Binary Edwards Curves

Reza Rezaeian Farashahi

Dept. of Mathematics and Computing Science
TU Eindhoven

joint work with:
Dan Bernstein (University of Illinois at Chicago) and Tanja Lange (TU Eindhoven)

ECC, Sep 24, 2008

Edwards curves

- Edwards generalized single example $x^2 + y^2 = 1 - x^2y^2$ by Euler/Gauss to whole class of curves.
- He showed that– after some field extensions – every elliptic curve over a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$ is birationally equivalent to one in the form

$$\mathrm{E}_c: \ x^2 + y^2 = c^2(1 + x^2y^2),$$

  where $c \in \mathbb{F}$, $c^5 \neq c$.
- The simple addition law on this form is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)} \right).$$

- Bernstein and Lange generalized to the form

$$\mathrm{E}_d: \ x^2 + y^2 = 1 + dx^2y^2,$$

  where $d \neq 0$, $d^4 \neq 1$.
- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.

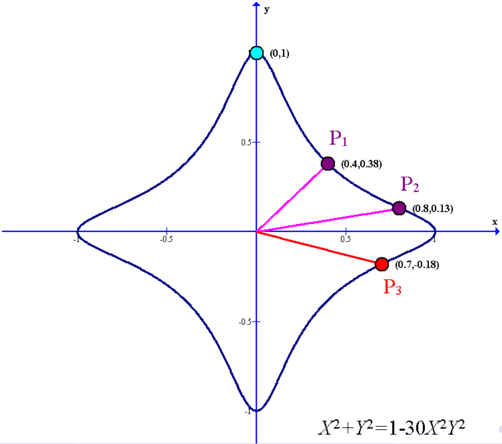
Edwards curves

- Edwards generalized single example $x^2 + y^2 = 1 - x^2y^2$ by Euler/Gauss to whole class of curves.
- He showed that– after some field extensions – every elliptic curve over a field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$ is birationally equivalent to one in the form
$$\mathrm{E}_c : \ x^2 + y^2 = c^2(1 + x^2y^2),$$
where $c \in \mathbb{F}$, $c^5 \neq c$.
- The simple addition law on this form is given by
$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{c(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{c(1 - x_1x_2y_1y_2)} \right).$$
- Bernstein and Lange generalized to the form
$$\mathrm{E}_d : \ x^2 + y^2 = 1 + dx^2y^2,$$
where $d \neq 0$, $d^4 \neq 1$.
- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.

Edwards curves

- The addition law on $\mathrm{E}_d: \; x^2 + y^2 = 1 + dx^2y^2$ is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$



Properties of Edwards curves

- Neutral element is $(0,1)$; this is an affine point.
- $-(x_1, y_1) = (-x_1, y_1)$.
- $(0,-1)$ has order 2; $(1,0)$ and $(-1,0)$ have order 4.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Very fast point addition 10M + 1S + 1D. (Even faster with Inverted Edwards coordinates.)
- Dedicated doubling formulas need only 3M + 4S.

Complete addition law

- If d is not a square the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- No exceptional points, completely uniform group operations.
- The set of curves with complete addition law is not complete!
- We need Edwards curve in characteristic 2!
- Even characteristic much more interesting for hardware … and soon also in software, cf. Intel's and Sun's current announcements to include binary instructions.

Complete addition law

- If d is not a square the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- No exceptional points, completely uniform group operations.
- The set of curves with complete addition law is not complete!
- We need Edwards curve in characteristic 2!
- Even characteristic much more interesting for hardware … and soon also in software, cf. Intel's and Sun's current announcements to include binary instructions.

Complete addition law

- If d is not a square the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are never 0; addition law is complete.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- No exceptional points, completely uniform group operations.
- The set of curves with complete addition law is not complete!
- We need Edwards curve in characteristic 2!
- Even characteristic much more interesting for hardware . . . and soon also in software, cf. Intel's and Sun's current announcements to include binary instructions.

The design of Binary Edwards Curves

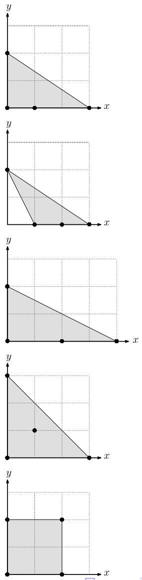
How to design a worthy binary partner?
Our wish-list after studying and experimenting with mostly small modifications of odd Edwards:

A binary Edwards curve should

- be a binary elliptic curve.
- look like an Edwards curve (in odd characteristic).
- have a complete addition law.
- have easy negation.
- have efficient doubling.
- have efficient additions.
- cover most ordinary binary elliptic curves.

Newton Polygons, in odd characteristic

- Short Weierstrass: $y^2 = x^3 + ax + b$
- Montgomery: $by^2 = x^3 + ax^2 + x$
- Jacobi quartic: $y^2 = x^4 + 2ax^2 + 1$
- Hessian: $x^3 + y^3 + 1 = 3dxy$
- Edwards: $x^2 + y^2 = 1 + dx^2y^2$

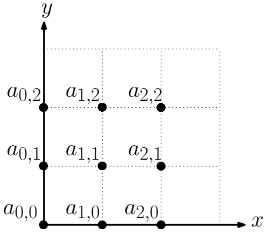


The design choices (I)

Let $\mathrm{E_B}$ is defined by $F(x,y)=0$.

- $\mathrm{E_B}$ should look like Edwards curve; so, $\mathtt{deg}_x(F)\le 2$ and $\mathtt{deg}_y(F)\le 2$; so,

$$\mathrm{E_B}: F(x,y)=\sum_{i=0}^{2}\sum_{j=0}^{2} a_{i,j}x^i y^j = 0.$$



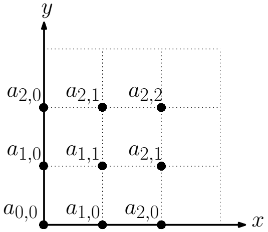
- $\mathrm{E_B}$ should have symmetric formulas, so $a_{i,j}=a_{j,i}$.
- $\mathrm{E_B}$ should be elliptic, so $a_{2,2}\neq 0$ or $a_{1,2}=a_{2,1}\neq 0$.
- If $a_{2,2}=0$, and $a_{1,2}=a_{2,1}\neq 0$ then there are three points at infinity. Moreover the addition law can not be complete (for sufficiently large fields).

The design choices (I)

Let $\mathrm{E_B}$ is defined by $F(x, y) = 0$.

- $\mathrm{E_B}$ should look like Edwards curve; so, $\mathtt{deg}_x(F) \leq 2$ and $\mathtt{deg}_y(F) \leq 2$; so,

$$\mathrm{E_B} : F(x, y) = \sum_{i=0}^{2} \sum_{j=0}^{2} a_{i,j} x^i y^j = 0.$$



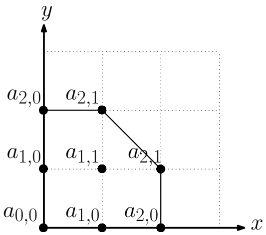
- $\mathrm{E_B}$ should have symmetric formulas, so $a_{i,j} = a_{j,i}$.
- $\mathrm{E_B}$ should be elliptic, so $a_{2,2} \neq 0$ or $a_{1,2} = a_{2,1} \neq 0$.
- If $a_{2,2} = 0$, and $a_{1,2} = a_{2,1} \neq 0$ then there are three points at infinity. Moreover the addition law can not be complete (for sufficiently large fields).

The design choices (I)

Let $\mathrm{E_B}$ is defined by $F(x,y)=0$.

- $\mathrm{E_B}$ should look like Edwards curve; so, $\mathtt{deg}_x(F) \le 2$ and $\mathtt{deg}_y(F) \le 2$; so,

$$\mathrm{E_B} : F(x,y) = \sum_{i=0}^{2}\sum_{j=0}^{2} a_{i,j}x^i y^j = 0.$$



- $\mathrm{E_B}$ should have symmetric formulas, so $a_{i,j} = a_{j,i}$.
- $\mathrm{E_B}$ should be elliptic, so $a_{2,2} \neq 0$ or $a_{1,2} = a_{2,1} \neq 0$.
- If $a_{2,2}=0$, and $a_{1,2}=a_{2,1}\neq 0$ then there are three points at infinity. Moreover the addition law can not be complete (for sufficiently large fields).

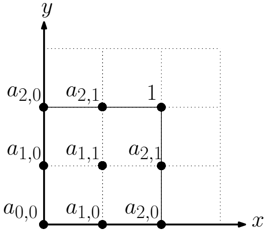
The design choices(II)

- So, $a_{2,2} = 1$ (scale by $a_{2,2}$).
- The projective model of

$$\mathrm{E_B} : \sum_{i=0}^{2} \sum_{j=0}^{2} a_{i,j} x^i y^j = 0$$

is defined by

$$\sum_{i=0}^{2} \sum_{j=0}^{2} a_{i,j} X^i Y^j Z^{4-i-j} = 0.$$



- Put $Z = 0$ to find the points at infinity. Then, $X^2Y^2 = 0$; so $(0 : 1 : 0)$ and $(1 : 0 : 0)$ are the points at infinity of $\mathrm{E_B}$.

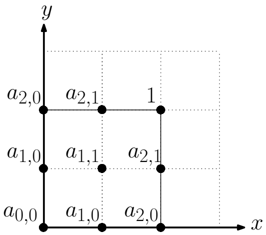
The design choices(II)

- So, $a_{2,2} = 1$ (scale by $a_{2,2}$).
- The projective model of

$$\mathrm{E_B} : \sum_{i=0}^{2} \sum_{j=0}^{2} a_{i,j} x^i y^j = 0$$

is defined by

$$\sum_{i=0}^{2} \sum_{j=0}^{2} a_{i,j} X^i Y^j Z^{4-i-j} = 0.$$



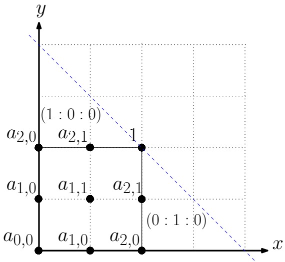
- Put $Z = 0$ to find the points at infinity. Then, $X^2Y^2 = 0$; so $(0:1:0)$ and $(1:0:0)$ are the points at infinity of $\mathrm{E_B}$.

The design choices(III)

- The points at infinity are singular.
- Study the point $(0:1:0)$, (blow-up the point), look at the Newton diagram at this point.
- Consider the polynomial corresponding to the edge γ:

$$f_\gamma = t^2 + a_{2,1}t + a_{2,0}.$$

- f_γ should be irreducible over $\mathbb{F}$, to make sure that blow-up needs field extension.
- So, $a_{2,1}, a_{2,0} \neq 0$.
- Scale curve by $x \longrightarrow a_{2,1}x$ and $y \longrightarrow a_{2,1}y$ to get $a_{2,1} = 1$.

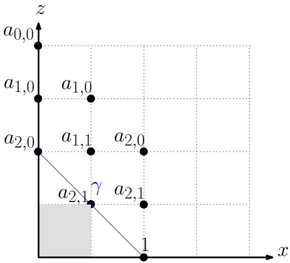


The design choices(III)

- The points at infinity are singular.
- Study the point $(0:1:0)$, (blow-up the point), look at the Newton diagram at this point.
- Consider the polynomial corresponding to the edge γ:

$$f_\gamma = t^2 + a_{2,1}t + a_{2,0}.$$

- f_γ should be irreducible over $\mathbb{F}$, to make sure that blow-up needs field extension.
- So, $a_{2,1}, a_{2,0} \neq 0$.
- Scale curve by $x \longrightarrow a_{2,1}x$ and $y \longrightarrow a_{2,1}y$ to get $a_{2,1} = 1$.

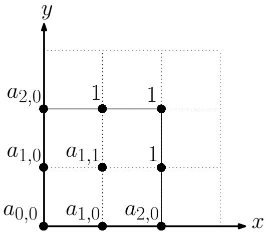


The design choices(III)

- The points at infinity are singular.
- Study the point $(0:1:0)$, (blow-up the point), look at the Newton diagram at this point.
- Consider the polynomial corresponding to the edge γ:

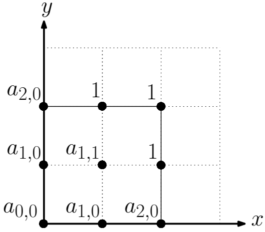
$$f_\gamma = t^2 + a_{2,1}t + a_{2,0}.$$

- f_γ should be irreducible over $\mathbb{F}$, to make sure that blow-up needs field extension.
- So, $a_{2,1}, a_{2,0} \neq 0$.
- Scale curve by $x \longrightarrow a_{2,1}x$ and $y \longrightarrow a_{2,1}y$ to get $a_{2,1} = 1$.



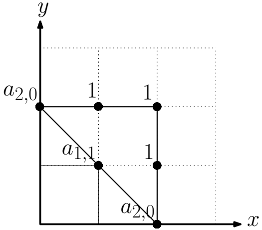
The design choices(IV)

- At most one of the $a_{0,0}$ or $a_{1,0}$ is zero.
  If $a_{0,0} = a_{1,0} = 0$, then $(0,0)$ is a singular point.
  (e.g., look at the Newton diagram at $(0,0)$).
- Because of the symmetry, with (x,y) also (y,x) is on curve.
- The simplest negation can be considered as $-(x,y) = (y,x)$.
- We have a 2-torsion points (α,α) for each root α of $a_{0,0} + a_{1,1}x^2 + x^4$. Also $(\alpha + \sqrt{a_{1,1}}, \alpha + \sqrt{a_{1,1}})$ is the other 2-torsion point.
- $\mathrm{E_B}$ is an ordinary elliptic curve if it has two 2-torsion points; i.e., $a_{1,1} \neq 0$.



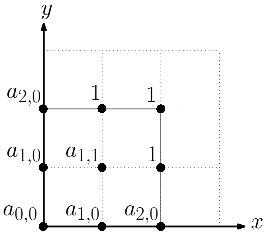
The design choices(IV)

- At most one of the $a_{0,0}$ or $a_{1,0}$ is zero.
  If $a_{0,0} = a_{1,0} = 0$, then $(0,0)$ is a singular point.
  (e.g., look at the Newton diagram at $(0,0)$).
- Because of the symmetry, with (x,y) also (y,x) is on curve.
- The simplest negation can be considered as $-(x,y) = (y,x)$.
- We have a 2-torsion points (α,α) for each root α of $a_{0,0} + a_{1,1}x^2 + x^4$. Also $(\alpha + \sqrt{a_{1,1}}, \alpha + \sqrt{a_{1,1}})$ is the other 2-torsion point.
- $\mathrm{E_B}$ is an ordinary elliptic curve if it has two 2-torsion points; i.e., $a_{1,1} \neq 0$.



The design choices(IV)

- At most one of the $a_{0,0}$ or $a_{1,0}$ is zero.
  If $a_{0,0} = a_{1,0} = 0$, then $(0,0)$ is a singular point.
  (e.g., look at the Newton diagram at $(0,0)$).
- Because of the symmetry, with (x, y) also (y, x) is on curve.
- The simplest negation can be considered as $-(x, y) = (y, x)$.
- We have a 2-torsion points (α, α) for each root α of $a_{0,0} + a_{1,1}x^2 + x^4$. Also $(\alpha + \sqrt{a_{1,1}}, \alpha + \sqrt{a_{1,1}})$ is the other 2-torsion point.
- $\mathrm{E_B}$ is an ordinary elliptic curve if it has two 2-torsion points; i.e., $a_{1,1} \neq 0$.

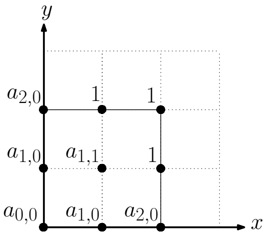


The design choices(V)

- Most convenient choices for 2-torsion points are $(0,0)$ and $(1,1)$.
- So $a_{0,0} = 0$ and $a_{1,1} = 1$.
- Rename $d_1 = a_{1,0}$, $d_2 = a_{2,0}$.
- The affine model should be absolutely irreducible and nonsingular.
- If (x_1, y_1) is a singular point of E_B, then

$$\begin{cases} F(x_1, y_1) = 0, \\ d_1 + x_1 + x_1^2 = 0, \\ d_1 + y_1 + y_1^2 = 0. \end{cases}$$

So, $x_1 = y_1$ or $x_1 + y_1 = 1$.
Then, $d_1 = 0$ or $d_1^2 + d_1 = d_2$.

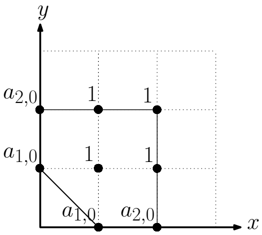


The design choices(V)

- Most convenient choices for 2-torsion points are $(0,0)$ and $(1,1)$.
- So $a_{0,0} = 0$ and $a_{1,1} = 1$.
- Rename $d_1 = a_{1,0}$, $d_2 = a_{2,0}$.
- The affine model should be absolutely irreducible and nonsingular.
- If (x_1, y_1) is a singular point of $\mathrm{E_B}$, then

$$\begin{cases} F(x_1, y_1) = 0, \\ d_1 + x_1 + x_1^2 = 0, \\ d_1 + y_1 + y_1^2 = 0. \end{cases}$$

So, $x_1 = y_1$ or $x_1 + y_1 = 1$.
Then, $d_1 = 0$ or $d_1^2 + d_1 = d_2$.

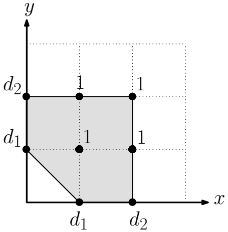


The design choices(V)

- Most convenient choices for 2-torsion points are $(0,0)$ and $(1,1)$.
- So $a_{0,0} = 0$ and $a_{1,1} = 1$.
- Rename $d_1 = a_{1,0}$, $d_2 = a_{2,0}$.
- The affine model should be absolutely irreducible and nonsingular.
- If (x_1, y_1) is a singular point of $\mathrm{E_B}$, then

$$\begin{cases} F(x_1, y_1) = 0, \\ d_1 + x_1 + x_1^2 = 0, \\ d_1 + y_1 + y_1^2 = 0. \end{cases}$$

So, $x_1 = y_1$ or $x_1 + y_1 = 1$.
Then, $d_1 = 0$ or $d_1^2 + d_1 = d_2$.

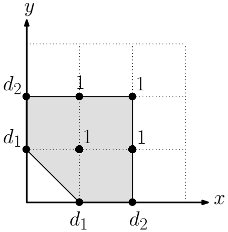


The design choices(V)

- Most convenient choices for 2-torsion points are $(0,0)$ and $(1,1)$.
- So $a_{0,0} = 0$ and $a_{1,1} = 1$.
- Rename $d_1 = a_{1,0}$, $d_2 = a_{2,0}$.
- The affine model should be absolutely irreducible and nonsingular.
- If (x_1, y_1) is a singular point of $\mathrm{E_B}$, then

$$\begin{cases} F(x_1, y_1) = 0, \\ d_1 + x_1 + x_1^2 = 0, \\ d_1 + y_1 + y_1^2 = 0. \end{cases}$$

So, $x_1 = y_1$ or $x_1 + y_1 = 1$.
Then, $d_1 = 0$ or $d_1^2 + d_1 = d_2$.



Binary Edwards Curves

Definition (Binary Edwards curve)

Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = 2$. Let d_1, d_2 be elements of $\mathbb{F}$ with $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$. The *binary Edwards curve with coefficients* d_1 *and* d_2 is the affine curve

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

Birational map to Weierstrass form

- Let $d = d_1^2 + d_1 + d_2$.
- The map $(x, y) \mapsto (u, v)$ defined by

$$u = \frac{d_1 d(x+y)}{xy + d_1(x+y)},$$
$$v = d_1 d\left(\frac{x}{xy + d_1(x+y)} + d_1 + 1\right)$$

is a birational equivalence from $\mathrm{E}_{\mathrm{B},d_1,d_2}$ to the elliptic curve

$$v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4 d^2$$

with j-invariant $1/(d_1^4 d^2)$.

- An inverse map is given as follows:

$$x = \frac{d_1(u+d)}{u + v + (d_1^2 + d_1)d},$$
$$y = \frac{d_1(u+d)}{v + (d_1^2 + d_1)d}.$$

Birational map to Weierstrass form

- Let $d = d_1^2 + d_1 + d_2$.
- The map $(x, y) \mapsto (u, v)$ defined by

$$u = \frac{d_1 d(x+y)}{xy + d_1(x+y)},$$
$$v = d_1 d\left(\frac{x}{xy + d_1(x+y)} + d_1 + 1\right)$$

  is a birational equivalence from $\mathrm{E}_{\mathrm{B},d_1,d_2}$ to the elliptic curve

$$v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + d_1^4 d^2$$

  with j-invariant $1/(d_1^4 d^2)$.
- An inverse map is given as follows:

$$x = \frac{d_1(u+d)}{u + v + (d_1^2 + d_1)d},$$
$$y = \frac{d_1(u+d)}{v + (d_1^2 + d_1)d}.$$

Properties of Binary Edwards Curves

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

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

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

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

- $(0,0)$ is the neutral element; $(1,1)$ has order 2.
- $-(x_1, y_1) = (y_1, x_1)$.
- $(x_1, y_1) + (1,1) = (x_1+1, y_1+1)$.

Properties of Binary Edwards Curves

$$\mathrm{E}_{\mathrm{B},d_1,d_2} : d_1(x+y) + d_2(x^2+y^2) = xy + xy(x+y) + x^2y^2.$$

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

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

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

- $(0,0)$ is the neutral element; $(1,1)$ has order 2.
- $-(x_1, y_1) = (y_1, x_1)$.
- $(x_1, y_1) + (1,1) = (x_1+1, y_1+1)$.

Edwards curve over $\mathbb{F}_{2^n}$

- For any points (x_1, y_1) and (x_2, y_2) the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero if $\mathrm{Tr}(d_2) \neq 0$.

  If $x_2 + y_2 = 0$ then the denominators are $d_1 \neq 0$. Otherwise $d_1/(x_2 + y_2) = x_1 + x_1^2$ and

$$\begin{aligned}
\frac{d_1}{x_2 + y_2} &= \frac{d_1(x_2 + y_2)}{x_2^2 + y_2^2} = \frac{d_2(x_2^2 + y_2^2) + x_2y_2 + x_2y_2(x_2 + y_2) + x_2^2y_2^2}{x_2^2 + y_2^2} \\
&= d_2 + \frac{x_2y_2 + x_2y_2(x_2 + y_2) + y_2^2}{x_2^2 + y_2^2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2} \\
&= d_2 + \frac{y_2 + x_2y_2}{x_2 + y_2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2}.
\end{aligned}$$

  So, $\mathrm{Tr}(d_2) = \mathrm{Tr}(x_1 + x_1^2) = 0$.

Edwards curve over $\mathbb{F}_{2^n}$

- For any points (x_1, y_1) and (x_2, y_2) the denominators $d_1 + (x_1 + x_1^2)(x_2 + y_2)$ and $d_1 + (y_1 + y_1^2)(x_2 + y_2)$ are nonzero if $\mathrm{Tr}(d_2) \neq 0$.
  If $x_2 + y_2 = 0$ then the denominators are $d_1 \neq 0$. Otherwise $d_1/(x_2 + y_2) = x_1 + x_1^2$ and

$$
\begin{aligned}
\frac{d_1}{x_2 + y_2} = \frac{d_1(x_2 + y_2)}{x_2^2 + y_2^2} &= \frac{d_2(x_2^2 + y_2^2) + x_2y_2 + x_2y_2(x_2 + y_2) + x_2^2y_2^2}{x_2^2 + y_2^2} \\
&= d_2 + \frac{x_2y_2 + x_2y_2(x_2 + y_2) + y_2^2}{x_2^2 + y_2^2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2} \\
&= d_2 + \frac{y_2 + x_2y_2}{x_2 + y_2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2}.
\end{aligned}
$$

  So, $\mathrm{Tr}(d_2) = \mathrm{Tr}(x_1 + x_1^2) = 0$.

Complete Edwards curve over $\mathbb{F}_{2^n}$

- Addition law for curves with $\mathrm{Tr}(d_2) = 1$ is complete.
- No exceptional points, completely uniform group operation.
- In particular, addition formulas can be used to double.
- Unified group operation!
- The first complete binary elliptic curves!
- Even better, every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curves $\mathrm{E}_{\mathrm{B},d_1,d_2}$, for $n \geq 3$.

Doubling

- $(x_3, y_3) = 2(x_1, y_1)$ with

$$x_3 = 1 + \frac{d_1(1 + x_1 + y_1)}{d_1 + x_1y_1 + x_1^2(1 + x_1 + y_1)}$$
$$y_3 = 1 + \frac{d_1(1 + x_1 + y_1)}{d_1 + x_1y_1 + y_1^2(1 + x_1 + y_1)}.$$

- That is:

$$x_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)},$$
$$y_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)}$$

Doubling

- $(x_3, y_3) = 2(x_1, y_1)$ with

$$x_3 = 1 + \frac{d_1(1 + x_1 + y_1)}{d_1 + x_1y_1 + x_1^2(1 + x_1 + y_1)}$$
$$y_3 = 1 + \frac{d_1(1 + x_1 + y_1)}{d_1 + x_1y_1 + y_1^2(1 + x_1 + y_1)}.$$

- That is:

$$x_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + y_1^2 + y_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)},$$
$$y_3 = 1 + \frac{d_1 + d_2(x_1^2 + y_1^2) + x_1^2 + x_1^4}{d_1 + x_1^2 + y_1^2 + (d_2/d_1)(x_1^4 + y_1^4)}$$

Doubling

- The projective formulas use $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$.
  The $3\mathbf{D}$ are multiplications by d_1, d_2/d_1, and d_2.
- Can choose at least one of these constant to be small or use curve with $d_1 = d_2$, then only $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for a doubling.
- Assume curves are chosen with small parameters.

System	Cost of doubling
Projective	$7\mathbf{M} + 4\mathbf{S}$; see HEHCC
Jacobian	$4\mathbf{M} + 5\mathbf{S}$; see HEHCC
Lopez-Dahab	$3\mathbf{M} + 5\mathbf{S}$; see Lopez-Dahab
Edwards	$2\mathbf{M} + 6\mathbf{S}$; new, complete
Lopez-Dahab $a_2 = 1$	$2\mathbf{M} + 5\mathbf{S}$; Kim-Kim
Edwards $d_1 = d_2$	$2\mathbf{M} + 5\mathbf{S}$; new, complete

- Explicit-Formulas Database:

  `www.hyperelliptic.org/EFD`

  contains also formulas for characteristic 2.

Doubling

- The projective formulas use $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$.
  The $3\mathbf{D}$ are multiplications by d_1, d_2/d_1, and d_2.
- Can choose at least one of these constant to be small or use curve with $d_1 = d_2$, then only $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for a doubling.
- Assume curves are chosen with small parameters.

System	Cost of doubling
Projective	$7\mathbf{M} + 4\mathbf{S}$; see HEHCC
Jacobian	$4\mathbf{M} + 5\mathbf{S}$; see HEHCC
Lopez-Dahab	$3\mathbf{M} + 5\mathbf{S}$; see Lopez-Dahab
Edwards	$2\mathbf{M} + 6\mathbf{S}$; new, complete
Lopez-Dahab $a_2 = 1$	$2\mathbf{M} + 5\mathbf{S}$; Kim-Kim
Edwards $d_1 = d_2$	$2\mathbf{M} + 5\mathbf{S}$; new, complete

- Explicit-Formulas Database:

  www.hyperelliptic.org/EFD

  contains also formulas for characteristic 2.

Doubling

- The projective formulas use $2\mathbf{M} + 6\mathbf{S} + 3\mathbf{D}$.
  The $3\mathbf{D}$ are multiplications by d_1, d_2/d_1, and d_2.
- Can choose at least one of these constant to be small or use curve with $d_1 = d_2$, then only $2\mathbf{M} + 5\mathbf{S} + 2\mathbf{D}$ for a doubling.
- Assume curves are chosen with small parameters.

System	Cost of doubling
Projective	$7\mathbf{M} + 4\mathbf{S}$; see HEHCC
Jacobian	$4\mathbf{M} + 5\mathbf{S}$; see HEHCC
Lopez-Dahab	$3\mathbf{M} + 5\mathbf{S}$; see Lopez-Dahab
Edwards	$2\mathbf{M} + 6\mathbf{S}$; new, complete
Lopez-Dahab $a_2 = 1$	$2\mathbf{M} + 5\mathbf{S}$; Kim-Kim
Edwards $d_1 = d_2$	$2\mathbf{M} + 5\mathbf{S}$; new, complete

- Explicit-Formulas Database:

  www.hyperelliptic.org/EFD

  contains also formulas for characteristic 2.

Differential addition I

- Compute $P+Q$ given P, Q, and $Q-P$.
- Represent $P=(x_1, y_1)$ by $w(P)=x_1+y_1$.
- Have $w(P)=w(-P)=w(P+(1,1))=w(-P+(1,1))$.
- Can double in this representation:
  Let $(x_4, y_4)=(x_2, y_2)+(x_2, y_2)$. Then

$$w_4=\frac{d_1 w_2^2+d_1 w_2^4}{d_1^2+d_1 w_2^2+d_2 w_2^4}=\frac{w_2^2+w_2^4}{d_1+w_2^2+(d_2/d_1) w_2^4}$$

- If $d_2=d_1$ then $$w_4=1+\frac{d_1}{d_1+w_2^2+w_2^4}.$$
- Projective version takes 1M+3S+2D (or 1M+3S+1D for $d_2=d_1$).

Differential addition I

- Compute $P+Q$ given P, Q, and $Q-P$.
- Represent $P=(x_1,y_1)$ by $w(P)=x_1+y_1$.
- Have $w(P)=w(-P)=w(P+(1,1))=w(-P+(1,1))$.
- Can double in this representation:
  Let $(x_4,y_4)=(x_2,y_2)+(x_2,y_2)$. Then

$$w_4=\frac{d_1w_2^2+d_1w_2^4}{d_1^2+d_1w_2^2+d_2w_2^4}=\frac{w_2^2+w_2^4}{d_1+w_2^2+(d_2/d_1)w_2^4}$$

- If $d_2=d_1$ then $$w_4=1+\frac{d_1}{d_1+w_2^2+w_2^4}.$$
- Projective version takes 1M+3S+2D (or 1M+3S+1D for $d_2=d_1$).

Differential addition II

- Let $(x_1, y_1) = (x_3, y_3) - (x_2, y_2)$, $(x_5, y_5) = (x_2, y_2) + (x_3, y_3)$.
- $$w_1 + w_5 = \frac{d_1 w_2 w_3 (1 + w_2)(1 + w_3)}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)},$$
  $$w_1 w_5 = \frac{d_1^2 (w_2 + w_3)^2}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)}.$$
- If $d_2 = d_1$ then
  $$w_1 + w_5 = 1 + \frac{d_1}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)},$$
  $$w_1 w_5 = \frac{d_1 (w_2 + w_3)^2}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)}.$$
- Some operations can be shared between differential addition and doubling.

Differential addition II

- Let $(x_1, y_1) = (x_3, y_3) - (x_2, y_2)$, $(x_5, y_5) = (x_2, y_2) + (x_3, y_3)$.
- $$w_1 + w_5 = \frac{d_1 w_2 w_3 (1 + w_2)(1 + w_3)}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)},$$
$$w_1 w_5 = \frac{d_1^2 (w_2 + w_3)^2}{d_1^2 + w_2 w_3 (d_1(1 + w_2 + w_3) + d_2 w_2 w_3)}.$$
- If $d_2 = d_1$ then
$$w_1 + w_5 = 1 + \frac{d_1}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)},$$
$$w_1 w_5 = \frac{d_1 (w_2 + w_3)^2}{d_1 + w_2 w_3 (1 + w_2)(1 + w_3)}.$$
- Some operations can be shared between differential addition and doubling.

Differential addition III

- Mixed differential addition: w_1 given as affine, $w_2 = W_2/Z_2$, $w_3 = W_3/Z_3$ in projective.

	general case	$d_2 = d_1$
mixed diff addition	6M+1S+2D	5M+1S+1D
mixed diff addition+doubling	6M+4S+4D	5M+4S+2D
projective diff addition	8M+1S+2D	7M+1S+1D
projective diff addition+doubling	8M+4S+4D	7M+4S+2D

- Note that the new diff addition formulas are complete.
- Lopez and Dahab use 6M+5S for mixed dADD&DBL.
- Stam uses 6M+1S for projective dADD; 4M+1S for mixed dADD addition; and 1M+3S+1D for DBL.
- Gaudry uses 5M+5S+1D for mixed dADD&DBL.

Differential addition III

- Mixed differential addition: w_1 given as affine, $w_2 = W_2/Z_2$, $w_3 = W_3/Z_3$ in projective.

	general case	$d_2 = d_1$
mixed diff addition	6M+1S+2D	5M+1S+1D
mixed diff addition+doubling	6M+4S+4D	5M+4S+2D
projective diff addition	8M+1S+2D	7M+1S+1D
projective diff addition+doubling	8M+4S+4D	7M+4S+2D

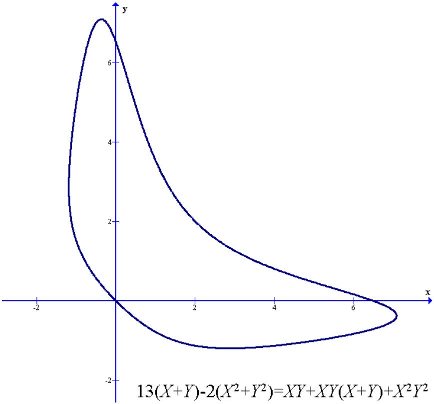
- Note that the new diff addition formulas are complete.
- Lopez and Dahab use 6M+5S for mixed dADD&DBL.
- Stam uses 6M+1S for projective dADD; 4M+1S for mixed dADD addition; and 1M+3S+1D for DBL.
- Gaudry uses 5M+5S+1D for mixed dADD&DBL.

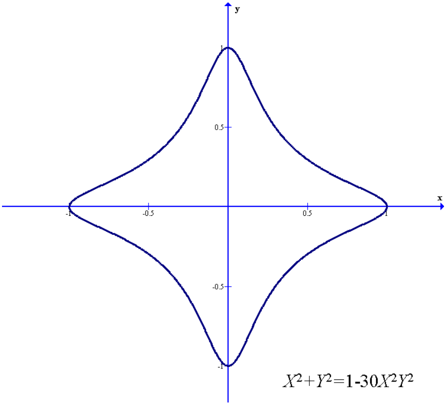
Summary

These curves are the first binary curves to offer complete addition laws. They are also surprisingly fast:

- ADD on binary Edwards curves takes 21M+1S+4D, mADD takes 13M+3S+3D.
- For small D and $d_1 = d_2$ much better: ADD in 16M+1S.
- Differential addition takes 8M+1S+2D; mixed version takes 6M+1S+2D.
- Differential addition+doubling (typical step in Montgomery ladder) takes 8M+4S+2D; mixed version takes 6M+4S+2D.

See our paper and the EFD for full details, speedups for $d_1 = d_2$, how to choose small coefficients, affine formulas, . . .


y
x
6
4
2
-2
-2
2
4
6
13(X+Y)-2(X²+Y²)=XY+XY(X+Y)+X²Y²


y
x
1
0.5
-0.5
-1
-1
-0.5
0.5
1
X²+Y²=1-30X²Y²