From now on: non-binary field k;
non-square $d \in k$.

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

is a commutative group with
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2},$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Birationally equivalent to
$(1/e)v^2 = u^3 + (4/e - 2)u^2 + u$
where $e = 1 - d$.

Represent $(x, y) \in E(k)$
by $(X : Y : Z) \in \mathbf{P}^2(k)$;
i.e., $(X, Y, Z) \in k^3$ with $Z \neq 0$
and $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$
represents $(X/Z, Y/Z) \in E(k)$.

$10\mathbf{M}$ (10 field mults)
$+\ 1\mathbf{S}$ (1 field squaring)
$+\ 1\mathbf{D}$ (1 field mult by d)
$+\ 7\mathbf{add}$ (7 field additions)
to obtain sum $(X_3 : Y_3 : Z_3)$
of $(X_1 : Y_1 : Z_1)$, $(X_2 : Y_2 : Z_2)$.

Don't have to make distinctions
for equal inputs, negatives, etc.

What if we *want* to make distinctions to gain speed?

For example, speed up doubling?

$$2(x, y)$$
$$= \left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyyy} \right)$$

What if we *want* to make distinctions to gain speed?
For example, speed up doubling?

$$2(x, y)$$
$$= \left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyy} \right)$$
$$= \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ save mults!

What if we *want* to make distinctions to gain speed?
For example, speed up doubling?

$2(x, y)$

$$= \left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyy} \right)$$

$$= \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ save mults!

$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ low deg (Joye)

What if we *want* to make distinctions to gain speed?
For example, speed up doubling?

$$2(x, y)$$
$$= \left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyy} \right)$$
$$= \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ save mults!
$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ low deg (Joye)
$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{2 - x^2 - y^2} \right)$$ even lower

What if we *want* to make distinctions to gain speed?
For example, speed up doubling?

$$2(x, y)$$
$$= \left(\frac{xy + yx}{1 + dxxyy}, \frac{yy - xx}{1 - dxxyy} \right)$$
$$= \left(\frac{2xy}{1 + dx^2y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ save mults!
$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{1 - dx^2y^2} \right)$$ low deg (Joye)
$$= \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{2 - x^2 - y^2} \right)$$ even lower
$$= \left(\frac{(x + y)^2}{x^2 + y^2} - 1, \frac{y^2 - x^2}{2 - x^2 - y^2} \right)$$

$3\mathbf{M}$ (3 field mults)

$+ 4\mathbf{S}$ (4 field squarings)

$+ 6\mathbf{add}$ (6 field additions)

to double $(X_1 : Y_1 : Z_1)$:

$$B = (X_1 + Y_1)^2,$$
$$C = X_1^2,$$
$$D = Y_1^2,$$
$$E = C + D,$$
$$H = Z_1^2,$$
$$J = E - 2H,$$
$$X_3 = (B - E)J,$$
$$Y_3 = E(C - D),$$
$$Z_3 = EJ.$$

Comparison of doubling costs if curve parameters are small:

System	Cost
Projective	$5\mathbf{M} + 6\mathbf{S}$
Projective if $a = -3$	$7\mathbf{M} + 3\mathbf{S}$
Hessian	$7\mathbf{M} + 1\mathbf{S}$
Doche/Icart/Kohel 3	$2\mathbf{M} + 7\mathbf{S}$
Jacobian	$1\mathbf{M} + 8\mathbf{S}$
Jacobian if $a = -3$	$3\mathbf{M} + 5\mathbf{S}$
Jacobi quartic	$2\mathbf{M} + 6\mathbf{S}$
Jacobi intersection	$3\mathbf{M} + 4\mathbf{S}$
Edwards	$3\mathbf{M} + 4\mathbf{S}$
Doche/Icart/Kohel 2	$2\mathbf{M} + 5\mathbf{S}$

EFD! EFD! EFD! EFD! EFD!

e.g. Doche/Icart/Kohel paper says $3\mathbf{M}+4\mathbf{S}$ for Doche/Icart/Kohel 2.

Jacobian $a = -3$ vs. Edwards:

	Jac-3	Edwards
Double	3**M**+5**S**	3**M**+4**S**
Triple	7**M**+7**S**	9**M**+4**S**
Add	11**M**+5**S**	10**M**+1**S**+1**D**
Readd	10**M**+4**S**	10**M**+1**S**+1**D**
Mixed	7**M**+4**S**	9**M**+1**S**+1**D**
Unified	unclear	10**M**+1**S**+1**D**

Jac-3 speedup for readd: Chudnovsky/Chudnovsky 1986; "Chudnovsky coordinates" etc.

Edwards tripling: Bernstein/Birkner/Lange/Peters 2007; independently Hisil/Carter/Dawson 2007.

A sensible ElGamal-type system (van Duin, `sci.crypt`, 2006):

Everyone knows standard point B, prime order q, on "Curve25519": $\mathbf{Z}/(2^{255}-19)$; $d = 1 - 1/121666$.

Signer has 32-byte secret key n. Everyone knows signer's 32-byte public key: compressed nB.

To verify (m, compressed R, t): verify $tB = H(R, m)R + nB$.

To sign m: generate a secret s; $R = sB$; $t = H(R, m)s + n \bmod q$.

Notes: 1. No inversions mod q.
2. Send R, not $H(R, m)$.

Batch verification of many $t_iB - h_iR_i = S_i$: check $\sum_i v_it_iB - \sum_i v_ih_iR_i - \sum_i v_iS_i = 0$ for random 128-bit v_i. (Naccache et al., Eurocrypt 1994; Bellare et al., Eurocrypt 1998)

Use subtractive multi-scalar multiplication algorithm: if $n_1 \geq n_2 \geq \cdots$ then $n_1P_1 + n_2P_2 + n_3P_3 + \cdots = (n_1 - qn_2)P_1 + n_2(qP_1 + P_2) + n_3P_3 + \cdots$ where $q = \lfloor n_1/n_2 \rfloor$. (credited to Bos and Coster by de Rooij, Eurocrypt 1994; see also tweaks by Wei Dai, 2007)

Verifying 100 signatures
requires a 201-scalar mult
with 101 256-bit scalars
and 100 128-bit scalars.

Subtractive algorithm then uses
$\approx 24.4 \cdot 256$ readds and
$\approx 0.8 \cdot 256$ mixed adds.

$\mathbf{S}/\mathbf{M} = 0.8$, small parameters:
$\approx 845\mathbf{M}$/signature with Jacobian;
$\approx 695\mathbf{M}$/signature with Edwards.
Use Edwards coordinates!

Can similar speeds be achieved
by genus-2 hyperelliptic curves?
Current attempts seem very slow.

We've counted mults
(with various $\mathbf{S}/\mathbf{M}, \mathbf{D}/\mathbf{M}$) for
Edwards, Jac-3, Hessian, et al.
in NAF; width-4 sliding windows;
JSF; accelerated ECDSA;
batch verification, as above;
fixed-point scalar mult; and
several side-channel situations.

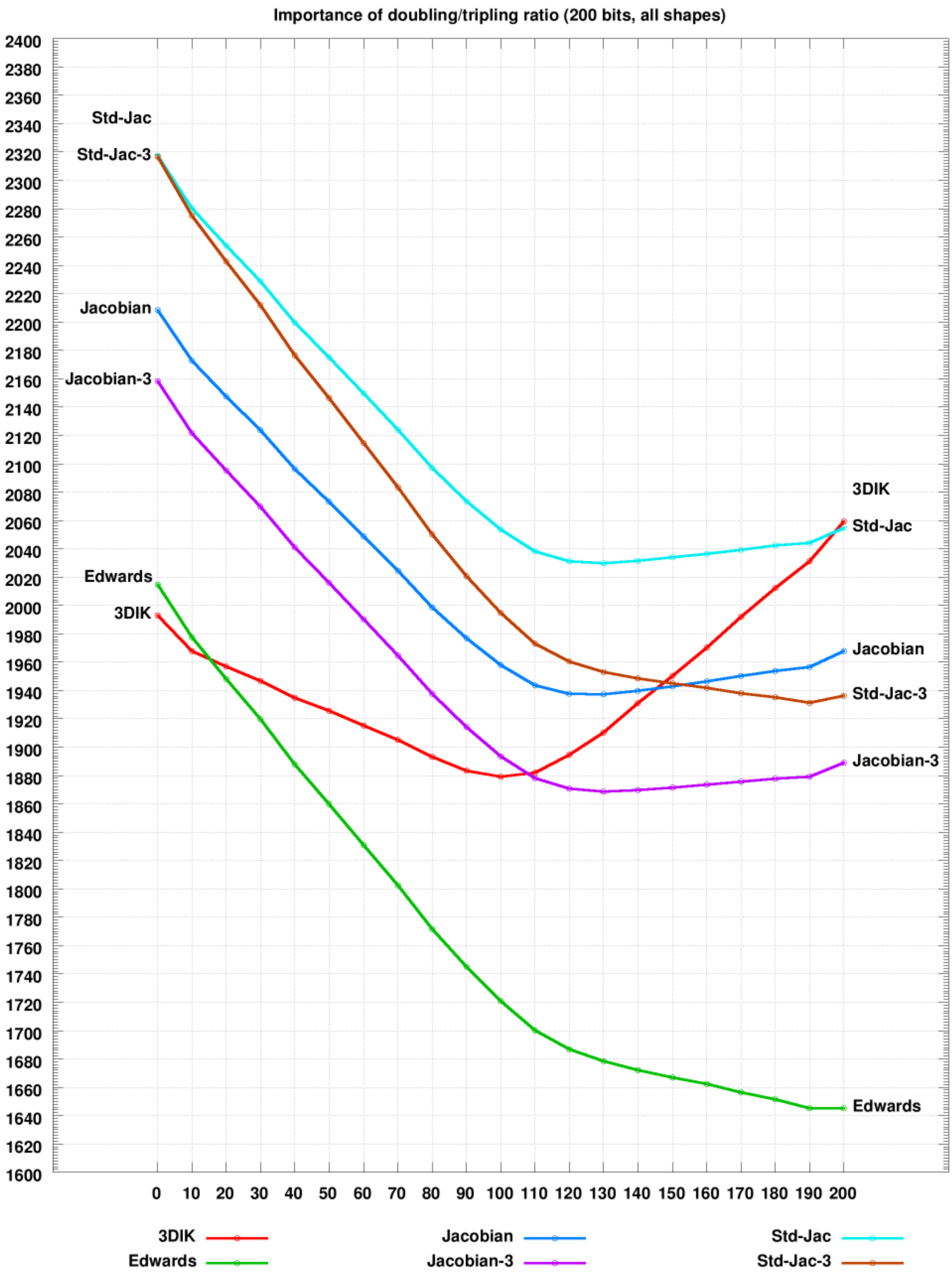
Edwards consistently wins!
Should even beat Montgomery
for big single-scalar mult.

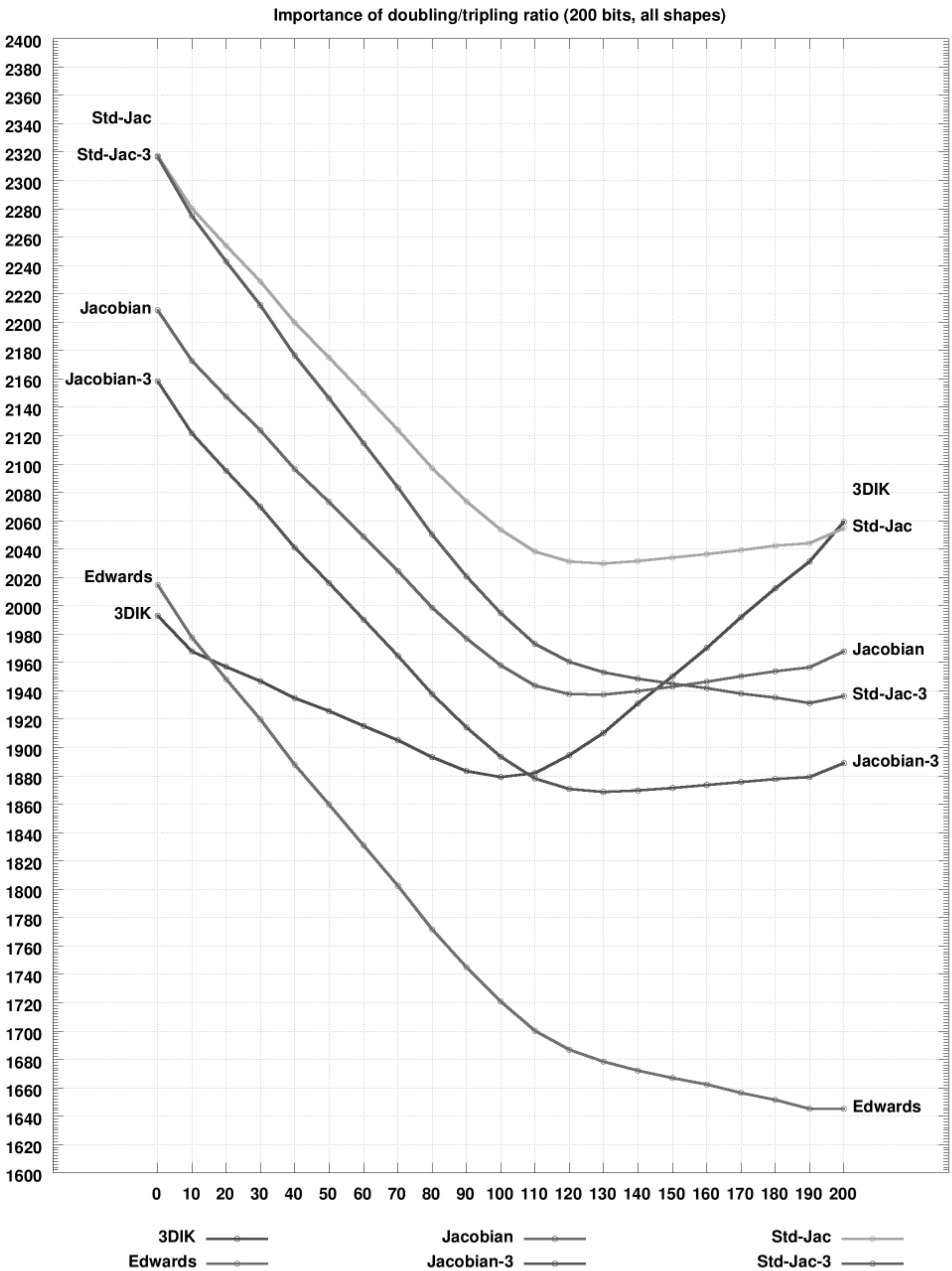
Need to measure overheads too.
Planning new Edwards software.
Expect new speed records.

Dimitrov/Imbert/Mishra 2005,
Doche/Imbert 2006:
Mix doublings with triplings to gain speed for single-scalar mult.

Bernstein/Birkner/Lange/Peters 2007: Have analyzed
Edwards, Jac-3, et al.
with 5423 combinations of
bit size, doubling/tripling ratio,
windowing strategy.
Planning more combinations.

Conclusions: Triplings *are* useful
for Jac-3, 3DIK, et al.
But Edwards wins solidly.


Importance of doubling/tripling ratio (200 bits, all shapes)
Std-Jac
Std-Jac-3
Jacobian
Jacobian-3
Edwards
3DIK
3DIK
Std-Jac
Jacobian
Std-Jac-3
Jacobian-3
Edwards
3DIK
Edwards
Jacobian
Jacobian-3
Std-Jac
Std-Jac-3


Importance of doubling/tripling ratio (200 bits, all shapes)
Std-Jac
Std-Jac-3
Jacobian
Jacobian-3
Edwards
3DIK
3DIK
Std-Jac
Jacobian
Std-Jac-3
Jacobian-3
Edwards
3DIK
Edwards
Jacobian
Jacobian-3
Std-Jac
Std-Jac-3

New directions in ECC

We're working on several items:

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!

Edwards for pairings!

Edwards for president!

Edwards implementations!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!
Edwards implementations!
Edwards standardization!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!
Edwards implementations!
Edwards standardization!

And beyond ECC:
Edwards for ECM!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!
Edwards implementations!
Edwards standardization!

And beyond ECC:
Edwards for ECM!
Edwards for ECPP!

`cr.yp.to/newelliptic.html`

New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!
Edwards implementations!
Edwards standardization!

And beyond ECC:
Edwards for ECM!
Edwards for ECPP!
Edwards for ECXYZ!

`cr.yp.to/newelliptic.html`

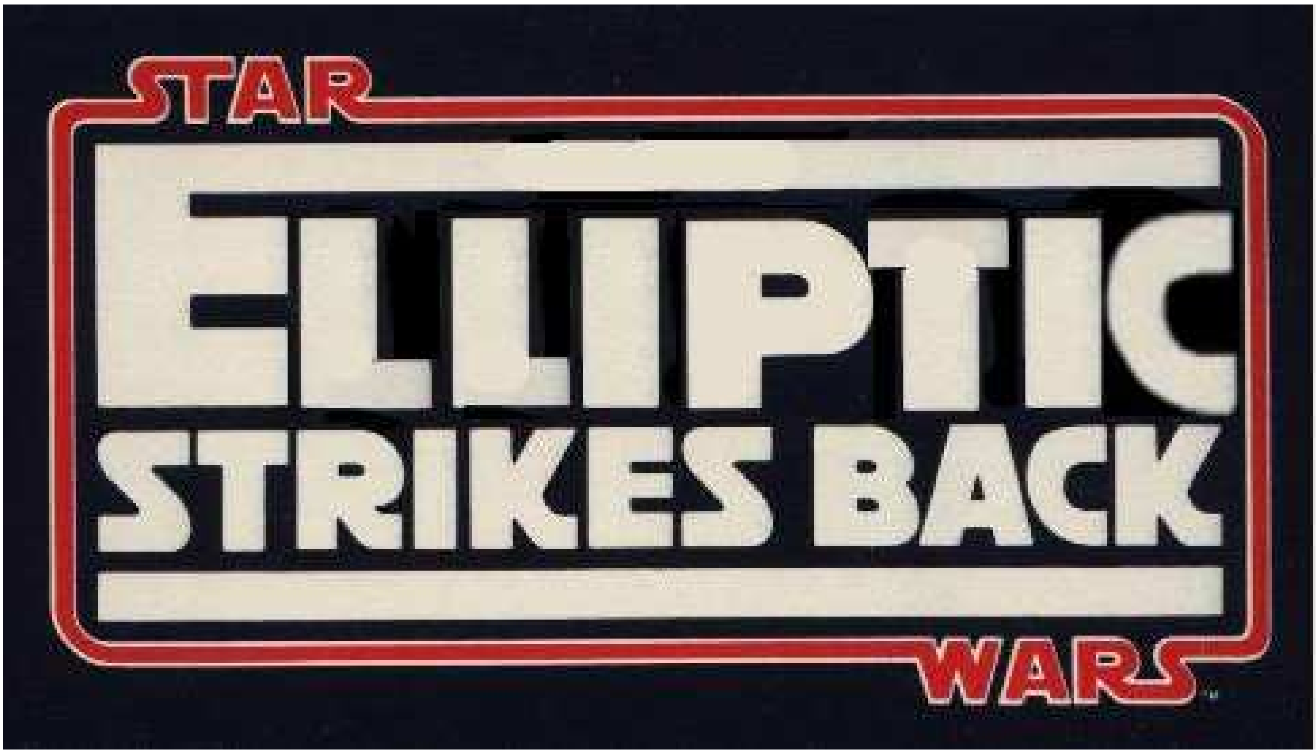
New directions in ECC

We're working on several items:

Edwards for precomputation!
Edwards for pairings!
Edwards for president!
Edwards implementations!
Edwards standardization!

And beyond ECC:
Edwards for ECM!
Edwards for ECPP!
Edwards for ECXYZ!
Return of the Hyperelliptic!

`cr.yp.to/newelliptic.html`


STAR
ELLIPTIC
STRIKES BACK
WARS