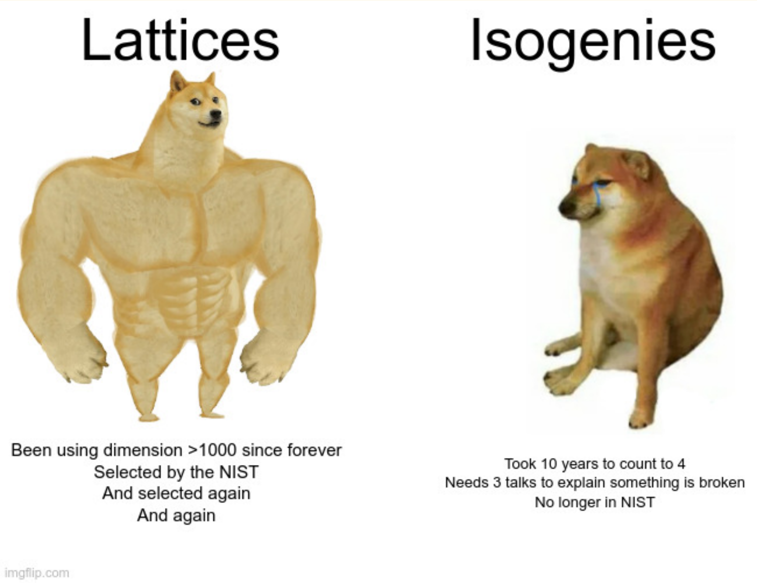
Finding a supersingular isogeny path with only one isogeny computation

2023/04/25 — Eurocrypt Rump Session, Lyon

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Context

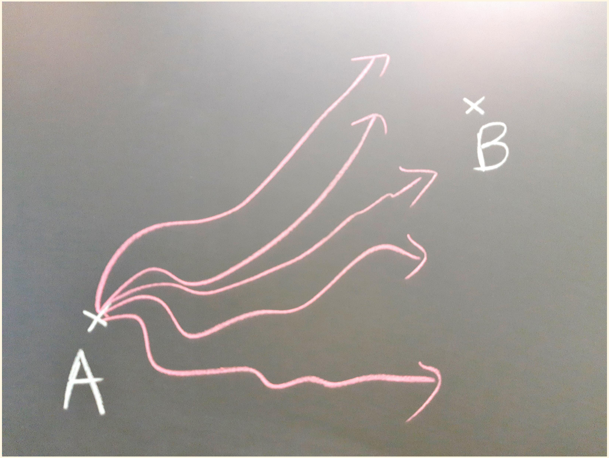

Lattices
Isogenies
Been using dimension >1000 since forever
Selected by the NIST
And selected again
And again
Took 10 years to count to 4
Needs 3 talks to explain something is broken
No longer in NIST
imgflip.com

Goal

- Luca[1] wants to compute a bicycle path between Zürich and Lyon
- He is only allowed to do one isogeny request!

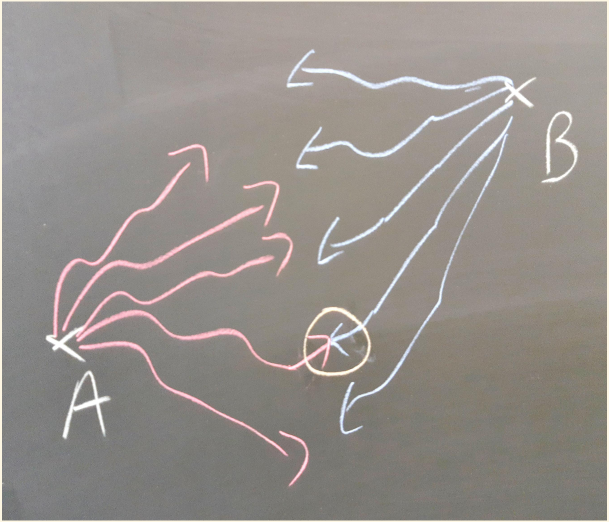
[1] any similarity to an actual person is purely coincidental…

Existing algorithms



Depth search

Existing algorithms



Meet in the middle

Existing algorithms

Special points

A solution

- $E, E'/\mathbb{F}_{p^2}$ two supersingular curves ($p \approx 256$ bits)
- Goal: find a 2^e-isogeny $\phi : E_1 \to E_2$

- $E_\lambda : y^2 = x(x-1)(x-\lambda)$ (Legendre)
- $A = \prod_{\lambda \in \mathbb{F}_{p^2} - \{0,1\}} E_\lambda$
- $K \subset A[2]$ generated by the 2-torsion points $(0,0)$ on each E_λ
- $\Phi : A \to B = A/K$ encodes the full supersingular 2-isogeny graph!

Complexity

- Computing a 2-isogeny in dimension $\approx 2^{512}$ may seem expensive
- Good news! Restricting to $A = \prod E_\lambda$ with E_λ supersingular we are only in dimension $\approx 2^{256}$
- The point $(0,0)$ on E_λ and on $E_{1/\lambda}$ encode the same isogeny

$\Rightarrow$ Gains a factor two!

To infinity and beyond

- Abelian scheme of unbounded dimension:

$$A = \coprod_{p} \prod_{\lambda \in \mathbb{F}_{p^2} - \{0,1\}} E_{\mathbb{F}_{p^2},\lambda}$$

- A single 2-isogeny encode all supersingular 2-isogeny graphs over all primes

Success?

Slogan: higher dimensional isogeny = the ability to put your bike in a train!