Beyond the SEA (algorithm): Computing the trace of a supersingular endomorphism

Travis Morrison

Virginia Tech

joint work with: Lorenz Panny, Jana Sotáková, Michael Wills

Isogenies and endomorphisms of elliptic curves

Let E, E' be elliptic curves over k.

Definition

An *isogeny* $\phi\colon E \to E'$ is a rational map which induces a group homomorphism $E(\overline{k}) \to E'(\overline{k})$. An *endomorphism* of E is an isogeny $\phi : E \to E$ (or the 0 map).

- If n is an integer, then the multiplication-by-n map

$$[n] : P \mapsto nP$$

  is an endomorphism of E
- If $k = \mathbb{F}_q$, then the *Frobenius endomorphism* of E is an endomorphism:

$$\begin{aligned} \pi_E &\colon E \to E \\ (x, y) &\mapsto (x^q, y^q). \end{aligned}$$

A cheatsheet

	Endomorphisms	Imaginary quadratic integers
Notation	α	$a + b\sqrt{-D}$
Involution	The dual map	complex conjugation
Norm	$\deg \alpha = \widehat{\alpha} \circ \alpha$	$\lvert a + b\sqrt{-D}\rvert^2 = a^2 + Db^2$
Trace	$\operatorname{tr} \alpha = \alpha + \widehat{\alpha}$	$2a$
Discriminant	$(\operatorname{tr} \alpha)^2 - 4 \deg \alpha$	$-4b^2 D$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then

$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then

$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$

- Hasse bound: $|\operatorname{tr} \pi_E| \leq 2\sqrt{q}$

Examples, again

- Let $[n]\colon E \to E$ be the multiplication-by-n map. We have

$$\deg[n] = n^2, \quad \operatorname{tr}[n] = 2n.$$

- Let π_E be the Frobenius endomorphism of $E/\mathbb{F}_q$. Then

$$\deg \pi_E = q, \quad \operatorname{tr} \pi_E = q + 1 - \#E(\mathbb{F}_q)$$

- Hasse bound: $|\operatorname{tr} \pi_E| \leq 2\sqrt{q}$
- More generally, if $\alpha \in \operatorname{End}(E)$, then

$$\operatorname{disc} \alpha = (\operatorname{tr} \alpha)^2 - 4 \deg \alpha \leq 0 \implies |\operatorname{tr} \alpha| \leq 2\sqrt{\deg \alpha}.$$

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Why? Ordinary case

Point counting! Also, $\mathrm{tr}\,\pi_E$ reveals the structure of $\mathbb{Z}[\pi_E]$ as an algebra.

Computing the trace of an endomorphism

Problem: computing traces of endomorphisms

Given an elliptic curve $E/\mathbb{F}_q$ and $\alpha \in \mathrm{End}(E)$, compute $\mathrm{Tr}\,\alpha := \alpha + \widehat{\alpha} \in \mathbb{Z}$.

Why? Ordinary case

Point counting! Also, $\mathrm{tr}\,\pi_E$ reveals the structure of $\mathbb{Z}[\pi_E]$ as an algebra.

Why? Supersingular case

If E is supersingular: computing traces lets us determine a multiplication table for basis elements of $\mathrm{End}(E)$ (or a suborder) (e.g. we can efficiently decide whether $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ generate $\mathrm{End}(E)$ as a $\mathbb{Z}$-lattice by checking whether $\det(\mathrm{tr}(\alpha_i\widehat{\alpha}_j)_{i,j}) = p^2$)

Schoof's algorithm

If we know

$$t_\ell \coloneqq \operatorname{tr} \alpha \pmod{\ell}$$

for primes ℓ such that $\prod_\ell \ell > 4\sqrt{\deg \alpha}$ then we can recover $\operatorname{tr} \alpha$ with the CRT.

Schoof's algorithm

If we know

$$t_\ell := \operatorname{tr} \alpha \pmod{\ell}$$

for primes ℓ such that $\prod_\ell \ell > 4\sqrt{\deg \alpha}$ then we can recover $\operatorname{tr} \alpha$ with the CRT.

Algorithm 2: Schoof's algorithm

Input: Ordinary $E/\mathbb{F}_q$
Output: $\operatorname{tr}(\pi_E)$
Set $\ell = 2$ and $M = 1$;
while $M \leq 4\sqrt{q}$ **do**
    Compute $t_\ell = \operatorname{tr} \pi_E \bmod \ell$;
    Update $M = M \cdot \ell$;
    Update ℓ with the next prime after ℓ;
Solve $t \equiv t_\ell \pmod{\ell}$ for $t \in [-2\sqrt{q}, 2\sqrt{q}]$ with CRT;
return t

Computing $t_\ell = \operatorname{tr}\alpha \bmod \ell$

Suppose $(\ell, q) = 1$. An endomorphism $\alpha \in \mathrm{End}(E)$ acts on $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix" $\alpha\big|_{E[\ell]} \in \mathrm{End}(E[\ell]) \cong M_2(\mathbb{Z}/\ell\mathbb{Z})$

Computing $t_\ell = \operatorname{tr}\alpha \bmod \ell$

Suppose $(\ell, q) = 1$. An endomorphism $\alpha \in \operatorname{End}(E)$ acts on $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix" $\alpha\big|_{E[\ell]} \in \operatorname{End}(E[\ell]) \cong M_2(\mathbb{Z}/\ell\mathbb{Z})$

Schoof's method for computing t_ℓ

Compute t_ℓ by computing the characteristic polynomial of $\alpha\big|_{E[\ell]}$.

We have

$$\operatorname{tr}\alpha \equiv \operatorname{Tr}\left(\alpha\big|_{E[\ell]}\right) \pmod{\ell}.$$

Computing $t_\ell = \operatorname{tr}\alpha \bmod \ell$

Suppose $(\ell, q) = 1$. An endomorphism $\alpha \in \operatorname{End}(E)$ acts on $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ as a "matrix" $\alpha\big|_{E[\ell]} \in \operatorname{End}(E[\ell]) \cong M_2(\mathbb{Z}/\ell\mathbb{Z})$

Schoof's method for computing t_ℓ

Compute t_ℓ by computing the characteristic polynomial of $\alpha\big|_{E[\ell]}$. We have

$$\operatorname{tr}\alpha \equiv \operatorname{Tr}\left(\alpha\big|_{E[\ell]}\right) \pmod{\ell}.$$

Rather than working with points in $E[\ell]$: find $0 \le c < \ell$ such that

$$\alpha\big|_{E[\ell]}{}^2 + [\deg\alpha]\big|_{E[\ell]} = c(\alpha\big|_{E[\ell]})$$

by working with the *division polynomial* ψ_ℓ, the monic polynomial vanishing precisely $x(P)$ for $P \neq 0 \in E[\ell]$

Since $\deg\psi_\ell = (\ell^2 - 1)/2$, we can compute t_ℓ in $\tilde{O}((\log p)^4)$ bit operations.

Elkies' method for computing $t_\ell = \operatorname{tr} \pi_E \bmod \ell$

For 50% of primes ℓ (asymptotically), ℓ is an *Elkies' primes* for E (E admits a $\mathbb{F}_q$-rational ℓ-isogeny ϕ) so π_E fixes $\ker \phi \subset E[\ell]$, and

$$\pi_E\big|_{\ker \phi} \in \mathsf{End}(\ker \phi) \cong \mathbb{Z}/\ell\mathbb{Z}$$

Elkies' method for computing $t_\ell = \operatorname{tr} \pi_E \bmod \ell$

For 50% of primes ℓ (asymptotically), ℓ is an *Elkies' primes* for E (E admits a $\mathbb{F}_q$-rational ℓ-isogeny ϕ) so π_E fixes $\ker \phi \subset E[\ell]$, and

$$\pi_E\big|_{\ker \phi} \in \operatorname{End}(\ker \phi) \cong \mathbb{Z}/\ell\mathbb{Z}$$

By working modulo the *kernel polynomial* $h(x)$ of ϕ, find $0 \le c < \ell$ such that

$$\alpha^2\big|_{\ker \phi} + [\deg \alpha]\big|_{\ker \phi} = c(\alpha\big|_{\ker \phi})$$

Then $t_\ell = c$. This gives a speedup of a factor of $\ell = O(\log p)$ in computing t_ℓ, because

$$\deg \psi_\ell = (\ell^2 - 1)/2, \quad \deg h(x) = \ell + 1.$$

Assuming heuristics including (but not limited to!) GRH, the SEA algorithm computes $\operatorname{tr} \pi_E$ in $O((\log p)^4)$ bit operations.

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_q$ is supersingular. Then $j(E) \in \mathbb{F}_{p^2}$.

- Assume E itself is defined over $\mathbb{F}_{p^2}$, and $j(E) \neq 0, 1728$.
- In this case, $\pi_E = [\pm p]$.

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_q$ is supersingular. Then $j(E) \in \mathbb{F}_{p^2}$.

- Assume E itself is defined over $\mathbb{F}_{p^2}$, and $j(E) \neq 0, 1728$.
- In this case, $\pi_E = [\pm p]$.

Then $E/\mathbb{F}_{p^2}$ has **all** of its ℓ-isogenies defined over $\mathbb{F}_{p^2}$.

- Every prime is an Elkies prime for supersingular E!
- But $\alpha \in \mathrm{End}(E)$ need not fix $\ker \phi$
- Instead: we compute $\mathrm{tr}\,\alpha \bmod \ell$ by finding c such that the characteristic equation

$$\alpha^2\big|_{\ker\phi} + [\deg \alpha]\big|_{\ker\phi} = c(\alpha\big|_{\ker\phi})$$

holds in $\mathrm{Hom}(\ker\phi, E[\ell])$

The SEA algorithm for supersingular endomorphisms

Suppose $E/\mathbb{F}_q$ is supersingular. Then $j(E) \in \mathbb{F}_{p^2}$.

- Assume E itself is defined over $\mathbb{F}_{p^2}$, and $j(E) \neq 0, 1728$.
- In this case, $\pi_E = [\pm p]$.

Then $E/\mathbb{F}_{p^2}$ has **all** of its ℓ-isogenies defined over $\mathbb{F}_{p^2}$.

- Every prime is an Elkies prime for supersingular E!
- But $\alpha \in \mathrm{End}(E)$ need not fix $\ker \phi$
- Instead: we compute $\mathrm{tr}\,\alpha$ mod ℓ by finding c such that the characteristic equation

$$\alpha^2|_{\ker \phi} + [\deg \alpha]|_{\ker \phi} = c(\alpha|_{\ker \phi})$$

holds in $\mathrm{Hom}(\ker \phi, E[\ell])$

Theorem (M.-Panny-Sotáková-Wills)

There is an algorithm for computing the trace of an endomorphism α of a supersingular $E/\mathbb{F}_{p^2}$. Assuming GRH and that $\deg \alpha = d^e$ with $e = O(\log p)$ and $d = O(1)$, the algorithm terminates in expected $\tilde{O}((\log p)^4)$ bit operations.

Beyond the SEA algorithm: computing t_ℓ for $\ell | \#E(\mathbb{F}_{p^2})$

Since we assume $E/\mathbb{F}_{p^2}$ is supersingular and $j(E) \neq 0, 1728$, we know $\#E(\mathbb{F}_p^2) = (p \pm 1)^2$. To compute $t_\ell = \operatorname{tr} \alpha \bmod \ell$ for $\ell | \#E(\mathbb{F}_{p^2})$:

1. find $P \neq 0 \in E[\ell](\mathbb{F}_{p^2})$
2. Compute $(\alpha + \widehat{\alpha})(P)$
3. solve a small discrete log: t_ℓ is the solution to

$$cP = (\alpha + \widehat{\alpha})(P).$$

Beyond the SEA algorithm: computing t_p

Let ω_E be an invariant differential for E. Then $\alpha^*\omega_E = c_\alpha \omega_E$ for some $c_\alpha \in \mathbb{F}_{p^2}$, and the map

$$\begin{aligned} \mathrm{End}(E) &\to \mathbb{F}_{p^2} \\ \alpha &\mapsto c_\alpha \end{aligned}$$

is a homomorphism of rings, and (when E is supersingular)

$$\operatorname{tr} \alpha \equiv \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} c_\alpha \pmod{p}.$$

Beyond the SEA algorithm: computing t_p

Let ω_E be an invariant differential for E. Then $\alpha^*\omega_E = c_\alpha \omega_E$ for some $c_\alpha \in \mathbb{F}_{p^2}$, and the map

$$\begin{aligned} \mathrm{End}(E) &\to \mathbb{F}_{p^2} \\ \alpha &\mapsto c_\alpha \end{aligned}$$

is a homomorphism of rings, and (when E is supersingular)

$$\operatorname{tr} \alpha \equiv \operatorname{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} c_\alpha \pmod{p}.$$

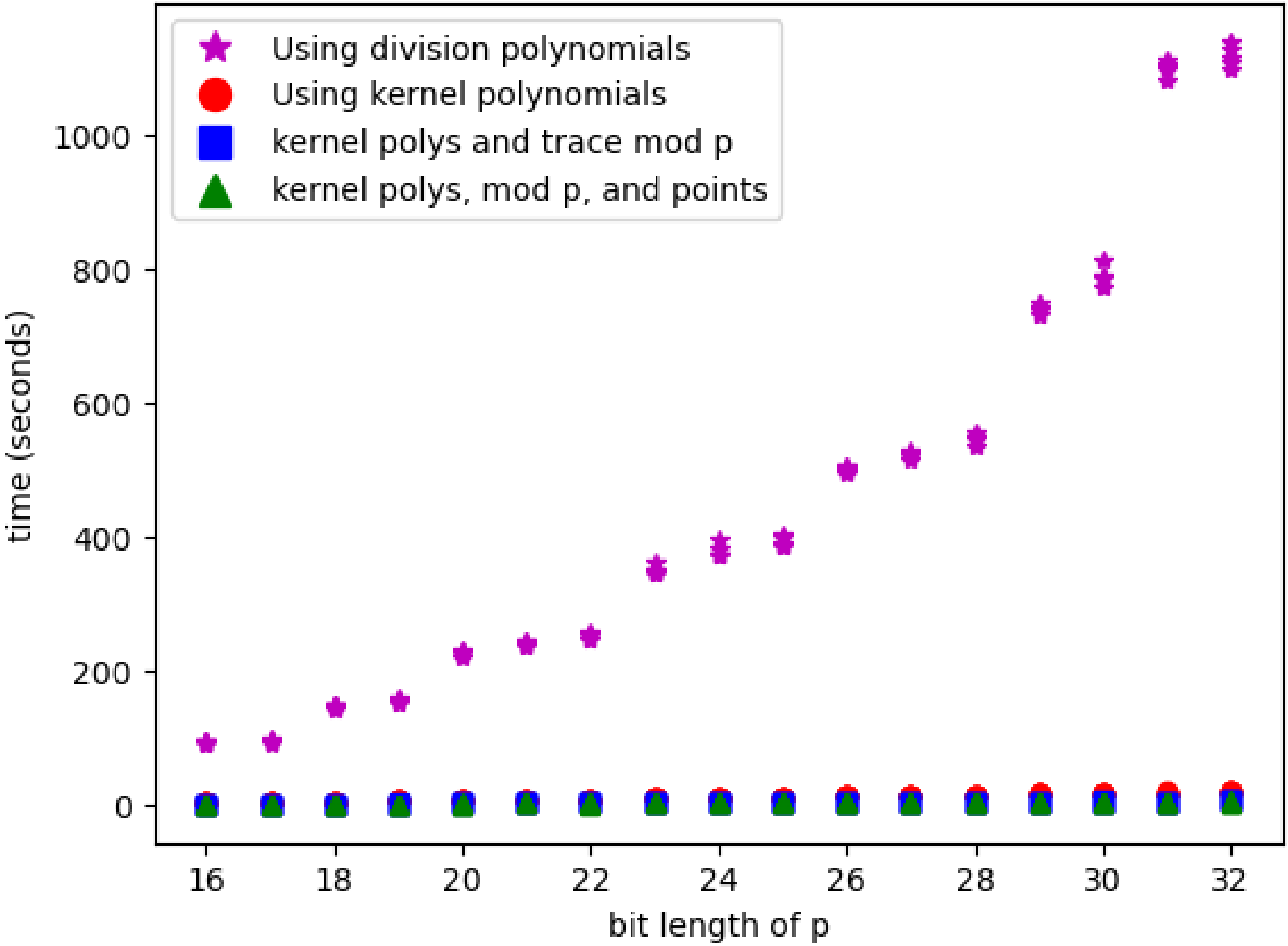
We can "read off" c_α from α: for separable α, we have

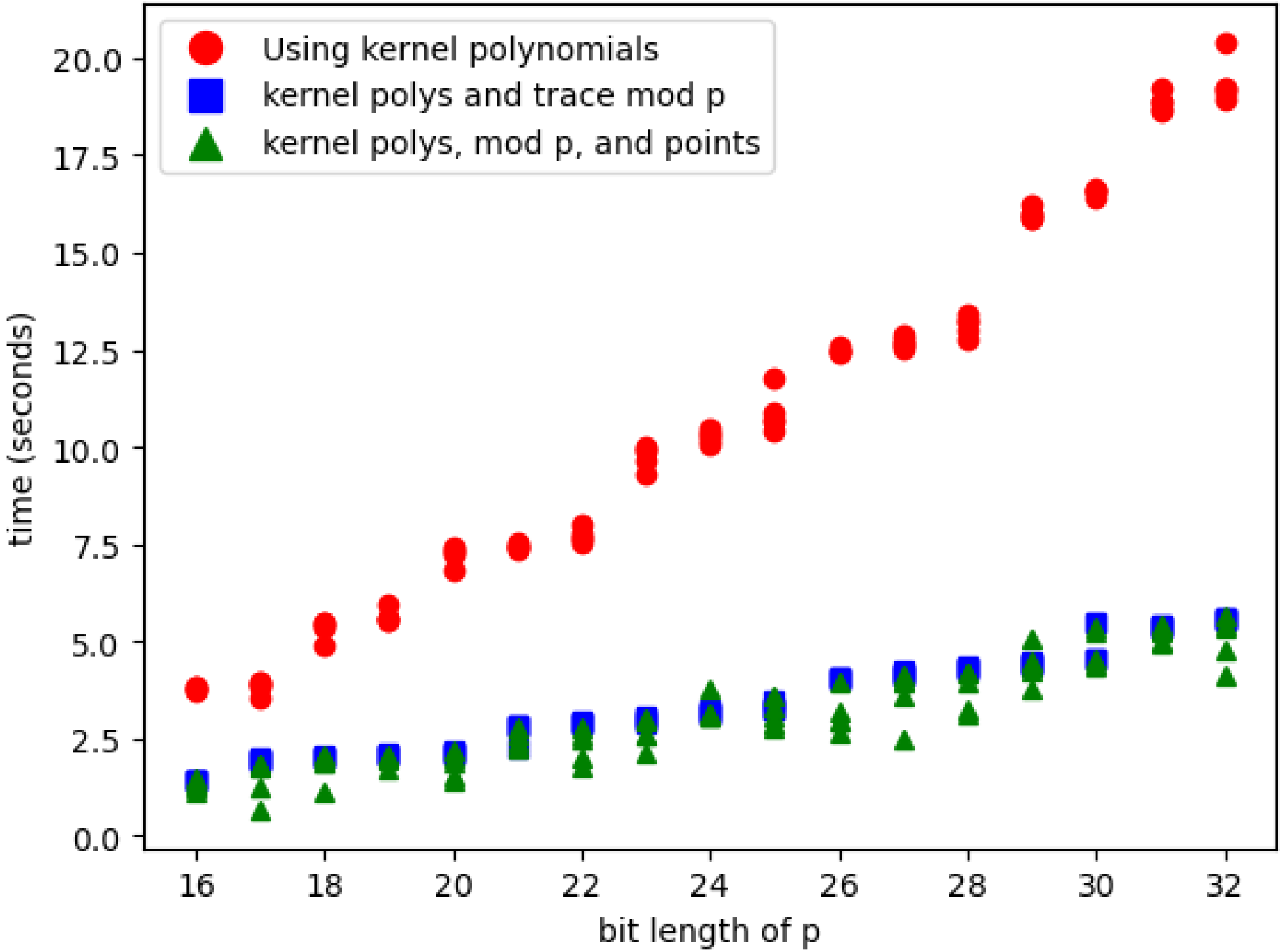
$$\alpha(x, y) = \left(\frac{N(x)}{D(x)}, c_\alpha \cdot \left(\frac{N(x)}{D(x)} \right)' y \right)$$

Timings

Implemented in sagemath. To demonstrate the asymptotic speedups offered:

1. For each $b \in [16, \ldots, 32]$, repeat 5 times:
   1. Compute random b-bit prime p, pseudorandom supersingular $E/\mathbb{F}_{p^2}$, and endomorphism $\alpha \in \mathrm{End}(E)$ of degree $\approx p^4$
   2. Compute $\mathrm{tr}\,\alpha$ using Schoof (i.e. get t_ℓ with division polynomials), SEA (i.e get t_ℓ with kernel polynomials), SEA + "mod p", SEA + "mod p" + "points"


Using division polynomials
Using kernel polynomials
kernel polys and trace mod p
kernel polys, mod p, and points
time (seconds)
0
200
400
600
800
1000
16
18
20
22
24
26
28
30
32
bit length of p


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