Climbing tall volcanoes

Steven Galbraith

University of Auckland, New Zealand

Come to NZ in December

- Joint meeting of NZ Math Society, Australian Math Society, American Math Society
- December 9-13, Auckland, New Zealand
- `ms-meet-2024.blogs.auckland.ac.nz`
- **Special sessions:**
  Arithmetic Geometry and Number Theory (Creutz, Kedlaya, Voight)
  Computational Number Theory and Applications (Galbraith, Harvey, Sutherland)
- Satellite workshop on Math of Crypto December 16, 17 and maybe 18.
  `sites.google.com/vt.edu/mathematical-cryptography-work`
- Registration open
- Book flights early!

Thanks

- ANTS reviewers and chairs
- Luca de Feo, Damien Robert, Valerie Gilchrist
- David Kohel at ANTS in 1998
  (Inspired my paper "Constructing isogenies between elliptic curves over finite fields", LMS Journal of Computation and Mathematics, 1999)
- Having a sabbatical in 2023 from being chair of department

Damien Robert's powerful idea

- The Kani theorem (used to break SIDH/SIKE) gives a way to represent isogenies of large prime degree using higher-dimensional isogenies of smooth degree.
- This idea gives a bunch of breakthroughs in cryptography and computational number theory:
- D. Robert, Evaluating isogenies in polylogarithmic time
- D. Robert, Some applications of higher dimensional isogenies to elliptic curves (overview of results)
- P. Dartois, A. Leroux, D. Robert, B. Wesolowski, SQISignHD: New Dimensions in Cryptography
- A. Page, D. Robert, Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time
- S. Kunzweiler, D. Robert, Computing modular polynomials by deformation

Results

Isogeny problem: Given ordinary $E_0, E_1/\mathbb{F}_q$ to compute $\mathbb{F}_q$-rational isogeny $\phi : E_0 \to E_1$ (if exists)

	1999	New
Worst case	$q^{1.5}$	$q^{0.4}$ (heuristic)
Usual ECC	$q^{0.25}$	$q^{0.25}$ (heuristic)
Pairing curves	$q^{1.5}$	$q^{0.25}$ (rigorous)

Descending isogeny: Given E_0 on crater compute descending N-isogeny (if exists)

1999	New
$N^3 = O(q^{1.5})$	$q^{0.5}$

All algorithms probabilistic; expected run times; exponential complexity is meaningful for ECC

Results

Isogeny problem: Given ordinary $E_0, E_1/\mathbb{F}_q$ to compute $\mathbb{F}_q$-rational isogeny $\phi : E_0 \to E_1$ (if exists)

	1999	New
Worst case	~~$q^{1.5}$~~ q	$q^{0.4}$ (heuristic)
Usual ECC	$q^{0.25}$	$q^{0.25}$ (heuristic)
Pairing curves	~~$q^{1.5}$~~ q	$q^{0.25}$ (rigorous)

Descending isogeny: Given E_0 on crater compute descending N-isogeny (if exists)

1999	New
$N^2 = O(q)$	$q^{0.5}$

All algorithms probabilistic; expected run times; exponential complexity is meaningful for ECC

Computing isogenies

Given $E/\mathbb{F}_q$ and N, want to compute a random $\mathbb{F}_q$-rational N-isogeny.

- Using modular polynomials is at least N^3, in general.
- Method in $\tilde{O}(N^2 \log(q))$ operations in $\mathbb{F}_q$ when know $\#E(\mathbb{F}_q)$:
  - Generate random $P \in E[N] \subset E(\mathbb{F}_{q^k})$ where $k = O(N)$, using quasi-linear field operations in $\mathbb{F}_{q^k}$.
  - Arrange that $\langle P \rangle$ is Galois invariant, then apply Vélu.

  (Square-root-Vélu doesn't help.)
- **Main tool:** Given $E_0, E_1/\mathbb{F}_q$ and N can compute *a representation of* an N-isogeny $\phi : E_0 \to E_1$ over $\mathbb{F}_q$ (if exists) in heuristic $\tilde{O}(\sqrt{N})$ operations in $\mathbb{F}_q$.
  Ingredients: Kani theorem (SIDH attack), D. Robert ideas, pairings.

Volcanoes (a type of isogeny graph)

- Let $E/\mathbb{F}_q$ be ordinary with $\#E(\mathbb{F}_q) = q + 1 - t$.
- Let π be the q-power Frobenius.
- Then $\mathbb{Z}[\pi]$ has discriminant $t^2 - 4q$.
- Let $t^2 - 4q = f^2 D_0$, where D_0 is discriminant of $K = \mathbb{Q}(\sqrt{t^2 - 4q})$.
- Conductor of endomorphism ring is $[\mathcal{O}_K : \mathrm{End}(E)] \mid f$.
- Level of volcano is set of $\cong$-classes of $E/\mathbb{F}_q$ with same $[\mathcal{O}_K : \mathrm{End}(E)]$.
- Crater is curves with $\mathrm{End}(E) = \mathcal{O}_K$.
- Floor is curves with $\mathrm{End}(E)$ of discriminant $t^2 - 4q$.
- I am putting as many primes into my volcano to make sure it is connected and small diameter.

Obstruction (explained in Kohel's thesis)

- Let $E_0, E_1/\mathbb{F}_q$ be ordinary elliptic curves and $N = [\mathrm{End}(E_0) : \mathrm{End}(E_1)]$.
- Then any $\mathbb{F}_q$-rational isogeny $\phi : E_0 \to E_1$ has degree divisible by N. (This is not true in the supersingular case, as exploited in SCALLOP for example.)
- Note that computing $\mathrm{End}(E)$ is efficient: Kohel (1996) gives $O(q^{1/3+o(1)})$; Bisson-Sutherland (2011) give subexponential; Robert (2022) gives polynomial-time method if $t^2 - 4q$ factored.

1999 result

- Typical case for ECC: flat volcano: $\tilde{O}(q^{1/4})$ (expected-time) algorithm. (Also when E_0 and E_1 are in the same level of the volcano.)
- Pairing crypto: $t^2 - 4q = -3f^2$ where $f \approx \sqrt{q}$ is divisible by a large prime N. Often have $N > q^{1/4}$.
  Pasta: $f = 3 \cdot 210890879 \cdot 3105272848117293044702858403 41$
  Geppetto: $f = 99609175647210028388479 3 \cdot$
  $3372803483588779922437226938165638185070812792197 9643$
- Old method needed $N^2 > q^{1/2}$ operations at least.
- New method: Since know E on crater ($D = -3$), can compute isogenies between E and given curves E_0, E_1 in $\tilde{O}(N^{1/2}) = \tilde{O}(q^{1/4})$ operations in $\mathbb{F}_q$. (In this case method is not heuristic.)

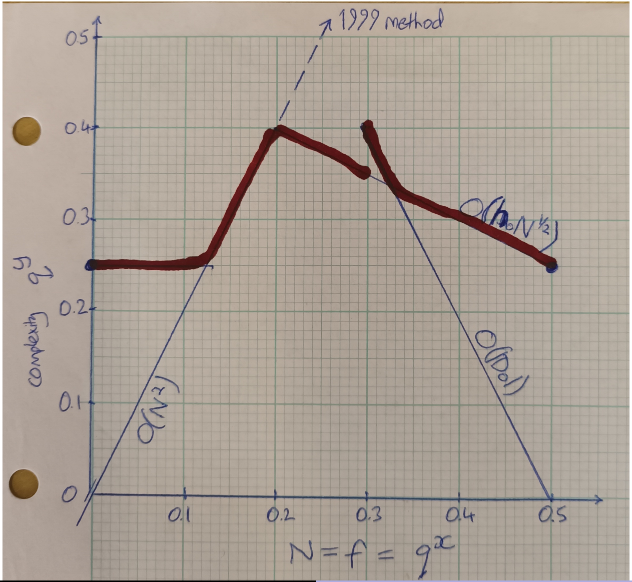
Main Result

Theorem: Given ordinary $E_0, E_1/\mathbb{F}_q$ with $\#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$, there is a heuristic probabilistic algorithm to compute an $\mathbb{F}_q$-rational isogeny $\phi : E_0 \to E_1$ that requires an expected $\tilde{O}(q^{2/5})$ field operations.

Proof of main result

- Let $E_0, E_1/\mathbb{F}_q$ be ordinary with $\#E_0(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$.
- Let $t^2 - 4q = f^2 D_0$ with factorisation of f known.
- Let f_0, f_1 be the conductors of E_0 and E_1.
- If $\mathrm{lcm}(f_0, f_1)$ is $q^{1/5}$-smooth then use 1999 methods (but **descend** to floor rather than ascend to crater): cost $\tilde{O}(q^{2/5}) + \tilde{O}(q^{1/4})$.
- If $|D_0| < q^{2/5}$ then use CM method to enumerate curves on crater and apply new $\sqrt{N}$ isogeny tool.
  Cost is $\tilde{O}(|D_0|) + \tilde{O}(h_0 N^{1/2})$, which one can show is $\tilde{O}(q^{2/5})$.
- If $|D_0| \geq q^{2/5}$ and one of the f_i is $q^{1/5}$-smooth then again enumerate curves on crater. Cost is $\tilde{O}(q^{2/5})$.
- If $|D_0| \geq q^{2/5}$ and both f_1 and f_2 have prime factor bigger than $q^{1/5}$ then descend to floor and do meet-in-middle algorithm.

Main result


1999 method
0.5
0.4
0.3
0.2
0.1
0
complexity q^y
$O(h_0 N^{1/2})$
$O(N^2)$
$O(|D_0|)$
0.1
0.2
0.3
0.4
0.5
$N = f = q^x$

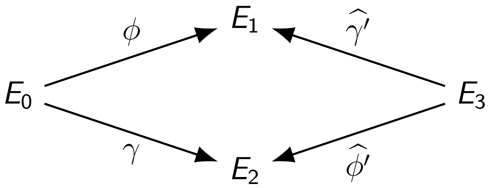
Lesson learned

The strategy from [Gal99] was to always ascend to the crater, but this is not optimal for all cases. In fact, in many cases descending is a better idea. Indeed, if we are not given a curve on the crater, and if the class number h_0 is large enough, then it is not feasible to compute a curve on the crater.

Second main result: Descending isogeny

- Given E_0 on crater want to compute descending $\mathbb{F}_q$-rational N-isogeny (if exists).
- Main case of concern is $q^{1/4} < N < 2q^{1/2}$.
- Previous method $O(N^2) = O(q)$.
- NEW:
- Choose random E and compute $\#E(\mathbb{F}_q)$ until get curve with $\#E_0(\mathbb{F}_q)$ points.
- Then apply new isogeny method to compute isogeny in $N^{1/2}$ time.

Kani construction



where $\gamma' \circ \phi = \phi' \circ \gamma$
defines an (M, M)-isogeny

$$F : E_0 \times E_3 \to E_1 \times E_2$$

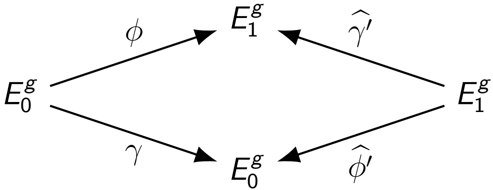
of polarized abelian varieties for $M = \deg(\phi) + \deg(\gamma)$, by

$$F(X, Y) = (\phi(X) - \widehat{\gamma'}(Y), \gamma(X) + \widehat{\phi'}(Y))$$

with explicit description of $\ker(F)$ in terms of ϕ, γ on $E_0[M]$.

Kani construction

Let $N = \deg(\phi)$. Let $m \in \mathbb{N}$ such that $M = N + m$ is power-smooth.
Let m be a sum of g squares, and $\gamma : E_0^g \to E_0^g$ the corresponding m-isogeny.
Extend ϕ to $E_0^g \to E_1^g$ as $\phi(X_1, \ldots, X_g) = (\phi(X_1), \ldots, \phi(X_g))$.



Defines an M-isogeny

$$F : E_0^g \times E_1^g \to E_1^g \times E_0^g.$$

Main tool

Theorem: Let E_0 and E_1 be elliptic curves over $\mathbb{F}_q$ that are connected by an isogeny $\phi : E_0 \to E_1$ over $\mathbb{F}_q$ of degree N.
Let $N > 1000$ be such that N is not divisible by any prime smaller than $4 \log(N) \log\log(N)$.
Then there is a (heuristic) algorithm to compute a representation of ϕ that can be evaluated on points in time polynomial in $\log(N)$ and the size of the representation of the points.
The expected complexity of the algorithm to compute the representation is $\tilde{O}(N^{1/2})$ operations in $\mathbb{F}_q$.

Proof sketch

- Let A be a product of Elkies primes ℓ, i.e., primes $\ell = O(\log(N))$ with $(\frac{t^2-4q}{\ell}) = +1)$ and $A^2 < N$.
- Let $M = 3^n A^2 > N$, so that $M = N + m = 3^n A^2$ is power-smooth and m a sum of g squares.
- Meet-in-middle the Kani isogeny

$$E_0^g \times E_1^g \xrightarrow{F_1} B \xleftarrow{\tilde{F}_2} E_1^g \times E_0^g .$$

- Need to guess ϕ on $E_0[3^{n/2}A]$.
  Choose Frobenius eigen-basis and use Weil pairing to reduce to $O(\sqrt{N})$ guesses. (See Castryck, Houben, Merz, Mula, van Buuren, Vercauteren.)
- Also guess ϕ on $E_0[4]$ to apply method of Dartois, Leroux, Robert, Wesolowski to check meet-in-middle.

Complexity

- Need to repeat $O(\sqrt{N})$ times until have guessed ϕ on $E_0[4 \cdot 3^{n/2} \cdot A]$.
- For each guess, we compute a $3^{n/2}A$ isogeny as a sequence of $\ell = O(\log(N))$ isogenies of $2g$-dimensional abelian varieties.
  The kernels are defined over $\mathbb{F}_{q^k}$ where $k = O(\ell) = O(\log(N))$.
  Hence the isogeny computation is polynomial in $\log(N)$.
- The algorithm is deterministic apart from the initial computation of sets of generators for $E_0[\ell]$.
- The complexity analysis is heuristic due to needing $O(\log(N))$ Elkies primes, but when $D_0 = O(1)$ then the complexity is rigorous due to results on primes in arithmetic progressions.

Final remarks

- For the case of pairing curves, when $|D_0| = O(1)$, the method is rigorous.
- **Open problem 1:** Do descending isogenies faster.
  Can we improve the "guessing E with $\#E_0(\mathbb{F}_q)$ points" method? eg as in Section 3 of Sutherland Hilbert Class Poly paper in Math Comp 2011.
- **Open problem 2:** Deterministic meet-in-middle algorithms for action of class group.
  This would result in deterministic algorithm for isogeny problem in the small class number case.
  Would be possible if Page-Robert was deterministic, or when class group is generated by small prime ideals and can find nice basis of relation lattice.
- **Open problem 3:** (KKM) In pairing crypto, is ECDLP on floor easier than ECDLP on crater?

Thank You

I'm rather inclined to think, personally, that maybe it's quite important, the getting down. And the complete climb of a mountain is reaching the summit and getting safely to the bottom again.

– Edmund Hilary