Optimizing double-base elliptic-curve single-scalar multiplication

(Joint work with Daniel J. Bernstein, Peter Birkner, Tanja Lange)

Christiane Peters

Technische Universiteit Eindhoven

Indocrypt 2007

Motivation

Speed-up techniques for elliptic-curve single-scalar multiplication

- choose different curve shapes
  (e.g. Edwards curves, Weierstrass form)
- choose different coordinate systems
  (e.g. inverted Edwards coordinates, Jacobian coordinates)
- use double-base chains
- use sliding-window methods

Question: How do all these techniques go together?

1. Different curve shapes and coordinate systems

2. Double-base number systems

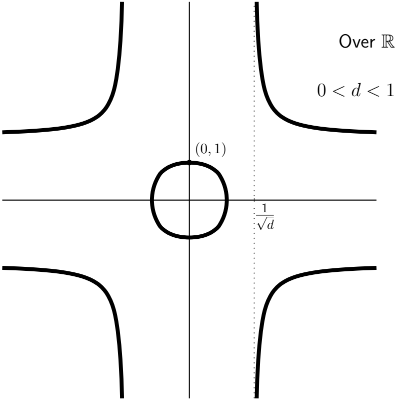
3. Experiments and results

Edwards curves

An elliptic curve E in Edwards form over a non-binary field is given by the equation

$$x^2 + y^2 = 1 + d\,x^2y^2,$$

where $d \neq 0, 1$.



From now on we will call a curve in this shape an Edwards curve.

Arithmetic on Edwards curves

Edwards addition law:

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

The addition law can also be used for doublings!!!

For higher efficiency one can use

$$[2](x_1, y_1) = \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right).$$

Tripling (also by Hisil/Carter/Dawson):

$$[3](x_1, y_1) =$$
$$\left(\frac{((x_1^2 + y_1^2)^2 - (2y_1)^2)}{4(x_1^2 - 1)x_1^2 - (x_1^2 - y_1^2)^2} x_1, \frac{((x_1^2 + y_1^2)^2 - (2x_1)^2)}{-4(y_1^2 - 1)y_1^2 + (x_1^2 - y_1^2)^2} y_1 \right).$$

Arithmetic on Edwards curves

Edwards addition law:

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

The addition law can also be used for doublings!!!

For higher efficiency one can use

$$[2](x_1, y_1) = \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right).$$

Tripling (also by Hisil/Carter/Dawson):

$$[3](x_1, y_1) =$$
$$\left(\frac{((x_1^2 + y_1^2)^2 - (2y_1)^2)}{4(x_1^2 - 1)x_1^2 - (x_1^2 - y_1^2)^2} x_1, \frac{((x_1^2 + y_1^2)^2 - (2x_1)^2)}{-4(y_1^2 - 1)y_1^2 + (x_1^2 - y_1^2)^2} y_1 \right).$$

Arithmetic on Edwards curves

Edwards addition law:

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

The addition law can also be used for doublings!!!
For higher efficiency one can use

$$[2](x_1, y_1) = \left(\frac{2 x_1 y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right).$$

Tripling (also by Hisil/Carter/Dawson):

$$[3](x_1, y_1) = \left(\frac{((x_1^2 + y_1^2)^2 - (2y_1)^2)}{4(x_1^2 - 1)x_1^2 - (x_1^2 - y_1^2)^2} x_1, \frac{((x_1^2 + y_1^2)^2 - (2x_1)^2)}{-4(y_1^2 - 1)y_1^2 + (x_1^2 - y_1^2)^2} y_1 \right).$$

Avoiding inversions

Consider the homogenized Edwards equation

$$E: (X^2 + Y^2)Z^2 = (Z^4 + dX^2Y^2)$$

A point $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$.

Bernstein/Lange (2007): Inverted Edwards coordinates

A point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ on

$$(X^2 + Y^2)Z^2 = X^2Y^2 + dZ^4$$

corresponds to $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$.

Avoiding inversions

Consider the homogenized Edwards equation

$$E: (X^2+Y^2)Z^2 = (Z^4 + dX^2Y^2)$$

A point $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$.

Bernstein/Lange (2007): Inverted Edwards coordinates

A point $(X_1 : Y_1 : Z_1)$ with $X_1Y_1Z_1 \neq 0$ on

$$(X^2+Y^2)Z^2 = X^2Y^2 + dZ^4$$

corresponds to $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve $x^2+y^2 = 1+dx^2y^2$.

Other curves forms

Short Weierstrass form $E : y^2 = x^3 + a_4 x + a_6$
with $a_4, a_6 \in \mathbb{F}_p$, $(p \geq 5)$, and $4a_4^3 + 27a_6^2 \neq 0$.

- Jacobian coordinates $Y^2 = X^3 + a_4 X Z^2 + a_6 Z^6$,
- "Standard Jacobian coordinates", i.e. $a_4 = -3$,
- "tripling-oriented Doche/Icart/Kohel curves"
  $Y^2 = X^3 + a(X + Z^2)^2 Z^2$.

More coordinate systems

- Jacobi quartics $Y^2 = X^4 + 2aX^2Z^2 + Z^4$,
- Hessian curves $X^3 + Y^3 + Z^3 = 3dXYZ$,
- Jacobi intersections $S^2 + C^2 = Z^2, aS^2 + D^2 = Z^2$,

Other curves forms

Short Weierstrass form $E : y^2 = x^3 + a_4x + a_6$

with $a_4, a_6 \in \mathbb{F}_p$, $(p \geq 5)$, and $4a_4^3 + 27a_6^2 \neq 0$.

- Jacobian coordinates $Y^2 = X^3 + a_4XZ^2 + a_6Z^6$,
- "Standard Jacobian coordinates", i.e. $a_4 = -3$,
- "tripling-oriented Doche/Icart/Kohel curves"
  $Y^2 = X^3 + a(X + Z^2)^2Z^2$.

More coordinate systems

- Jacobi quartics $Y^2 = X^4 + 2aX^2Z^2 + Z^4$,
- Hessian curves $X^3 + Y^3 + Z^3 = 3dXYZ$,
- Jacobi intersections $S^2 + C^2 = Z^2, aS^2 + D^2 = Z^2$,

Comparison

$\mathbf{M}$: general multiplications, $\mathbf{S}$: squarings

Curve shape	ADD	mADD	DBL	TRI
3DIK	$11\mathbf{M}+6\mathbf{S}$	$7\mathbf{M}+4\mathbf{S}$	$2\mathbf{M}+7\mathbf{S}$	$6\mathbf{M}+6\mathbf{S}$
Edwards	$10\mathbf{M}+1\mathbf{S}$	$9\mathbf{M}+1\mathbf{S}$	$3\mathbf{M}+4\mathbf{S}$	$9\mathbf{M}+4\mathbf{S}$
ExtJQuartic	$8\mathbf{M}+3\mathbf{S}$	$7\mathbf{M}+3\mathbf{S}$	$3\mathbf{M}+4\mathbf{S}$	$4\mathbf{M}+11\mathbf{S}$
Hessian	$12\mathbf{M}+0\mathbf{S}$	$10\mathbf{M}+0\mathbf{S}$	$7\mathbf{M}+1\mathbf{S}$	$8\mathbf{M}+6\mathbf{S}$
InvEdwards	$9\mathbf{M}+1\mathbf{S}$	$8\mathbf{M}+1\mathbf{S}$	$3\mathbf{M}+4\mathbf{S}$	$9\mathbf{M}+4\mathbf{S}$
JacIntersect	$13\mathbf{M}+2\mathbf{S}$	$11\mathbf{M}+2\mathbf{S}$	$3\mathbf{M}+4\mathbf{S}$	$4\mathbf{M}+10\mathbf{S}$
Jacobian	$11\mathbf{M}+5\mathbf{S}$	$7\mathbf{M}+4\mathbf{S}$	$1\mathbf{M}+8\mathbf{S}$	$5\mathbf{M}+10\mathbf{S}$
Jacobian-3	$11\mathbf{M}+5\mathbf{S}$	$7\mathbf{M}+4\mathbf{S}$	$3\mathbf{M}+5\mathbf{S}$	$7\mathbf{M}+7\mathbf{S}$
Std-Jac	$12\mathbf{M}+4\mathbf{S}$	$8\mathbf{M}+3\mathbf{S}$	$3\mathbf{M}+6\mathbf{S}$	$9\mathbf{M}+6\mathbf{S}$
Std-Jac-3	$12\mathbf{M}+4\mathbf{S}$	$8\mathbf{M}+3\mathbf{S}$	$4\mathbf{M}+4\mathbf{S}$	$9\mathbf{M}+6\mathbf{S}$

Details → Explicit-formulas database.
`http://www.hyperelliptic.org/EFD`.

1. Different curve shapes and coordinate systems

2. Double-base number systems

3. Experiments and results

Double-bases: base $\{2, 3\}$

Dimitrov, Jullien, Miller (1997): compute $[n]P$ as $\sum_{i \geq 1} c_i 2^{a_i} 3^{b_i}$ with $c_i = \pm 1$.

Dimitrov, Imbert and Mishra at Asiacrypt 2005: require

$$a_1 \geq a_2 \geq a_3 \geq \ldots, \text{ and } \qquad b_1 \geq b_2 \geq b_3 \geq \ldots$$

Benefit:	Horner-like evaluation; a_1 doublings, b_1 triplings needed.
Cost:	More additions.

Double-bases: base $\{2, 3\}$

Dimitrov, Jullien, Miller (1997): compute $[n]P$ as $\sum_{i \geq 1} c_i 2^{a_i} 3^{b_i}$ with $c_i = \pm 1$.

Dimitrov, Imbert and Mishra at Asiacrypt 2005: require

$$a_1 \geq a_2 \geq a_3 \geq \ldots, \text{ and } \qquad b_1 \geq b_2 \geq b_3 \geq \ldots$$

Benefit:	Horner-like evaluation; a_1 doublings, b_1 triplings needed.
Cost:	More additions.

Sliding window method

Doche and Imbert at Indocrypt 2006: Replace $c_i = \pm 1$ by $\pm c_i \in S$, where S is one of the sets

$$\{1\}, \{1, 2, 2^2, 3, 3^2\}, \ldots, \{1, 2, \ldots, 2^4, 3, \ldots, 3^4\},$$
$$\{1, 5, 7\}, \ldots, \{1, 5, 7, 11, 13, 17, 19, 23, 25\}.$$

Benefit:	Fewer additions.
Cost:	Precompute $[c]P$ for $c \in S$.

This paper

Bernstein/Birkner/Lange/P. 2007:

- more coordinate systems,
- account for costs of (inversion-free) precomputations,
- new faster formulas for arithmetic for different coordinate systems,
- larger variety of coefficient sets S:

$$\{1\},\ \{1,2,3\},\{1,2,3,4,9\},\ldots\{1,2,3,4,8,9,16,27,81\},$$
$$\{1,5\},\{1,5,7\},\ldots,\{1,5,7,11,13,17,19,23,25\},$$
$$\{1,2,3,5\},\ \{1,2,3,5,7\},\ldots\{1,2,3,5,7,9,11,13,15,17,19,23,25\}$$

Experiments show: none of the optimal results for scalars of bitlength ≥ 200 uses a set of precomputed points previously analyzed for double-base scalar multiplication.

1. Different curve shapes and coordinate systems

2. Double-base number systems

3. Experiments and results

Doubling-Tripling ratio

Given the restriction on the exponents,
vary maximal power of 2 and 3 in the representation $\sum_i c_i 2^{a_i} 3^{b_i}$ of an ℓ-bit scalar n.

a_0:	upper bound for exponents of 2,	$0 \leq a_0 \leq \ell$
b_0:	upper bound for exponents of 3,	$b_0 = \lceil (\ell - a_0)/\lg 3 \rceil$

Optimal parameters for each curve shape for $\ell = 256$

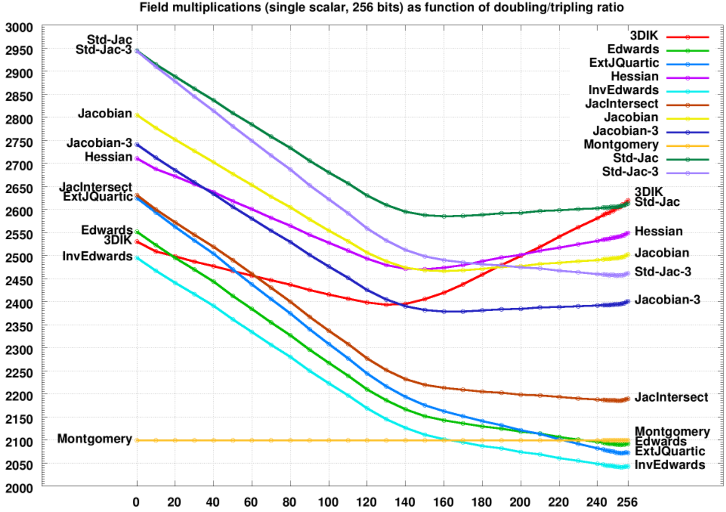
We assume $1\mathbf{S} = 0.8\mathbf{M}$ and $\mathbf{D} = 0\mathbf{M}$.

Curve shape	Mults	a_0	a_0/ℓ	S
3DIK	2393.193800	130	0.51	$\{1, 2, 3, 5, \ldots, 13\}$
Edwards	2089.695120	252	0.98	$\{1, 2, 3, 5, \ldots, 15\}$
ExtJQuartic	2071.217580	253	0.99	$\{1, 2, 3, 5, \ldots, 15\}$
Hessian	2470.643200	150	0.59	$\{1, 2, 3, 5, \ldots, 13\}$
InvEdwards	2041.223320	252	0.98	$\{1, 2, 3, 5, \ldots, 15\}$
JacIntersect	2266.135540	246	0.96	$\{1, 2, 3, 5, \ldots, 15\}$
Jacobian	2466.150480	160	0.62	$\{1, 2, 3, 5, \ldots, 13\}$
Jacobian-3	2378.956000	160	0.62	$\{1, 2, 3, 5, \ldots, 13\}$

We got similar results for $\ell = 160, 256, 300, 400, 500$.

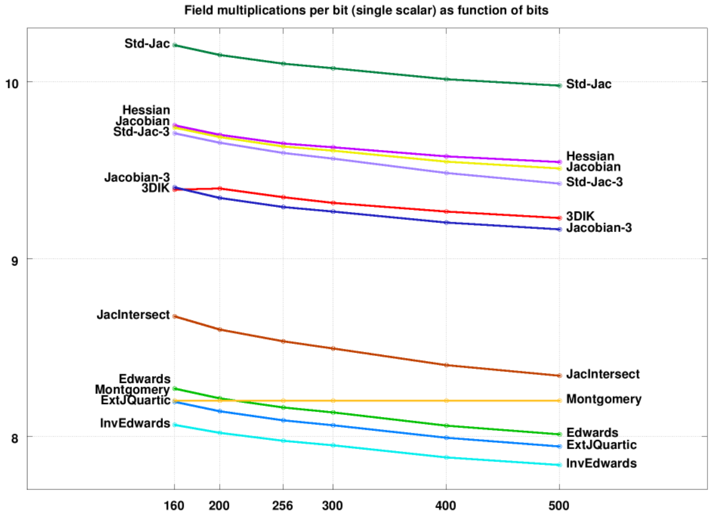
For each a_0: double-base representation for $10,000$ integers of bit-length 256.

Multiplications (256-bit single scalars) as function of doubling/tripling ratio



For each a_0: double-base representation for $10,000$ integers of bit-length $\ell = 256$.

Multiplications per bit



Conclusions

Triplings do help curves in Jacobian coordinates, tripling-oriented Doche/Icart/Kohel curves, Hessian curves.

The fastest systems are Edwards, Extended Jacobi-Quartics and Inverted Edwards:

They

- need the lowest number of multiplications for a_0 closest to the bitlength ℓ,
- use larger sets of precomputations
- and fewer triplings;
- have fast addition formulas (precomputations less costly)
- and in particular very fast doublings.