Binary Edwards Curves

Tanja Lange

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

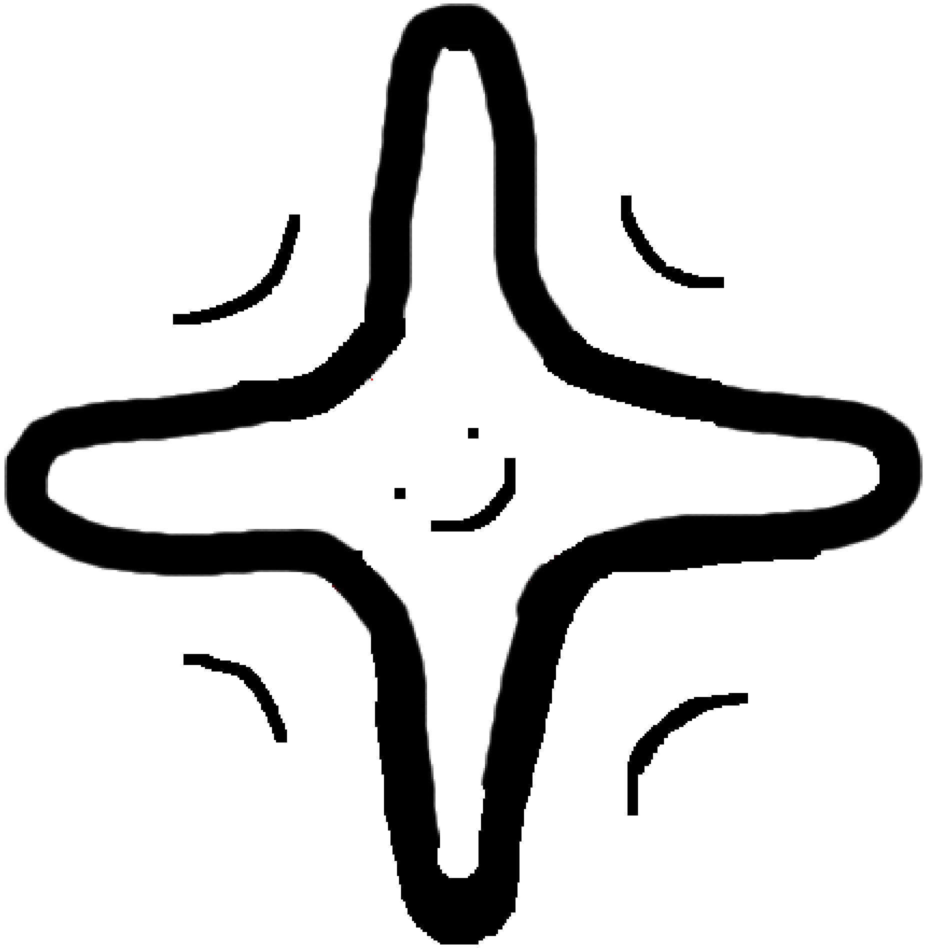
20.06.2008

joint work with Daniel J. Bernstein, University of Illinois at Chicago, USA

and

Reza Rezaeian Farashahi, Eindhoven, Netherlands

Edwards Curves – a new star(fish) is born

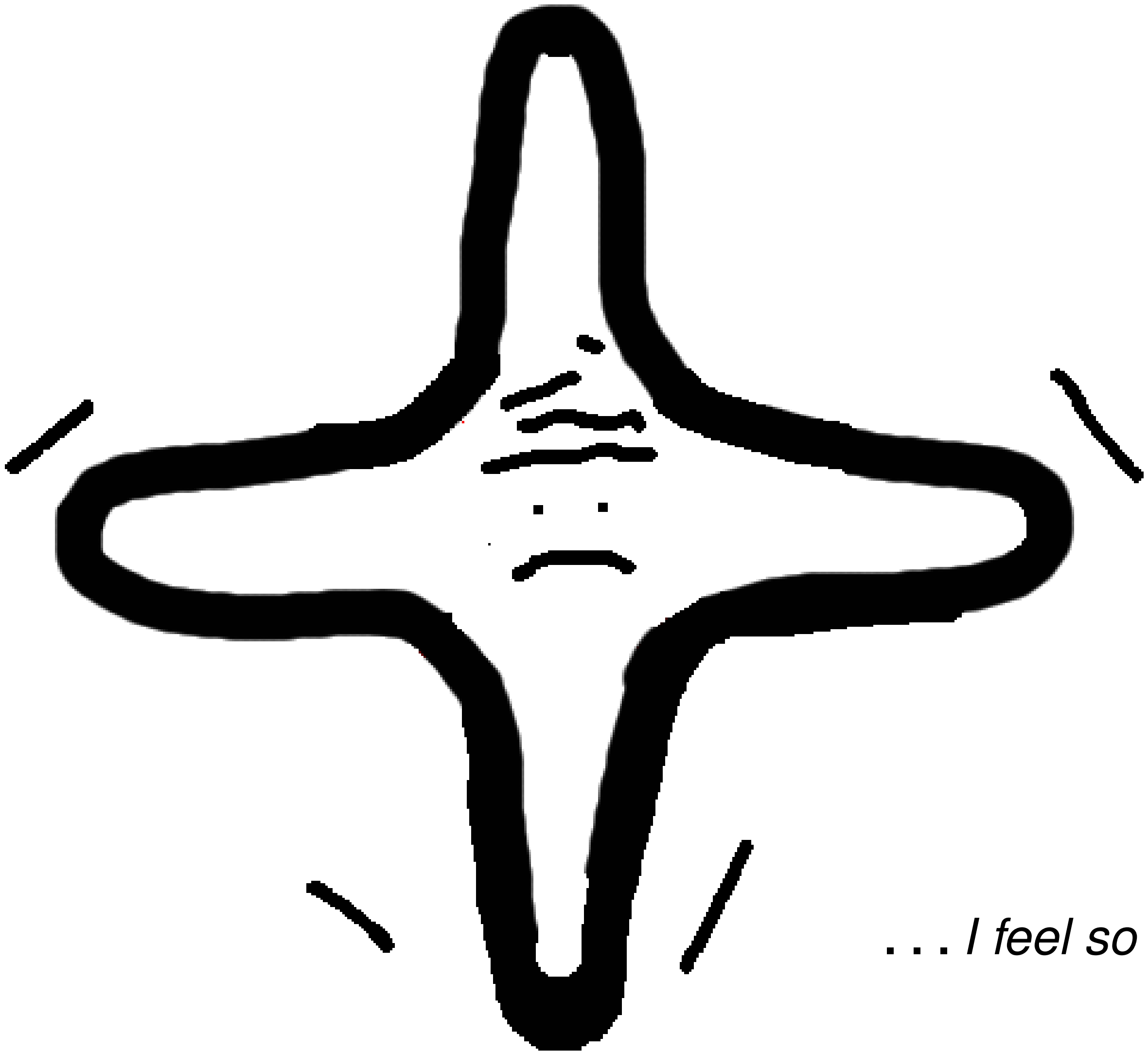


lecture circuit:

Hoboken
Turku
Warsaw
Fort Meade, Maryland
Melbourne
Ottawa (SAC)
Dublin (ECC)
Bordeaux
Bristol
Magdeburg
Seoul
Malaysia (Asiacrypt)
Chennai
Bangalore (AAECC)
⋮

Rennes

One year passes . . .



. . . *I feel so odd* . . .

Exceptions, $2 \neq 0$ ...

Fix a field k of characteristic different from 2. Fix $c, d \in k$ such that $c \neq 0$, $d \neq 0$, and $dc^4 \neq 1$. Consider the *Edwards addition law*

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

$x^2 + y^2 = a^2(1 + x^2 y^2), a^5 \neq a$
describes an elliptic curve over field k of odd characteristic.

Theorem 2.1. *Let k be a field in which $2 \neq 0$. Let E be an elliptic curve over k such that the group $E(k)$ has an element of order 4. Then*

How can there be an incomplete set of complete curves???

How to design a worthy binary partner?

Our wish-list early February 2008:

A binary Edwards curve should

- be elliptic.
- look like an Edwards curve.
- have a complete addition law.
- cover most (all?) ordinary binary elliptic curves.
- have an easy to compute negation.
- have efficient doublings.
- have efficient additions.

How to design a worthy binary partner?

Our wish-list early February 2008:

A binary Edwards curve should

- be elliptic.
- look like an Edwards curve.
- have a complete addition law.
- cover most (all?) ordinary binary elliptic curves.
- have an easy to compute negation.
- have efficient doublings.
- have efficient additions.
- be found before the CHES deadline, February 29th.

Completeness

- Addition formulas on affine points are given by rational functions on $C \times C$.
- Bosma and Lenstra state that the smallest number of equations to describe the group law is two.
- Each group law has exceptional divisor.
- Can avoid Bosma/Lenstra if points on exceptional divisor are defined over an extension field.
- If non-singular rational points at infinity exist and the field is sufficiently large they are reached as output of the addition formulas.
- To enable complete addition formulas need:
  - points at infinity are singular;
  - blow-ups are not defined over ground field;
  - denominators really do not vanish.

Attention

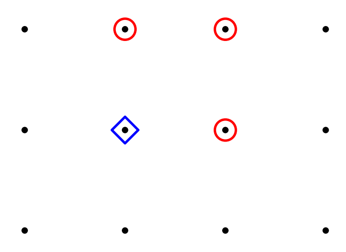
- Aim for curve with singular points at infinity; ensure that blow-up is defined over extension field.
- No rational points at infinity on desingularization is necessary condition (for sufficiently large fields) but it is not sufficient.
- Last point *"denominators really do not vanish"* is important!

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

  is an addition formula on Edwards curve.
- It is not even unified; denominator of y_3 vanishes for doubling.

The design choices

- Want x-degree ≤ 2, y-degree ≤ 2, i.e.



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

- Want symmetric formulas, i.e. $a_{ij} = a_{ji}$.
- Want elliptic, i.e. $(1,1)$ needs to be an interior point of Newton polygon. This means at least one of $a_{22} \neq 0$ and $a_{12} = a_{21} \neq 0$.
- If $a_{22} = 0$ and $a_{12} = a_{21} \neq 0$ then there are three non-singular points at infinity $\Rightarrow$ addition law cannot be complete (for sufficiently large fields).
- Thus largest degree term x^2y^2 (scale by a_{22}).

Binary Edwards curves?

$$a_{00} + a_{10}(x+y) + a_{11}xy + a_{20}(x^2+y^2) + a_{21}xy(x+y) + x^2y^2$$

- Study projective equation
  $$a_{00}Z^4 + a_{10}(X+Y)Z^3 + a_{11}XYZ^2 + a_{20}(X^2+Y^2)Z^2 + a_{21}XY(X+Y)Z + X^2Y^2 = 0$$
  to find points at infinity ($Z=0$):
  $0 + X^2Y^2 = 0 \Rightarrow (1:0:0)$ and $(0:1:0)$.
- Are these points singular? Study $(1:0:0)$:

$$G(y,z) = a_{00}z^4 + a_{10}(1+y)z^3 + a_{11}yz^2 + a_{20}(1+y^2)z^2 + a_{21}y(1+y)z + y^2$$
$$G_y(y,z) = a_{10}z^3 + a_{11}z^2 + a_{21}z$$
$$G_z(y,z) = a_{10}(1+y)z^2 + a_{21}y(1+y)$$

  Both derivatives vanish at $(0,0)$, point is singular.
- Point $(0:1:0)$ same by symmetry.

Blow-up I

$$\begin{aligned} G(y,z) &= a_{00}z^4 + a_{10}(1+y)z^3 + a_{11}yz^2 + a_{20}(1+y^2)z^2 + \\ &\quad a_{21}y(1+y)z + y^2. \end{aligned}$$

Use $y = uz$ to obtain

$$\begin{aligned} G(uz,z) &= a_{00}z^4 + a_{10}(1+uz)z^3 + a_{11}uz^3 + a_{20}(1+u^2z^2)z^2 + \\ &\quad a_{21}u(1+uz)z^2 + u^2z^2. \end{aligned}$$

and divide by z^2 to obtain

$$\begin{aligned} H(u,z) &= a_{00}z^2 + a_{10}(1+uz)z + a_{11}uz + a_{20}(1+u^2z^2) + \\ &\quad a_{21}u(1+uz) + u^2. \end{aligned}$$

Blow-up II

Field of definition for points with $z = 0$ on blow-up

$$\begin{aligned} H(u,z) &= a_{00}z^2 + a_{10}(1+uz)z + a_{11}uz + a_{20}(1+u^2z^2) + \\ &\quad a_{21}u(1+uz) + u^2. \end{aligned}$$

satisfy $H(u,0) = a_{20} + a_{21}u + u^2$.

Points at infinity defined over k if $u^2 + a_{21}u + a_{20}$ is reducible.

Blow-up II

Field of definition for points with $z = 0$ on blow-up

$$\begin{aligned} H(u,z) &= a_{00}z^2 + a_{10}(1+uz)z + a_{11}uz + a_{20}(1+u^2z^2) + \\ &\quad a_{21}u(1+uz) + u^2. \end{aligned}$$

satisfy $H(u,0) = a_{20} + a_{21}u + u^2$.

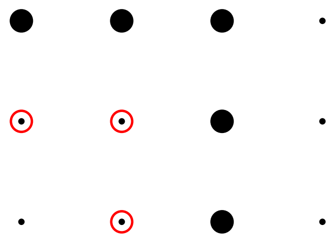
Points at infinity defined over k if $u^2 + a_{21}u + a_{20}$ is reducible.

Want that blow-up is defined only over quadratic extension, so in particular $a_{20}, a_{21} \neq 0$.

Then $H_u(u,z) = a_{10}z^2 + a_{11}z + a_{21}$ is nonzero in $z = 0$, so blow-up is non-singular.

Scale curve by $x \to a_{21}x, y \to a_{21}y$ to get $a_{21} = 1$.

Non-singular affine model

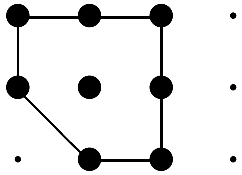


- All affine points should be non-singular.
  $F(x, y) =$
  $a_{00} + a_{10}(x + y) + a_{11}xy + a_{20}(x^2 + y^2) + xy(x + y) + x^2y^2$
  $F_x(x, y) = a_{10} + a_{11}y + y^2$
  $F_y(x, y) = a_{10} + a_{11}x + x^2$
- If $a_{00} = 0$ then $(0, 0)$ is on the curve and thus a_{10} must be non-zero.
- Vice versa, if $a_{10} = 0$ then (a, b) with $a, b \in \{0, a_{11}\}$ satisfy both partial derivative equations. So
  $a_{00} \notin \{0, a_{11}^3, a_{10}a_{11} + a_{20}a_{11}^2\}$
- In particular, at most one of a_{10} and a_{00} can be 0.

Some choices

- Symmetry enforces that with (x, y) also (y, x) is on curve. Simplest possible negation: $-(x, y) = (y, x)$. There are other choices, several with surprisingly expensive negation.
- We want an ordinary binary curve, i.e. one with a point of order 2. So there should be two points fixed under negation.
- Fixed points are (α, α) and $(\alpha + \sqrt{a_{11}}, \alpha + \sqrt{a_{11}})$, where $\alpha, \alpha + \sqrt{a_{11}}$ are the solutions of $a_{00} + a_{11}x^2 + x^4$.
  To have two different solutions request $a_{11} \neq 0$.
- Most convenient choices are $a_{00} = 0, a_{11} = 1$, neutral element $(0, 0)$, point of order 2 is $(1, 1)$.
- Rename $d_1 = a_{10}, d_2 = a_{20}$.

Binary Edwards curves



Let $d_1 \neq 0$ and $d_2 \neq d_1^2 + d_1$ then

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

is a binary Edwards curve with parameters d_1, d_2.
Map $(x,y) \mapsto (u,v)$ defined by

$$u = d_1(d_1^2 + d_1 + d_2)(x+y)/(xy + d_1(x+y)),$$
$$v = d_1(d_1^2 + d_1 + d_2)(x/(xy + d_1(x+y)) + d_1 + 1)$$

is a birational equivalence from E_{B,d_1,d_2} to the elliptic curve

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

an ordinary elliptic curve in Weierstrass form.

Properties of binary Edwards curves

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

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

$$x_3 = \frac{d_1(x_1+x_2) + d_2(x_1+y_1)(x_2+y_2) + (x_1+x_1^2)(x_2(y_1+y_2+1)+y_1y_2)}{d_1+(x_1+x_1^2)(x_2+y_2)},$$
$$y_3 = \frac{d_1(y_1+y_2) + d_2(x_1+y_1)(x_2+y_2) + (y_1+y_1^2)(y_2(x_1+x_2+1)+x_1x_2)}{d_1+(y_1+y_1^2)(x_2+y_2)}.$$

  if denominators are nonzero.
- Neutral element is $(0,0)$; $(1,1)$ has order 2.
- $-(x,y) = (y,x)$.
- $(x_1,y_1) + (1,1) = (x_1+1, y_1+1)$.
- Addition compatible with addition on Weierstrass curve.

Edwards curves over finite fields

- Addition law for curves with $\mathrm{Tr}(d_2) = 1$ is complete.
- 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 $x_2 + y_2 = 0$ then the denominators are $d_1 \neq 0$.
  Otherwise $d_1/(x_2 + y_2) = x_1 + x_1^2$ and

$$\frac{d_1}{x_2 + y_2} = \frac{d_1(x_2 + y_2)}{x_2^2 + y_2^2} = \frac{d_2(x_2^2 + y_2^2) + x_2y_2 + x_2y_2(x_2 + y_2) + x_2^2y_2^2}{x_2^2 + y_2^2}$$

$$= d_2 + \frac{x_2y_2 + x_2y_2(x_2 + y_2) + y_2^2}{x_2^2 + y_2^2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2}$$

$$= d_2 + \frac{y_2 + x_2y_2}{x_2 + y_2} + \frac{y_2^2 + x_2^2y_2^2}{x_2^2 + y_2^2}$$

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

Generality

- Each ordinary curve over $\mathbb{F}_{2^n}$ isomorphic to $v^2 + uv = u^3 + a_2u^2 + a_6$ for some $a_2 \in \mathbb{F}_{2^n}$, $a_6 \in \mathbb{F}_{2^n}^*$.
- If $\mathrm{Tr}(a_2) = \mathrm{Tr}(a_2')$ then $v^2 + uv = u^3 + a_2u^2 + a_6$ and $v^2 + uv = u^3 + a_2'u^2 + a_6$ are isomorphic: there exists b such that $a_2' = a_2 + b + b^2$, use $v \mapsto v + bu$.
- For each a_2, a_6 can find birationally equivalent binary Edwards curve

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

- Can even restrict to binary Edwards curves with $\mathrm{Tr}(d_2) = 1$.
- Every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve if $n \geq 3$.

Proof I

- For each $\delta, \epsilon \in \mathbb{F}_2$ define

$$D_{\delta,\epsilon} = \left\{ d_1 \in \mathbb{F}_{2^n}^* : \mathrm{Tr}(d_1) = \delta,\ \mathrm{Tr}(\sqrt{a_6}/d_1^2) = \epsilon \right\}.$$

- For $d_1 \in D_{\mathrm{Tr}(a_2)+1,1}$ put $d_2 = d_1^2 + d_1 + \sqrt{a_6}/d_1^2$. Then $\mathrm{Tr}(d_2) = \mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$, i.e. d_1, d_2 belong to complete binary Edwards curve.
- It birationally equivalent to $v^2 + uv = u^3 + (d_1^2 + d_2)u^2 + a_6$ since $d_1^4(d_1^4 + d_1^2 + d_2^2) = a_6$ and $\mathrm{Tr}(d_1^2 + d_2) = \mathrm{Tr}(d_1) + \mathrm{Tr}(d_2) = \mathrm{Tr}(a_2)$.
- Show that $D_{\mathrm{Tr}(a_2)+1,1}$ is nonempty.
- $\#D_{00} + \#D_{01} = 2^{n-1} - 1$ ($d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(d_1) = 0$).
- $\#D_{01} + \#D_{11} = 2^{n-1}$ ($d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(\sqrt{a_6}/d_1^2) = 1$).

Proof II

Bound $\#D_{00} + \#D_{11}$, i.e. $d_1 \in \mathbb{F}_{2^n}^*$ with $\mathrm{Tr}(d_1 + \sqrt{a_6}/d_1^2) = 0$:

- Two choices of $s \in \mathbb{F}_{2^n}$ per such d_1 s.t. $s^2 + s = d_1 + \sqrt{a_6}/d_1^2$, i.e. two points $(U_1, V_1) = (d_1, d_1 s)$ on elliptic curve $V^2 + UV = U^3 + \sqrt{a_6}$.
- $(0,0)$ and P_∞ do not appear.
- Curve has $2^n + 1 + t$ points for t in $[-2\sqrt{2^n}, 2\sqrt{2^n}]$, thus $\#D_{00} + \#D_{11} = 2^{n-1} + (t-1)/2$.

$$
\begin{aligned}
2\#D_{01} &= (\#D_{00} + \#D_{01}) + (\#D_{01} + \#D_{11}) - (\#D_{00} + \#D_{11}) \\
&= 2^{n-1} - 1 + 2^{n-1} - 2^{n-1} - (t-1)/2 = 2^{n-1} - (t+1)/2 \\
2\#D_{11} &= 2^n - 2\#D_{01} = 2^{n-1} + (t+1)/2.
\end{aligned}
$$

$(\sqrt{2^n} - 1)^2 \geq (\sqrt{8} - 1)^2 > 2$ implies $2^n > 2\sqrt{2^n} + 1 \geq |t| + 1$, so both D_{01} and D_{11} are nonempty.

Doubling

- Nice doubling formulas (use curve equation to simplify)

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

- In projective coordinates:
  2M+ 6S+3D, where the 3D are multiplications by d_1, d_2/d_1, and d_2.
- Can choose at least one of these constants to be small.

Comparison with other doubling formulas

Assume curves are chosen with small coefficients.

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

Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

contains already some formulas for characteristic 2; including some speed-ups for non-Edwards coordinates.

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 III

- Mixed differential addition: w_1 given as affine, $w_2 = W_2/Z_2$, $w_3 = W_3/Z_3$ in projective.
- Non-mixed addition, i.e. $w_1 = W_1/Z_1$, is faster when using the multiplicative approach $w_1 w_5$.

	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

- 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.

Operation counts

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 much better: ADD in 18M+2S+7D.
- 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 preprint (ePrint 2008/171) or

`cr.yp.to/papers.html#edwards2`

for full details, speedups for $d_1 = d_2$, how to choose small coefficients, affine formulas, ...

Happy End!