Faster Addition and Doubling on Elliptic Curves

Daniel J. Bernstein and Tanja Lange

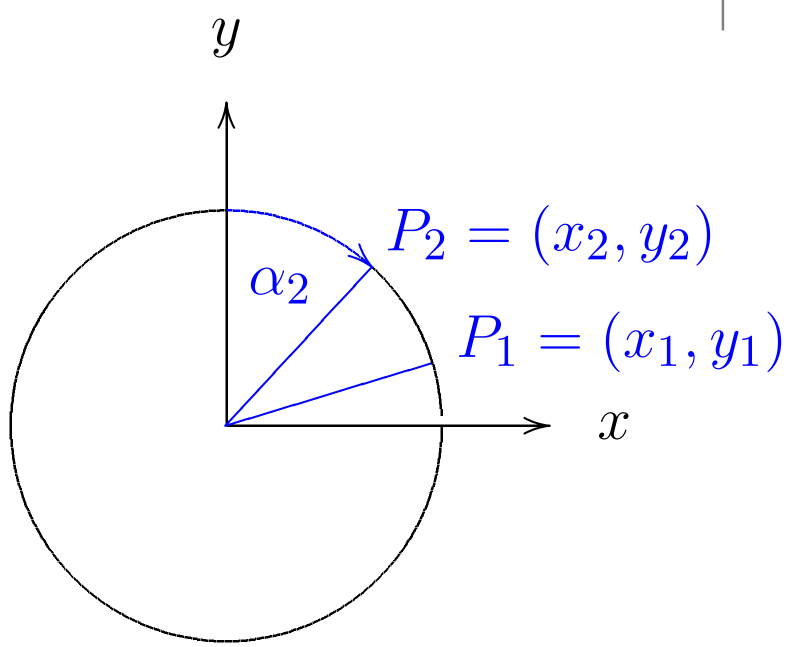
University of Illinois at Chicago and Technische Universiteit Eindhoven

djb@cr.yp.to
tanja@hyperelliptic.org

03 December 2007

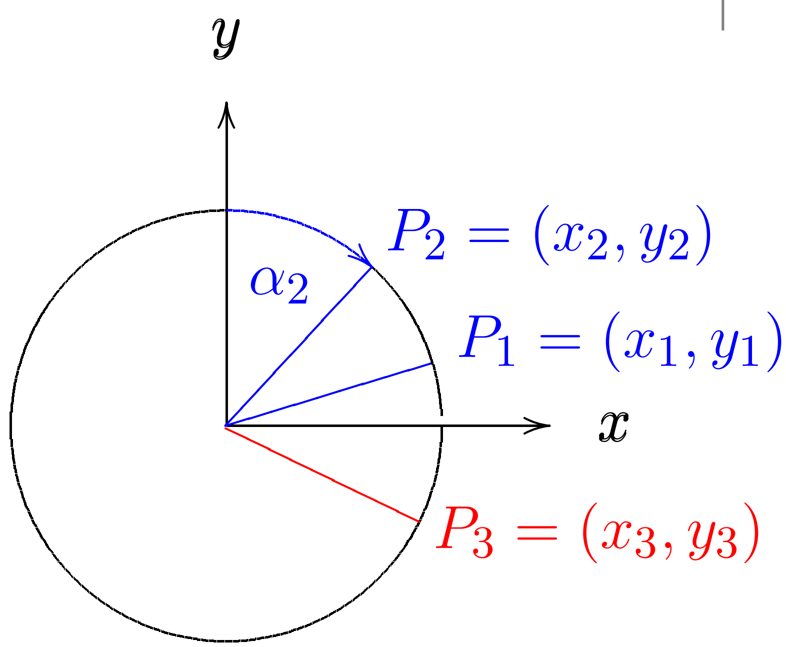
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



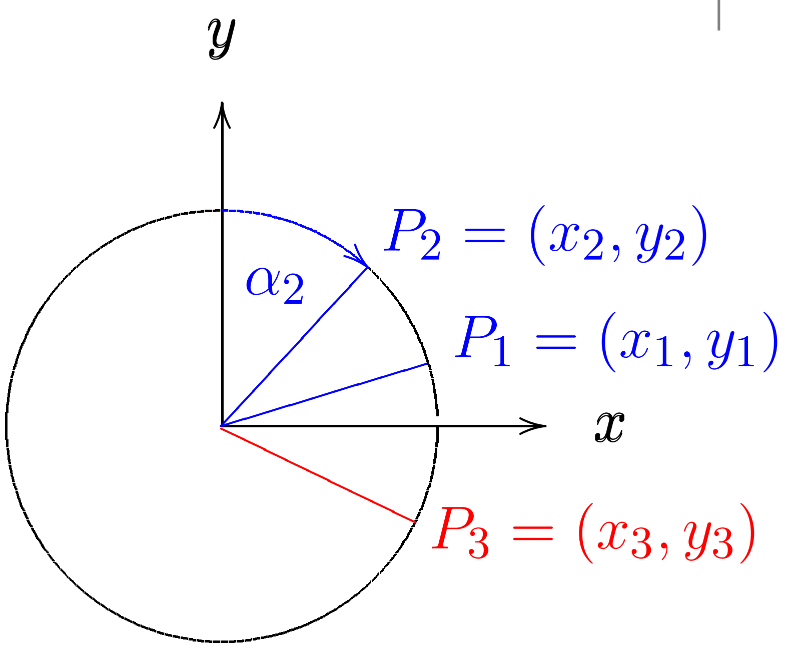
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x,y) \in k \times k | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i),\ y_i = \cos(\alpha_i)$



$$
\begin{aligned}
x_3 &= \sin(\alpha_1 + \alpha_2) \\
&= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2)
\end{aligned}
$$

$$
\begin{aligned}
y_3 &= \cos(\alpha_1 + \alpha_2) \\
&= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2)
\end{aligned}
$$

Addition of angles defines commutative group law
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

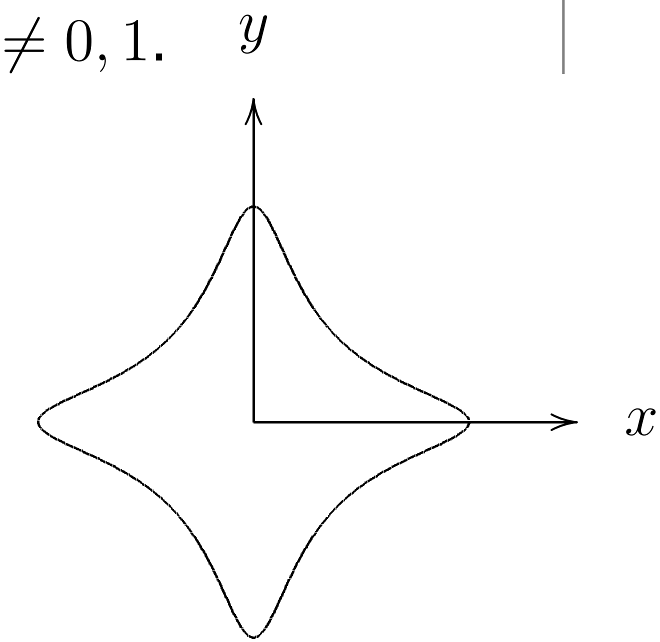
$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Now 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:

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

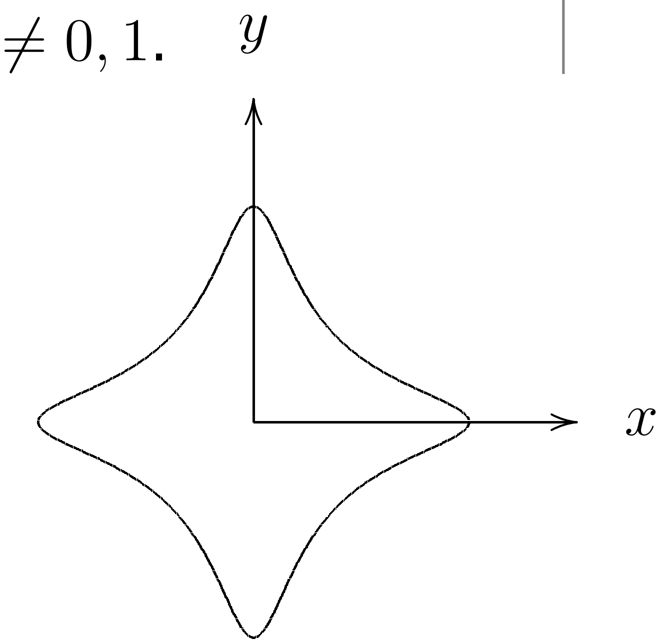
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



Now 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:

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

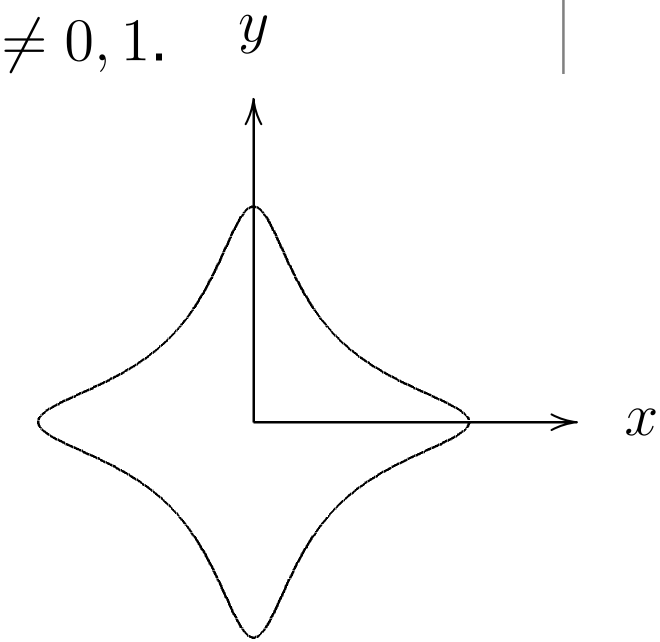
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

Now 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:

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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

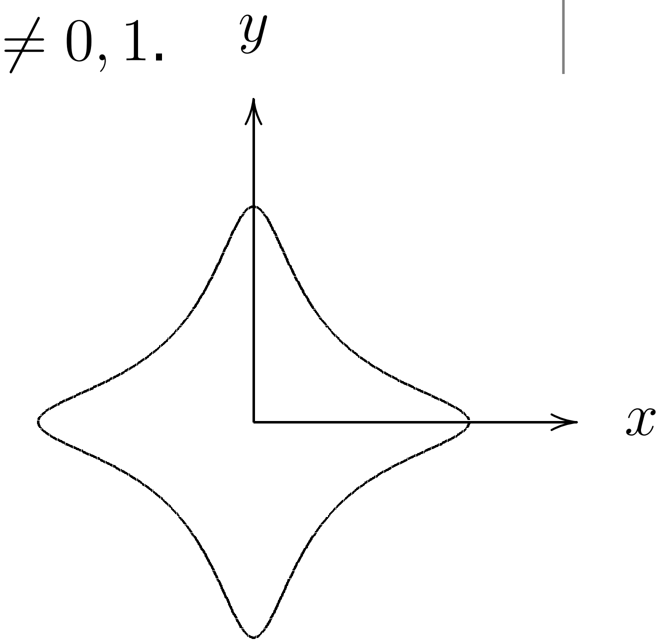
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

Now 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:

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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

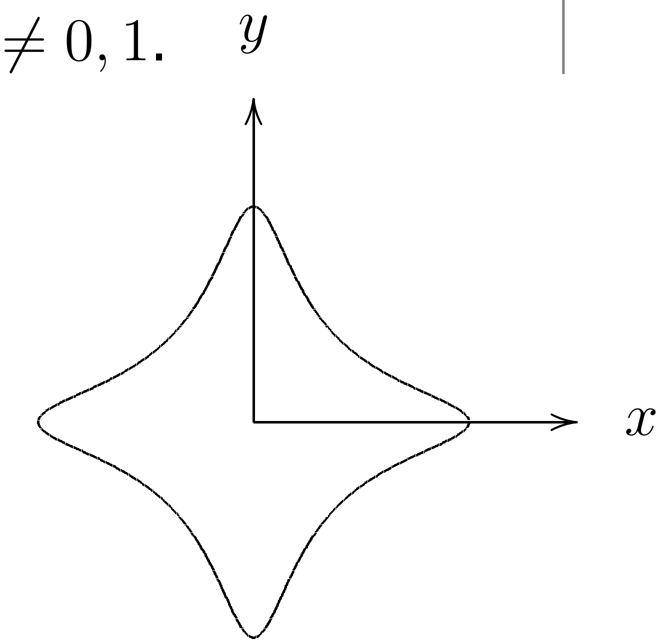
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).

Now 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:

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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

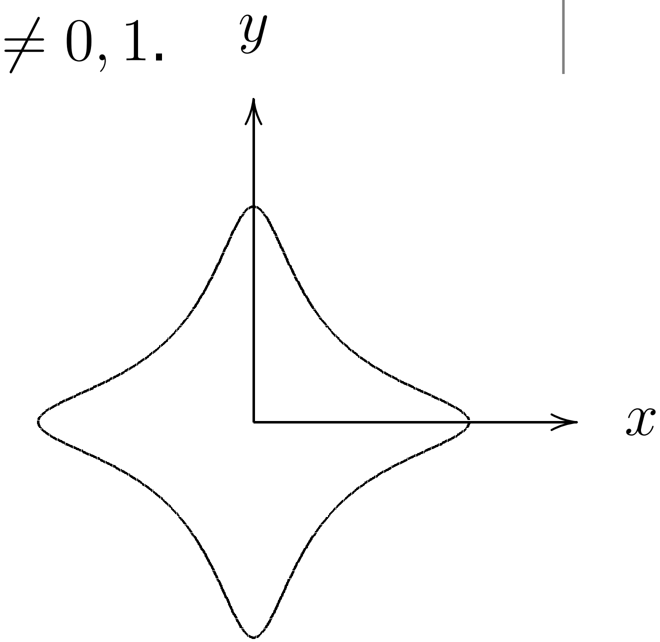
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).
- $-(x_1, y_1) =$

Now 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:

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



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

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 $(0, 1)$ (like on circle).
- $-(x_1, y_1) = (-x_1, y_1)$.

Explicit formulas: addition

- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- Avoid inversions: Use $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ to represent $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$, i. e., $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for $\lambda \neq 0$.
- Addition formulas in projective coordinates:

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

- Needs 10M + 1S + 1D + 7A.

Explicit formulas: doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1}\right)$$
  $$= \left(\frac{2 x_1 y_1}{1 + d(x_1 y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1 y_1)^2}\right)$$

Explicit formulas: doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1}\right)$$
$$= \left(\frac{2 x_1 y_1}{1 + d(x_1 y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1 y_1)^2}\right)$$

  Use curve equation $x^2 + y^2 = 1 + d x^2 y^2$.

Explicit formulas: doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \frac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1}\right)$$
  $$= \left(\frac{2x_1y_1}{1 + d(x_1y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1y_1)^2}\right)$$
  $$= \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)}\right)$$

Explicit formulas: doubling

- $$(x_1, y_1) + (x_1, y_1) = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right)$$
$$= \left(\frac{2 x_1 y_1}{1 + d(x_1 y_1)^2}, \frac{y_1^2 - x_1^2}{1 - d(x_1 y_1)^2} \right)$$
$$= \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right)$$
- Doubling formulas in projective coordinates:
$$\begin{aligned} B &= (X_1 + Y_1)^2;\ C = X_1^2;\ D = Y_1^2; \\ E &= C + D;\ H = Z_1^2;\ J = E - 2H; \\ X_3 &= (B - E) \cdot J;\ Y_3 = E \cdot (C - D);\ Z_3 = E \cdot J. \end{aligned}$$
- Needs 3M + 4S + 6A.

Relationship to elliptic curves

- 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 $v(u + u_4) = 0$.

Complete addition law

- Neutral element is affine point on curve.
- Addition works to add P and P.
- Addition works to add P and $-P$.
- For d not a square in k, the Edwards addition law is complete. Denominators in $x_3,\ y_3$ are never 0: Points $(1:0:0)$ and $(0:1:0)$ are singular; correspond to the four solutions of $v(u+u_4)=0$ other than $(0,0)$. But those four points are minimally defined over $k(\sqrt{d})$.
- Edwards addition law allows omitting all checks.
- Addition just works to add P and any Q.
- Only complete addition law in the literature.
- About 25% of all elliptic curves over fixed finite field have point of order 4 with non-square d.

Weierstrass projective Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $E : Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3$; $(x, y) \sim (X/Z, Y/Z)$

Addition: $P \neq \pm Q$

$A = Y_2 Z_1 - Y_1 Z_2, B = X_2 Z_1 - X_1 Z_2,$
$C = A^2 Z_1 Z_2 - B^3 - 2B^2 X_1 Z_2$
$X_3 = BC, Z_3 = B^3 Z_1 Z_2$
$Y_3 = A(B^2 X_1 Z_2 - C) - B^3 Y_1 Z_2,$

Doubling $P = Q \neq -P$

$A = a_4 Z_1^2 + 3X_1^2, B = Y_1 Z_1,$
$C = X_1 Y_1 B, D = A^2 - 8C$
$X_3 = 2BD, Z_3 = 8B^3$.
$Y_3 = A(4C - D) - 8Y_1^2 B^2$

- No inversion is needed – good for most implementations
- General ADD: 12M+2S
- DBL: 7M+5S
- Fast . . . but very different performance of ADD and DBL

Weierstrass Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1)$, $Q = (X_2 : Y_2 : Z_2)$, $P \oplus Q = (X_3 : Y_3 : Z_3)$
on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$; $(x, y) \sim (X/Z^2, Y/Z^3)$

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$
$D = Y_2 Z_1^3, E = B - A, F = D - C$
$X_3 = 2(-E^3 - 2AE^2 + F^2)$
$Z_3 = E(Z_1 + Z_2)^2 - Z_1^2 - Z_2^2$
$Y_3 = 2(-CE^3 + F(AE^2 - X_3))$,

Doubling $P = Q \neq -P$

$A = Y_1^2, B = Z_1^2$
$C = 4X_1 A, D = 3X_1^2 + a_4 B^2$
$X_3 = -2C + D^2$
$Z_3 = (Y_1 + Z_1)^2 - A - B$
$Y_3 = -8A^2 + D(C - X_3)$.

- General ADD: 11M+5S
- mixed ADD ($\mathcal{J} + \mathcal{A} = \mathcal{J}$): 8M+3S
- DBL: 3M+7S (one M by a_4); for $a_4 = -3$: 3M+5S

Chudnovsky Jacobian Coordinates

$P = (X_1 : Y_1 : Z_1 : Z_1^2 : Z_1^3)$, $Q = (X_2 : Y_2 : Z_2 : Z_2^2 : Z_2^3)$,
$P \oplus Q = (X_3 : Y_3 : Z_3 : Z_3^2 : Z_3^3)$ on $Y^2 = X^3 + a_4 X Z^4 + a_6 Z^6$;
$(x, y) \sim (X/Z^2, Y/Z^3)$

Addition: $P \neq \pm Q$

$A = X_1 Z_2^2, B = X_2 Z_1^2, C = Y_1 Z_2^3,$
$D = Y_2 Z_1^3, E = B - A, F = D - C$
$X_3 = 2(-E^3 - 2AE^2 + F^2)$
$Z_3 = E(Z_1 + Z_2)^2 - Z_1^2 - Z_2^2$
$Y_3 = 2(-CE^3 + F(AE^2 - X_3))$,
Z_3^2, Z_3^3,

Doubling $P = Q \neq -P$

$A = Y_1^2,$
$C = 4X_1 A, D = 3X_1^2 + a_4(Z_1^2)^2$
$X_3 = -2C + D^2$
$Z_3 = (Y_1 + Z_1)^2 - A - Z_1^2$
$Y_3 = -8A^2 + D(C - X_3)$
Z_3^2, Z_3^3

- General ADD: 10M+4S
- mixed ADD ($\mathcal{J} + \mathcal{A} = \mathcal{J}$): 8M+3S
- DBL: 3M+7S (one M by a_4)

Montgomery Form

Generalized to arbitrary multiples
$[n]P = (X_n : Y_n : Z_n), [m]P = (X_m : Y_m : Z_m)$ with known difference $[m-n]P$ on

$$E_M : By^2 = x^3 + Ax^2 + x$$

Addition: $n \neq m$

$$\begin{aligned} X_{m+n} &= Z_{m-n}\big((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\big)^2, \\ Z_{m+n} &= X_{m-n}\big((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\big)^2 \end{aligned}$$

Doubling: $n = m$

$$\begin{aligned} 4X_nZ_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2, \\ X_{2n} &= (X_n + Z_n)^2(X_n - Z_n)^2, \\ Z_{2n} &= 4X_nZ_n\big((X_n - Z_n)^2 + \big((A+2)/4\big)(4X_nZ_n)\big). \end{aligned}$$

An addition takes 4M and 2S whereas a doubling needs only 3M and 2S. Order is divisible by 4.

Side-channel atomicity

- Chevallier-Mames, Ciet, Joye 2004
  Idea: build group operation from identical blocks.
- Each block consists of:

  1 multiplication, 1 addition, 1 negation, 1 addition;

  fill with cheap dummy additions and negations

  ADD $(\mathcal{A} + \mathcal{J})$ needs 11 blocks
  DBL $(2\mathcal{J})$ needs 10 blocks

. . .									. . .
	ADD$_9$	ADD$_{10}$	ADD$_{11}$	DBL$_1$	DBL$_2$	DBL$_3$	DBL$_4$	DBL$_5$	

- Requires that M and S are indistinguishable from their traces.
- No protection against fault attacks.

Unified Projective coordinates

- Brier, Joye 2002
  Idea: unify how the slope is computed.
- improved in Brier, Déchène, and Joye 2004
- $$\lambda = \frac{(x_1 + x_2)^2 - x_1 x_2 + a_4 + y_1 - y_2}{y_1 + y_2 + x_1 - x_2} = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & (x_1, y_1) \neq \pm(x_2, y_2) \\ \frac{3x_1^2 + a_4}{2y_1} & (x_1, y_1) = (x_2, y_2) \end{cases}$$

  Multiply numerator & denominator by $x_1 - x_2$ to see this.
- Proposed formulae can be generalized to projective coordinates.
- Some special cases may occur, but with very low probability, e. g. $x_2 = y_1 + y_2 + x_1$. Alternative equation for this case.

Hessian curves

$$E_H : X^3 + Y^3 + Z^3 = cXYZ.$$

Addition: $P \neq \pm Q$

$$X_3 = X_2 Y_1^2 Z_2 - X_1 Y_2^2 Z_1$$
$$Y_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1$$
$$Z_3 = X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2$$

Doubling $P = Q \neq -P$

$$X_3 = Y_1(X_1^3 - Z_1^3)$$
$$Y_3 = X_1(Z_1^3 - Y_1^3)$$
$$Z_3 = Z_1(Y_1^3 - X_1^3)$$

- Curves were first suggested for speed
- Joye and Quisquater show

$$[2](X_1 : Y_1 : Z_1) = (Z_1 : X_1 : Y_1) \oplus (Y_1 : Z_1 : X_1)$$

- Unified formulas need 12M.
- Doubling is done by an addition, but not automatically – only unified, not strongly unified.

Jacobi intersections

- Chudnovsky and Chudnovsky 1986; Liardet and Smart CHES 2001
- Elliptic curve given as intersection of two quadratics

$$s^2 + c^2 = 1 \text{ and } as^2 + d^2 = 1.$$

- Points $(S : C : D : Z)$ with $(s, c, d) = (S/Z, C/Z, D/Z)$.
- Neutral element is $(0, 1, 1)$.

$$\begin{aligned}
S_3 &= (Z_1C_2 + D_1S_2)(C_1Z_2 + S_1D_2) - Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\
C_3 &= Z_1C_2C_1Z_2 - D_1S_2S_1D_2 \\
D_3 &= Z_1D_1Z_2D_2 - aS_1C_1S_2C_2 \\
Z_3 &= Z_1C_2^2 + D_1S_2^2.
\end{aligned}$$

- Unified formulas need 13M + 2S + 1D.

Jacobi quartics

- Billet and Joye AAECC 2003

$$E_J : Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4.$$

$$\begin{aligned} X_3 &= X_1 Z_1 Y_2 + Y_1 X_2 Z_2 \\ Z_3 &= (Z_1 Z_2)^2 - \epsilon (X_1 X_2)^2 \\ Y_3 &= (Z_3 + 2\epsilon (X_1 X_2)^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) + \\ & \quad 2\epsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + Z_1^2 X_2^2). \end{aligned}$$

- Unified formulas need 10M+3S+D+2E
- Can have ϵ or δ small
- Needs point of order 2; for $\epsilon = 1$ the group order is divisible by 4.
- Some recent speed ups due to Duquesne, to Hisil/Carter/Dawson and to Feng/Wu.

Extended Jacobi quartics

- Duquesne 2007

$$E_J : Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4.$$

with coordinates $(X_1, Y_1, Z_1, X_1^2, 2X_1Z_1, Z_1^2, X_1^2 + Z_1^2)$

$$\begin{aligned} X_3 &= !X@\#Y\$\% \\ Y_3 &= \text{ Why ask Y?} \\ Z_3 &= 3.14159265358979323846264338327950288419 71 \end{aligned}$$

- Some recent speed ups due to Hisil/Carter/Dawson.
- Faster addition . . .

There is help!

Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

Doubling speed overview

System	Cost of doubling (as of today)
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	7M+1S; see Hisil/Carter/Dawson '07
Doche/Icart/Kohel-3	2M+7S+2D; see B./Birkner/L./Peters
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB '01
Jacobi quartic	2M+6S+1D; see EFD
Ext. Jacobi quartic	3M+4S; see Hisil/Carter/Dawson '07
Jacobi intersection	3M+4S; EFD
Edwards	3M+4S;
Doche/Icart/Kohel-2	2M+5S+2D; EFD

- Edwards fastest for general curves, no D.

Addition speed overview

System	Cost of addition
Doche/Icart/Kohel-2	12M+5S+1D; EFD
Doche/Icart/Kohel-3	11M+6S+1D; see B./Birkner/L./Peters '07
Jacobian	11M+5S; EFD
Jacobi intersection	13M+2S+1D; see Liardet/Smart '01
Projective	12M+2S; see Chudnovsky/Chudnovsky '86
Jacobi quartic	10M+3S+1D; see Billet/Joye '03
Hessian	12M; see Sylvester (1800's)
Edwards	10M+1S+1D
Ext. Jacobi quartic	8M+3S+1D; EFD (based on Duquesne)

OOPS!

Inverted Edwards coordinates

Bernstein/Lange, to appear at AAECC 2007

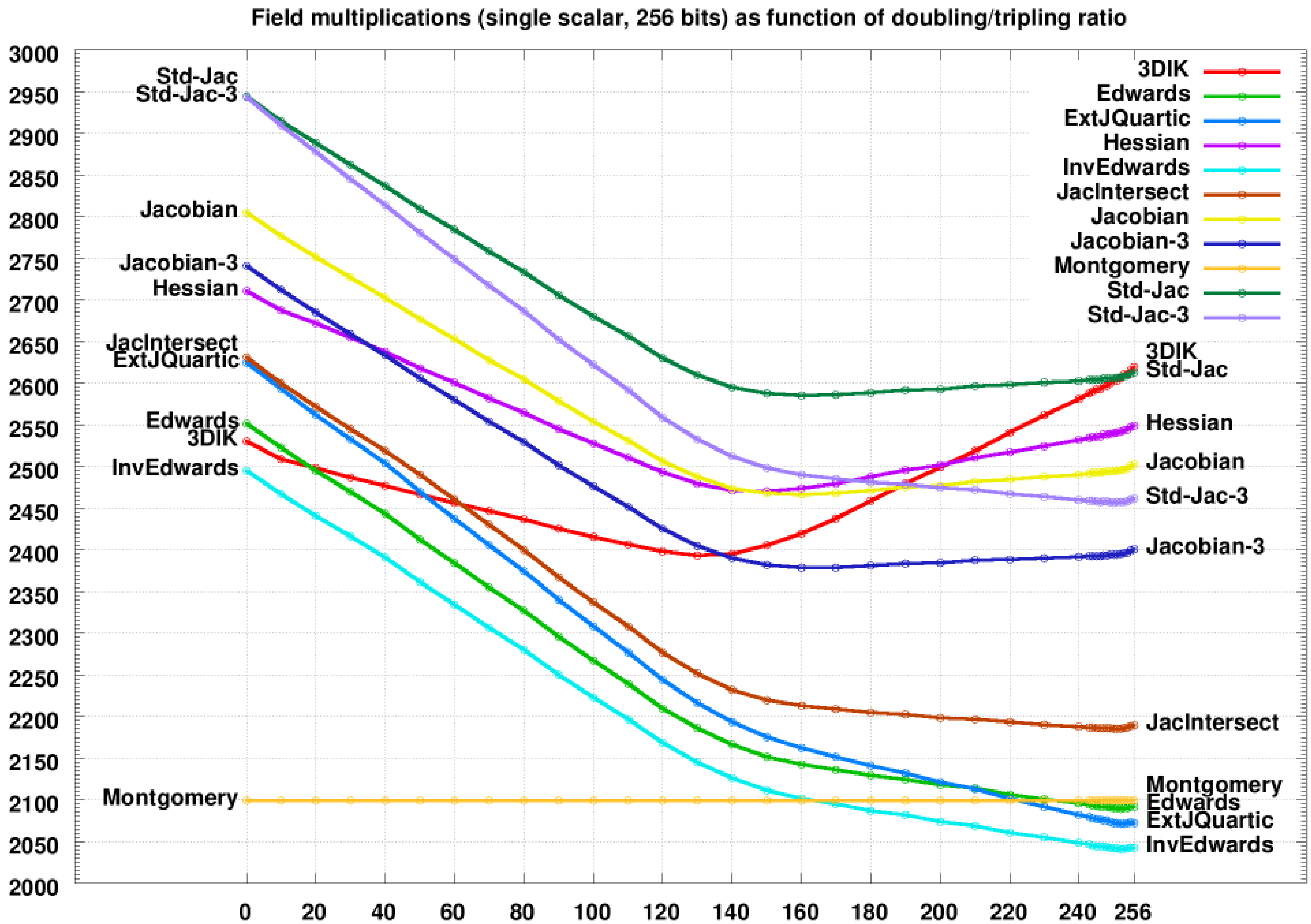
- Using the representation $(X_1 : Y_1 : Z_1)$ for the affine point $(Z_1/X_1, Z_1/Y_1)$ ($X_1Y_1Z_1 \neq 0$) gives operation counts:
  - Doubling takes 3M+4S+1D.
  - Addition takes 9M+1S+1D.
- This saves 1M for each addition compared to standard Edwards coordinates.
- Doubling slower by 1D; so choose small d.
- Extended Jacobi quartics need 8M+3S+1D to add.
- Inverted Edwards coordinates are strongly unified system – but not complete.

Addition speed overview

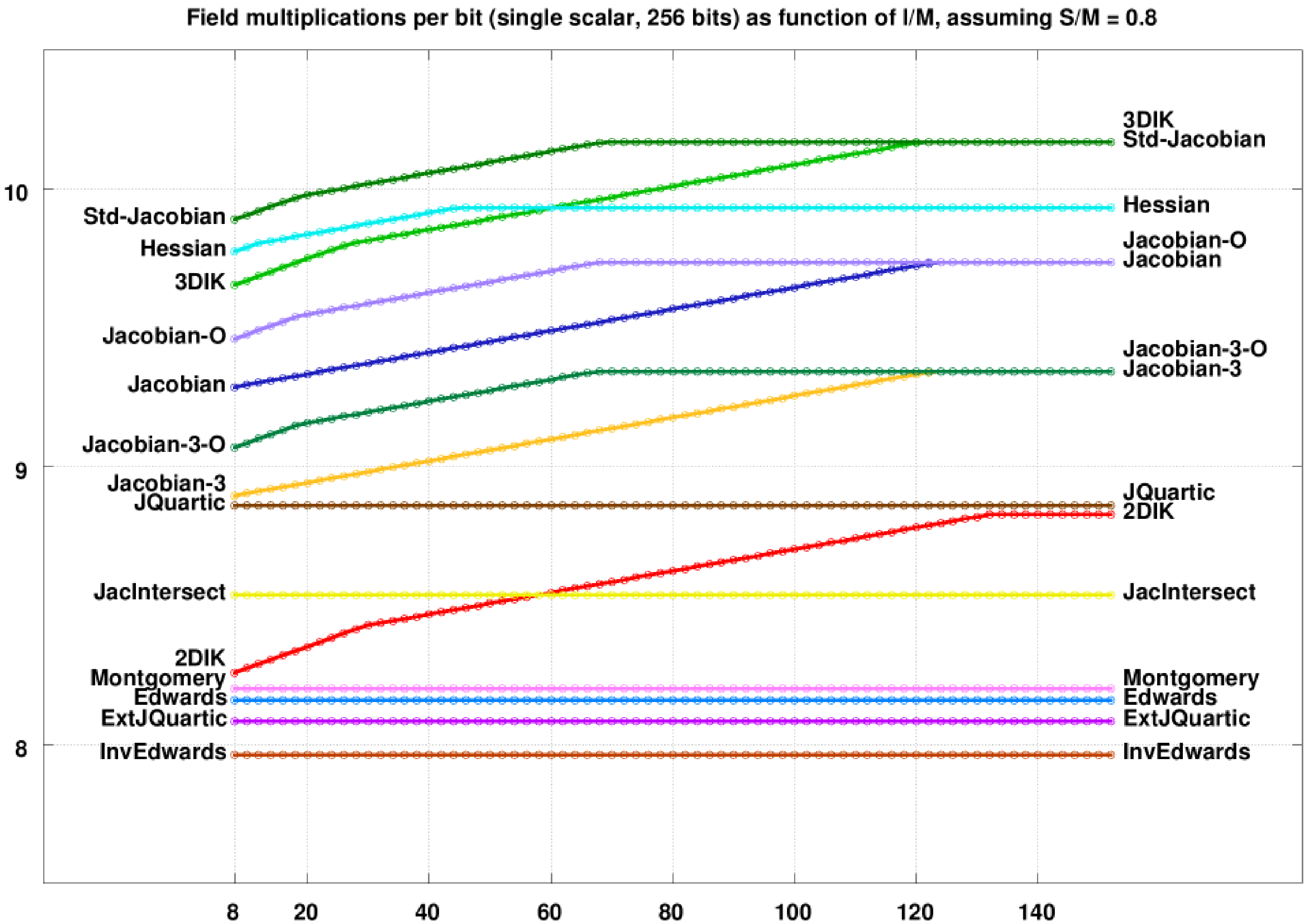
System	Cost of addition
Doche/Icart/Kohel-2	12M+5S+1D; EFD
Doche/Icart/Kohel-3	11M+6S+1D; see B./Birkner/L./Peters ’07
Jacobian	11M+5S; EFD
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Projective	12M+2S; see Chudnovsky/Chudnovsky ’86
Jacobi quartic	10M+3S+1D; see Billet/Joye ’03
Hessian	12M; see Sylvester (1800’s)
Edwards	10M+1S+1D
Ext. Jacobi quartic	8M+3S+1D; EFD (based on Duquesne)
Inverted Edwards	9M+1S+1D; see B./L. ’07

- New speed leader: inverted Edwards.

Influence of triplings, Indocrypt'07



Influence of inversions, Fq8 2007



Edwards everywhere

- Edwards for SSCA (fastest unified addition).

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.
- First implementation results: Edwards for ECM, faster than Montgomery!

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.
- First implementation results: Edwards for ECM, faster than Montgomery!
- In progress: Edwards for ECPP.

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.
- First implementation results: Edwards for ECM, faster than Montgomery!
- In progress: Edwards for ECPP.
- In progress: Edwards for president.

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.
- First implementation results: Edwards for ECM, faster than Montgomery!
- In progress: Edwards for ECPP.
- In progress: Edwards for characteristic 2.

Edwards everywhere

- Edwards for SSCA (fastest unified addition).
- Edwards for multi-scalar multiplication.
- Twisted Edwards curves: Edwards for more curves, higher speeds.
- First implementation results: Edwards for ECM, faster than Montgomery!
- In progress: Edwards for ECPP.
- In progress: Edwards for characteristic 2.
- In progress: Edwards for genus 2.

Thank you for your attention!

Details on the blow-up

- Points with $v(u+u_4)=0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1-(4u_4^3/v_4^2)$.
- $u=-u_4$ is u-coordinate of a point iff

$$\begin{aligned}&(-u_4)^3+(v_4^2/u_4^2-2u_4)(u_4)^2+u_4^2(u_5)\\ =\ & v_4^2-4u_4^3 = v_4^2 d\end{aligned}$$

  is a square, i. e., iff d is a square.
- $v=0$ corresponds to $(0,0)$ which maps to $(0,-1)$ on Edwards curve and to solutions of $u^2+(v_4^2/u_4^2-2u_4)u+u_4^2=0$. Discriminant is

$$(v_4^2/u_4^2-2u_4)^2-4u_4^2 = v_4^4 d,$$

  i. e., points defined over k iff d is a square.

References

- Harold M. Edwards, "A normal form for elliptic curves" Bulletin of the AMS, **44**, 393–422, 2007.
- B./Birkner/L./Peters, "Optimizing double-base elliptic-curve single-scalar multiplication", Indocrypt 2007, pp. 167–182. Online.
- B./L. "Analysis and optimization of elliptic-curve single-scalar multiplication" Proceedings of Fq8, to appear. Online.
- B./L. "Inverted Edwards coordinates", AAECC 2007, pp. 20–27. Online.
- B./Birkner/L./Peters, "Twisted Edwards Curves", submitted.
- B./Birkner/L./Peters, "ECM using Edwards curves", submitted.