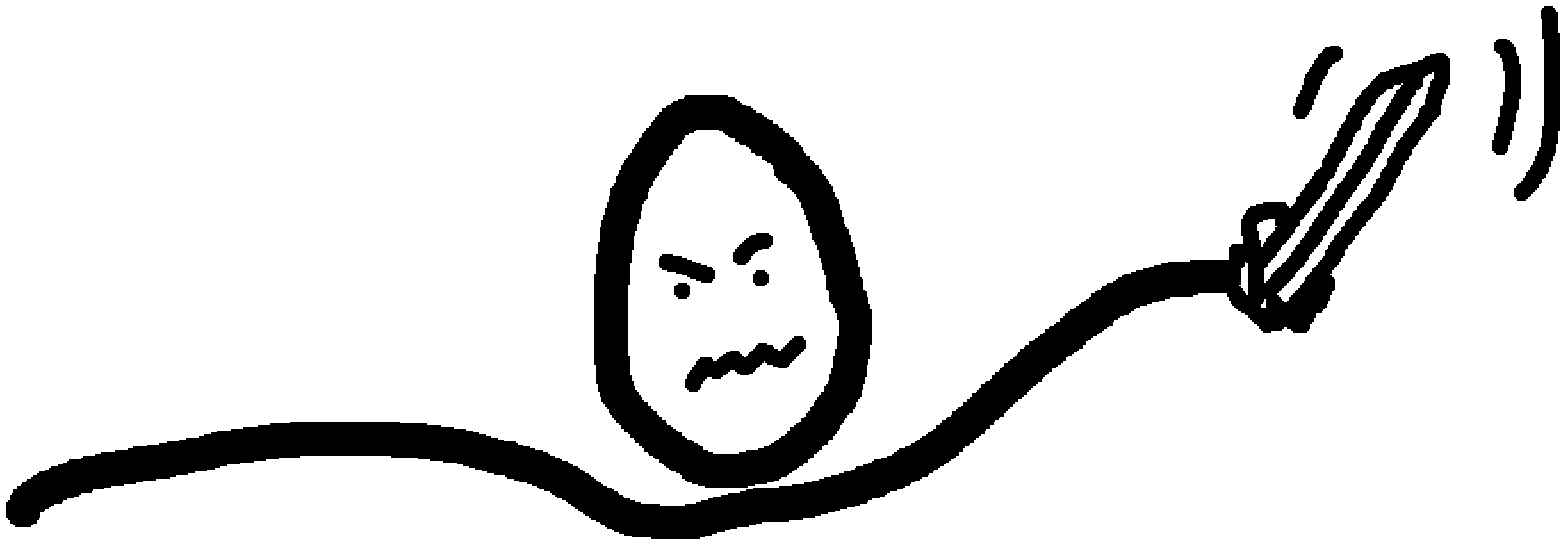
Rump Eurocrypt'07 – Elliptic strikes back

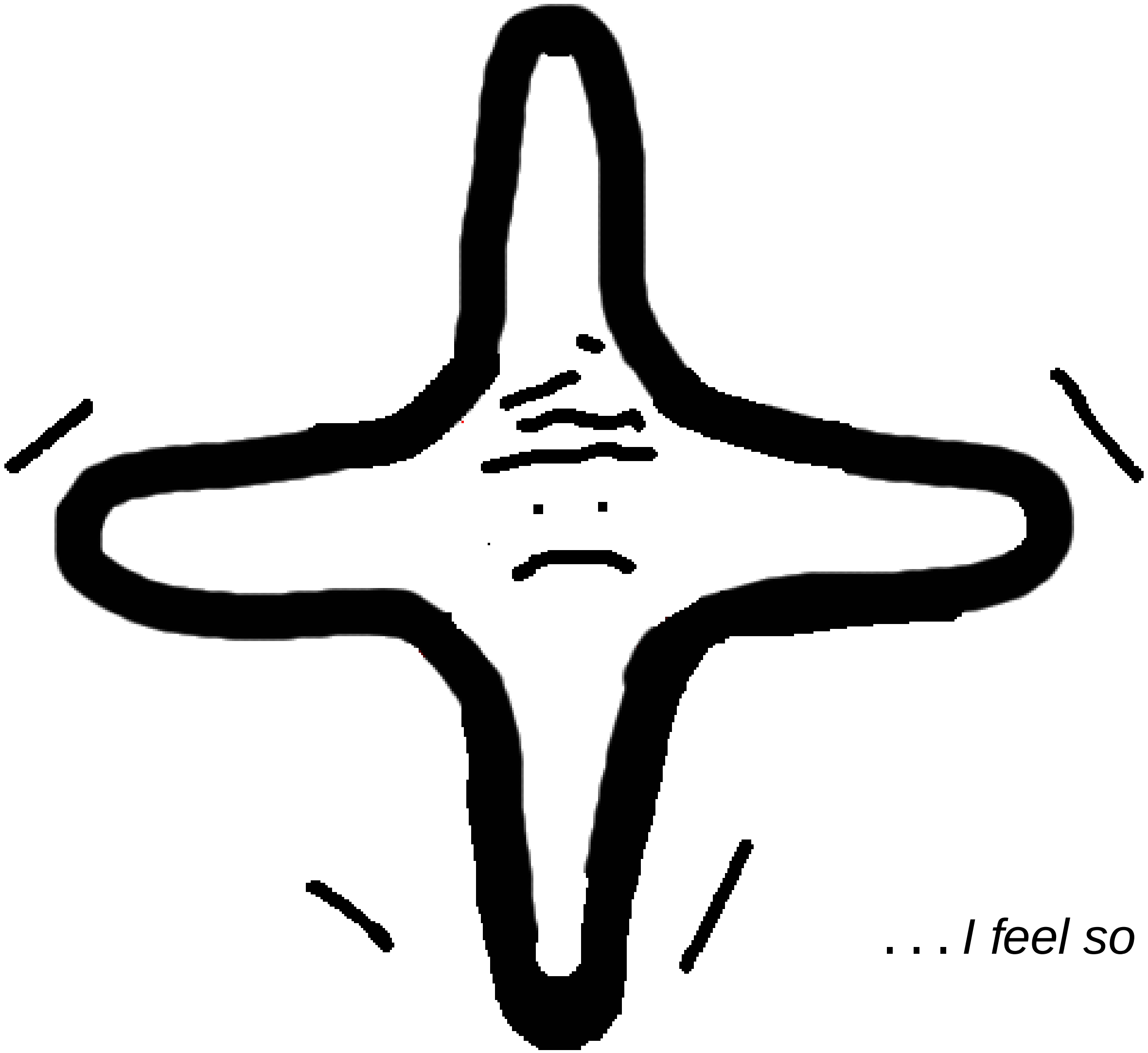


Edwards Curves – a new star(fish) is born

<u>2007 conference lecture circuit:</u>

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

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*

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

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

How can there be an incomplete set of complete curves???

After extensive (finite) field studies . . .

(joint work with Reza Rezaeian Farashahi)

- Assume $d_1, d_2 \in \mathbb{F}_{2^n}$, $d_1 \neq 0$, $\mathrm{Tr}(d_2) = 1$. Then

$$d_1(x+y) + d_2(x+y)^2 = xy + xy(x+y) + x^2y^2$$

describes an elliptic curve.
(Curve shape is symmetric and has highest term x^2y^2 like 'classic' Edwards curves $x^2 + y^2 = 1 + dx^2y^2$.)

- Neutral element is $(0, 0)$. Negative of (x, y) is (y, x).
- The addition law on this curve is complete! It works for adding arbitrary points – doubling, adding negatives, adding the neutral element, . . .
- Every ordinary elliptic curve over $\mathbb{F}_{2^n}$ is birationally equivalent to a complete binary Edwards curve.

Timeline (after some early aborts)

- February 13th, 2008: Binary Edwards curves born
- February 15th, 2008: Binary Edwards takes first steps
- February 15th, 2008: Binary Edwards curves are complete (!) for $d_2 = 1$ and n odd.
- February 16th, 2008: Binary Edwards plays with d_1, d_2
- February 20th, 2008: Binary Edwards adds differentially
- February 29th, 2008: Binary Edwards reaches all ordinary curves
- March 31st, 2008: Intel announces that next year's chips will have "carry-less multiplication (PCMULQDQ)" (aka $\mathbb{F}_{2^n}$ support).
- Rumors have it that other chip manufacturers follow, now that characteristic 2 is finally complete.

Operation counts

These curves are the first binary curves to offer complete addition laws. They are also surprisingly fast:

- DBL on binary Edwards curves takes 2M+6S+3D.
- ADD on binary Edwards curves takes 21M+1S+4D, mADD takes 13M+3S+3D.
- Differential addition ($P + Q$ given P, Q, and $Q - P$) 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 preprint (soon on ePrint) currently on

`cr.yp.to/papers.html#edwards2`

for full details, speedups for $d_1 = d_2$, how to choose small coefficients, affine formulas, . . .

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

Meanwhile we improved the Explicit-Formulas Database

`www.hyperelliptic.org/EFD`

for elliptic curves in large characteristic.

EFD2 is in preparation; our paper already has some speed-ups for Lopez-Dahab coordinates.

Happy End!