Computing traces of endomorphisms

Travis Morrison [1] Lorenz Panny [2] Jana Sotáková [3] Michael Wills [1]

[1]Virginia Tech

[2]TU Munich, Germany

[3]University of Amsterdam and QuSoft

October 11, 2023 Leuven

One endomorphism

This talk: $\mathbb{F}_q$ finite field of characteristic $p \gg 0$ and $E/\mathbb{F}_q$ elliptic curve

Endomorphisms and algebraic integers

endomorphisms	algebraic numbers	(notation)
endomorphism $\varphi : E \to E$	$\alpha \in \mathcal{O}$	α
dual map $\hat{\varphi}$	conjugate $\overline{\alpha} \in \mathcal{O}$	
$\deg(\varphi)$	$\mathrm{nrd}(\alpha) = \alpha\overline{\alpha}$	$n \in \mathbb{Z}$
$\mathrm{tr}(\varphi) = \varphi + \hat{\varphi}$	$\mathrm{trd}(\alpha) = \alpha + \overline{\alpha}$	$t \in \mathbb{Z}$

With notation as above, α is a root of the monic integral polynomial

$$f_\alpha(x) = x^2 - tx + n$$

with $t^2 - 4n < 0$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{t^2 - 4n})$ is an imaginary quadratic field.

If α is a scalar multiplication, then $t^2 - 4n = 0$.

More endomorphisms?

Let E be supersingular. Standard approach to compute endomorphism rings:

Find cycles in the isogeny graph, represented as compositions of (possibly many) isogeny steps of small degree (typically $2, 3, 5$). Say you find α, β.

Identify the order generated by α, β

The norms are easy (by construction); can compute traces of α, β. To identify the order, need to compute the *trace pairing*, i.e. compute

$$\mathrm{trd}(\alpha\overline{\beta}).$$

From this, obtain an embedding $\mathbb{Z}\langle\alpha, \beta\rangle \hookrightarrow B_{p,\infty}$.

Computing traces

- from the definition of trace:

$$t = \mathrm{tr}(\alpha) = \alpha + \overline{\alpha} \quad \Rightarrow \quad \varphi + \hat{\varphi} = [t]$$

- from the characteritic equation:

$$\alpha^2 - t\alpha + n = 0 \quad \Rightarrow \quad [t]\varphi = \varphi^2 + [n]$$

Strategy:

(Assume we know n.) Find t such that $\varphi^2 + [n] = [t]\varphi$.

Schoof's algorithm

Recall that point counting is computing trace of Frobenius:

$$\#E(\mathbb{F}_q) = 1 + q - t$$

Schoof's approach

Compute t mod ℓ_i for increasing primes ℓ_i until $\prod \ell_i > 4\sqrt{q}$, reconstruct using CRT.

Hasse intervals: $|t| \leq 2\sqrt{q}$.

Apply to endomorphisms

Compute t mod ℓ_i for increasing primes ℓ_i until $\prod \ell_i > 4\sqrt{n}$, reconstruct using CRT.

Negative discriminants: $t^2 - 4n \leq 0 \iff |t| \leq 2\sqrt{n}$.

Computing mod ℓ

Goal: Find t such that $\varphi^2 + [n] = [t]\varphi$.

Torsion points

Assume that $n = \deg(\varphi)$ is coprime to ℓ. For any $P \in E(\mathbb{F}_q)[\ell]$, set

$$Q = (\varphi^2 + [n])(P)$$
$$R = \varphi(P)$$

Then $[t]R = Q$ and we can recover $t \bmod \ell$ by computing this discrete logarithm.

Useful extension

For any point P of order M, we can obtain $t \bmod \operatorname{ord}(\varphi(P)) \leftarrow$ some divisor of M.

Working with all torsion points

Suppose E is given as $E : y^2 = x^3 + ax + b$.

Schoof's trick

Instead of finding points in $E[\ell]$, use the division polynomial $\psi_\ell(x)$ in the ring

$$\mathcal{R}_\ell = \mathbb{F}_q[x, y]/(\psi_\ell(x), y^2 - x^3 - ax - b)$$

and check the equality $\varphi^2 + [n] = [t]\varphi$ in $\mathcal{R}_\ell$.

Zero divisors.

Zero divisors g in $\mathcal{R}_\ell$ give factors of $\psi_\ell(x)$, and we would instead like to work in

$$\mathcal{R}_g = \mathbb{F}_q[x, y]/(g(x), y^2 - x^3 - ax - b)$$

Schoof-Atkin-Elkies

Point counting:

(Elkies) If E admits a $\mathbb{F}_q$-rational isogeny, we can reconstruct its kernel polynomial $g(x)$ and compute in $\mathcal{R}_g = \mathbb{F}_q[x,y]/(g(x), y^2 - x^3 - ax - b)$.

- Corresponds to restricting everything to the subgroup defined by $g(x)$.
- Division polynomials have degree $\frac{\ell^2-1}{2}$, whereas kernel polynomials $\frac{\ell-1}{2}$.
- For supersingular elliptic curves, all isogenies already defined over $\mathbb{F}_{p^2}$.

Caveat

Endomorphisms have no special reasons to fix nice subgroups.

Computing for endomorphisms

- $C \subset E[\ell]$ cyclic of size ℓ,
- g its corresponding kernel polynomial,
- $\alpha \in \mathrm{End}(E)$ an endomorphism with $\ell \nmid \mathrm{nrd}(\alpha)$.

Reducing mod g

Denote by $\alpha|_C$ the image of the defining rational maps of α in $\mathcal{R}_g = \mathbb{F}_q[x, y]/(g(x), y^2 - x^3 - ax - b)$.

Computing modulo g

The reduction mod g is additive: $(\alpha + \beta)|_C = \alpha|_C + \beta|_C$ but is not a homomorphism under the "just take the rational maps" operation:

$$\alpha^2|_C \neq \alpha|_C \circ \alpha|_C$$

Note that $\alpha(C) \neq C$ in general, so this composition does not make sense.

Story so far

α endomorphism of E.
Trying to find t such that $\alpha^2 + [n] = [t]\alpha$.

Strategy

1. If $\ell \mid \#E(\mathbb{F}_q)$: evaluate both $\alpha^2 + [n]$ and α at some ℓ-torsion point, and compute $[t]$ from a discrete log;
2. Otherwise,
   2.1 find a kernel polynomial $g(x)$ corresponding to some ℓ-isogeny [BMSS],
   2.2 compute in the ring $\mathcal{R}_g$.

Isogeny primes

Isogenistas like forcing p such that our curves have lots of available torsion.

Differential magic

Acting on differentials

Let $\varphi : E \to E'$ be an isogeny in *standard form*

$$\varphi(x, y) = \left(F(x), c_\varphi \cdot y \cdot F'(x)\right).$$

Then $\varphi \mapsto c_\varphi$ is a nice map into $\mathbb{F}_q$ whenever we can:

1. it is additive when we can: for $\varphi_1, \varphi_2 : E \to E'$ we have

$$c_{\varphi_1+\varphi_2} = c_{\varphi_1} + c_{\varphi_2}$$

2. it is multiplicative when we can: for $\varphi : E \to E'$ and $\psi : E' \to E''$ we have

$$c_{\psi\circ\varphi} = c_\psi \cdot c_\varphi$$

mod p magic

Endomorphisms have the extra condition that $\alpha : E \to E$.

For endomorphisms,

the map $\alpha \mapsto c_\alpha$ is a ring homomorphism

$$\mathrm{End}(E) \to \mathbb{F}_q.$$

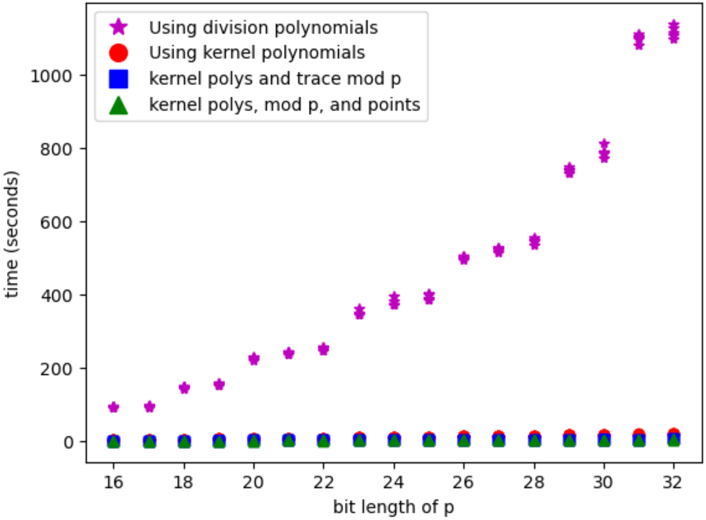
In particular, if α satisfies the equation $x^2 - tx + n$, then so does c_α.

Computing trace mod p.

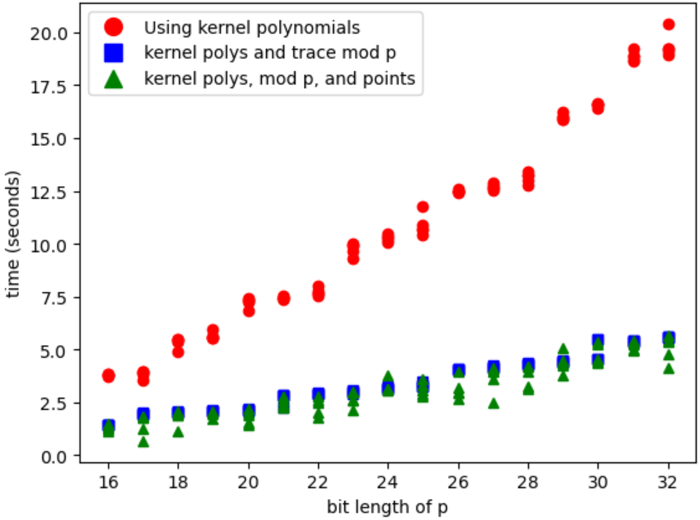
If α is separable, then $c_\alpha \neq 0$ and we can recover

$$t = c_\alpha + n/c_\alpha \quad \text{in } \mathbb{F}_p$$

Some timings for computing a trace of random endomorphism



Zooming in



Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
time (seconds)
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
16
18
20
22
24
26
28
30
32
bit length of p

Code demo?

Work in progress[1]

COMPUTING SUPERSINGULAR TRACES

TRAVIS MORRISON, LORENZ PANNY, JANA SOTÁKOVÁ, AND MICHAEL WILLS

[1] Progress: we are finishing the write-up and we're cleaning up the code!