ECM using Edwards curves

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

12.09.2009

joint works with subsets of $\{$Christophe Arène (IML), Daniel J. Bernstein (UIC), Peter Birkner (TU/e), Tien-Ren Chen (NTU), Chen-Mou Cheng (NTU), Michael Naehrig (TU/e), Christiane Peters (TU/e), Christophe Ritzenthaler (IML), and Bo-Yin Yang (Academia Sinica)$\}$

Brief summary of Edwards curves

- Published by Edwards in 2007, suggested for cryptographic applications by Bernstein/L. in 2007.
- Curve equation over field k of characteristic 0 or p:

$$x^2 + y^2 = 1 + dx^2y^2, \ d \notin \{0, 1\}.$$

- Addition law
$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2} \right).$
Neutral element is $(0, 1)$ and $-(x_1, y_1) = (-x_1, y_1)$.
- Singular points at infinity $\Omega_1 = (1 : 0 : 0), \Omega_2 = (0 : 1 : 0)$. Singularities blow up over (minimally) $k(\sqrt{d})$ giving two points of order 2 over Ω_1 and two points of order 4 over Ω_2 (check by using birational equivalence with Weierstrass curves).

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 $v(u + u_4) = 0$.
- Addition on Edwards and Weierstrass corresponds.

Exceptional points of the map

- 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

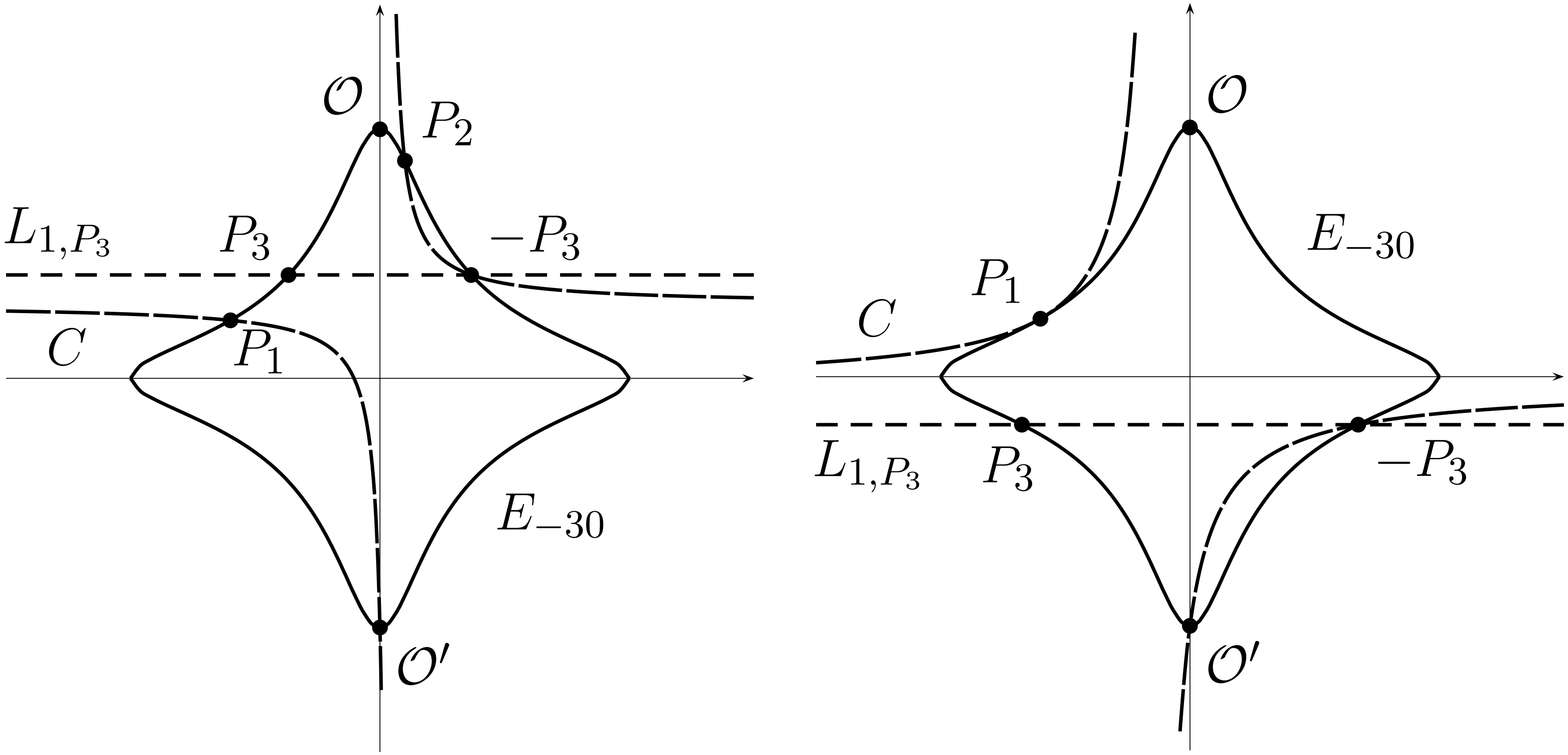
$$\begin{aligned} &(-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_4) \\ = \quad & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  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

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

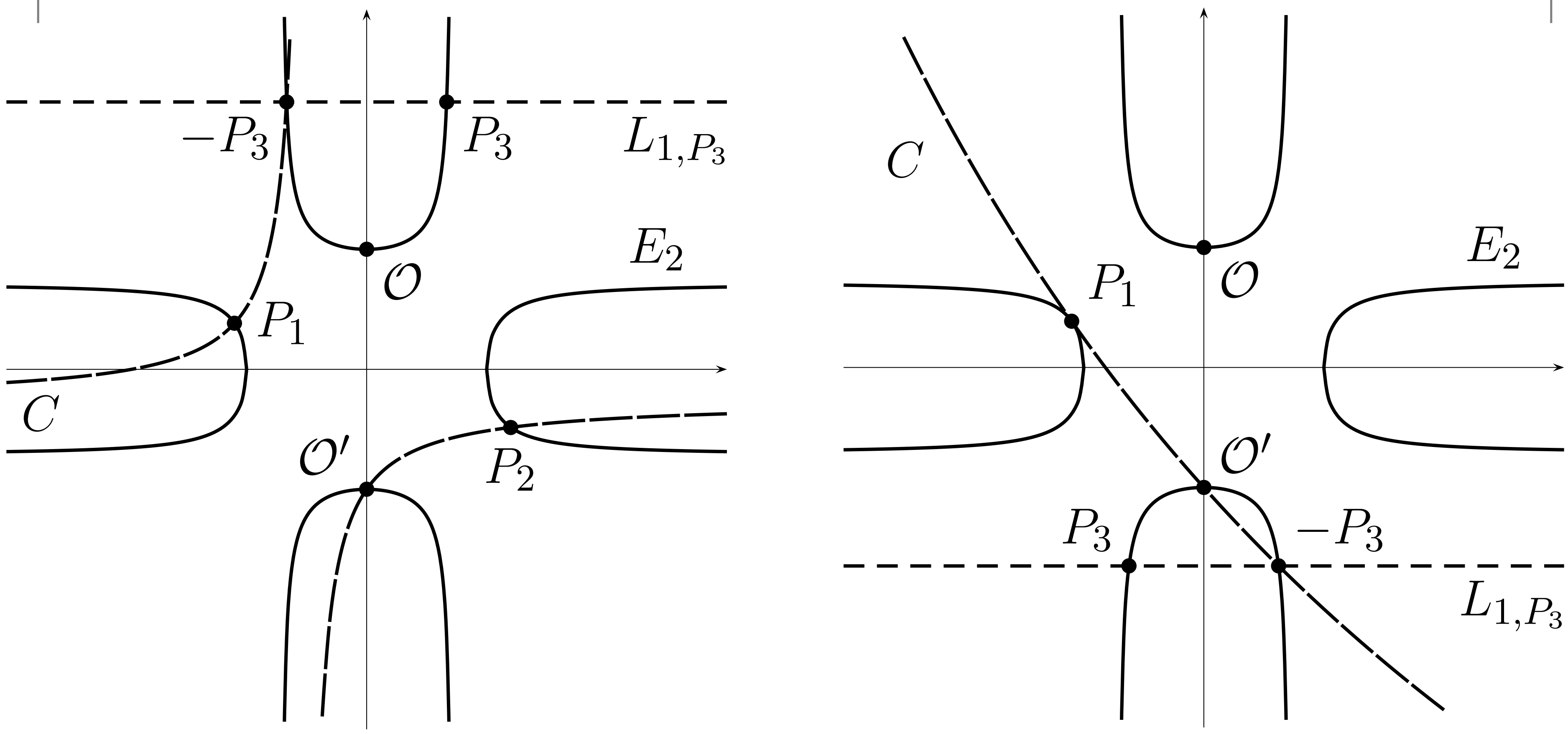
  i. e., points defined over K iff d is a square.

Pictures I



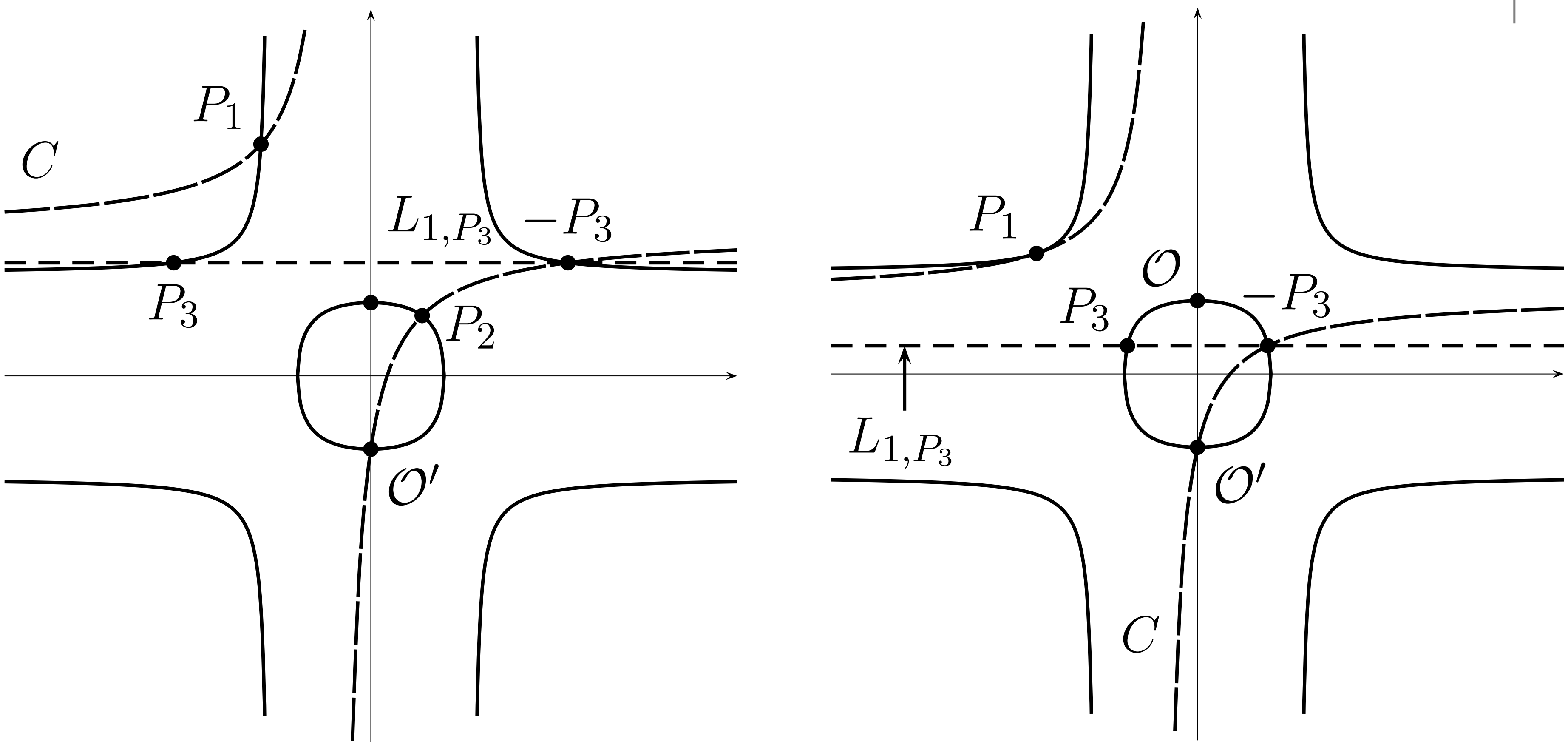
Addition and doubling over $\mathbb{R}$ for $d < 0$.

Pictures II



Addition and doubling over $\mathbb{R}$ for $d > 1$.

Pictures III



Addition and doubling over $\mathbb{R}$ for $0 < d < 1$.

Twisted Edwards curves

- Curve equation over field k of characteristic 0 or p:

$$ax^2 + y^2 = 1 + dx^2y^2, \; a, d \neq 0, a \neq d.$$

- Points at infinity:
  - $a = e^2, d = \square$: $(\pm e, 0)$ have order 4, two points of order 2 over Ω_1 and two points of order 4 over Ω_2; subgroup isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$.
  - $a = e^2, d \neq \square$: $(\pm e, 0)$ have order 4, blow-ups of Ω_1, Ω_2 are defined over quadratic extension field, no k-rational points at infinity; subgroup isom. to $\mathbb{Z}/4$.
  - $a \neq \square, d = \square$: two points of order 2 over Ω_1, none over Ω_2; subgroup isom. to $\mathbb{Z}/2 \times \mathbb{Z}/2$.
  - $a \neq \square, d \neq \square$: two points of order 4 over Ω_2, none over Ω_1; subgroup isom. to $\mathbb{Z}/4$.

ECM as part of NFS

- Optimize phase 1 and 2.
- Can choose different coordinate systems in the two phases (standard choice is Montgomery for phase 1, affine for phase 2).
- Phase 1 can use a prime-by-prime strategy or work with a signed window expansion of the scalar.
- For scalars of 256 bits and more inverted Edwards curves are cheaper than Montgomery curves. Scalars in ECM are much larger than this.
- Different conclusion than Loebenberger!?

ECM as part of NFS

- Optimize phase 1 and 2.
- Can choose different coordinate systems in the two phases (standard choice is Montgomery for phase 1, affine for phase 2).
- Phase 1 can use a prime-by-prime strategy or work with a signed window expansion of the scalar.
- For scalars of 256 bits and more inverted Edwards curves are cheaper than Montgomery curves. Scalars in ECM are much larger than this.
- Different conclusion than Loebenberger!?
- Survey by Loebenberger left out several publications.

Efficient arithmetic on Edwards curves

- "Faster group operations on elliptic curves" by Hisil, Wong, Carter Dawson, mADD = 9M, no multiplication by curve constants.

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

  These addition formulas are not unified; this is no problem for ECM where one searches for "failures" to the addition law.

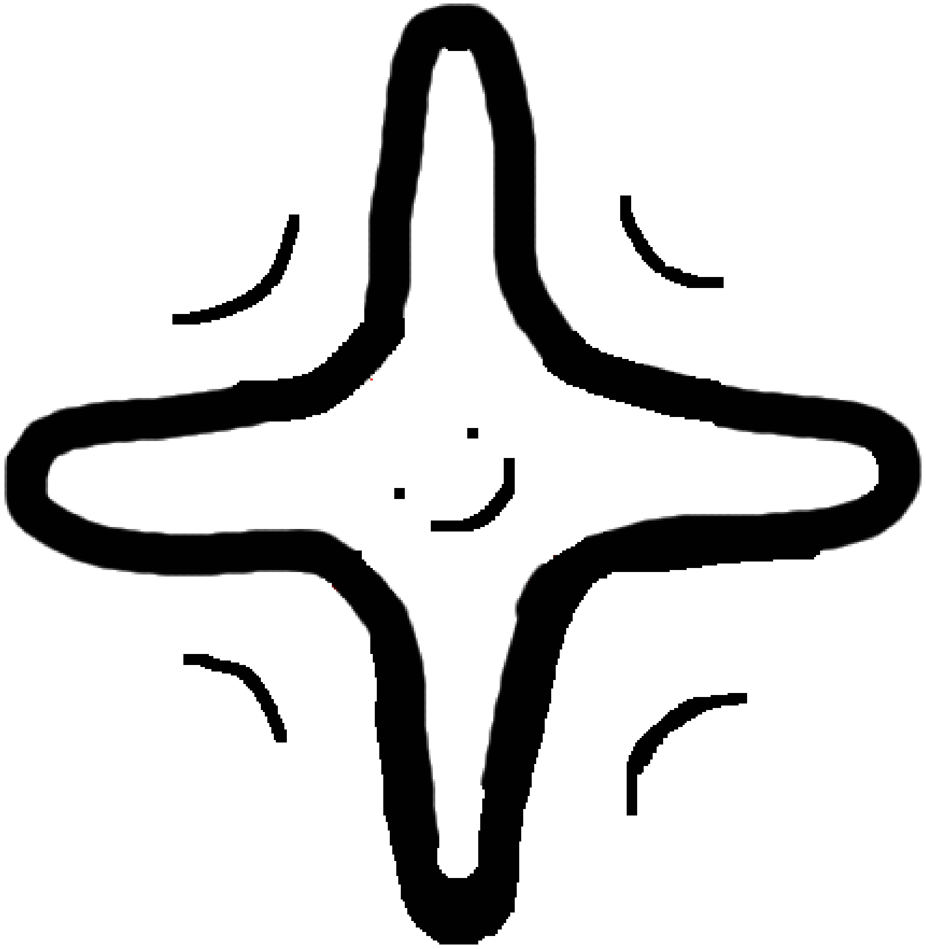
- "Twisted Edwards Curves Revisited" by Hisil, Wong, Carter Dawson, introducing extended Edwards coordinates $(X : Y : Z : T)$ with $T = XY/Z$. Gives ADD=9M (+1D with a for twisted) in general.

Extended Edwards coordinates

- For twisted with $a = -1$ even ADD=8M. Mixed versions save 1M: mADD=7M.
- Extended representation is not good for doubling. should be used only for addition; so do main doublings as $2\mathcal{E} \to \mathcal{E}$, last doubling as $2\mathcal{E} \to \mathcal{E}^e$, and $\mathcal{E}^e + \mathcal{E}^e \to \mathcal{E}$ in the scalar multiplication in stage 1. Stage 2 has mostly additions anyway.
- Complete overview of curve shapes, coordinates, addition formulas including faster differential addition than Montgomery at `www.hyperelliptic.org/EFD`.

Design Choices

- Use Edwards curves!



Design Choices

- Use Edwards curves!
- Field arithmetic might make multiplications by small integers faster; this does not generally work in Montgomery representation of integers.
- There are several multiplications by the coordinates of the base point; there are some multiplications by a and in inverted Edwards coordinates by d.
- Can pick small height base point (x_1, y_1), some a and compute d as $d = (ax_1^2 + y_1^2 - 1)/(x_1^2 y_1^2)$. The resulting d has small height, too. Good choices for a are 1 (Edwards) and -1 (particularly fast extended addition).
- Make sure not to choose $(x_1, y_1) \in \{(\pm 1, 0), (0, \pm 1), (\pm c, \pm c)\}$ for any c since these definitely have small order over $\mathbb{Q}$.

Small order points I

- ECM succeeds in factoring n if $[s]P = (0,1)$ modulo some divisor of n.
- If over $\mathbb{Q}$ the base point P has small order $k|s$ then $[s]P = (0,1)$ modulo all divisors of n, no factorization.
- But: it is interesting to have a large torsion subgroup over $\mathbb{Q}$ to increase the smoothness probability of ord(P).
- Some handwaving:
  - Modulo prime p the number of points on E is in the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
  - Chance of smooth group order depends on size.
  - If k divides group order the unknown part gets smaller.
  - Strong handwaving: assume that the smoothness probability is not affected.

Small order points II

- Success rate does go up with size of torsion group (see Dan's talk).
- Over $\mathbb{Q}$ there are only finitely many points of finite order.
- More precisely: Theorem of Mazur.
  Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of E is isomorphic to one of the following fifteen groups:
  - $\mathbb{Z}/m$ for $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,
  - $\mathbb{Z}/2 \times \mathbb{Z}/2m$ for $m \in \{1, 2, 3, 4\}$.
- Search for curves with large torsion subgroup and positive rank, choose base point as a free point.
- Edwards curves have m divisible by 4. For twisted Edwards only $2 \mid m$ guaranteed.

Edwards curves with large torsion

- Interesting(=large) choices are $\mathbb{Z}/12$ and $\mathbb{Z}/2 \times \mathbb{Z}/8$. Preprint shows that $\mathbb{Z}/2 \times \mathbb{Z}/6$ does not work for twisted Edwards curves.
- When do curves have a point of order 8? Assume that P_8 doubles to $(1, 0)$.
- $[2](x_8, y_8) = \left(\frac{2x_8y_8}{x_8^2+y_8^2}, \frac{y_8^2-x_8^2}{2-(x_8^2+y_8^2)}\right)$.
- $y_8^2 - x_8^2 = 0 \Rightarrow x_8 = \pm y_8 \Rightarrow x_8^2 + x_8^2 = 1 + dx_8^2x_8^2$, i.e. $d = (2x_8^2 - 1)/x_8^4$.
- Also need that $d = \square$ to have first $\mathbb{Z}/2$ component.
- For $u \notin \{0, -1, -2\}$, $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives square $d = (2x_8^2 - 1)/x_8^4$.

Edwards curves with $\mathbb{Z}/12$

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

- Any Edwards curve with a point of order 3 automatically has $\mathbb{Z}/12$ – and cannot have more.
- Use $(x_1^2 + y_1^2)^2 - (2y_1)^2 = 0$ and obtain condition: curve has this structure if there exists a y_6 so that $d = (2y_6 + 1)/(y_6^3(y_6 + 2))$ and such that $-(y_6^2 + 2y_6)$ is a square.
- Points of finite order are then

point	$(0, 1)$	$(0, -1)$	$(\pm x_3, y_3)$	$(\pm 1, 0)$	$(\pm x_3, -y_3)$	$(\pm y_3, \pm x_3)$
order	1	2	3	4	6	12

Choose other point as basepoint.

Existing constructions

- Two main constructions to obtain large torsion subgroup and a base point that is in the free part.
- Suyama has parameterization that guarantees $\mathbb{Z}/6$ over $\mathbb{Q}$. Modulo any prime the group order is divisible by 4 but not so over $\mathbb{Q}$.
- Have translated this representation to Edwards curves. Height of base point and coefficient does not grow too quickly (linear family of curves).
- Atkin-Morain curves have even larger torsion subgroup $\mathbb{Z}/2 \times \mathbb{Z}/8$ – easy to generate, but the height of the coefficients grows quickly (elliptic family of curves).
- We translated Atkin-Morain to Edwards form.

How to avoid large height coefficients

- This tuning is only useful if the multiplication implementation notices that size of the factors.
- Use flexibility of twisted Edwards curves and projective coordinates
  - If $d = b/c$, with b, c small, extend both to have $c = e^2$ for some e and $d = b'/(e^2)$. Then the curve is isomorphic to the twisted Edwards curve with $a = e^2$ and $d = b'$ (y unchanged, new x is x/e). All values remain small.
  - Instead of working with $(x_1, y_1) = (r/t, v/w)$ which modulo n would get huge work with projective basepoint $(rw : tv : rw)$ (or divide by gcd).
- Make list of such curves and use in implementations where the field arithmetic caters for multiplication by words.

How to find such curves

- Want curve with small height coefficient, base point and rank ≥ 1.
- Parametrization: for $u \notin \{0, -1, -2\}$, $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives square $d = (2x_8^2 - 1)/x_8^4$.
- Put $u = a/b$ and search for solutions (a, b, e, f), where (e, f) is a point on the curve but different from all torsion points, i.e. different from $(0, \pm 1), (\pm, 0)$ and $e \neq f$.
- Speed up search by restricting range of u and picking only 1 curve per isomorphism class.
- Computed more than 100 curves with 12 or 16 torsion points.
  `http://cr.yp.to/factorization/goodcurves.html`

Platform dependent tuning – GPU

- Platform is highly parallel, has restricted memory.
- Use windowing with large window – scalar is way longer than modulus ($B_1 = 2^{13}$).
- Use affine base point and precomputations.

Platform dependent tuning – GPU

- Platform is highly parallel, has restricted memory.
- Use windowing with large window – scalar is way longer than modulus ($B_1 = 2^{13}$).
- Use affine base point and precomputations.
- Severe storage restrictions! No precomputations possible. No advantages for small numbers.
- Only possible to use NAF of scalar.

Platform dependent tuning – GPU

- Platform is highly parallel, has restricted memory.
- Use windowing with large window – scalar is way longer than modulus ($B_1 = 2^{13}$).
- Use affine base point and precomputations.
- Severe storage restrictions! No precomputations possible. No advantages for small numbers.
- Only possible to use NAF of scalar.
- Way out: parallelize formulas, then 2 processors share memory.
- Problem:
  - DBL: 4M+3S,
  - mADD: 9M,

  both odd; seems to ask for idle stages.

Elliptic Curves

- Develop new formulas; pipeline two operations:
  - DBL-DBL: 4M+3S+6a,
  - mADD-DBL: 7M+1S+7a,
  - DBL+mADD: 6M+2S+8a.
- These numbers are even – and we manged to get perfect parallelism, i.e. no wait-stages for multiplications.
- Result: This freed up enough storage so that we can store 8 points: P, [3]P, [5]P, . . . , [15]P
- Given the size of the moduli, even larger windows would be desirable. Maybe on the next generation ;–)

DBL-DBL

Step	MAU 1	MAU 2	
1	$A = X_1^2$	$B = Y_1^2$	S
2	$X_1 = X_1 + Y_1$	$C = A + B$	a
3	$X_1 = X_1^2$	$Z_1 = Z_1^2$	S
4	$X_1 = X_1 - C$	$Z_1 = Z_1 + Z_1$	a
5	$B = B - A$	$Z_1 = Z_1 - C$	a
6	$X_1 = X_1 \times Z_1$	$Y_1 = B \times C$	M
7	$A = X_1 \times X_1$	$Z_1 = Z_1 \times C$	M
8	$Z_1 = Z_1^2$	$B = Y_1^2$	S
9	$Z_1 = Z_1 + Z_1$	$C = A + B$	a
10	$B = B - A$	$X_1 = X_1 + Y_1$	a
11	$Y_1 = B \times C$	$X_1 = X_1 \times X_1$	M
12	$B = Z_1 - C$	$X_1 = X_1 - C$	a
13	$Z_1 = B \times C$	$X_1 = X_1 \times B$	M
			4M+3S+6a

Horizontal line indicates beginning of second operation.

mADD-DBL

Step	MAU 1	MAU 2	
1	B=$x_2 \times Z_1$	C=$y_2 \times Z_1$	M
2	A=$X_1 \times Y_1$	Z_1=$B \times C$	M
3	E=$X_1 - B$	F=$Y_1 + C$	a
4	X_1=$X_1 + C$	Y_1=$Y_1 + B$	a
5	E=$E \times F$	Y_1=$X_1 \times Y_1$	M
6	F=$A + Z_1$	B=$A - Z_1$	a
7	E=$E - B$	Y_1=$Y_1 - F$	a
8	Z_1=$E \times Y_1$	X_1=$E \times F$	M
9	Y_1=$Y_1 \times B$	A=$X_1 \times X_1$	M
10	Z_1=Z_1^2	B=Y_1^2	S
11	Z_1=$Z_1 + Z_1$	C=$A + B$	a
12	B=$B - A$	X_1=$X_1 + Y_1$	a
13	Y_1=$B \times C$	X_1=$X_1 \times X_1$	M
14	B=$Z_1 - C$	X_1=$X_1 - C$	a
15	Z_1=$B \times C$	X_1=$X_1 \times B$	M
			7M+1S+7a

DBL-mADD

Step	MAU 1	MAU 2	
1	$A = X_1^2$	$B = Y_1^2$	S
2	$X_1 = X_1 + Y_1$	$C = A + B$	a
3	$X_1 = X_1^2$	$Z_1 = Z_1^2$	S
4	$X_1 = X_1 - C$	$Z_1 = Z_1 + Z_1$	a
5	$B = B - A$	$Z_1 = Z_1 - C$	a
6	$X_1 = X_1 \times Z_1$	$Y_1 = B \times C$	M
7	$Z_1 = Z_1 \times C$	$A = X_1 \times Y_1$	M
8	$B = x_2 \times Z_1$	$C = y_2 \times Z_1$	M
9	$E = X_1 - B$	$F = Y_1 + C$	a
10	$X_1 = X_1 + C$	$Y_1 = Y_1 + B$	a
11	$E = E \times F$	$Z_1 = B \times C$	M
12	$F = A + Z_1$	$B = A - Z_1$	a
13	$E = E - B$	$Z_1 = X_1$	a
14	$A = Z_1 \times Y_1$	$X_1 = E \times F$	M
15	$A = A - F$		a
16	$Z_1 = E \times A$	$Y_1 = A \times B$	M
			6M+2S+8a

The end!