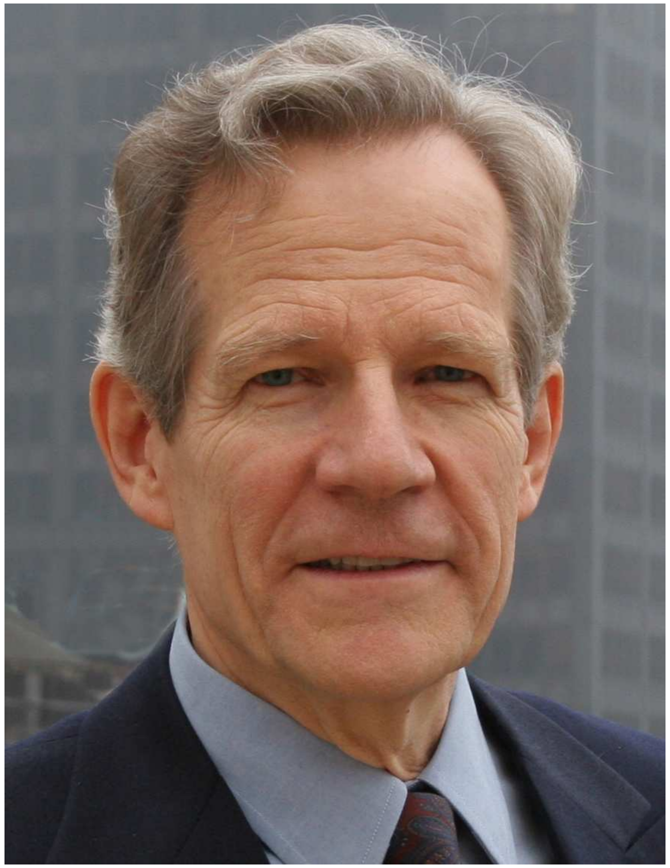
Binary Edwards Curves

Daniel J. Bernstein | Tanja Lange
University of Illinois at Chicago and Technische Universiteit Eindhoven
djb@cr.yp.to | tanja@hyperelliptic.org

12.08.2008

joint work with Reza Rezaeian Farashahi, Eindhoven

Harold M. Edwards

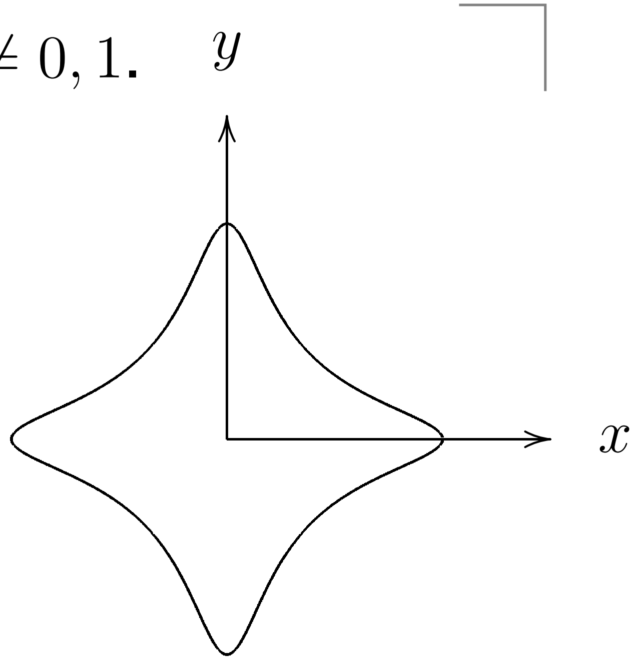


- Edwards generalized single example $x^2 + y^2 = 1 - x^2y^2$ by Euler/Gauss to whole class of curves.
- Shows that – after some field extensions – every elliptic curve over field k of odd characteristic is birationally equivalent to a curve of the form $x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
- Edwards gives addition law for this generalized form, shows equivalence with Weierstrass form, proves addition law, gives theta parameterization . . . in his paper Bulletin of the AMS, **44**, 393–422, 2007

How to add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Generalization covers more curves over k.

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- 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.

Relationship to Weierstrass form

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0, 0)$. Then Weierstrass form:
$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$
- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1+y)/(1-y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.
- Addition on Edwards and Weierstrass corresponds.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\dfrac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \dfrac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\dfrac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\dfrac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\dfrac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\dfrac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

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.
- Having addition law work for doubling removes some checks from the code and gives SCA protection (might leak Hamming weight, though).

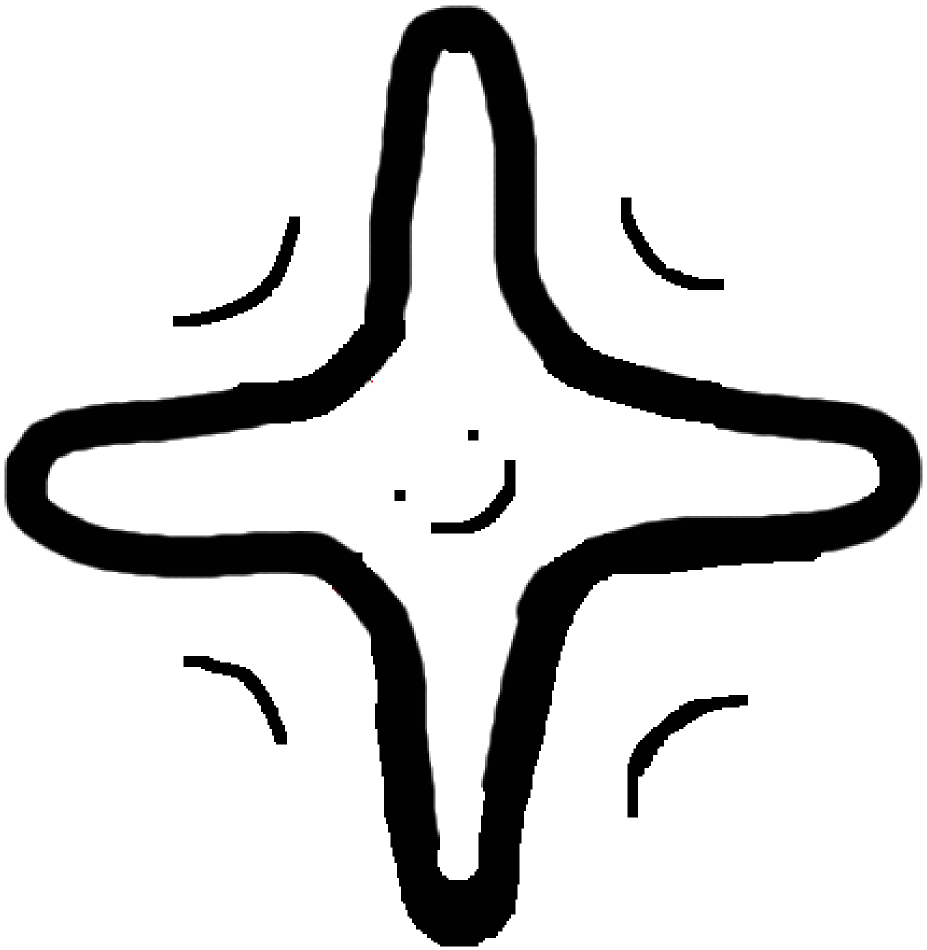
Fast addition law

- Very fast point addition 10M + 1S + 1D. (Even faster with Inverted Edwards coordinates.)
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstrass curves.
  - Point addition 12M + 4S.
  - Doubling formulas need only 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstrass curves) and many more operations (mixed addition, re-addition, tripling, scaling,. . .) see

  `www.hyperelliptic.org/EFD`

  for the Explicit-Formulas Database.

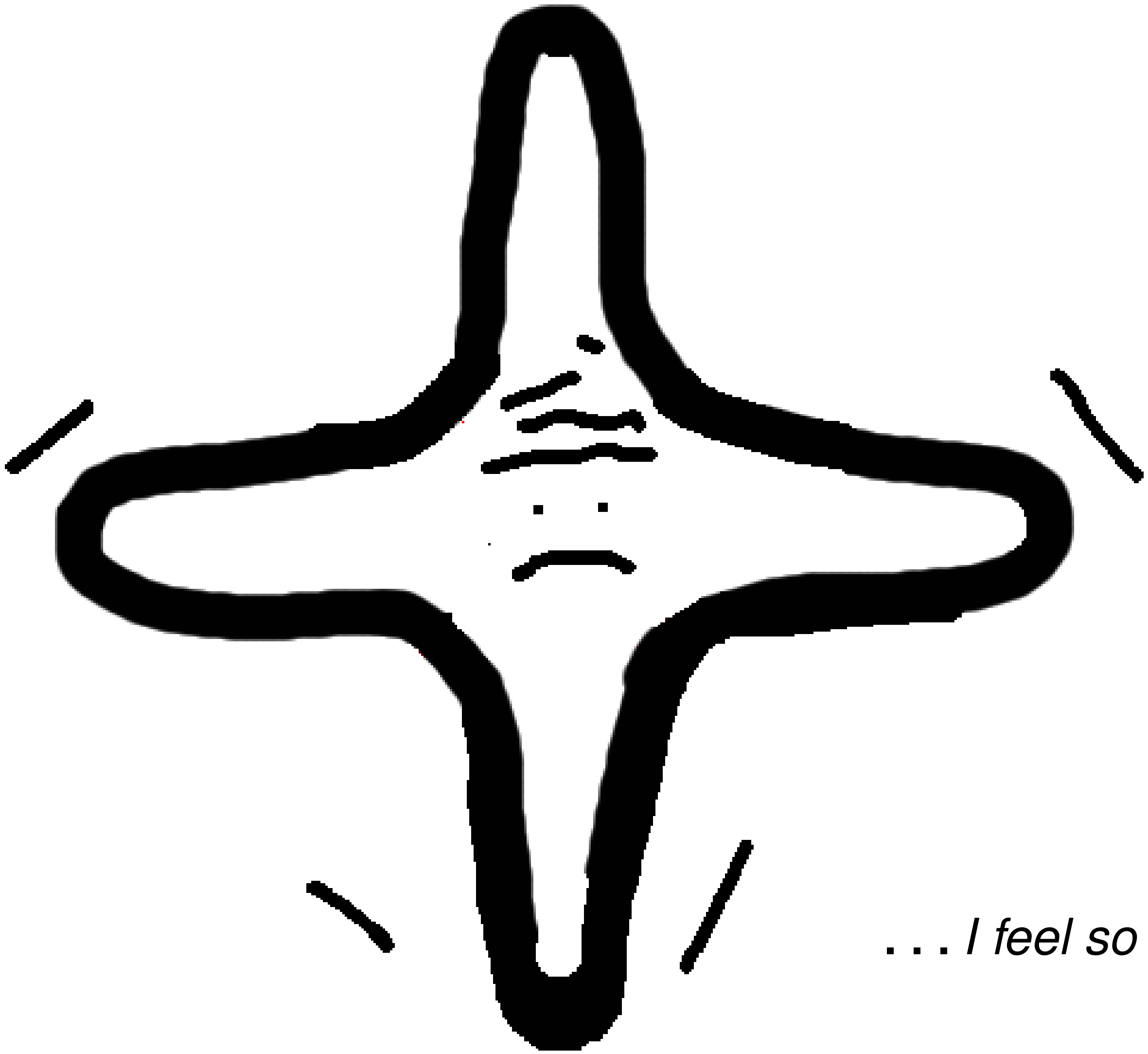
Edwards Curves – a new star(fish) is born



lecture circuit:

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

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*

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

$x^2 + y^2 = a^2(1 + x^2y^2), a^5 \neq a$
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*

Even characteristic much more interesting for hardware …

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*

Even characteristic much more interesting for hardware . . .
and soon also in software, cf. Intel's and Sun's current announcements to include binary instructions.

How to design a worthy binary partner?

Our wish-list (early February 2008) after studying and experimenting with mostly small modifications of odd Edwards:

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) after studying and experimenting with mostly small modifications of odd Edwards:

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.

Binary Edwards curves

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

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

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

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

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

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

  if denominators are nonzero.
- Neutral element is $(0, 0)$; again, this is an affine point.
- $(1, 1)$ has order 2.
- $-(x, y) = (y, x)$.
- $(x_1, y_1) + (1, 1) = (x_1 + 1, y_1 + 1)$.

Edwards curves over finite fields $\mathbb{F}_{2^n}$

- Trace is map $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2;\ \alpha \mapsto \sum_{i=0}^{n-1} \alpha^{2^i}$.
- For any points $(x_1, y_1), (x_2, y_2)$ 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 $\mathrm{Tr}(d_2) = 1$.
- In particular, addition formulas can be used to double.
- Addition law for curves with $\mathrm{Tr}(d_2) = 1$ is not only strongly unified but even complete.
- No exceptional points, completely uniform group operations.
- These are 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 curve if $n \geq 3$.

Generality & 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 or use curves where $d_1 = d_2$ is possible; then only 2M+ 5S+2D for a doubling.

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
Edwards $d_1 = d_2$	2M+5S; new, complete

Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

contains also formulas for characteristic 2; including some speed-ups for non-Edwards coordinates, e.g. 2M + 4S +2D for case considered by Kim-Kim.

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 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.

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 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, ...

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 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, $\ldots$ (only updates, no patents, pending).

Happy End!