Explicit isogenies and endomorphisms of low-genus Jacobians: theory and applications

Benjamin Smith

Team **GRACE**

INRIA Saclay–Île-de-France
Laboratoire d'Informatique de l'École polytechnique (LIX)

Workshop on curves and applications
Calgary
August 18, 2013

0: Why?

Why study isogenies and endomorphisms?

You don't study vector spaces without matrices.
You wouldn't study a group without its quotients and embeddings.

So: we shouldn't study Jacobians
without their homomorphisms and endomorphisms.

The fundamental homomorphisms and endomorphisms are isogenies:
Geometrically surjective, with finite kernel.

Motivation

Isogenies and endomorphisms of low-genus Jacobians have important applications over number fields and over finite fields.

Why the focus on low genus?

Because isogenies of high-genus Jacobians are (almost) as rare as hen's teeth.

Hen's teeth, you say?

For $g > 3$, the quotient of a Jacobian by a finite
(and maximally Weil-isotropic) subgroup is
a Principally Polarized Abelian Variety, but *generally not a Jacobian*.

Look at the moduli spaces:

- PPAVs: moduli space $\mathcal{A}_g$ dim $g(g+1)/2$
- Jacobians: moduli space $\mathcal{M}_g$, dim $3g-3$ $^+$*ive codimension for* $g > 3$

Nevertheless:

Can construct families of pairs $(\mathcal{X}_1, \mathcal{X}_2)$ over number fields
with (absolutely simple) isogenous Jacobians
in *arbitrarily high genus*: Mestre 2009, S. 2010, S. 2011...

(But these are just curiosities.)

I feel a need for speed

Today: applications of isogenies and endomorphisms in curve-based crypto (so, over $\mathbb{F}_q$).

- Central role in Point Counting
- Scalar Multiplication algorithms
- Moving instances of the Discrete Logarithm Problem

Definition

We say an isogeny $\mathcal{J}_{\mathcal{X}_1} \to \mathcal{J}_{\mathcal{X}_2}$ is *efficient* if we can compute the image of elements of $\mathcal{J}_{\mathcal{X}_1}(\mathbb{F}_q)$ in $O(1)$ $\mathbb{F}_q$-operations.

- In practice: "efficient" = "cost of a few group operations".
- $[m]$ is not efficient (in our sense) for $m \gg 0$ (!)

1: Point Counting

Gaudry–Kohel–S., Asiacrypt 2011

The genus 2 point counting problem

Let $\mathcal{H}/\mathbb{F}_p$ be a genus 2 curve: we want to determine $\#\mathcal{J}_{\mathcal{H}}(\mathbb{F}_p)$.

The only vaguely practical algorithm for large p is Schoof–Pila:

- (Crucially) polynomial in $\log p$
- (Also polynomial in field extension degree)
- Exponential in g (never implemented for $g > 2$)

Gaudry–Schost, 2009: Old record for $g = 2$: 128 bit p

O(days) per curve, which is way too slow.

"...to reach the level of AES-256, is still science-fiction..."

The Weil polynomial

Point counting algorithms don't directly count points:
They compute the characteristic polynomial $\chi(X)$ of the Frobenius endomorphism π, which fixes the $\mathbb{F}_p$-points on $\mathcal{J}_{\mathcal{H}}$.

$$\chi(X) = X^4 - s_1 X^3 + (s_2 + 2p)X^2 - ps_1 X + p^2,$$

where

$$|s_1| \leq 4\sqrt{p} \qquad \text{and} \qquad |s_2| \leq 4p.$$

- $\chi(\pi) = [0]$: so for all D in $\mathcal{J}_{\mathcal{H}}(\mathbb{F}_p)$, we have $\pi^4(D) - [s_1]\pi^3(D) + [s_2 + 2p]\pi^2(D) - [ps_1]\pi(D) + [p^2]D = 0$
- $\chi(1) = \#\mathcal{J}_{\mathcal{H}}(\mathbb{F}_p)$

Schoof's algorithm

1. Compute $\chi(X)$ mod ℓ for small primes ℓ
2. Recombine to get $\chi(X)$ (Chinese Remainder Theorem)

- CRT+PNT: Need $O(\log p)$ primes ℓ, largest in $O(\log p)$
- $\chi(X)$ mod ℓ is the characteristic polynomial of π restricted to the ℓ-torsion $\mathcal{J}_{\mathcal{H}}[\ell](\overline{\mathbb{F}}_p) \cong (\mathbb{Z}/\ell\mathbb{Z})^4$
- Compute a generic ℓ-torsion point D; find coeffs of $\chi(X)$ mod ℓ via a small dim-2 DLP on D ($O(\ell)$ group ops).
- The ℓ-torsion is defined by a kernel ideal of degree $O(\ell^4)$, so group operations in $\mathcal{J}_{\mathcal{H}}[\ell]$ cost $\widetilde{O}(\ell^4)$ field operations *(cf. division polynomials of degree $O(\ell^2)$ for elliptic curves)*
- Computing the kernel ideal costs $\widetilde{O}(\ell^6)$ $\mathbb{F}_p$-ops *(cf. $\widetilde{O}(\ell^3)$ for elliptic curves)*

Why is genus 2 point counting slow?

$$\mathrm{Complexity}(\chi \bmod \ell, g = 2) = \mathrm{Complexity}(\chi \bmod \ell, g = 1)^2$$

- Elliptic curves: $\mathbb{Z}[X]/(\chi(X))$ is a **quadratic** imaginary ring.
- Genus 2: $\mathbb{Z}[X]/(\chi(X))$ is a **quartic** imaginary ring.

$\mathbb{Z}[X]/\chi(X)$ has a **real** subring $\mathbb{Z}[\phi] \subset \mathbb{Q}(\sqrt{D})$ for some $D > 0$.
(We say $\mathcal{H}$ has *real multiplication* (RM) by $\mathbb{Q}(\sqrt{D})$).

Idea: choose $\mathcal{H}$ such that it has known RM by $\mathbb{Z}[\phi]$
where ϕ is an efficient endomorphism,
then *compute* $\chi(X)$ *mod primes in* $\mathbb{Z}[\phi]$ *instead of primes in* $\mathbb{Z}$.

The general situation: genus looks like genus 1 squared

Elliptic Curves

$$
\begin{tikzcd}
\mathbb{Z}[X]/(\chi(X)) \arrow[d, dash, "2"'] \\
\mathbb{Z}
\end{tikzcd}
$$

Genus 2

$$
\begin{tikzcd}
\mathbb{Z}[X]/(\chi(X)) \arrow[d, dash, "2"'] \\
\mathbb{Z}[\phi] \arrow[d, dash, "2"'] \\
\mathbb{Z}
\end{tikzcd}
$$

With efficient RM: genus 2 looks like genus 1

Elliptic Curves

$$\begin{tikzcd} \mathbb{Z}[X]/(\chi(X)) \arrow[d, dash, "2"'] \\ \mathbb{Z} \end{tikzcd}$$

Genus 2

$$\begin{tikzcd} \mathbb{Z}[X]/(\chi(X)) \arrow[d, dash, "2"'] \\ \mathbb{Z}[\phi] \arrow[d, dash, "2"'] \\ \mathbb{Z} \end{tikzcd}$$

Efficient RM: extension known!

An example of efficient RM

Consider the Tautz–Top–Verberkmoes family

$$\mathcal{C} : y^2 = x^5 - 5x^3 + 5x + t.$$

We have an explicit endomorphism ϕ defined by

$$\phi((u, v)) = (x^2 - \tau ux + u^2 + \tau^2 - 4, y - v)$$

where $\tau = \zeta_5 + \zeta_5^{-1}$ (in $\mathbb{F}_q$ if $q \not\equiv \pm 2 \bmod 5$).

We have $\phi^2 + \phi - 1 = 0$, so
$\mathcal{J}_{\mathcal{C}}$ has efficient RM by $\mathbb{Z}[\phi] \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Other families: *(Mestre, Hashimoto, Brumer...)*

Real primes

Suppose ℓ does not divide $\operatorname{disc}(\mathbb{Z}[\phi])$. Then either

- $(\ell) = (\ell)$ (inert: ℓ stays prime in $\mathbb{Z}[\phi]$)
  $\implies \deg \mathcal{J}_{\mathcal{H}}[\ell] = O(\ell^4)$
- $(\ell) = \mathfrak{a}_1\mathfrak{a}_2$ (ℓ splits into two prime ideals in $\mathbb{Z}[\phi]$)
  $\implies \mathcal{J}_{\mathcal{H}}[\ell] = \mathcal{J}_{\mathcal{H}}[\mathfrak{a}_1] \oplus \mathcal{J}_{\mathcal{H}}[\mathfrak{a}_2]$, with $\deg \mathcal{J}_{\mathcal{H}}[\mathfrak{a}_i] = O(\ell^2)$

  Example: $(1009) = (33 - 4\sqrt{5})(33 + 4\sqrt{5})$ in $\mathbb{Z}[\sqrt{5}]$

Cebotarev density: asymptotically, half the primes split in $\mathbb{Z}[\phi]$.
Splitting is determined by a simple congruence condition.

If ϕ is efficient, then we can explicitly
compute in $\mathcal{J}_{\mathcal{H}}[\mathfrak{a}_1]$ and $\mathcal{J}_{\mathcal{H}}[\mathfrak{a}_2]$ instead of $\mathcal{J}_{\mathcal{H}}[\ell]$.

Getting real

There exist 2-parameter families of curves with efficient RM endomorphisms.

- Families form codim-1 subvarieties of dim-3 moduli space. *In English:* we **only lose 1 degree of freedom** (from 3) in random curve selection.
- We know, **in advance**, which primes ℓ split (density 1/2)
- Use only split primes: still $O(\log p)$ of size $O(\log p)$
- For the split ℓ,
  - kernel ideal degree drops from $O(\ell^4)$ to $O(\ell^2)$
  - group operations in kernel drop from $\widetilde{O}(\ell^4)$ to $\widetilde{O}(\ell^2)$ $\mathbb{F}_p$-ops
  - Cost of computing kernel drops from $\widetilde{O}(\ell^6)$ to $\widetilde{O}(\ell^3)$ $\mathbb{F}_p$-ops
- Total complexity drops from $\widetilde{O}(\log^8 p)$ to $\widetilde{O}(\log^5 p)$ bit ops

Purely theoretical cuteness

Comparison with elliptic curve point counting

- Schoof for Elliptic Curves / $\mathbb{F}_p$:

  proven $\widetilde{O}(\log^5 p)$ *bit ops*
- Schoof–Elkies–Atkin for Elliptic Curves / $\mathbb{F}_p$:

  heuristic $\widetilde{O}(\log^4 p)$ *bit ops*
- RM Schoof–Pila for genus 2 / $\mathbb{F}_p$:

  proven $\widetilde{O}(\log^5 p)$ *bit ops*

So point counting has the same unconditional complexity
for genus 2 explicit-RM curves over $\mathbb{F}_p$
as for elliptic curves *over the same* $\mathbb{F}_p$!

Keeping it real

We searched for a secure genus 2 curve in the explicit $\mathbb{Q}(\sqrt{5})$-RM family

$$\mathcal{H} : y^2 = x^5 - 5x^3 + 5x + t$$

over $\mathbb{F}_p$ with $q = 2^{128} + 573$.

Computing $\chi(T)$ for any $t \in \mathbb{F}_p$: about 3 Core2 core-hours at 2.83GHz; we use the split primes $\ell \leq 131$.

We ran 245 trials, finding 27 prime-order Jacobians.

We found that the Jacobian of the curve at

$$t = 75146620714142230387068843744286456025$$

has prime order, and so does its quadratic twist.

Keeping it surreal

From the realm of science fiction...

1024 bits

We computed $\chi(T)$ for $\mathcal{H} : y^2 = x^5 - 5x^3 + 5x + t$
over $\mathbb{F}_p$ with $q = 2^{512} + 1273$ and

$$t = 29085666333787272437998261129919801749774533\\ 00368095776223256986807375270272014471477919\\ 88284560426970082027081672153243497592108531\\ 6560590832659122351278.$$

This took about 80 core-days (same setup as before);
we only used the split primes $\ell \leq 419$.

The cardinality is

$$
\begin{aligned}
\#\mathcal{J}_{\mathcal{H}}(\mathbb{F}_p) = {} & 1797693134862315907729305190789024733617 9\\
& 7697894230657273430081157732675805502375 7\\
& 3705948956144184541720417180780929444962 7\\
& 6345280122736480532381892625890207485181 8\\
& 0898888687577372373289203253158846463934 6\\
& 2965754493894524803468668112345681706310 6\\
& 4854408448693873966658594221866364422587 1\\
& 268417790010511900552 0.
\end{aligned}
$$

2: Scalar Multiplication

S., Asiacrypt 2013

Geometry: Use It or Lose It

Elliptic curves are a source of concrete groups
that perform essentially as well as black-box groups...

BUT

..there's nothing black-box about a smooth plane cubic

Problems:

Destructive Exploit the geometry to solve DLPs faster (reduce security)

Constructive Exploit the geometry to make cryptosystems more efficient

Eigenvalues of endomorphisms

We have a cryptosystem in a cyclic group $\mathcal{G} \cong \mathbb{Z}/N\mathbb{Z}$, embedded in an elliptic curve $\mathcal{E}$.

$$\mathrm{End}(\mathcal{G}) = \mathbb{Z}/N\mathbb{Z}$$
$$\mathrm{End}(\mathcal{E}) \supseteq \mathbb{Z}[\pi], \qquad \text{where } \pi : (x, y) \longmapsto (x^q, y^q) \text{ (Frobenius)}$$

If $\psi \in \mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ restricts to an endomorphism of $\mathcal{G}$ (that is, $\psi(\mathcal{G}) \subseteq \mathcal{G}$) —and this happens pretty much all the time—then

$$\psi(P) = [\lambda_\psi]P \qquad \text{for all } P \in \mathcal{G}$$

We call λ_ψ the *eigenvalue* of ψ on $\mathcal{G}$. *Note:* $-N/2 < \lambda_\psi < N/2$.

Scalar multiplication with an endomorphism

Consider scalar multiplication: we want to compute $[m]P$.
Abstractly, we can do this with $\log_2 m$ doubles.

Suppose $\psi \in \mathrm{End}(\mathcal{E})$ has eigenvalue λ_ψ in $\mathbb{Z}/N\mathbb{Z}$.
If

$$m \equiv a + b\lambda_\psi \pmod{N},$$

then

$$[m]P = [a]P \oplus [b]\psi(P)$$

—and we can compute the RHS using multiexponentation.
Hence

- if ψ can be evaluated fast *(time/space $<$ few doubles)*, and
- if we can find a and b significantly shorter than m,

then we can compute $[m]P$ significantly faster.

Scalar multiplication with an endomorphism

Lemma

If $|\lambda_\psi| > N^{1/2}$, then we can find a and b such that

$$a + b\lambda_\psi \equiv m \pmod{N}$$

with

$$a \text{ and } b \text{ in } O(\sqrt{N}).$$

(Even better: can compute a and b easily)

Great! Now all we need is a source of good $\mathcal{E}$ equipped with fast ψ...
...and this turns out to be highly nontrivial.

Note: integer multiplications and Frobenius do not make good ψ.

GLV Curves (Gallant–Lambert–Vanstone, CRYPTO 2001)

Start with an explicit CM curve over $\overline{\mathbb{Q}}$ and reduce mod p.

Example (CM by $\sqrt{-1}$)

Let $p \equiv 1 \pmod{4}$; let i be a square root of -1 in $\mathbb{F}_p$. Then the curves

$$\mathcal{E}_a : y^2 = x^3 + ax$$

have an explicit (and extremely efficient) endomorphism

$$\psi : (x, y) \longmapsto (-x, iy).$$

Good scalar decompositions: this $\lambda_\psi \equiv \sqrt{-1} \pmod{N}$.

Limitations of GLV

The curves $\mathcal{E}_a/\mathbb{F}_p : y^2 = x^3 + ax$ look perfect...
...but we are not always free to choose our own prime p.

Example

The 256-bit prime $p = 2^{255} - 19$ offers very fast field arithmetic.
The $\mathbb{F}_p$-isomorphism classes of $\mathcal{E}_a/\mathbb{F}_p$ are represented by $a = 1, 2, 4, 8$.

$$\text{Largest prime factor of } \#\mathcal{E}_a(\mathbb{F}_p) = \begin{cases} 199 \text{ bits} & \text{if } a = 1 \\ 239 \text{ bits} & \text{if } a = 2 \\ 175 \text{ bits} & \text{if } a = 4 \\ 173 \text{ bits} & \text{if } a = 8 \end{cases}$$

So we pay for fast arithmetic with at least 17 (/256) bits of group order, which is about 9 (/128) bits of security.

Other GLV curves

We can try other explicit CM curves... But there are hardly any of them!

- ψ fast (generally) implies deg ϕ very small
- deg ϕ small, $\phi \notin \mathbb{Z} \implies \mathbb{Z}[\phi]$ has small discriminant Δ
- curves with CM by discriminant Δ have j-invariant classified by Hilbert polynomials H_Δ
- H_Δ has very small degree, typically 1 for tiny Δ
- $\implies$ only one j-invariant per Δ
- Only 2, 4, or 6 twists (curves) per j-invariant
- $\implies$ a handful of suitable curves, none of which might have (almost)-prime reduction mod p

Only 18 GLV curves with endomorphisms faster than doubling.
No guarantee *any* of them have good cryptographic group orders mod p.

Curve rarity is a critical weakness of the GLV technique.

GLS Curves (Galbraith–Lin–Scott, EUROCRYPT 2009)

Start with any curve over $\mathbb{F}_p$, extend to $\mathbb{F}_{p^2}$, and use p-th powering on the quadratic twist.

Example

Let $p \equiv 5 \pmod 8$, take A, B, in $\mathbb{F}_p$, take μ in $\mathbb{F}_{p^2}$ with μ nonsquare:

$$\mathcal{E}/\mathbb{F}_{p^2} : y^2 = x^3 + \mu^2 Ax + \mu^3 B$$

has an efficient endomorphism

$$\psi : (x, y) \longmapsto (-x^p, iy^p) \quad \text{where } i^2 = -1.$$

p-th powering in $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{D})$ almost free: $(a_0 + a_1\sqrt{D})^p = a_0 - a_q\sqrt{D}$

Good scalar decompositions: $\lambda_\psi \equiv \sqrt{-1} \pmod N$.

Twist security: the problem with GLS

GLS offers p different j-invariants with an extremely fast endomorphism.
Some of these j-invariants should give prime/secure order curves.

Solves the secure curve choice problem for fixed p!

Weak point: built-in twist-insecurity.

- Some fast curve arithmetic (eg. Montgomery) is twist-agnostic
- Fouque–Réal–Lercier–Vallette attack: sneak in a point on the twist $\implies$ can recover secret keys by solving DLogs on the twist
- So we need almost-prime order for both the curve *and* its twist

GLS curves: twist is (by construction) a subfield curve, and its largest prime factor is in $O(p)$ instead of $O(p^2)$: *built-in weakness*.

New endomorphisms

Consider a general elliptic curve $\mathcal{E} : y^2 = x^3 + Ax + B$ over $\mathbb{F}_{p^2}$.

No obvious endomorphisms, apart from

- $[m]$ for $m \in \mathbb{Z}$ *(eigenvalue m, too slow for big m !)*
- Frobenius $\pi : (x, y) \to (x^{p^2}, y^{p^2})$ *(fixes $\mathbb{F}_{p^2}$-points: eigenvalue 1)*, and
- Linear combinations: too slow!

We would like to use the sub-Frobenius

$$\pi_0 : (x, y) \longmapsto (x^p, y^p),$$

but it's **not an endomorphism**: it is an **isogeny** mapping us onto

$${}^{(p)}\mathcal{E} : y^2 = x^3 + A^p x + B^p$$

...which, over $\mathbb{F}_{p^2}$, coincides with the Galois conjugate of $\mathcal{E}$.

New endomorphisms

We've mapped onto the wrong curve! We need to get back to $\mathcal{E}$.

We have another p-powering isogeny ${}^{(p)}\pi_0 : {}^{(p)}\mathcal{E} \to \mathcal{E}$,
but the composition ${}^{(p)}\pi_0\pi_0$ is π (Frobenius), no use!

Idea: What if $\mathcal{E}$ was the reduction mod p of a **quadratic** $\mathbb{Q}$**-curve**?

$\mathbb{Q}$-curves

Definition

A **quadratic $\mathbb{Q}$-curve of degree** d is

- an elliptic curve $\widetilde{\mathcal{E}} : y^2 = x^3 + Ax + B$ over a quadratic field $\mathbb{Q}(\sqrt{\Delta})$,
- *without* complex multiplication,
- s.t. $\exists$ a d-isogeny $\widetilde{\phi} : \widetilde{\mathcal{E}} \longrightarrow {}^{\sigma}\widetilde{\mathcal{E}} : y^2 = x^3 + \sigma(A)x + \sigma(B)$.

Here σ is conjugation on $\mathbb{Q}(\sqrt{\Delta})$, and $\widetilde{\phi}$ can be defined over $\mathbb{Q}(\sqrt{\Delta}, \sqrt{-d})$.

Where do we find quadratic $\mathbb{Q}$-curves of degree d? Look at the map

$$X_0(d) \longrightarrow X^*(d) := X_0(d)/\langle \text{Atkin–Lehners} \rangle.$$

- $\mathbb{Q}$-curves correspond to irrational preimages of points in $X^*(d)(\mathbb{Q})$
- $X_0(d) \cong \mathbb{P}^1$ for small d; can give one-parameter families of $\mathbb{Q}$-curves

From $\mathbb{Q}$-curves to endomorphisms

Start with a $\mathbb{Q}$-curve: we have a d-isogeny

$$\widetilde{\phi} : \widetilde{\mathcal{E}} \longrightarrow {}^{\sigma}\widetilde{\mathcal{E}} \qquad \text{over} \qquad \mathbb{Q}(\sqrt{\Delta}, \sqrt{-d}).$$

Reduce $\widetilde{\phi}$ modulo a prime p inert in $\mathbb{Q}(\sqrt{\Delta})$ to get a d-isogeny

$$\phi : \mathcal{E} \longrightarrow {}^{(p)}\mathcal{E} \qquad \text{over} \qquad \mathbb{F}_{p^2}.$$

Then compose with $\pi_0 : {}^{(p)}\mathcal{E} \to \mathcal{E}$ to get a degree-dp endomorphism

$$\psi := \pi_0 \circ \phi \text{ in } \mathrm{End}(\mathcal{E}).$$

Using ${}^{\sigma}\widetilde{\phi} \circ \widetilde{\phi} = [\pm d]$ (since $\widetilde{\mathcal{E}}$ has no CM), we see that

$$\psi^2 = [\pm d]\pi_{\mathcal{E}}.$$

When d is very small: ψ is fast, with a big eigenvalue ($\pm\sqrt{\pm d} \pmod{N}$).

Example: Universal quadratic $\mathbb{Q}$-curve of degree 2

Example (Hasegawa)

Let Δ be any squarefree discriminant, $t \in \mathbb{Q}$ a free parameter, and

$$\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{\Delta}) : y^2 = (x-4)(x^2+4x+18t\sqrt{\Delta}-14)$$

$$^{\sigma}\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{\Delta}) : y^2 = (x-4)(x^2+4x-18t\sqrt{\Delta}-14)$$

There exists a 2-isogeny $\widetilde{\phi} : \widetilde{\mathcal{E}} \to {}^{\sigma}\widetilde{\mathcal{E}}$, defined by

$$\widetilde{\phi} : (x,y) \longmapsto \left(f(x), \frac{y}{\sqrt{-2}} f'(x) \right) \text{ where } f(x) = -\frac{x}{2} - \frac{9(1+t\sqrt{\Delta})}{x-4}$$

- Good reduction mod every prime $p > 3$ inert in $\mathbb{Q}(\sqrt{\Delta})$
- Given a fast prime p: choose Δ st p is inert $\Longrightarrow$ *fast field arithmetic*
- $2p - \epsilon$ different j-invariants in $\mathbb{F}_{p^2}$ (w/ codomains) $\Longrightarrow$ *curve choice!*

Example: degree-$2p$ endomorphisms

For any $p > 3$, let Δ be a nonsquare mod p. For every $t \in \mathbb{F}_p$,

$$\mathcal{E}_t/\mathbb{F}_{p^2} : y^2 = x^3 - 6(5 - 3t\sqrt{\Delta})x + 8(7 - 9t\sqrt{\Delta})$$

has an efficiently computable endomorphism

$$\psi : (x, y) \longmapsto \left(f(x^p), \frac{y^p}{\sqrt{-2}} f'(x^p) \right) \text{ where } f(x^p) = \frac{-x^p}{2} - \frac{9(1 - t\sqrt{\Delta})}{(x^p - 4)}$$

such that $\psi^2 = [\pm 2]\pi_{\mathcal{E}_t}$. Note: ψ is faster than doubling.

Example (160-bit curves)

Work over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{2})$ with $p = 2^{80} - 93$; take $t = 4556$. Then

- *secure order*: $\#\mathcal{E}_{4556}(\mathbb{F}_{p^2}) = 2 \cdot (\text{159-bit prime})$
- *twist-secure*: $\#\mathcal{E}'_{4556}(\mathbb{F}_{p^2}) = 2 \cdot (\text{159-bit prime})$

...And 160-bit scalar multiplications become 80-bit multiexponentiations.

More generally: other degrees

$$g(X_0(d)) = 0 \implies \text{family of degree-}dp\text{ endomorphisms}$$

- $d = 1$: degenerate case, recover GLS
- $d = 3$: we construct prime-order twist-secure curves
- $d = 5$: we construct prime-order twist-prime-order curves
- $d \geq 7$: even more curves... but slower, less interesting.

Example (From $d = 3$ family)

Work over $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$ with $p = 2^{127} - 1$: very fast arithmetic.
Take $t = 122912611041315220011572494331480107107$; then

- $\#\mathcal{E}_{3,t}(\mathbb{F}_p(\sqrt{-1})) = 3 \cdot (253\text{-bit prime})$ *secure*
- $\#\mathcal{E}'_{3,t}(\mathbb{F}_p(\sqrt{-1})) = 254\text{-bit prime}$ *twist secure!*

Any scalar multiplication on this curve requires at most 127 doubles.

Going further

We have 1-parameter families of elliptic curves over $\mathbb{F}_{p^2}$ with efficient endomorphisms of degree $1p$ (GLS), $2p$, $3p$, $5p$, $7p$.

That's more than enough curves over $\mathbb{F}_{p^2}$!

Question: can we find more curves efficient endomorphisms over the prime field $\mathbb{F}_p$?