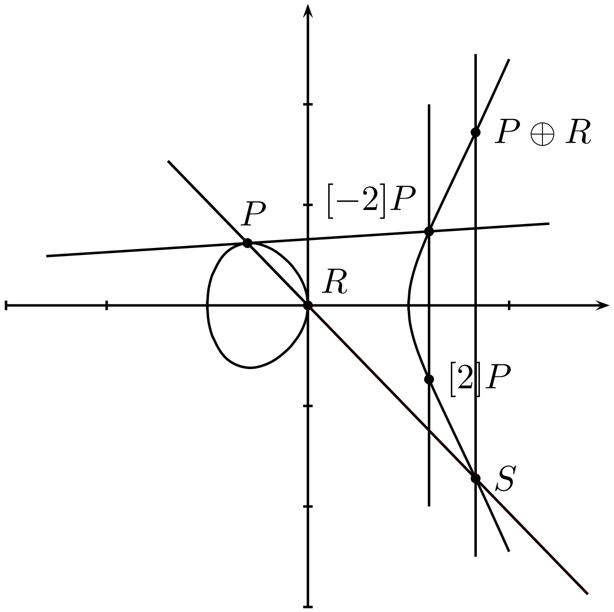
Fast scalar multiplication on elliptic curves

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

12.07.2007

Group Law (q odd)

$$E : y^2 = x^3 + a_4 x + a_6,\ a_i \in \mathbb{F}_q$$



In general, for $(x_P, y_P) \neq (x_R, -y_R)$:

$$(x_P, y_P) \oplus (x_R, y_R) =$$
$$= (x_{P\oplus R}, y_{P\oplus R}) =$$
$$= (\lambda^2 - x_P - x_R, \lambda(x_P - x_{P\oplus R}) - y_P),$$

where

$$\lambda = \begin{cases} (y_R - y_P)/(x_R - x_P) & \text{if } x_P \neq x_R, \\ (3x_P^2 + a_4)/(2y_P) & \text{else.} \end{cases}$$

Thanks to Andreas for explaining this picture in detail!

- Addition (ADD) takes 1I + 2M + 1S.
- Doubling (DBL) takes 1I + 2M + 2S.

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: 5M+6S+1D (D=M by a_4)

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 $P = Q \neq -P$

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

- Again no inversion
- General ADD: 11M+5S
- mixed ADD ($\mathcal{J} + \mathcal{A} = \mathcal{J}$): 7M+4S
- DBL: 1M+8S+1D; for $a_4 = -3$: 3M+5S

Jacobi quartic

- Billet and Joye AAECC 2003: Jacobi-Model

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

- Can use same formulas for ADD and DBL

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

- ADD needs 10M+3S+1D+2E; DBL needs 1M+9S+1D
- Unified formulas need 10M+3S+D+2E
- Can have ϵ or δ small.

Hessian curves

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

Addition: $P \neq \pm Q$	Doubling $P = Q \neq -P$
$X_3 = X_2 Y_1^2 Z_2 - X_1 Y_2^2 Z_1$	$X_3 = Y_1(X_1^3 - Z_1^3)$
$Y_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1$	$Y_3 = X_1(Z_1^3 - Y_1^3)$
$Z_3 = X_2 Y_2 Z_1^2 - X_1 Y_1 Z_2^2$	$Z_3 = Z_1(Y_1^3 - X_1^3)$

- ADD needs 12M, DBL needs 6M + 3S
- Joye and Quisquater suggested Hessian Curves for unified group operations using

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

- Unified formulas need 12M.
- Needs point of order 3.

Different coordinate systems

For many more coordinate systems, the group law, operation counts (and improvements) for the explicit formulas, MAGMA-based proofs of their correctness, lots of entertainment visit the

Explicit Formulas Database

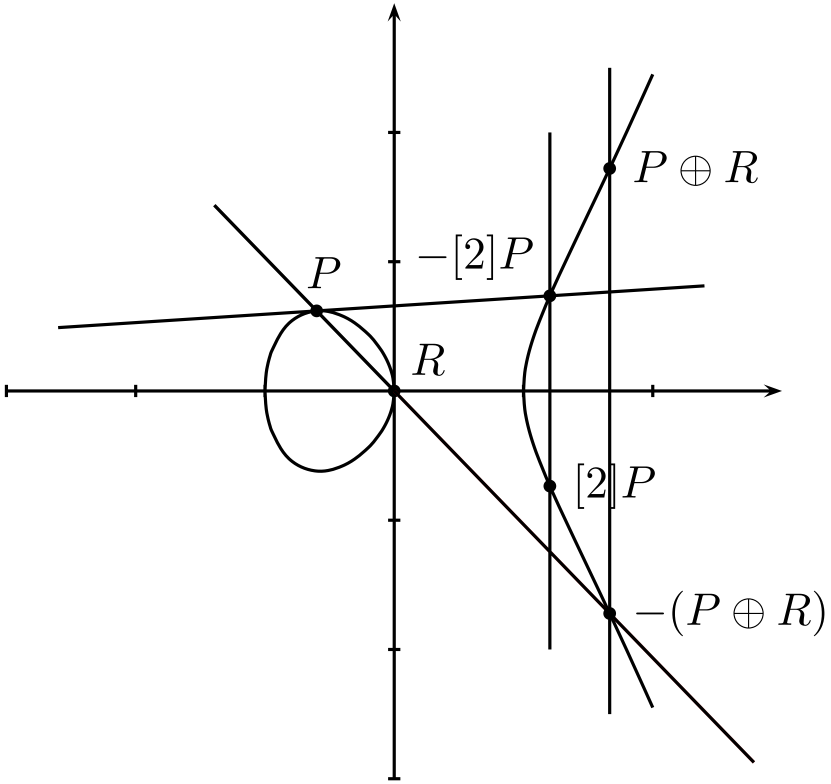
`http://www.hyperelliptic.org/EFD`

Edwards coordinates

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

So Dan and I expected …



Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

$$x^2 + y^2 = a^2(1 + x^2y^2).$$

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

$$x^2 + y^2 = a^2(1 + x^2y^2).$$

Nonsingular if and only if $a^5 \neq a$.

Addition on Elliptic Curves

At Mathematics: Algorithms and Proofs in Leiden, January 2007, Harold M. Edwards gave a talk on Addition on Elliptic Curves

But there it was – the elliptic curve:

$$x^2 + y^2 = a^2(1 + x^2y^2).$$

Nonsingular if and only if $a^5 \neq a$.
To see that this is indeed an elliptic curve, use $z = y(1 - a^2x^2)/a$ to obtain

$$z^2 = x^4 - (a^2 + 1/a^2)x^2 + 1.$$

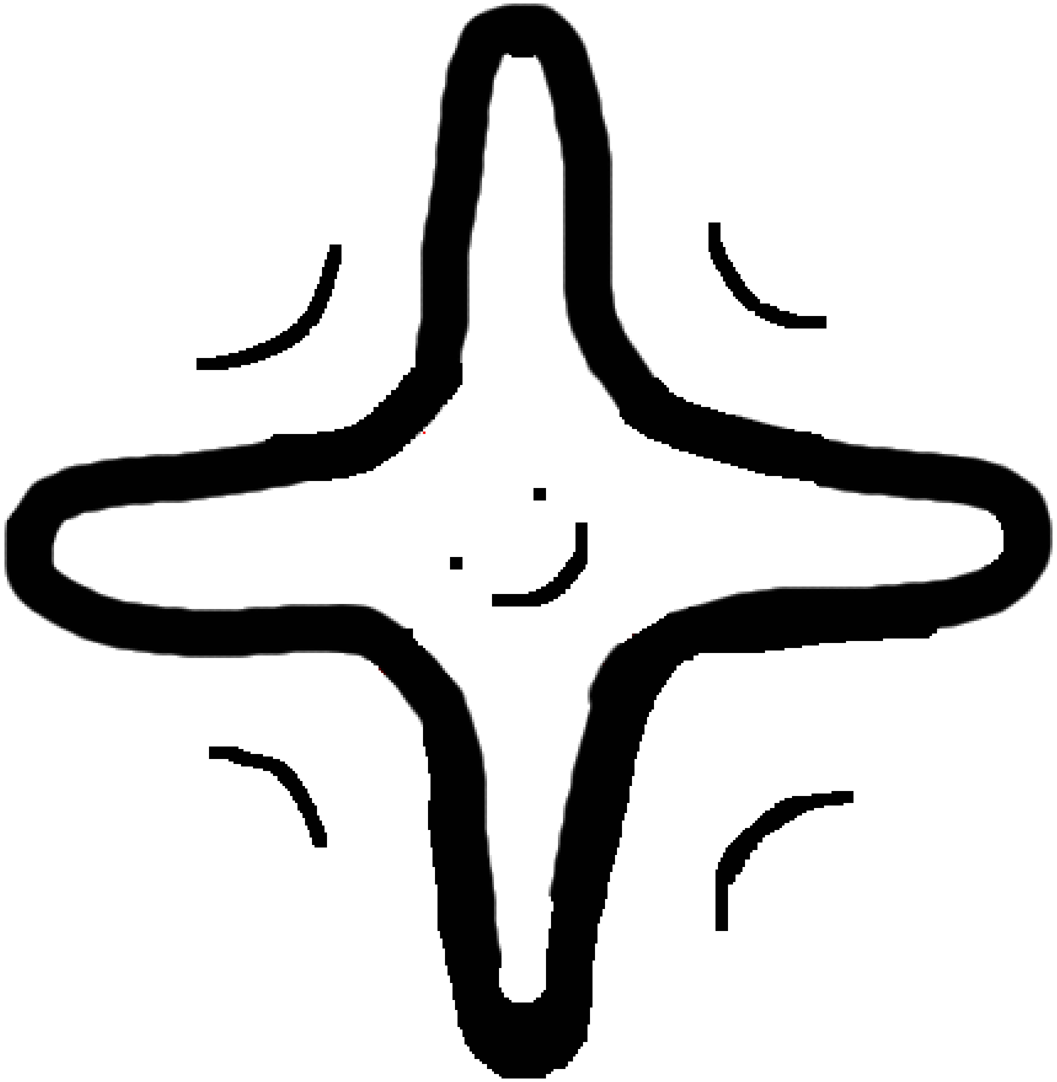
Edwards curves

- More details:
  Harold M. Edwards Jr., Bulletin of the AMS, electronic April 9, 2007
- Edwards shows that generically every elliptic curve can be written in this form – over some extension field.
- Gauss (and this is basically the only mention of this form that Edwards and we could dig out) shows that

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

  is elliptic. To transform this curve we need $\sqrt{-1}$ in the field.

Snapshot



Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + d x_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - d x_P x_Q y_P y_Q)} \right).$
- $[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)} \right).$

Edwards coordinates

Introduce further parameter and relabel

$$x^2+y^2=c^2(1+dx^2y^2),\ c,d\neq 0, dc^4\neq 1.$$

- Neutral element is $(0,c)$, this is an affine point!
- $-(x_P,y_P)=(-x_P,y_P)$.
- $P+Q=\left(\frac{x_Py_Q+y_Px_Q}{c(1+dx_Px_Qy_Py_Q)},\frac{y_Py_Q-x_Px_Q}{c(1-dx_Px_Qy_Py_Q)}\right).$
- $[2]P=\left(\frac{x_Py_P+y_Px_P}{c(1+dx_Px_Py_Py_P)},\frac{y_Py_P-x_Px_P}{c(1-dx_Px_Py_Py_P)}\right).$
- Unified group operations!
- If d is not a square, formulas even strongly unified (NO exceptional cases)

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2), \; c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$

$$\begin{aligned}
A &= Z_P \cdot Z_Q;\; B = A^2;\; C = X_P \cdot X_Q;\; D = Y_P \cdot Y_Q;\\
E &= (X_P + Y_P) \cdot (X_Q + Y_Q) - C - D;\; F = d \cdot C \cdot D;\\
X_{P \oplus Q} &= A \cdot E \cdot (B - F);\; Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F);\\
Z_{P \oplus Q} &= c \cdot (B - F) \cdot (B + F).
\end{aligned}$$

Edwards coordinates

Introduce further parameter and relabel

$$x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \neq 0, dc^4 \neq 1.$$

- Neutral element is $(0, c)$, this is an affine point!
- $-(x_P, y_P) = (-x_P, y_P)$.
- $P + Q = \left(\frac{x_P y_Q + y_P x_Q}{c(1 + dx_P x_Q y_P y_Q)}, \frac{y_P y_Q - x_P x_Q}{c(1 - dx_P x_Q y_P y_Q)}\right).$

$$\begin{aligned}
A &= Z_P \cdot Z_Q;\ B = A^2;\ C = X_P \cdot X_Q;\ D = Y_P \cdot Y_Q;\\
E &= (X_P + Y_P) \cdot (X_Q + Y_Q) - C - D;\ F = d \cdot C \cdot D;\\
X_{P \oplus Q} &= A \cdot E \cdot (B - F);\ Y_{P \oplus Q} = A \cdot (D - C) \cdot (B + F);\\
Z_{P \oplus Q} &= c \cdot (B - F) \cdot (B + F).
\end{aligned}$$

Needs 10M + 1S + 1C + 1D + 7A. At least one of c, d small.

Fastest unified addition-or-doubling formulae

System	Cost of unified addition-or-doubling
Projective	11M+6S+1D; see Brier/Joye ’03
Projective if $a_4 = -1$	13M+3S; see Brier/Joye ’02
Jacobi intersection	13M+2S+1D; see Liardet/Smart ’01
Jacobi quartic ($\epsilon = 1$)	10M+3S+1D; see Billet/Joye ’01
Hessian	12M; see Joye/Quisquater ’01
Edwards ($c = 1$)	10M+1S+1D

- Exactly the same formulae for doubling (no re-arrangement like in Hessian; no if-else)
- No exceptional cases if d is not a square. Formulae correct for all affine inputs (incl. $(0, c), -P$).
- Caveat: Edwards curves have points of order 4, namely $(\pm c, 0)$.

But wait – there's more!

How about non-unified doubling?

$$[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)}\right)$$

$$= \left(\frac{2 x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)}\right)$$

How about non-unified doubling?

$$
\begin{aligned}
[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)}\right) \\
&= \left(\frac{2 x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)}\right) \\
&= \left(\frac{2 c x_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))}\right)
\end{aligned}
$$

Use curve equation $x^2 + y^2 = c^2(1 + dx^2y^2)$.

How about non-unified doubling?

$$
\begin{aligned}
[2]P &= \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)}\right)\\
&= \left(\frac{2x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)}\right)\\
&= \left(\frac{2c x_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))}\right)\\
&= \left(\frac{2c x_P y_P}{x_P^2 + y_P^2}, \frac{c(y_P^2 - x_P^2)}{2c^2 - (x_P^2 + y_P^2)}\right)
\end{aligned}
$$

How about non-unified doubling?

$$[2]P = \left(\frac{x_P y_P + y_P x_P}{c(1 + d x_P x_P y_P y_P)}, \frac{y_P y_P - x_P x_P}{c(1 - d x_P x_P y_P y_P)}\right)$$

$$= \left(\frac{2 x_P y_P}{c(1 + d(x_P y_P)^2)}, \frac{y_P^2 - x_P^2}{c(1 - d(x_P y_P)^2)}\right)$$

$$= \left(\frac{2 c x_P y_P}{c^2(1 + d(x_P y_P)^2)}, \frac{c(y_P^2 - x_P^2)}{c^2(2 - (1 + d(x_P y_P)^2))}\right)$$

$$= \left(\frac{2 c x_P y_P}{x_P^2 + y_P^2}, \frac{c(y_P^2 - x_P^2)}{2c^2 - (x_P^2 + y_P^2)}\right)$$

Inversion-free version needs 3M + 4S + 3C + 6A.
Can always choose $c = 1$ by isomorphic transformations!
Assume this in the following, D refers to multiplications by d.

Very fast doubling formulae

System	Cost of doubling
Projective	5M+6S+1D; EFD
Projective if $a_4 = -3$	7M+3S; EFD
Hessian	6M+3S; see Joye/Quisquater ’01
Jacobi quartic	1M+9S+1D; see Billet/Joye ’01
Jacobian	1M+8S+1D; EFD
Jacobian if $a_4 = -3$	3M+5S; see DJB ’01
Jacobi intersection	3M+4S; see Liardet/Smart ’01
Edwards ($c = 1$)	3M+4S;
Doche/Icart/Kohel	2M+5S+2D; see Doche/Icart/Kohel ’06

- Edwards fastest for general curves, no D.
- Operation counts & formulas as in the EFD (often faster than original).

Fastest addition formulae

System	Cost of addition
Doche/Icart/Kohel	12M+5S+1D; see Doche/Icart/Kohel '06
Jacobian	11M+5S; EFD
Jacobi intersection	13M+2S+1D; see Liardet/Smart '01
Projective	12M+2S; HECC
Jacobi quartic	10M+3S+1D; see Billet/Joye '03
Hessian	12M; see Joye/Quisquater '01
Edwards ($c = 1$)	10M+1S+1D

- EFD and full paper also contain costs for mixed addition (mADD) and re-additions (reADD).
- mADD: ADD where one input has $Z = 1$.
- reADD: non-mixed ADD where one point has been added before and computations have been cached.

Single-scalar multiplication using NAF

System	1 DBL, 1/3 mADD
Projective	8M+6.67S+1D
Projective if $a_4 = -3$	10M+3.67S
Hessian	9.33M+3S
Jacobi quartic	3.67M+10S+1.33D
Jacobian	3.33M+9.33S+1D
Jacobian if $a_4 = -3$	5.33M+6.33S
Jacobi intersection	6.67M+4.67S+0.333D
Doche/Icart/Kohel	4.67M+6.33S+2.33D
Edwards	6M+4.33S+0.333D

For comparison: Montgomery arithmetic takes 5M+4S+1D per bit.

Signed width-4 sliding windows

These counts include the precomputations.

System	0.98 DBL, 0.17 reADD, 0.025 mADD, 0.0035 ADD
Projective	7.17M+6.28S+0.982D
Projective if $a_4 = -3$	9.13M+3.34S
Hessian	8.18M+2.95S
Jacobi quartic	2.71M+9.42S+1.18D
Jacobian	2.85M+8.64S+0.982D
Jacobian if $a_4 = -3$	4.82M+5.69S
Doche/Icart/Kohel	4.2M+5.86S+2.16D
Jacobi intersection	5.09M+4.32S+0.194D
Edwards	4.86M+4.12S+0.194D

For comparison: Montgomery arithmetic takes 5M+4S+1D per bit. Edwards solidly faster!

Many more comparisons &
applications in preprint, available at

`http://www.hyperelliptic.org/tanja/newelliptic/`

Update soon! (Hopefully tonight)