Efficient Implementation of Pairings

Tanja Lange

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

14.08.2009

Elliptic curves

- For $p > 3$ (prime) let $\mathbb{F}_p$ denote the finite field with p elements and let $E/\mathbb{F}_p$ be an elliptic curve defined over $\mathbb{F}_p$.
- For a field extension $\bar{\mathbb{F}}_p \subset L \subset \mathbb{F}_p$ let $E(L)$ denote the group of L-rational points on E.
- Hasse's theorem: $|E(\mathbb{F}_p)| = p + 1 - t,\ |t| \leq 2\sqrt{p}$ and t is called the trace of the Frobenius endomorphism.
- m-torsion points: $E[m] = \{P \in E = E(\bar{\mathbb{F}}_p) | [m]P = \mathcal{O}\}$.
- L-rational m-torsion points:
  $E[m](L) = \{P \in E(L) | [m]P = \mathcal{O}\}$.
- If $p \nmid m$ we have $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

The embedding degree

- Let $r \neq p$ be a large prime dividing $|E(\mathbb{F}_p)|$. The embedding degree of E with respect to r is the smallest integer k s.t.
$$r | p^k - 1.$$
This means, the embedding degree k is the order of p modulo r.
- If $k > 1$ the smallest extension of $\mathbb{F}_p$ which contains the group μ_r of r-th roots of unity is $\mathbb{F}_{p^k}$;
- the same k is minimal so that $E(\mathbb{F}_{p^k})$ contains all r-torsion points, i.e. $E[r] \subset E(\mathbb{F}_{p^k})$.
- For crypto-sized curve E and prime divisor r the embedding degree K is usually very large (size of p).

Tate-Lichtenbaum pairing

The Tate pairing is a map

$$\begin{aligned} \langle \cdot, \cdot \rangle : E[r](\mathbb{F}_{p^k}) \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) &\rightarrow \mathbb{F}_{p^k}/(\mathbb{F}_{p^k})^r, \\ (P, Q) &\mapsto f_{r,P}(D_Q), \end{aligned}$$

where the divisor D_Q is equivalent to the divisor $(Q) - (\mathcal{O})$and its support is disjoint from the support of $(f_{r,P}) = r(P) - r(\mathcal{O})$.
Result is a class in $\mathbb{F}_{p^k}/(\mathbb{F}_{p^k})^r$,
and Q is a representative of a class in $E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$.

Reduced Tate-Lichtenbaum pairing

This T_r defines a bilinear and non-degenerate map

$$\text{TL} : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/\mathbb{F}^{*r}_{q^k}$$

as r-folds are in the kernel of T_r.
To achieve unique value in $\mathbb{F}_{q^k}$ rather than class do final exponentiation

$$\tilde{T}_r = T_r(P,Q)^{(q^k-1)/r}.$$

Often

$$\mathrm{TL} : E(\mathbb{F}_{q})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}^*_{q^k}/\mathbb{F}^{*r}_{q^k}.$$

The function F_P is built iteratively and evaluated in each round. This is known as Miller's algorithm.

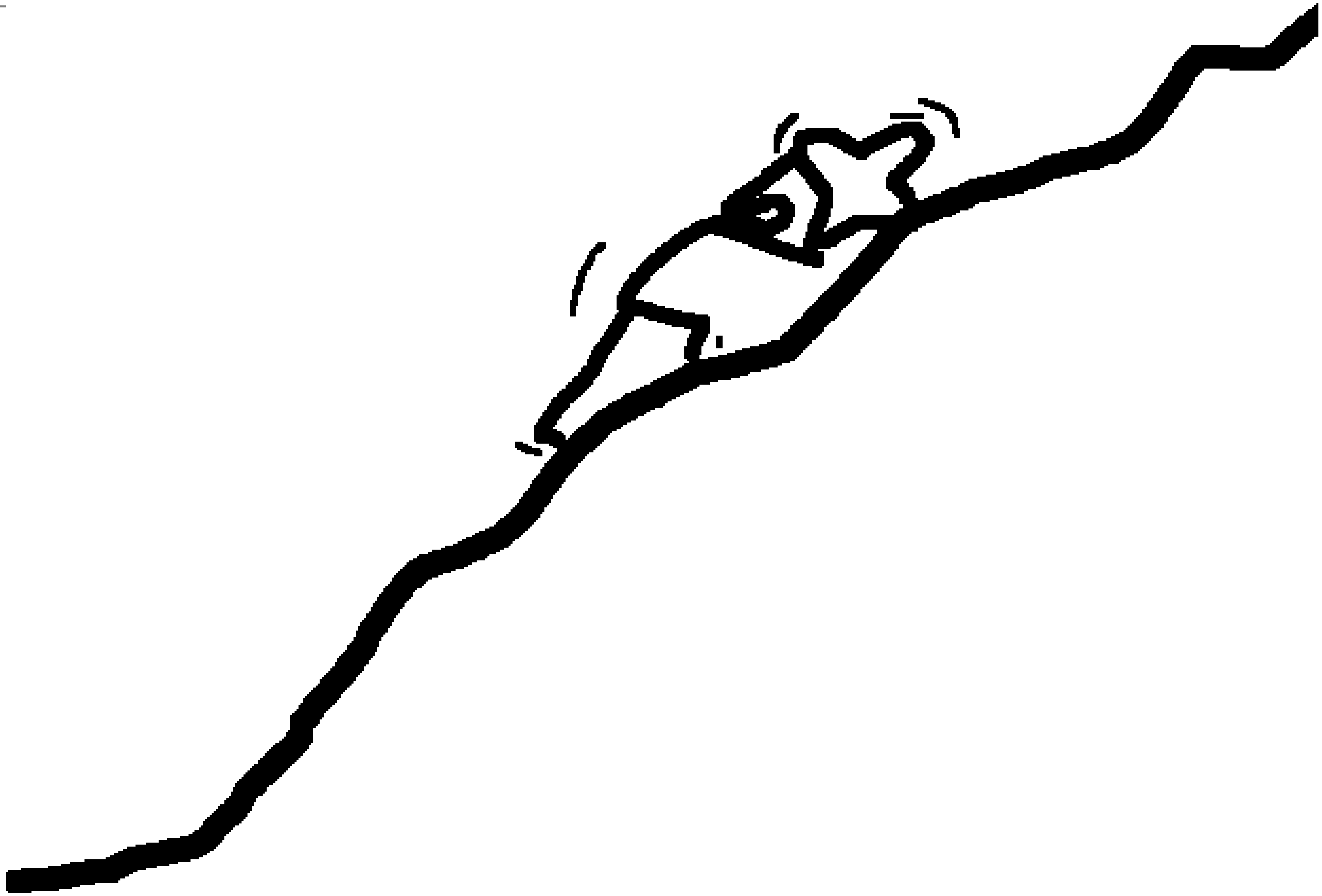
Reducing the loop length

- Variants of the Tate pairing.
- It is possible to reduce the loop length in Miller's algorithm significantly and still get a pairing.
- Ate pairing:

$$\begin{aligned} \mathrm{ate}: E[r](\mathbb{F}_{p^k}) \times E[r](\mathbb{F}_p) &\rightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \\ (Q, P) &\mapsto f_{T,Q}(P)^{\frac{p^k-1}{r}}. \end{aligned}$$

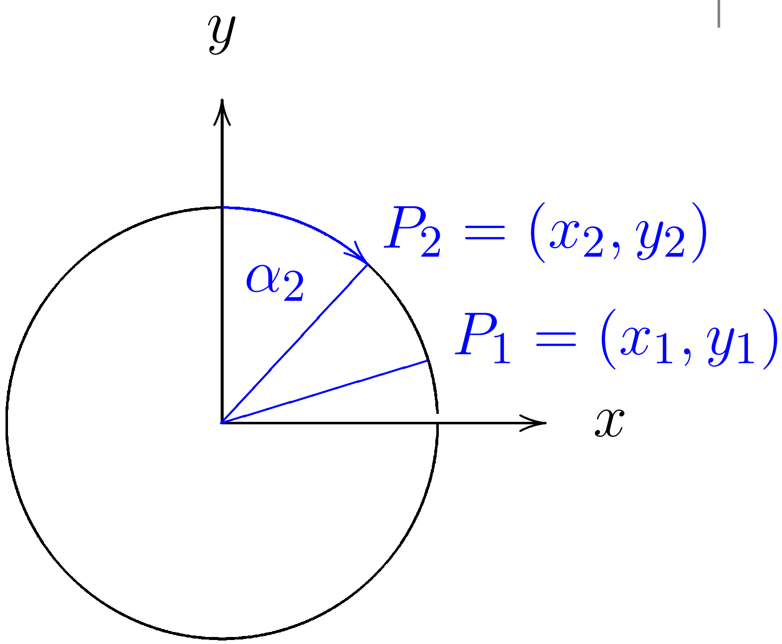
  Here $T = t - 1$, and $\log_2 T \sim \log_2 r$.
- Other variants even shorter. Optimal pairing $\log_2 r/\varphi(k)$.
- Can be combined with twisting. Result by Hess, Smart, and Vercauteren: Let $d \geq 2$, $d|k$, and let E admit twists of degree d. There exists a unique twist E' of E of degree d with $r \mid |E'(\mathbb{F}_{p^{k/d}})|$.

Everything is done – start over!



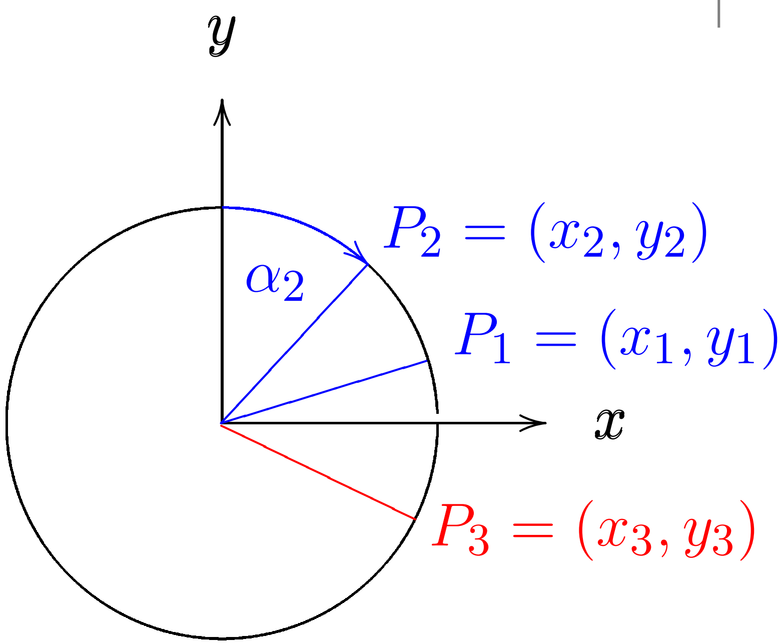
Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x, y) \in K \times K | x^2 + y^2 = 1\}$



Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x, y) \in K \times K | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i), \ y_i = \cos(\alpha_i)$

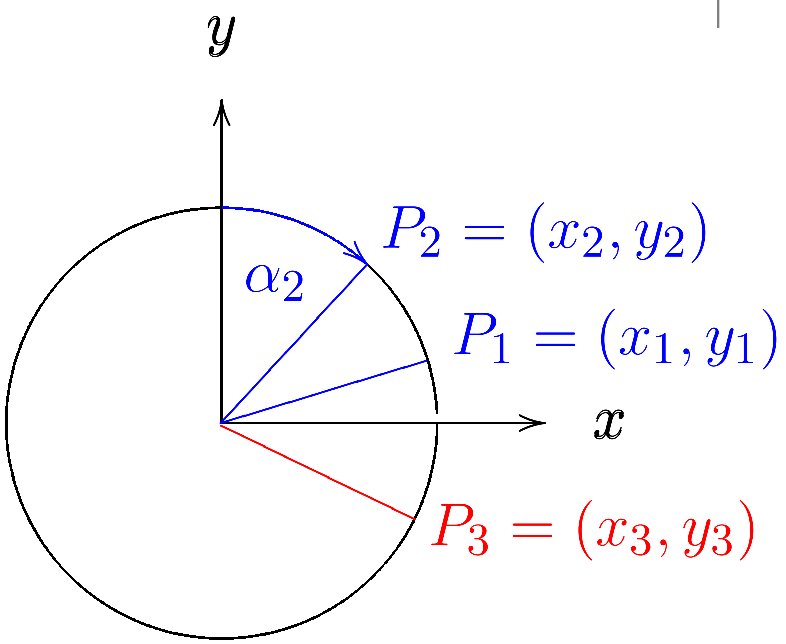


Do you know how to add on a circle?

Let K be a field with $2 \neq 0$.
Circle: $\{(x, y) \in K \times K | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i), \; y_i = \cos(\alpha_i)$

$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \end{aligned}$$

$$\begin{aligned} y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \end{aligned}$$



Addition of angles defines commutative group law
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

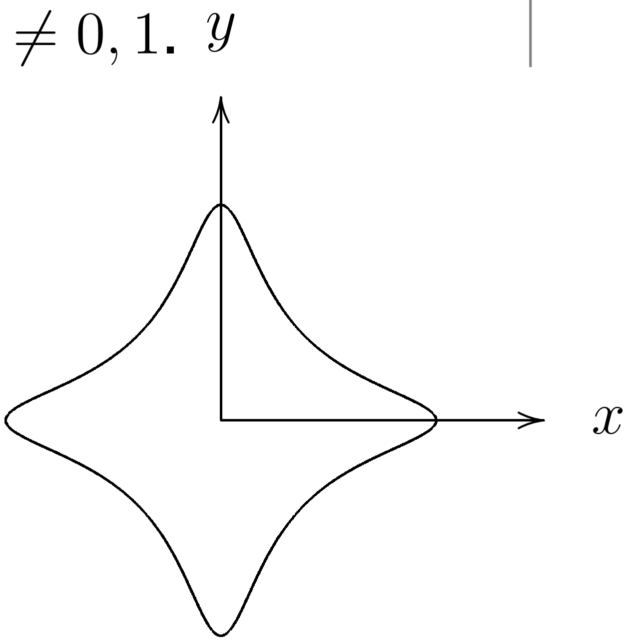
$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Addition on Edwards curves

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in K \times K | x^2 + y^2 = 1 + dx^2y^2\}$$

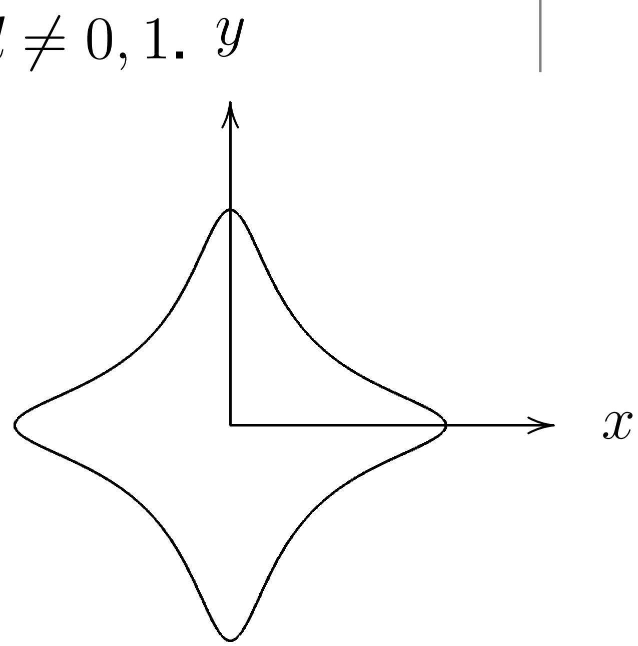
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



Addition on Edwards curves

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in K \times K | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

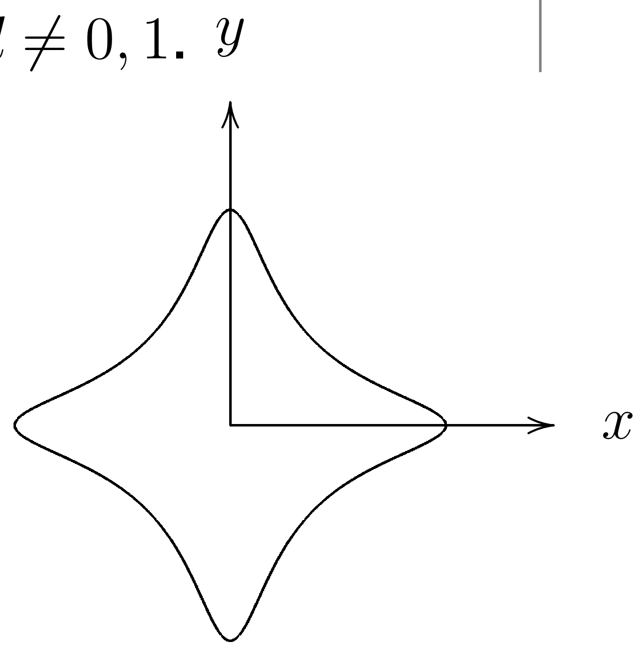
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Addition on Edwards curves

Let K be a field with $2 \neq 0$. Let $d \in K$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in K \times K | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$; $-(x_1, y_1) = (-x_1, y_1)$.
- This works for $P + P, P + (-P), P + (0, 1)$ etc., addition law is complete if $d \neq \square$ in K.

Fast addition law

- Very fast point addition 10M + 1S + 1D. Even faster with Inverted Edwards coordinates (9M+1S+1D) and Extended Edwards coordinates (8M+1S+1D).
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature.
- For comparison: IEEE standard P1363 provides “the fastest arithmetic on elliptic curves” by using Jacobian coordinates on Weierstrass curves.
  - Point addition 12M + 4S.
  - Doubling formulas need only 4M + 4S.
- For more curve shapes, better algorithms (even for Weierstrass curves) and many more operations (mixed addition, re-addition, tripling, scaling,. . .) see `www.hyperelliptic.org/EFD`.

Relationship to Weierstrass 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.

Complete addition law

- Previous slide shows that for $d \neq \square$ in K all points of the Weierstrass curve map to the affine part of the Edwards curve; where we extend the map by $P_\infty \mapsto (0,1)$ and $(0,0) \mapsto (0,-1)$.
- Geometric description: The other missing points from the Weierstrass curve correspond to the blow-ups of $(1:0:0)$ and $(0:1:0)$ on the Edwards curve. They blow up to two points each on the desingularization of the curve. On both the Weierstrass and the Edwards side these points are defined over $K(\sqrt{d})$.
- Attention: Having no K-rational points at infinity does not guarantee that the formulas are complete:

$$(x_3, y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

is addition on Edwards curve . . . and fails for doublings.

Twisted Edwards curves

$$\mathrm{E}_{a,d}: \; ax^2 + y^2 = 1 + dx^2y^2,$$

with $a, d \in K^*, \; a \neq d$.

- Isomorphic to plain Edwards curve $\mathrm{E}_{1,d/a}$ for $a = \square$.
- Set of twisted Edwards curves invariant under quadratic twists.
- Addition formulas very similar to Edwards curves

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Arithmetic complete only for $a = \square, d \neq \square$.
- Operation count same as Edwards (except for 1A in DBL and ADD).

Edwards curves for ...

- Edwards curves are great for fast implementations of scalar multiplication $[n]P$.
- Edwards curves are great for lazy implementations of scalar multiplication $[n]P$.
- Edwards curves are great for SCA-protected implementations of scalar multiplication $[n]P$.
- Edwards curves are great for teaching elliptic curves.
- How about pairings? Loop shortening etc. does not depend on curve representation; but how to compute the Miller function? How to compute the analogue of the line functions?

Miller's algorithm

Let $k > 1$ be the embedding degree of E w.r.t. r,
$P \in E(\mathbb{F}_p)[r]$, $Q \in E(\mathbb{F}_{p^k})$,
$r = (r_{l-1}, \ldots, r_1, r_0)_2$.
Compute the Tate pairing as:

1. $R \leftarrow P$, $f \leftarrow 1$
2. for $i = l - 2$ to 0 do
   (a) $f \leftarrow f^2 \cdot g_{R,R}(Q),\ R \leftarrow 2R$ //doubling step
   (b) if $r_i = 1$ then
   $f \leftarrow f \cdot g_{R,P}(Q),\ R \leftarrow R + P$ //addition step
3. $f \leftarrow f^{(p^k-1)/r}$

Previous attempts

Das, Sarkar [Pairing 2008]:

- Express functions $g_{R,R}$ and $g_{R,P}$ in the Miller loop by transformation to Montgomery form.
- Resulting Miller function has huge degree; explicit formulas for supersingular curves with $k = 2$ with much lower degree. Still very slow.

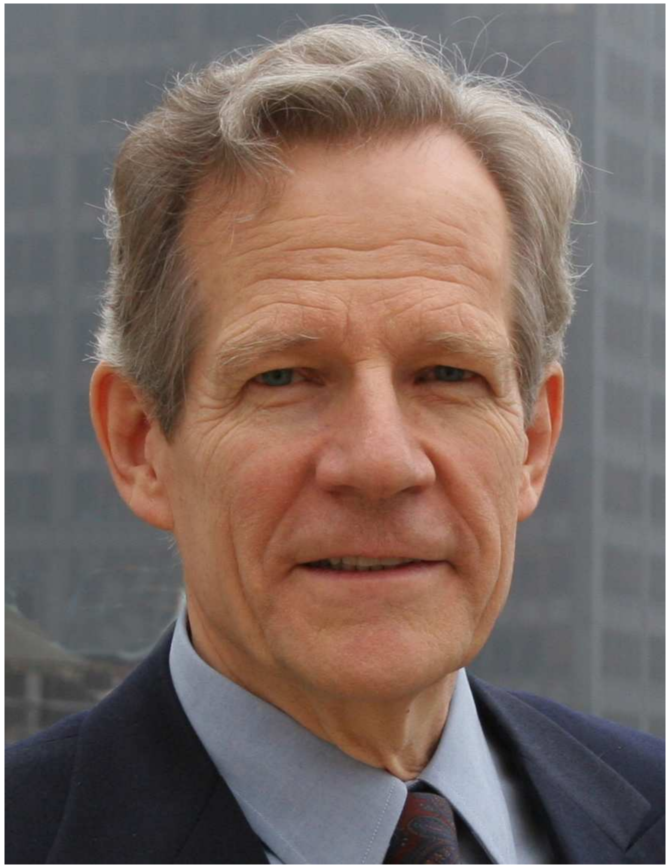
Ionica, Joux [Indocrypt 2008]:

- Compute Miller functions on a curve

$$v^2u = (1 + du)^2 - 4u.$$

- Actually compute 4th power of the Tate pairing.
- Explicit formulas for even k. Slow!

Understanding Edwards addition



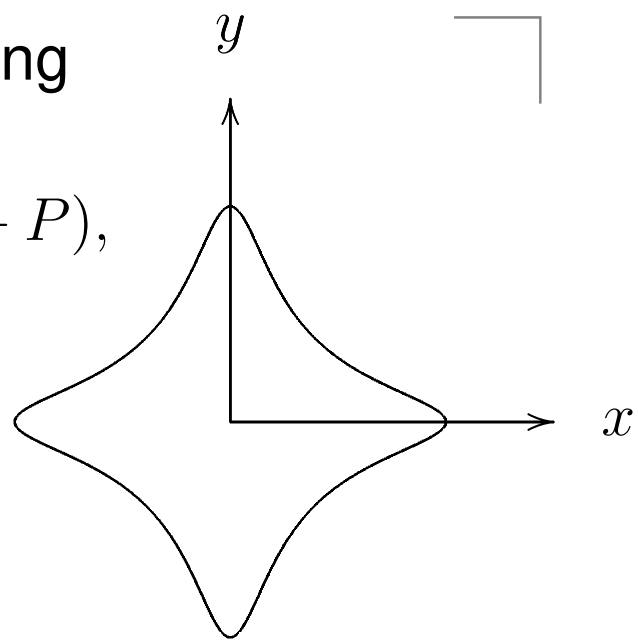
- The Gauss/Euler example ($d = -1$) is mentioned in some books.
- Edwards generalized this single example to whole class of curves;
- showed how to do arithmetic on this curve;
- gives several proofs of the addition law, e.g. algebraically; via holomorphic differentials; via algebraic variations.
- does not give any geometric interpretation.
- But does have much more! Bulletin of the AMS, **44**, 393–422, 2007

Pairings on Edwards curves

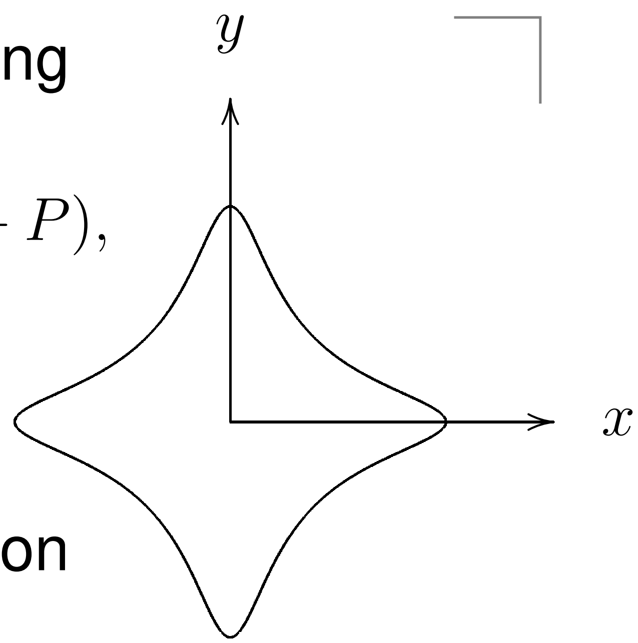
- Joint work with Christophe Arène (IML), Michael Naehrig (TU/e), and Christophe Ritzenthaler (IML).
- Will make heavy use of Bézout's theorem:
  The number of intersection points between a curve of degree n and a curve of degree m is mn (counting multiplicities). This covers the affine points and those at infinity ($Z = 0$). The intersection points might be defined over an extension field.
- Other important concept are degree-0 divisors as explained in Victor Miller's talk.

Geometric addition law

- Would like to find function $g_{R,P}$ depending on two input points P, R such that
$$\operatorname{div}(g_{R,P}) = \frac{f_1}{f_2} = R + P - \mathcal{O} - (R+P),$$
where $\mathcal{O} = (0,1)$ and $R + P$ is the Edwards sum of $R + P$.



Geometric addition law



- Would like to find function $g_{R,P}$ depending on two input points P, R such that
$$\operatorname{div}(g_{R,P}) = \frac{f_1}{f_2} = R + P - \mathcal{O} - (R+P),$$
where $\mathcal{O} = (0,1)$ and $R+P$ is the Edwards sum of $R+P$.
- Equation has degree 4, so expect $4\deg(f)$ intersection points by intersection with function f.
- Functions f_i cannot be linear generically (would have 4 intersection points; need to eliminate 2 out of each).
- Quadratic functions f_i could offer enough freedom of cancellation (8 intersection points).
- Problem: conic is determined by 5 points; not enough control over intersection points.

Conic sections

- Solution: observe that points at infinity $\Omega_1 = (1:0:0)$ and $\Omega_2 = (0:1:0)$ are singular and have multiplicity 2.
- Conic determined by passing through the 5 points $R, P, (0,-1), \Omega_1$, and Ω_2 has only one more intersection point Q; then $Q = -(R+P)$.
- Use f_2 to "replace" $(0,-1)$ by $(0,1)$ and $-(R+P)$ by $R+P = (X_3 : Y_3 : Z_3)$, i.e. put

$$f_2 = l_1 \cdot l_2, \text{ with } l_1 = Z_3Y - Y_3Z \text{ and } l_2 = X.$$

- Conic through $(0,-1), \Omega_1$, and Ω_2 has shape

$$C : c_{Z^2}(Z^2 + YZ) + c_{XY}XY + c_{XZ}XZ = 0,$$

where $(c_{Z^2} : c_{XY} : c_{XZ}) \in \mathbb{P}^2(K)$.

Theorem

(a) If $P_1 \neq P_2$, $P_1 \neq \mathcal{O}'$ and $P_2 \neq \mathcal{O}'$, then

$$\begin{aligned} c_{Z^2} &= X_1X_2(Y_1Z_2 - Y_2Z_1), \\ c_{XY} &= Z_1Z_2(X_1Z_2 - X_2Z_1 + X_1Y_2 - X_2Y_1), \\ c_{XZ} &= X_2Y_2Z_1^2 - X_1Y_1Z_2^2 + Y_1Y_2(X_2Z_1 - X_1Z_2). \end{aligned}$$

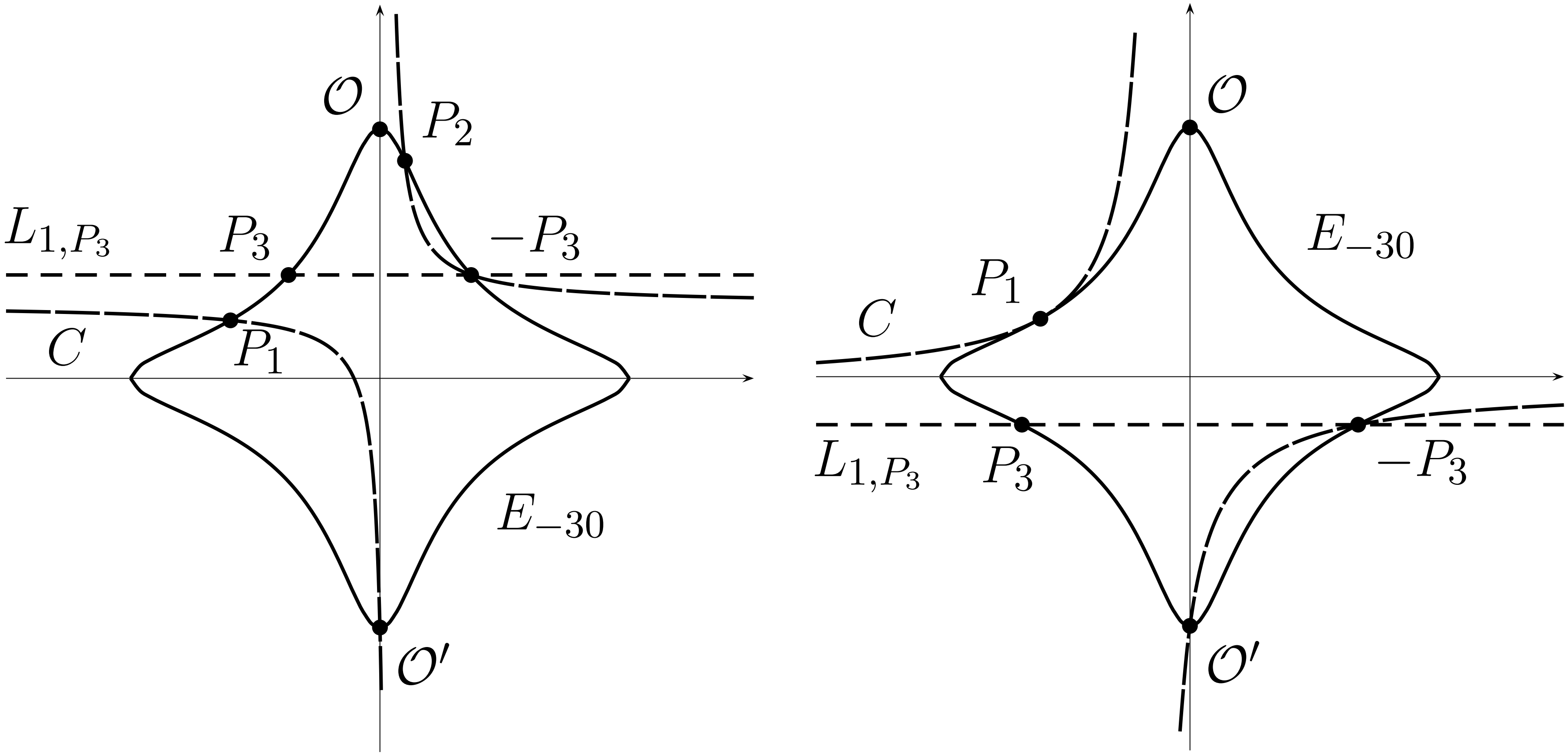
(b) If $P_1 \neq P_2 = \mathcal{O}'$, then

$$c_{Z^2} = -X_1,\ c_{XY} = Z_1,\ c_{XZ} = Z_1.$$

(c) If $P_1 = P_2$, then

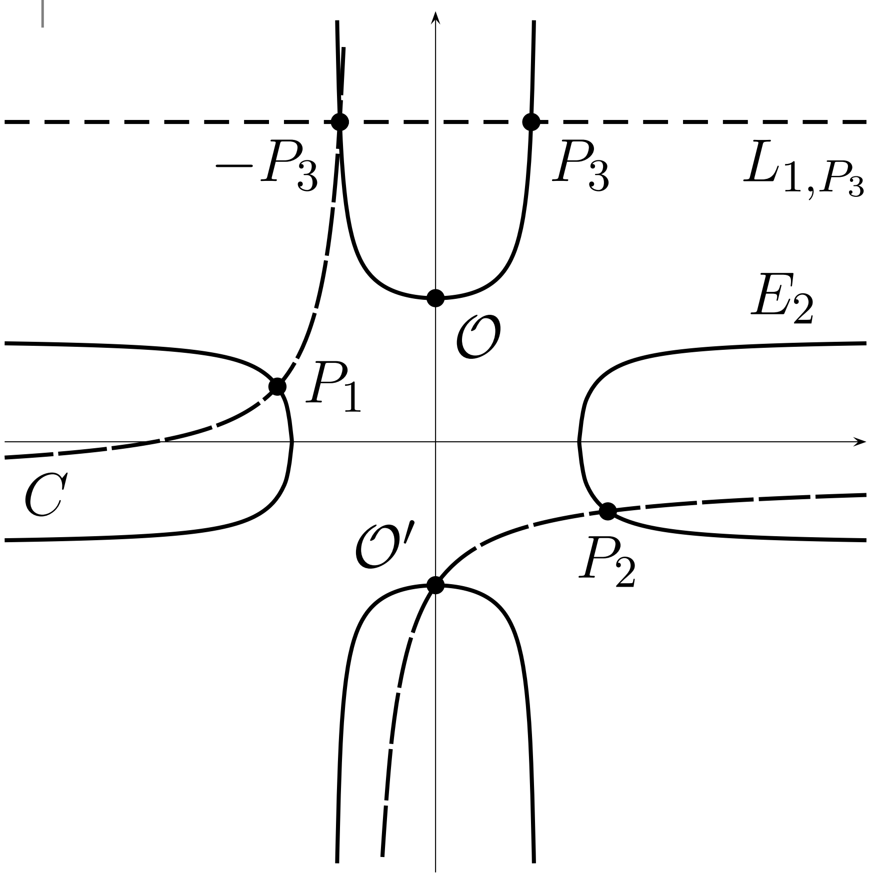
$$\begin{aligned} c_{Z^2} &= X_1Z_1(Z_1 - Y_1), \\ c_{XY} &= dX_1^2Y_1 - Z_1^3, \\ c_{XZ} &= Z_1(Z_1Y_1 - aX_1^2). \end{aligned}$$

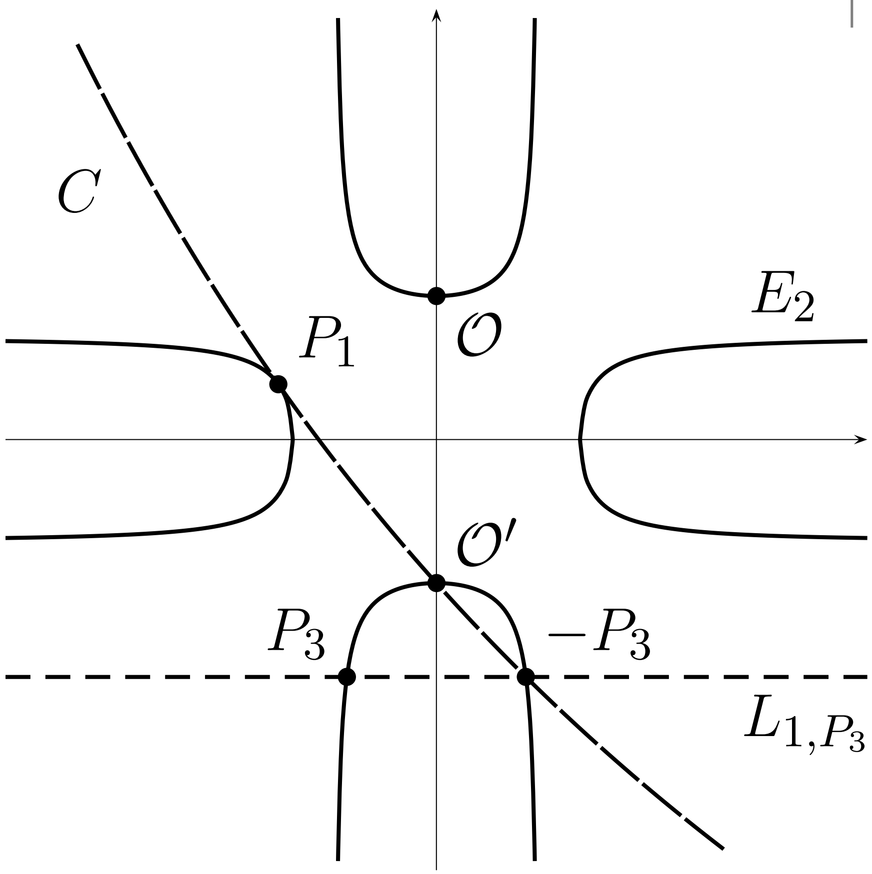
Pictures I



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

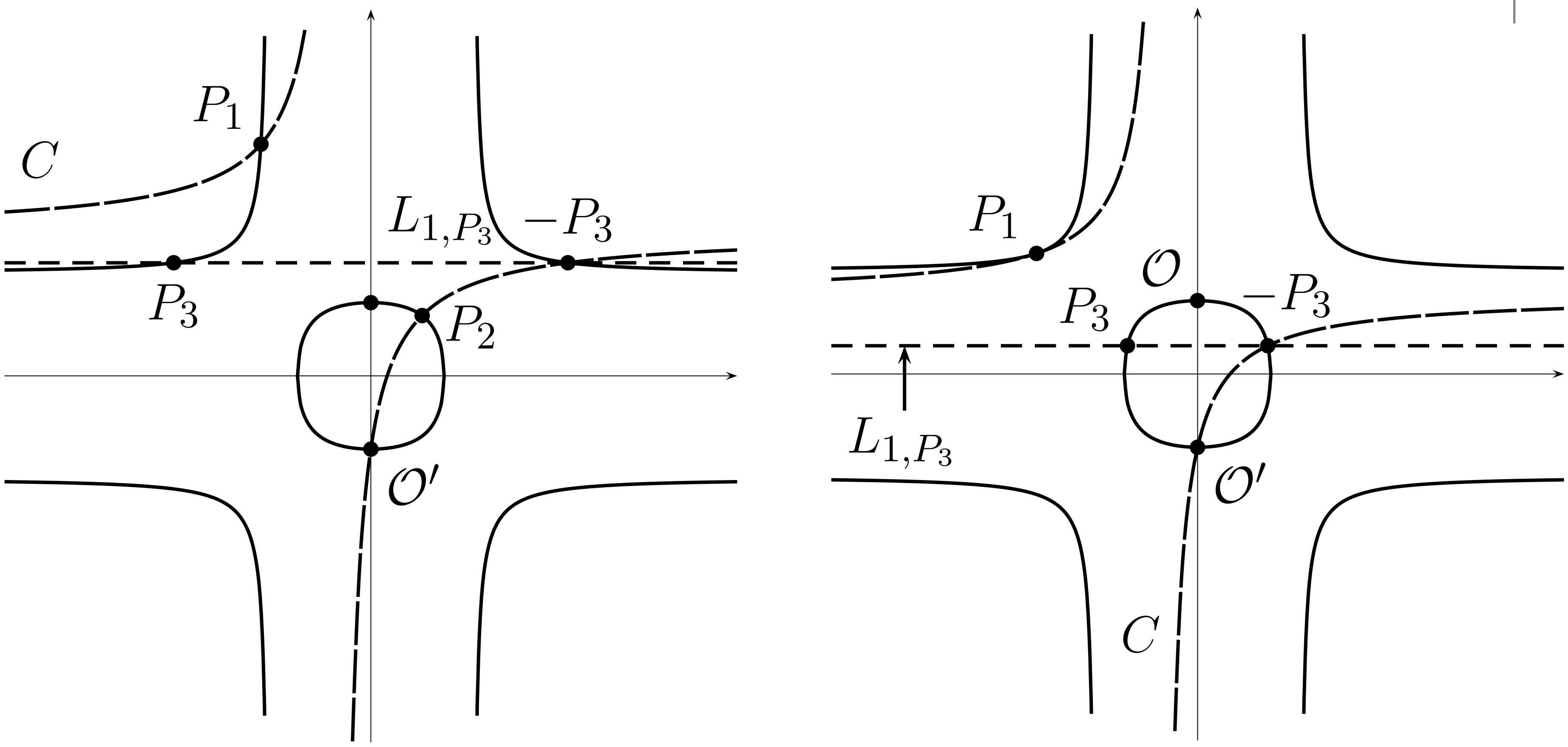
Pictures II





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

Pictures III



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

Pairings on Edwards curves

- Addition procedures are not complete. (Conic for addition is independent of curve while that for doubling needs tangent.)
- Will now detail implications for reduced Tate pairing:

  $$(P, Q) \mapsto f_P(Q)^{(p^k-1)/r},$$

  where $P \in E(\mathbb{F}_p)[r]$, E has embedding degree k with respect to r, and $\mathrm{div}(f_P) = rP - r\mathcal{O}$.
- Ate pairing computes group operations on $E'(\mathbb{F}_{p^{k/d}})$; make sure that this curve has order divisible by 4 (and don't bother with $E(\mathbb{F}_p)$). Cannot have that both have point of order 4 for $d > 2$ by result of Steven Galbraith.

Miller function on twisted Edwards curves I

Assume an even embedding degree k.

- Represent $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(\alpha)$ where $\alpha^2 = \delta \in \mathbb{F}_{p^{k/2}}$.
- Use quadratic twist $E_{\delta a, \delta d}(\mathbb{F}_{p^{k/2}})$ to represent second pairing argument $Q = \psi(Q')$:

$$\begin{aligned} \psi : E_{\delta a,\delta d}(\mathbb{F}_{p^{k/2}}) &\rightarrow E_{a,d}(\mathbb{F}_{p^k}), \\ Q' = (x_0, y_0) &\mapsto (x_0\alpha, y_0). \end{aligned}$$

- Here $y_0 \in \mathbb{F}_{p^{k/2}}$ lies in a proper subfield of $\mathbb{F}_{p^k}$.
- In Miller's algorithm compute
  $f^2 \cdot g_{R,R}(\psi(Q'))$ (doubling step) and
  $f \cdot g_{R,P}(\psi(Q'))$ (addition step).

Miller function on twisted Edwards curves II

- Compute

$$\begin{aligned}\frac{h_1}{l_1 l_2}(x_0\alpha, y_0) &= \frac{c_{Z^2}(1+y_0) + c_{XY}x_0\alpha y_0 + c_{XZ}x_0\alpha}{(Z_3 y_0 - Y_3)x_0\alpha} \\ &= \frac{c_{Z^2}\frac{1+y_0}{x_0\delta}\alpha + c_{XY}y_0 + c_{XZ}}{Z_3 y_0 - Y_3},\end{aligned}$$

  where $(X_3 : Y_3 : Z_3)$ are the coord. of $[2]R$ or $R+P$,
- in $2(k/2)\mathbf{m}$ over $\mathbb{F}_p$ given the coefficients c_{Z^2}, c_{XY}, c_{XZ} and precomputed $\eta = \frac{1+y_0}{x_0\delta}$.
- Note that $Z_3 y_Q - Y_3 \in \mathbb{F}_{p^{k/2}}$. Discard it since final exponentiation maps it to 1 anyway.

Explicit formulas

- Use explicit formulas with extended Edwards coordinates by Hisil, et. al. [Asiacrypt 2008] for point doubling and addition in Miller's algorithm.
- Can reuse large parts of the computation for coefficients of the conic.
- Use even embedding degree and quadratic twist to represent second pairing argument Q, i.e. multiplications with coordinates x_Q and y_Q cost $k/2$ multiplications in $\mathbb{F}_p$.
- Compute conic coefficients in doubling step with $6\mathbf{m} + 5\mathbf{s} + 1\mathbf{m_a}$, in addition step with $14\mathbf{m} + 1\mathbf{m_a}$ (mixed addition $12\mathbf{m} + 1\mathbf{m_a}$).
- Use 2-isogenies to have $a = 1$ and thus $\mathbf{m_a} = 0$.

Comparison

	DBL	mADD	ADD
$\mathcal{J}$	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m_{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = -3$	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{J}, a_4 = 0$	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
$\mathcal{E}$	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m_d}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s}$	$12\mathbf{m}$	$14\mathbf{m}$

Comparison

	DBL	mADD	ADD
$\mathcal{J}$	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m}_{\mathbf{a_4}}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$1\mathbf{m} + 11\mathbf{s} + 1\mathbf{m}_{\mathbf{a_4}}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = -3$	$7\mathbf{m} + 4\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$6\mathbf{m} + 5\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{J}, a_4 = 0$	$6\mathbf{m} + 5\mathbf{s}$	$9\mathbf{m} + 3\mathbf{s}$	—
this paper	$3\mathbf{m} + 8\mathbf{s}$	$6\mathbf{m} + 6\mathbf{s}$	$9\mathbf{m} + 6\mathbf{s}$
$\mathcal{P}, a_4 = 0,\ a_6 = b^2$ Costello et al.	$3\mathbf{m} + 5\mathbf{s}$	$10\mathbf{m} + 2\mathbf{s}$ $+1\mathbf{m}_{\mathbf{b}}$	$13\mathbf{m} + 2\mathbf{s}$ $+1\mathbf{m}_{\mathbf{b}}$
$\mathcal{E}$	$8\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	$14\mathbf{m} + 4\mathbf{s} + 1\mathbf{m}_{\mathbf{d}}$	—
$\mathcal{E}$, this paper	$6\mathbf{m} + 5\mathbf{s}$	$12\mathbf{m}$	$14\mathbf{m}$

Pairing friendly Edwards curves

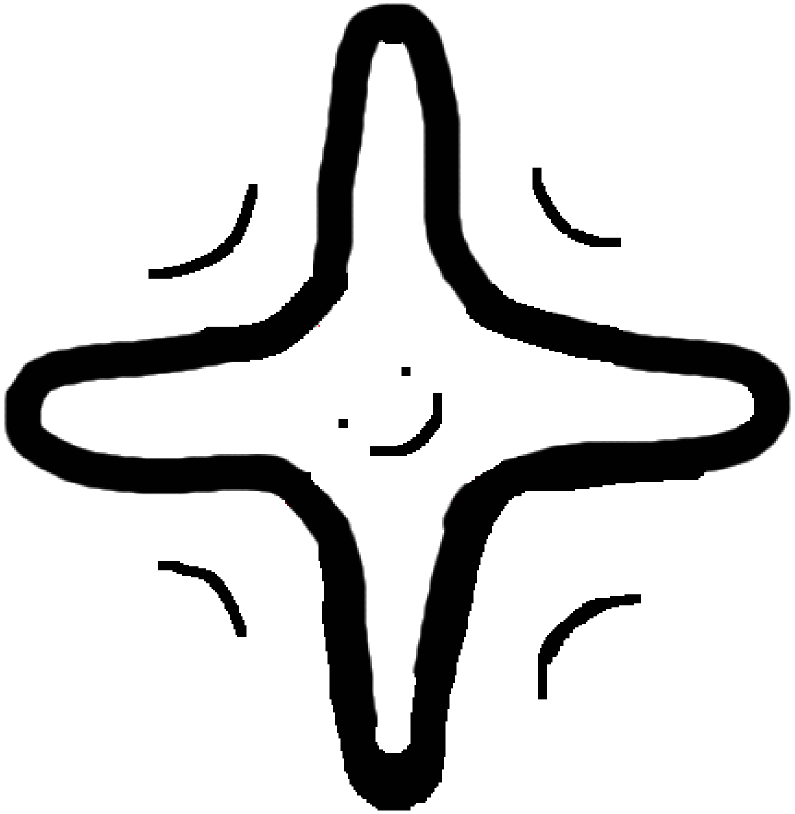
n	160	192	224	256	320	512
p^k	1248	1776	2432	3248	4800	15424
$\rho \cdot k$	7.80	9.25	10.86	12.67	15	30.13

$k = 8, \rho = 1.50$ following Example 6.10 in taxonomy paper:
$D = 1$, $\lceil \log(n) \rceil = 267, \lceil \log(h) \rceil = 133, \lceil \log(p) \rceil = 401$

$$\begin{aligned}
p &= 326816000195375683981422692840809505556419603605344210467517909503792181753784857\\
&\quad 7548206867473587369969429214840474559317,\\
n &= 133392486801388615111969646482668382660908529878176013752617390075068036872364881,\\
h &= 5 \cdot 7730839564540529681 \cdot 15845840683775553774,\\
d &= 212312742600408851440726004433267325162408534870549588701800531572539253229991874\\
&\quad 91701381125724984507626273646524438.
\end{aligned}$$

More curves and the explicit formulas in preprint.

Thank you for your attention!



Explicit formulas and more curve examples in preprint

`http://eprint.iacr.org/2009/155`