twisted Edwards Coordinates

According to Bernstein et al.[**?**], we can work on the projective twisted Edwards curve to avoid inversions.

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2.$$

For $Z_1 \neq 0$ the homogeneous point $(X_1 : Y_1 : Z_1)$ represents the affine point $(X_1/Z_1, Y_1/Z_1)$ on $E_{E,a,d}$.

Addition in Projective Twisted Coordinates. The following formulas compute $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1)+(X_2 : Y_2 : Z_2)$ in $9M+1S+2D+7add$, where the 2D are one multiplication by a and one by d:

$$\begin{aligned}
A &= Z_1 \cdot Z_2;\\
B &= dA^2;\\
C &= X_1 \cdot X_2;\\
D &= Y_1 \cdot Y_2;\\
E &= C \cdot D;\\
H &= C - aD;\\
I &= (X_1 + Y_1) \cdot (X_2 + Y_2) - C - D;\\
X_3 &= (E + B) \cdot H;\\
Y_3 &= (E - B) \cdot I;\\
Z_3 &= A \cdot H \cdot I.
\end{aligned}$$

Doubling in Projective Twisted Coordinates. The following formulas compute $(X_3 : Y_3 : Z_3) = 2(X_1 : Y_1 : Z_1)$ in $3M + 4S + 2D + 6add$, where the 2D are pme multiplication by a and one by $2d$:

$$\begin{aligned}
A &= X_1^2;\\
B &= Y_1^2; U = aB;\\
C &= A + U;\\
D &= A - U;\\
E &= (X_1 + Y_1)^2 - A - B;\\
X_3 &= C \cdot D;\\
Y_3 &= E \cdot (C - 2dZ_1^2);\\
Z_3 &= D \cdot E
\end{aligned}$$

4 JubJub

Jubjub is a twisted Edwards curve of the form

$$-x^2 + y^2 = 1 + dx^2y^2$$

built over the BLS12-381 scalar field, with $d = -\frac{10240}{10241}$. It has a complete addition law that avoids edge cases with doubling and identities, making it convenient to work with inside of an arithmetic circuit.

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 + x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$