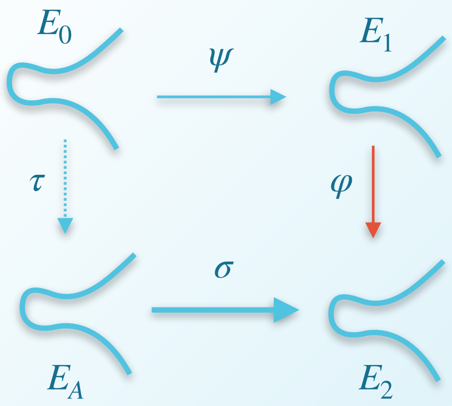
Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves

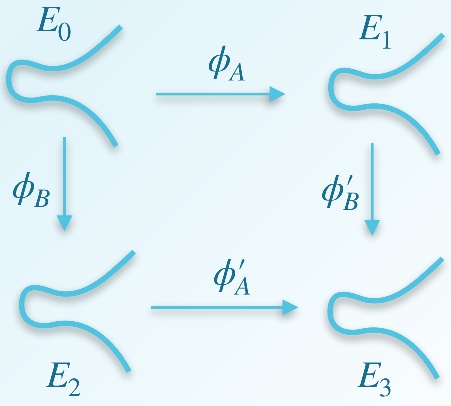
Benjamin Benčina, Péter Kutas, Simon-Philipp Merz, Christophe Petit,
Miha Stopar, and Charlotte Weitkämper

privacy + scaling explorations

Isogeny-based cryptography

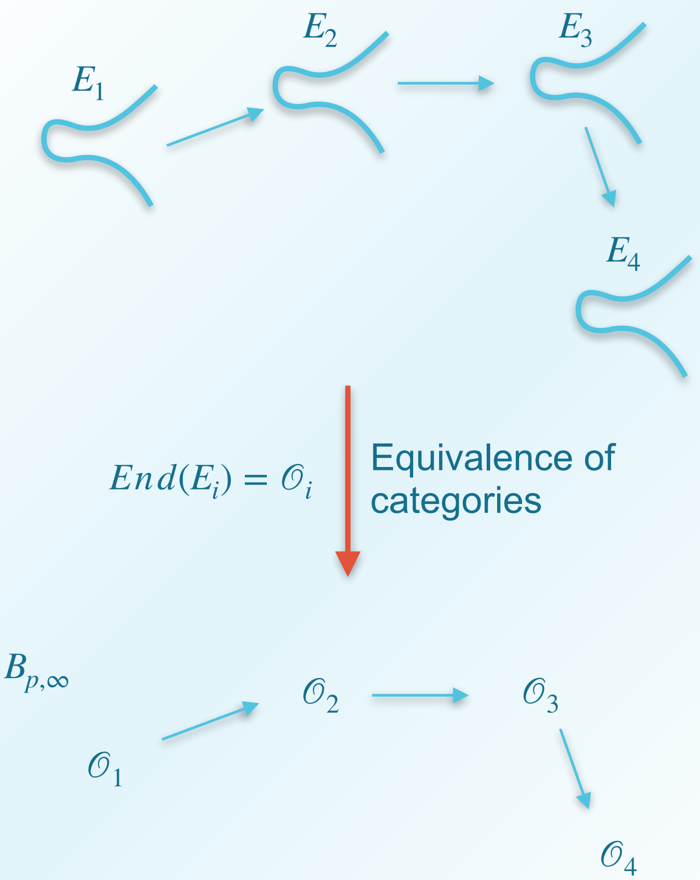
- A promising candidate for post-quantum cryptography.
- The *pure isogeny problem*—finding an explicit isogeny between two elliptic curves.
- Most isogeny-based protocols rely on the pure isogeny problem or on some variants of this problem.





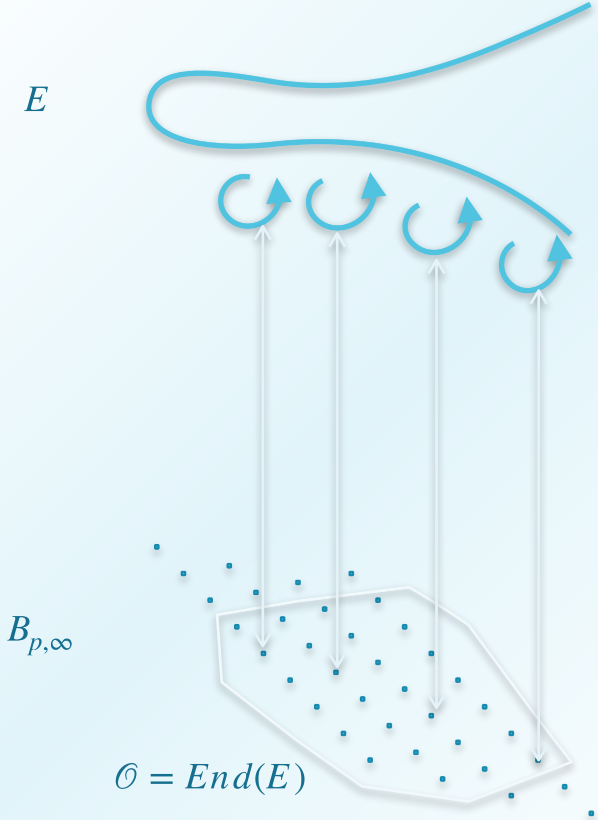
Deuring correspondence

There is a bijection between conjugacy classes of supersingular j-invariants and maximal orders (up to isomorphisms) of the quaternion algebra.



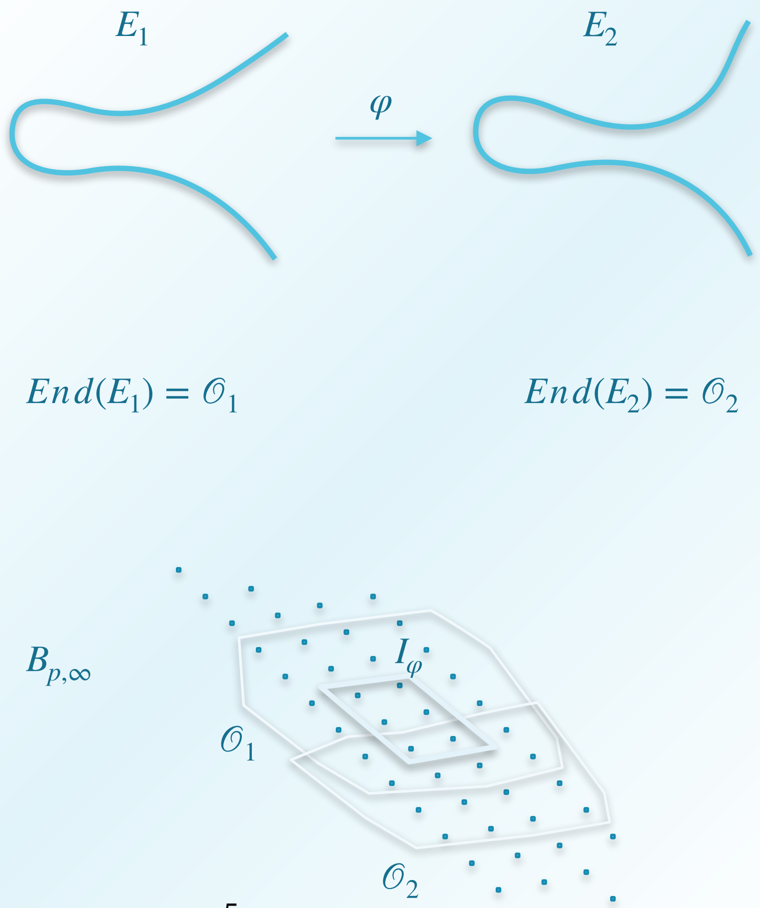
Deuring correspondence

Let E be a supersingular elliptic curve over finite field of characteristic p. $End(E)$ is a maximal order $\mathcal{O}$ in the quaternion algebra $B_{p,\infty}$.



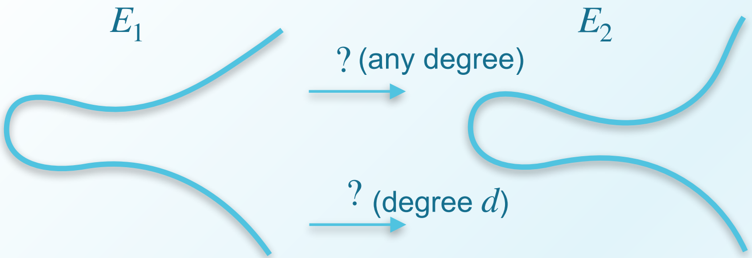
Deuring correspondence

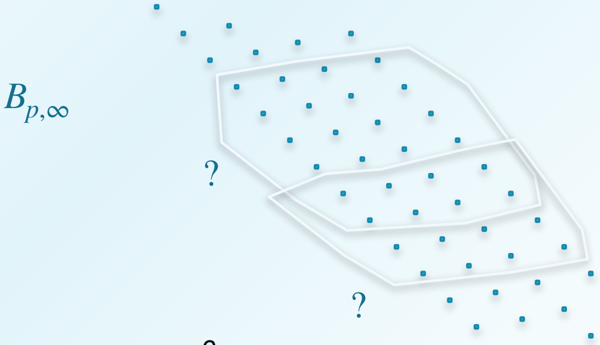
An equivalence of categories of isogenies between supersingular elliptic curves over $\bar{\mathbb{F}}_p$ and the left ideals of maximal orders of $B_{p,\infty}$.



Hard problems

- Computing the endomorphism ring of a supersingular elliptic curve.
- Computing any isogeny between two supersingular elliptic curves.
- Computing a degree d isogeny between two supersingular elliptic curves if it exists.





Implications of improved computation of degree-d isogeny

Security of some schemes

Exploring SIDH-based signature parameters by Basso, Chen, Fouotsa, Kutas, Laval, Marco, Saah is based on on the hardness of finding fixed-degree isogenies.

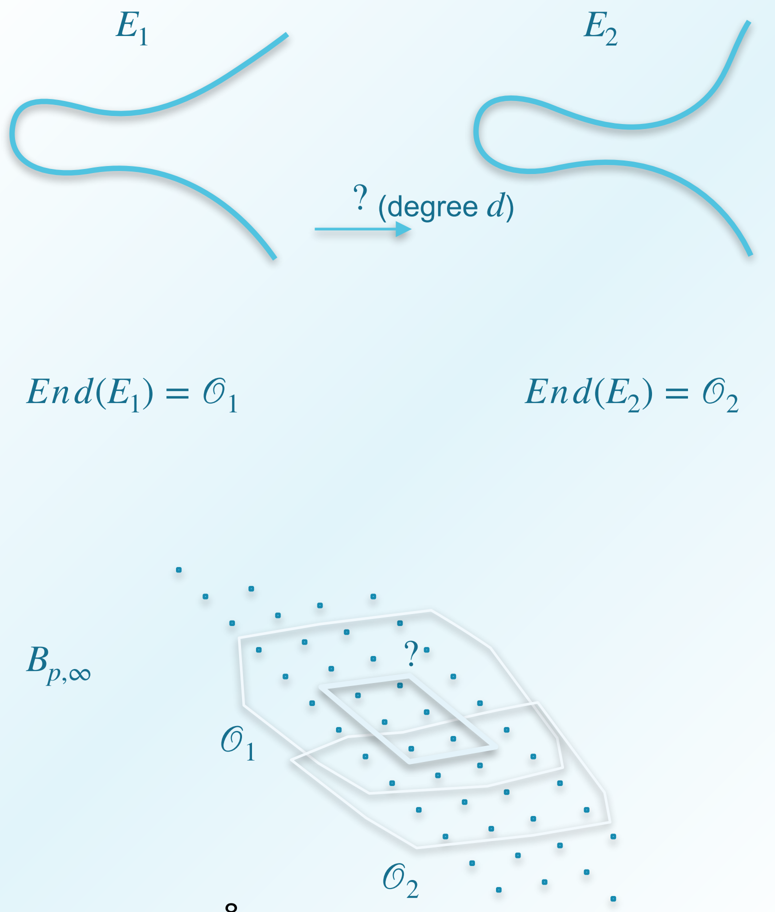
Performance

Speed-up of SQIsign: not being able to compute an isogeny of optimal length slows down the protocol significantly.

Fixed degree isogeny

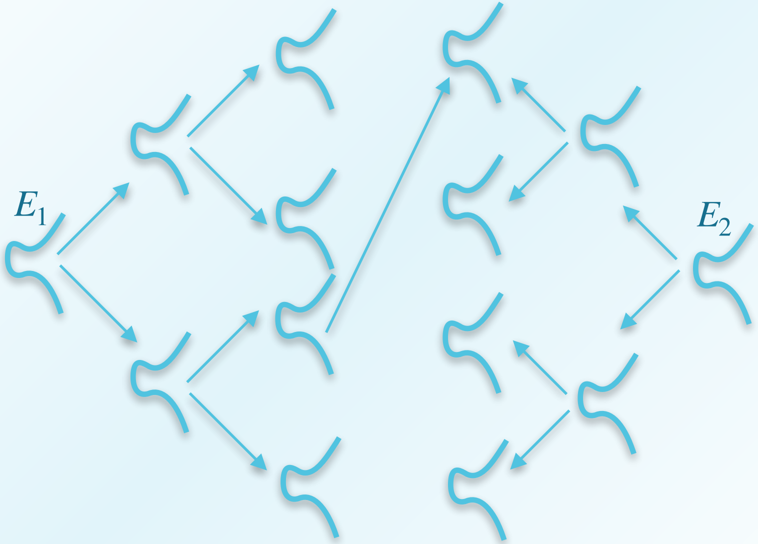
Let $\epsilon > 0$ such that $d \approx p^{\frac{1}{2}+\epsilon}$. Up to what value of ϵ can we compute an isogeny of degree d?

(there exist strategies to compute an isogeny of degree $< p^{\frac{1}{2}}$ and $> p^3$)



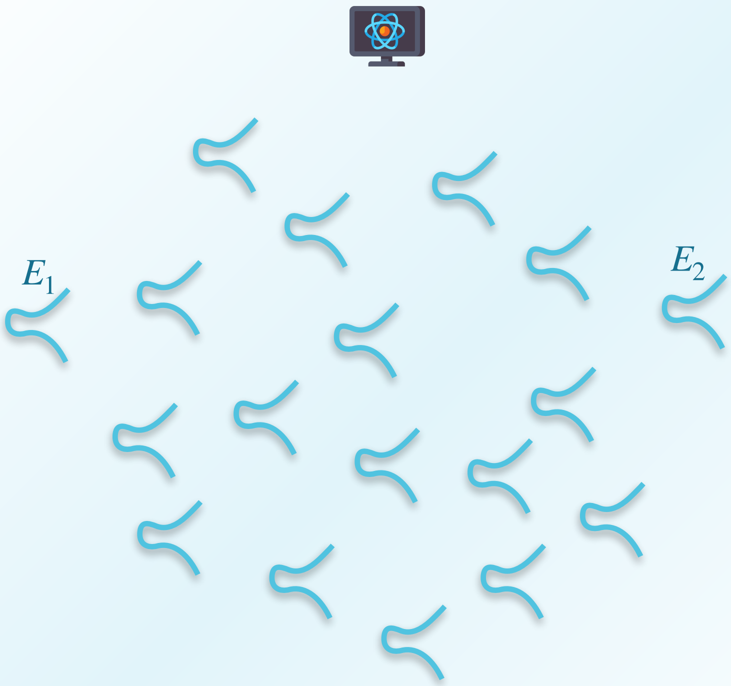
State-of-the-art for fixed degree isogeny

- Exhaustive search over all outgoing isogenies: cost $O(d)$.
- Meet-in-the-middle: cost $O^*(\sqrt{d})$ time and memory (smooth d).
- van Oorschot-Wiener collision search variants: cost depends heavily on available memory.



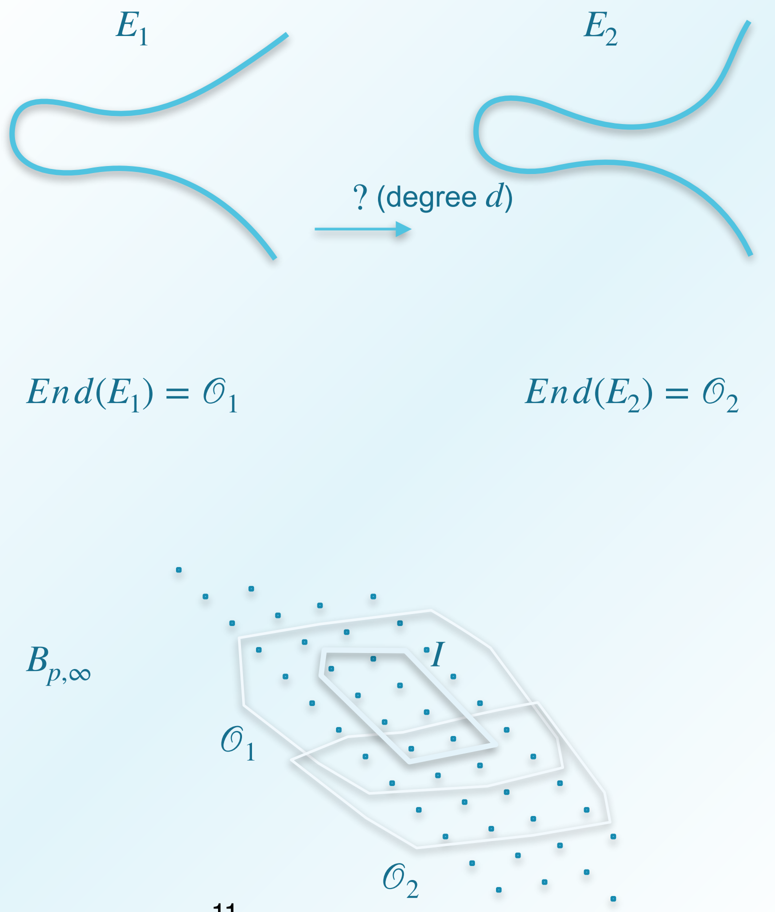
State of the art (quantum)

- Grover's algorithm improves exhaustive search to $O^*(\sqrt{d})$.
- (Tani's algorithm: $d^{\frac{1}{3}}$)



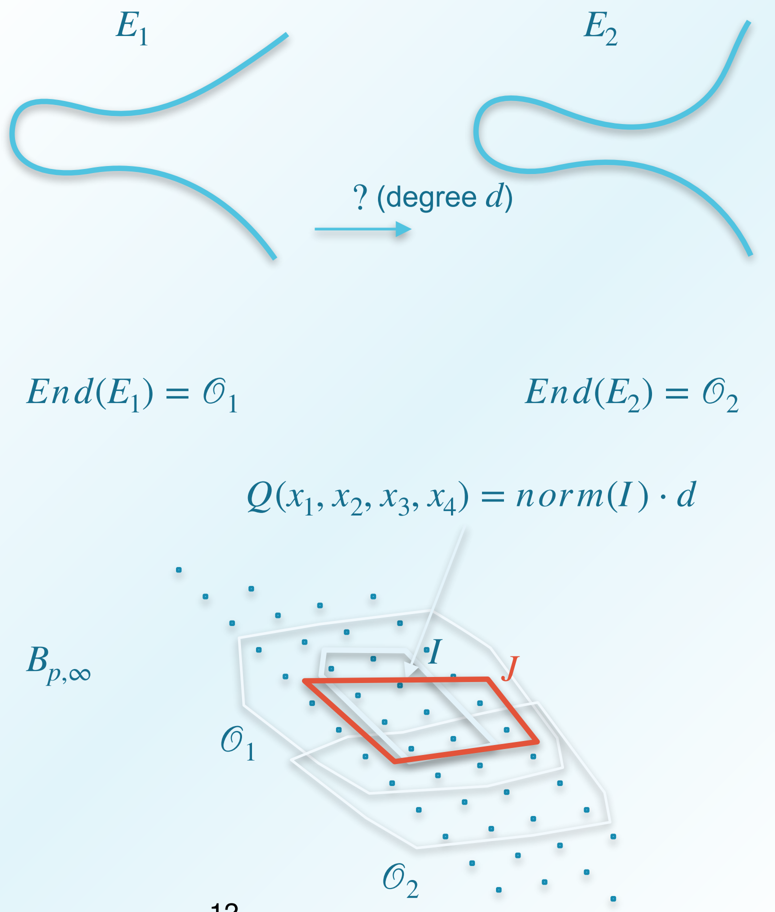
Our strategy

- Compute $End(E_1) = \mathcal{O}_1, End(E_2) = \mathcal{O}_2$ (Eisenträger et al.).
- Compute connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (Kirschmer-Voight).



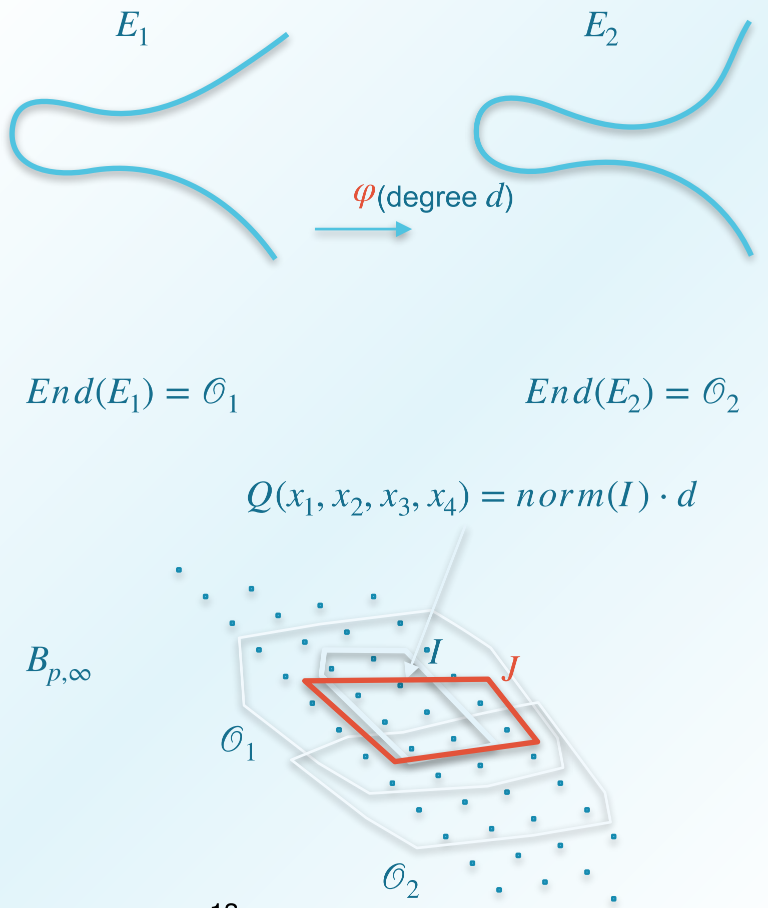
Our strategy

- Compute the norm form associated to I (reduced Gram matrix): $x^T \bar{I} I x = Q(x_1, x_2, x_3, x_4)$.
- Represent d via this norm form: $Q(x_1, x_2, x_3, x_4) = norm(I) \cdot d$.
- Compute an ideal J equivalent to I: $J = I \dfrac{\bar{x}}{norm(I)}$.



Our strategy

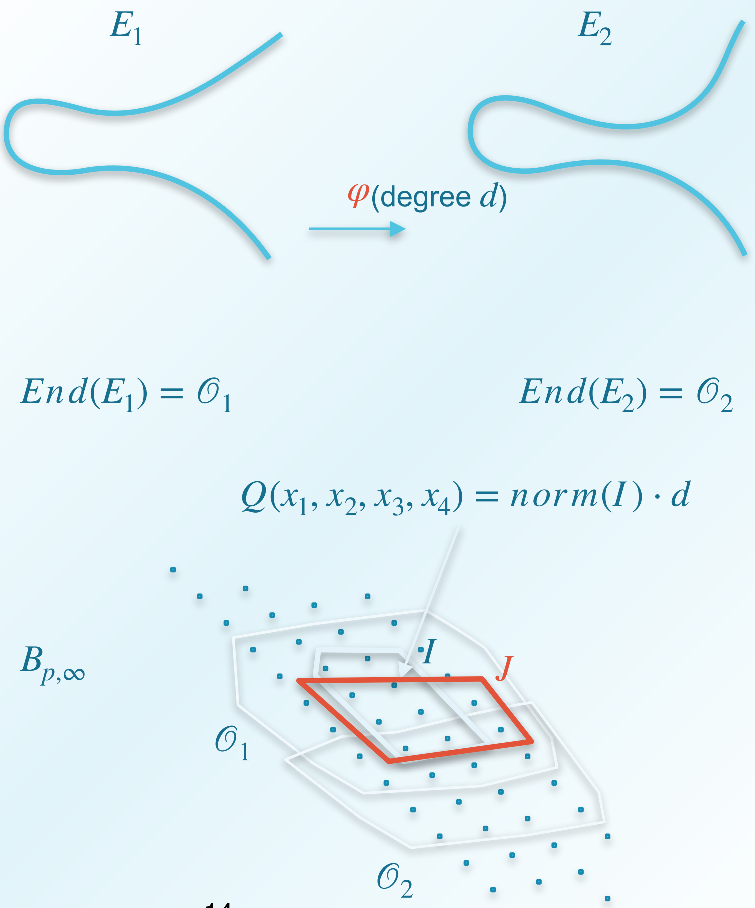
- We have an ideal J of norm d and can convert it to the isogeny of degree d.



Solving quadratic form: Cornacchia and Coppersmith

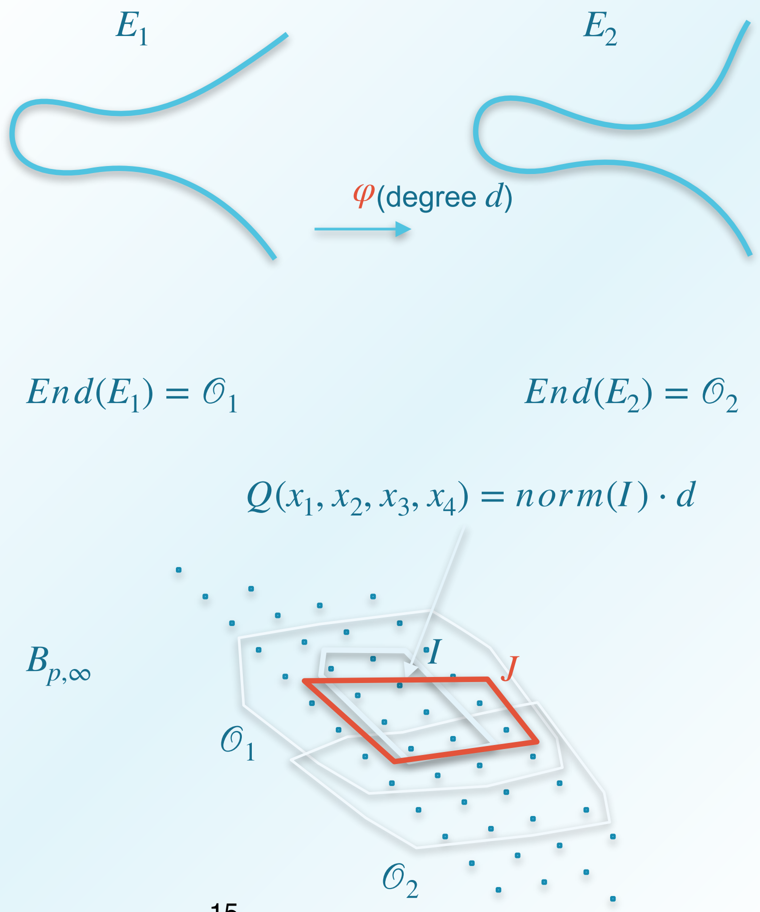
- Cornacchia algorithm is an algorithm for solving the Diophantine equation $x_1^2 + \Delta x_2^2 = m$ where $1 \leq \Delta < m$ and Δ and m are coprime.

- Coppersmith algorithm is a method to find small integer zeroes of polynomials modulo a given integer.



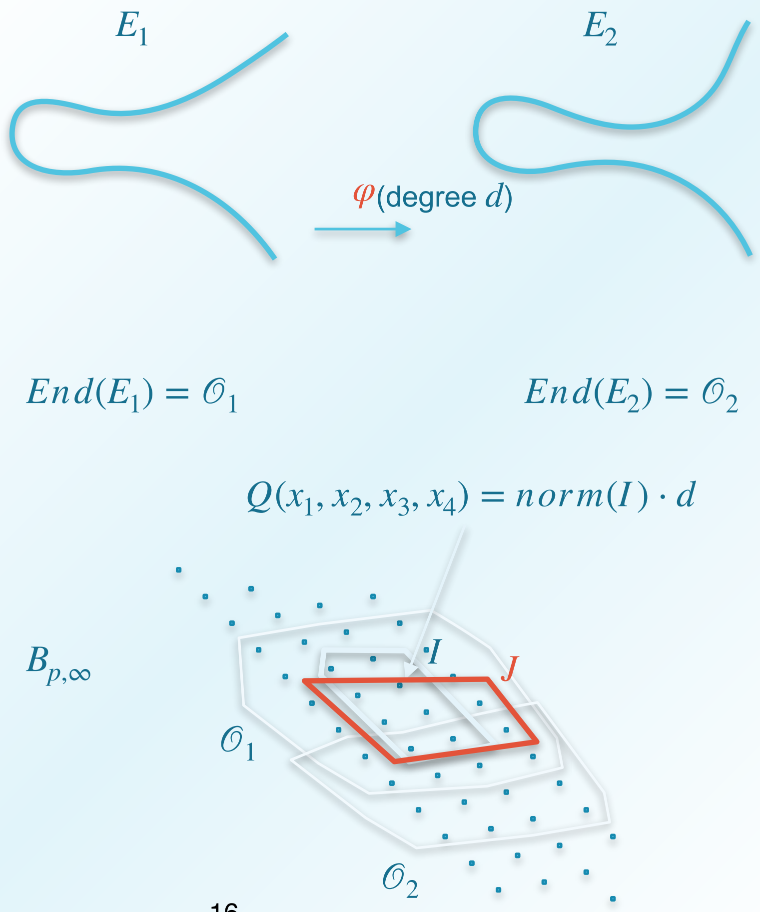
Cornacchia algorithm

- We guess x_3 and x_4.
- Change of variables to get the form $x_1^2 + \Delta x_2^2 = m$.
- If m does not have too many prime factors, we get the solution. Otherwise, we make a new guess for x_3 and x_4.



Coppersmith algorithm

- Used in attacks on RSA when parts of the secret key are known.
- Multiple variants: Coppersmith, Coron, Bauer-Joux.
- We guess x_3 and x_4 (or only x_4).



Bivariate Coron

- Guess x_3 and x_4.
- Get two algebraically independent polynomials.
- Obtain the root by computing resultants.

$$q(x,y) = 1 + a_{10}x + a_{01}y + a_{11}xy$$

$$W = ||q(xX, yY)||_\infty$$

$$W \le n < 2W$$

$$q_{ij}(x,y) = x^i y^j X^{k-1} Y^{k-j} q(x,y)$$

1	x	y	xy	x^2	x^2y	y^2	xy^2	x^2y^2
XY	$a_{10}X^2Y$	$a_{01}XY^2$	$a_{11}X^2Y^2$					
	XY		$a_{01}XY^2$	$a_{10}X^2Y$	$a_{11}X^2Y^2$			
		XY	$a_{10}X^2Y$			$a_{01}XY^2$	$a_{11}X^2Y^2$	
			XY		$a_{10}X^2Y$		$a_{01}XY^2$	$a_{11}X^2Y^2$
				X^2n				
					X^2Yn			
						Y^2n		
							XY^2n	
								X^2Y^2n

Bauer-Joux

- Guess x_4.
- Get three algebraically independent polynomials.
- Obtain the root by computing resultants.

$$p(x, y, z) = 1 + axy + byz$$

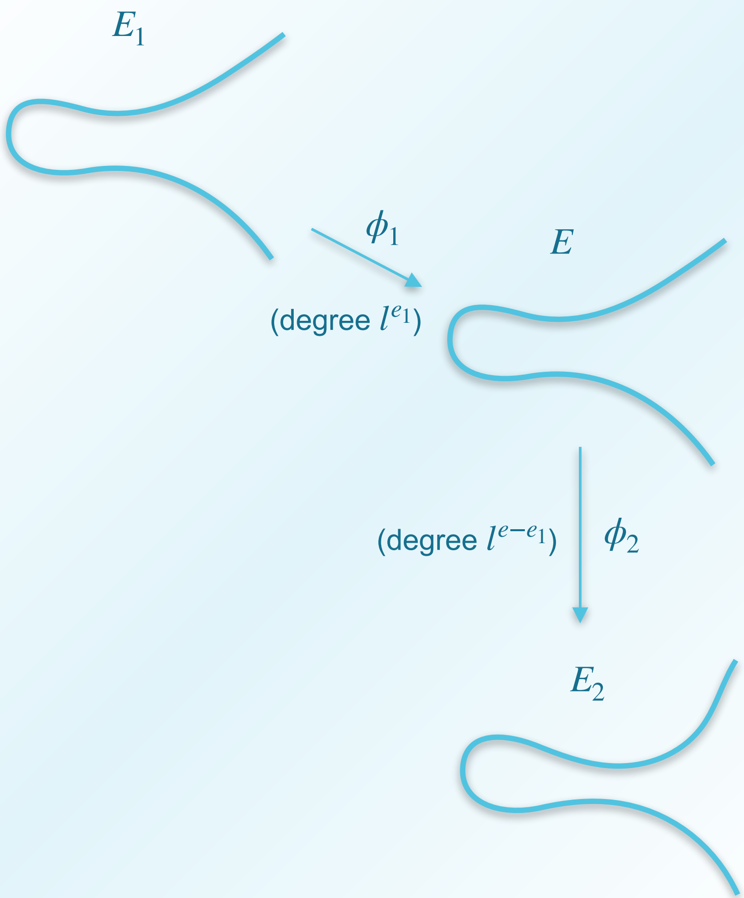
$$\begin{pmatrix}
1 & & & & & & 1 & 0 \\
 & X^{-1}Y^{-1} & & & & & a & 0 \\
 & & Y^{-1}Z^{-1} & & & & b & 0 \\
 & & & X^{-1} & & & 0 & 1 \\
 & & & & X^{-2}Y^{-1} & & 0 & a \\
 & & & & & X^{-1}Y^{-1}Z^{-1} & 0 & b
\end{pmatrix}$$

$$\begin{pmatrix}
 & & 1 & 0 \\
 & & 0 & 1 \\
 & & 0 & 0 \\
 & & 0 & 0 \\
 & & 0 & 0 \\
 & & 0 & 0
\end{pmatrix}$$

$$\begin{pmatrix}
 & & & 1 & 0 \\
 & & & 0 & 1 \\
 & & b_1 & 0 & 0 \\
 & & b_2 & 0 & 0 \\
 & & b_3 & 0 & 0 \\
 & & b_4 & 0 & 0
\end{pmatrix}$$

Hybrid approach

- $d = l^e \approx p^{\frac{1}{2}+\epsilon}$
- Guess l^{e_1}-isogeny $\phi_1 : E_1 \to E$.
- Use ϕ_1 to compute $End(E)$ from $End(E_1)$.
- Solve the fixed-degree isogeny problem with E and E_2 for degree l^{e-e_1} to obtain ϕ_2, or guess again.
- Compose ϕ_2 with ϕ_1.



Results

- The best approach turned out to be the hybrid approach, it has a better time complexity than meet-in-the-middle algorithms in the range $\frac{1}{2} \leq \epsilon \leq \frac{3}{4}$ on a classical computer.
- For quantum computers, Cornacchia provides the fastest quantum algorithm, with that we improve the time complexity in the range $0 < \epsilon < \frac{5}{2}$.
- Our strategy is essentially memory-free while meet-in-the-middle algorithms require exponential memory storage.

Method	Cost (classical)	Cost (quantum)	Condition on size
State-of-the-art (general d)	$\frac{1}{2} + \epsilon$	$\frac{1}{4} + \frac{\epsilon}{2}$	
State-of-the-art (large d)	$\frac{1}{2}$	$\frac{1}{4}$	$\epsilon > \frac{5}{2}$
State-of-the-art (smooth d)	$\frac{1}{4} + \frac{\epsilon}{2}$	$\frac{1}{4} + \frac{\epsilon}{2}$	
Cornacchia	$max\{\frac{1}{2}, \epsilon\} + log_p L[\frac{1}{3}]$	$max\{\frac{1}{4}, \frac{\epsilon}{2}\}$	
Coppersmith (bivariate)	$\frac{1}{2}$	$\frac{1}{4}$	$\epsilon < \frac{1}{2}$
Coppersmith (trivariate)	$\frac{1}{2}$	$\frac{1}{4}$	$\epsilon < \frac{1}{4}$
Hybrid approach (smooth d)	$max\{\frac{1}{2}, \epsilon - \frac{1}{8}\}$	$\frac{1}{4} + \frac{\epsilon}{2}$	$\frac{1}{4} < \epsilon < \frac{3}{4}$

Open problem: no guessing

- Coron / Bauer-Joux on four variables.
- The problem of algebraic dependency of the polynomials.

Thank you!

PSE Discord

Questions?