Breaking SIDH in polynomial time

2023/04/25 — Eurocrypt, Lyon

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Isogeny evaluation and interpolation

- Evaluation: evaluate an isogeny on a point
- N-evaluation problem: given
  1. $\phi : E_1 \to E_2$ an N-isogeny ($N = \deg \phi = \# \operatorname{Ker} \phi$),
  2. a point $P \in E_1(\mathbb{F}_q)$,

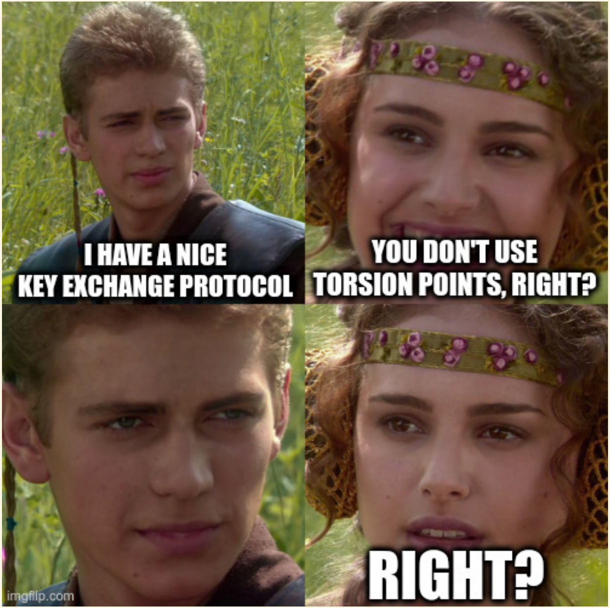
  evaluate $\phi(P)$

- Interpolation: reconstruct an isogeny from its image on a torsion basis
- (N, N')-interpolation problem: given
  1. $N = \deg \phi$,
  2. $(P_1, \phi(P_1)), (P_2, \phi(P_2))$ for (P_1, P_2) a basis of $E_1[N']$,
  3. $P \in E_1(\mathbb{F}_q)$

  evaluate $\phi(P)$

- SIDH: the key exchange uses the $N_A = 2^a$ and $N_B = 3^b$ evaluation problems
- Solving the interpolation problem (SSI-T) = breaking SIDH

Isogeny evaluation and interpolation



Evaluation vs Interpolation

Evaluation:

- [Vélu 1971, Kohel 1996]: for $\phi : E_1 \to E_2$ an N-isogeny,

$$x(\phi(P)) = \frac{g(x(P))}{h(x(P))},$$

$\deg g, \deg h < N, h(x) = \mathrm{Ker}\,\phi$

$\Rightarrow$ evaluate $\phi(P)$ in $O(N)$ operations in $\mathbb{F}_q$ (given its kernel)

- Linear time

Interpolation:

- Interpolate $\frac{g}{h}(x)$ from $(x(P_1), x(\phi(P_1))), (x(2P_1), x(\phi(2P_1))), \ldots$
- Quasi linear time

Fast evaluation:

- N smooth: decompose ϕ into a product of small isogenies
- Logarithmic time

Double and add

- Fast evaluation when N has a large prime factor?
- If $\phi = [\ell]$ ($N = \ell^2$): double and add in $O(\log \ell)$

- $\Phi : E^2 \to E^2, (P_1, P_2) \mapsto (P_1 + P_2, P_1 - P_2)$ is a 2-isogeny in dimension 2 [Riemann]
- $\Phi = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$
- Double: $\Phi(T, T) = (2T, 0)$
- Add: $\Phi(T, P) = (T + P, T - P)$

- Evaluate ℓP = composition of $O(\log \ell)$ evaluations of Φ, projections $E^2 \to E$ and embeddings $E \to E^2$
- Double and add on E = 2-isogenies in dimension 2

Kani's lemma [Kani 1997] ($g = 1$), [R. 2022] ($g>1$)

- A, B, C, D principally polarised abelian varieties
- $\alpha : A \to B$ a a-isogeny, $\beta : A \to C$ a b-isogeny
- $\alpha' : C \to D$ a a-isogeny, $\beta' : C \to D$ a b-isogeny with $\beta'\alpha = \alpha'\beta$:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \big\downarrow{\scriptstyle \beta} & & \big\downarrow{\scriptstyle \beta'} \\ C & \xrightarrow{\alpha'} & D \end{array}$$

- $\Phi = \begin{pmatrix} \alpha & \widetilde{\beta'} \\ -\beta & \widetilde{\alpha'} \end{pmatrix} : A \times D \to B \times C$
- Φ is an $a + b$-isogeny with respect to the product polarisations
- Ker $\Phi = \{\tilde{\alpha}(P), \beta'(P) \mid P \in B[a+b]\}$ (if a is prime to b)

Using Kani's lemma for the interpolation

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha'} \\ E_1' & \xrightarrow{\phi'} & E_2' \end{array}$$

- $\phi : E_1 \to E_2$ an N-isogeny
- Goal: replace ϕ by Φ an N'-isogeny
- Find $\alpha : E_1 \to E_1'$ an m-isogeny, with $N' = N + m$
- Kani's lemma: $\Phi : E_1 \times E_2' \to E_1' \times E_2$ is an N'-isogeny
- We know $\phi(E[N'])$ and we can evaluate α on $E[N'] \Rightarrow$ recover Ker Φ (or Ker $\widetilde{\Phi}$)
- Evaluate Φ, hence ϕ at any point: $\Phi(P, 0) = (\alpha(P), -\phi(P))$
- Evaluation is fast if N' is (power) smooth

Examples:

- m smooth [Castryck–Decru; Maino–Martindale]
- $m = \ell^2$: take $\alpha = [\ell]$
- $\mathrm{End}(E_1)$ has an efficient endomorphism α of norm m [Castryck–Decru; Wesolowski]

Using Kani's lemma for the interpolation

The general case: Zahrin's trick

- $\alpha = \begin{pmatrix} a_1 & a_2 \\ -a_2 & a_1 \end{pmatrix}$ endomorphism of norm $m = a_1^2 + a_2^2$ on E^2
- Gaussian integers $\mathbb{Z}[i]$
- $\alpha = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix}$ endomorphism of norm $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ on E^4
- Hamilton's quaternion algebra
- Evaluating α: $O(\log m)$ arithmetic operations
- Every integer is a sum of four squares

$$\begin{array}{ccc} E_1^4 & \xrightarrow{\phi} & E_2^4 \\ \downarrow \alpha & & \downarrow \alpha \\ E_1^4 & \xrightarrow{\phi} & E_2^4 \end{array}$$

- $\Phi : E_1^4 \times E_2^4 \to E_1^4 \times E_2^4$ is an N'-isogeny

Kani's lemma + Zahrin's trick = the embedding lemma [R. 2022]

- A N-isogeny $\phi : A \to B$ in dimension g can always be efficiently embedded into a N' isogeny $\Phi : A' \to B'$ in dimension $8g$ (and sometimes $4g, 2g$) for any $N' \geq N$

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \big\downarrow & & \big\uparrow \\ A' & \xrightarrow{\Phi} & B' \end{array}$$

- Considerable flexibility (at the cost of going up in dimension)

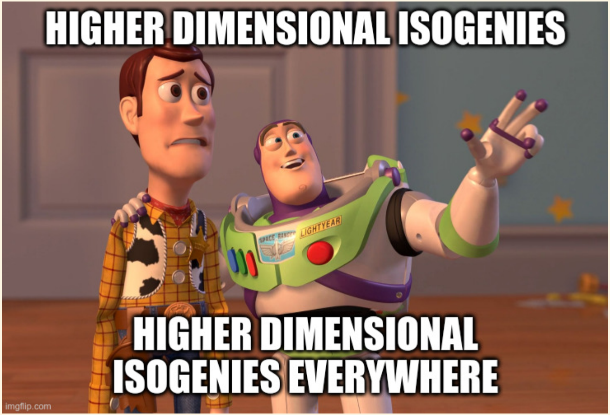
- Reduces the (N, N')-interpolation problem to the N'-evaluation problem (in higher dimension)
- Only needs $N'^2 \geq N$ (uses the dual isogeny)

$\Rightarrow$ Solves the interpolation problem when N' is (power) smooth

- Amazing fact: does not requires Ker ϕ, works even if N is prime

- Breaks SIDH: [Castryck–Decru], [Maino–Martindale] in dimension 2, [R.] in dimension 4 or 8
- Constructive applications: efficient representation of any isogeny, computing ordinary endomorphism rings, canonical lifts, point counting, modular and class polynomials, new cryptographic protocols in higher dimension …

Kani's lemma + Zahrin's trick = the embedding lemma [R. 2022]



Algorithms for N-isogenies in higher dimension

- [Cosset-R. (2014), Lubicz-R. (2012–2022)]: An N-isogeny in dimension g can be evaluated in linear time $O(N^g)$ arithmetic operations in the theta model given generators of its kernel
- Warning: exponential dependency 2^g or 4^g in the dimension g

- [Couveignes-Ezome (2015)]: Algorithm in $O(N^g)$ in the Jacobian model
- Not hard to extend to product of Jacobians
- Restricted to $g \leq 3$

How expensive is an isogeny in dimension g in the theta model?

- Naive estimate: ℓ^e-isogeny $= e$ ℓ-isogenies $= e \times O(\ell^g)$
  $= C \times 2^g$ (number of coordinates) $\times \ell^g$ (size of kernel) $\times (1+g)$ (g points to push)

SIKE	$g=1$	$g=2$	$g=4$	$g=8$
SIKEp434 (2^{216})	14476	80376	1546608	416370768
SIKEp503 (2^{250})	17060	94860	1826700	491877900
SIKEp610 (2^{305})	21350	118950	2292990	617612190
SIKEp751 (2^{372})	26576	148296	2861016	770779416
SIKEp964 (2^{486})	35904	200844	3879828	1045623348

Number of field operations (estimate)

g	Naive ratios	Estimated ratios
2	×6	×5.5
4	×160	×110
8	×75000	×29000

Conclusion


IT IS TIME TO GO.
Was I a good protocol?
NO.
I was told you
were among the best
imgflip.com
seebangnow

Conclusion