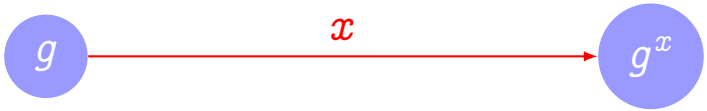
How to solve the supersingular endomorphism ring problem

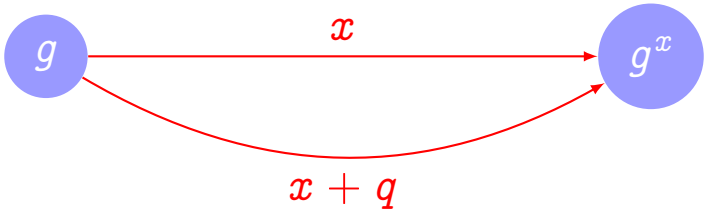
Luca De Feo
IBM Research Zürich

September 7, 2026, Mathematics of Post-Quantum Cryptography, Raitenhaslach

A group



A group



Several generators

$$g_1 \qquad g_2 \qquad g_3 \qquad g_4 \qquad g_5$$

Several generators

$$g_1^{7} \quad g_2^{19} \quad g_3^{39} \quad g_4^{67} \quad g_5^{0} \quad = 1$$

Several generators

$$g_1^{7} \quad g_2^{19} \quad g_3^{39} \quad g_4^{67} \quad g_5^{0} \quad = 1$$
$$g_1^{27} \quad g_2^{39} \quad g_3^{51} \quad g_4^{63} \quad g_5^{75} \quad = 1$$

Several generators

$$
\begin{aligned}
g_1^{7} \quad g_2^{19} \quad g_3^{39} \quad g_4^{67} \quad g_5^{0} &= 1 \\
g_1^{27} \quad g_2^{39} \quad g_3^{51} \quad g_4^{63} \quad g_5^{75} &= 1 \\
g_1^{31} \quad g_2^{47} \quad g_3^{63} \quad g_4^{79} \quad g_5^{95} &= 1
\end{aligned}
$$

Several generators

$$
\begin{aligned}
g_1^{7} \quad g_2^{19} \quad g_3^{39} \quad g_4^{67} \quad g_5^{0} &= 1 \\
g_1^{27} \quad g_2^{39} \quad g_3^{51} \quad g_4^{63} \quad g_5^{75} &= 1 \\
g_1^{31} \quad g_2^{47} \quad g_3^{63} \quad g_4^{79} \quad g_5^{95} &= 1 \\
g_1^{35} \quad g_2^{55} \quad g_3^{75} \quad g_4^{95} \quad g_5^{12} &= 1
\end{aligned}
$$

Several generators

$$
\begin{aligned}
g_1^{7} \quad g_2^{19} \quad g_3^{39} \quad g_4^{67} \quad g_5^{0} &= 1 \\
g_1^{27} \quad g_2^{39} \quad g_3^{51} \quad g_4^{63} \quad g_5^{75} &= 1 \\
g_1^{31} \quad g_2^{47} \quad g_3^{63} \quad g_4^{79} \quad g_5^{95} &= 1 \\
g_1^{35} \quad g_2^{55} \quad g_3^{75} \quad g_4^{95} \quad g_5^{12} &= 1
\end{aligned}
$$

$$\mathbb{Z}^5/\Lambda \longrightarrow G$$

The isogeny problem

The isogeny problem

Algebra  Geometry

Isogenies

Algebraic morphisms: $\left(\dfrac{5x^2+5x+4}{x+1}, \quad y\dfrac{2x^2+4x-4}{x^2+2x+1}\right)$

Group morphisms: $\varphi(P+Q) = \varphi(P) + \varphi(Q)$

Isogenies

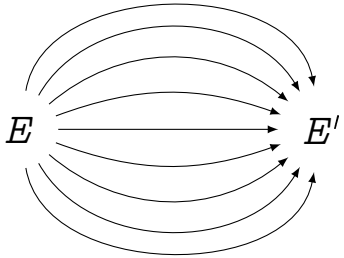
Algebraic morphisms: $\left(\dfrac{5x^2+5x+4}{x+1}, \quad y\dfrac{2x^2+4x-4}{x^2+2x+1}\right)$

$\longmapsto$ Interpolation

Group morphisms: $\varphi(P+Q) = \varphi(P) + \varphi(Q)$

$\longmapsto$ Groups **of** morphisms

“Classes” of isogenies



$$\mathrm{Hom}(E, E')$$

Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

- A measure of “size”;

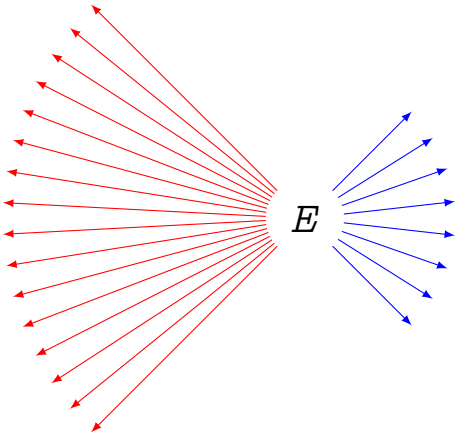
Degree

$$\deg(\varphi) \in \mathbb{N}^+$$

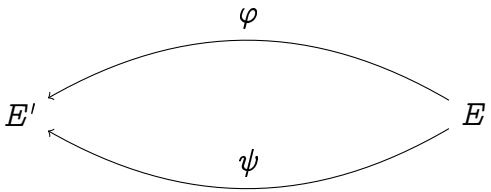
- A measure of “size”;
- Multiplicative.

$$\deg(\psi \circ \varphi) = \deg(\psi)\deg(\varphi)$$

The larger the degree, the more isogenies

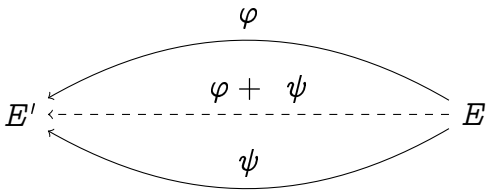


Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

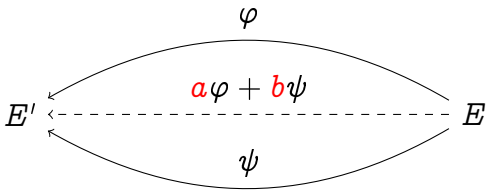
Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

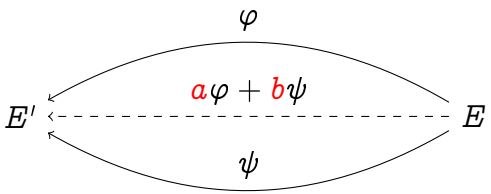
Lattices of isogenies



$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

$$(a\varphi + b\psi)(P) := [a]\varphi(P) + [b]\psi(P)$$

Lattices of isogenies

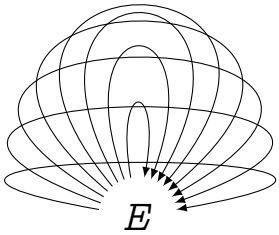


$$\varphi, \psi \in \mathrm{Hom}(E, E')$$

$$(a\varphi + b\psi)(P) := [a]\varphi(P) + [b]\psi(P)$$

- $\deg(a\varphi) = a^2 \deg(\varphi)$,
- $\left|\deg(\varphi + \psi) - \deg(\varphi) - \deg(\psi)\right| \leq 2\sqrt{\deg(\varphi)\deg(\psi)}$,
- deg is a positive definite quadratic form.

Endomorphisms



$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$

$$(\varphi \circ \psi)(P) := \varphi(\psi(P))$$

$$\varphi \circ (\psi + \chi) = \varphi \circ \psi + \varphi \circ \chi$$

Endomorphism rings

$$\mathbb{Q}(\sqrt{-p})$$

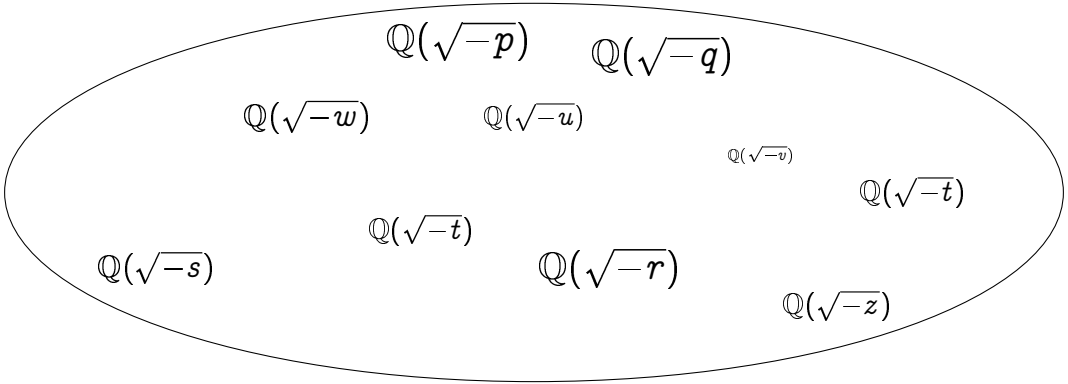
Quadratic imaginary field

Endomorphism rings

$\mathbb{Q}(\sqrt{-p})$ $\mathbb{Q}(\sqrt{-q})$

$$i^2 = -p \qquad j^2 = -q \qquad ij = -ji$$

Endomorphism rings



Quaternion algebra

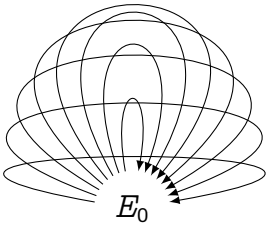
$$i^2 = -p \qquad j^2 = -q \qquad ij = -ji$$

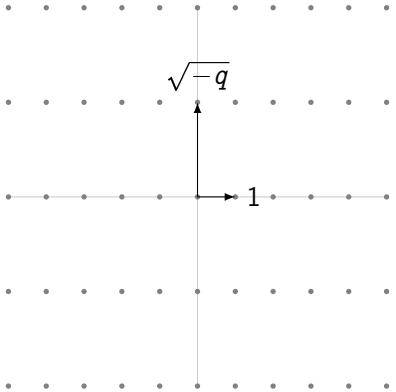
Orders

$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ i \\ j \\ ij \end{pmatrix}$$

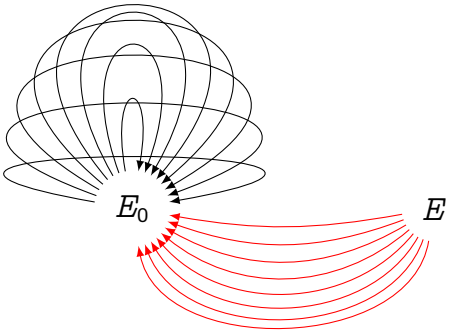
Order type:

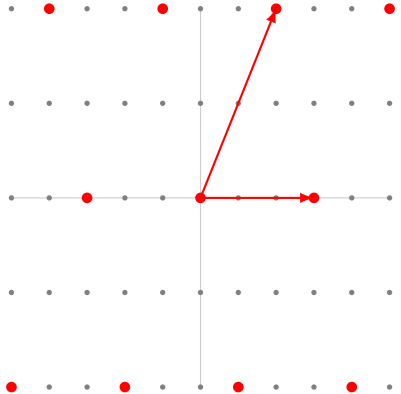
$$\mathcal{O} \simeq \alpha \mathcal{O} \alpha^{-1}$$



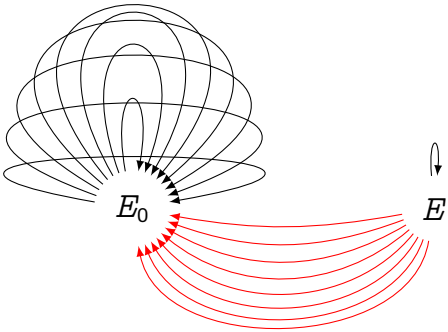


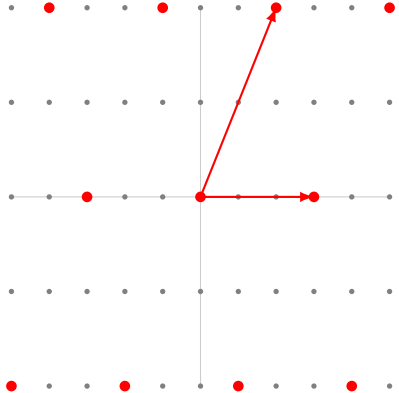
$\mathbb{Z}[\sqrt{-q}]$



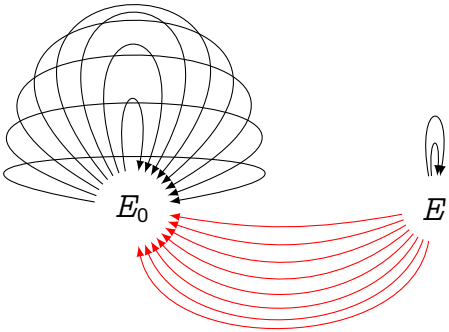


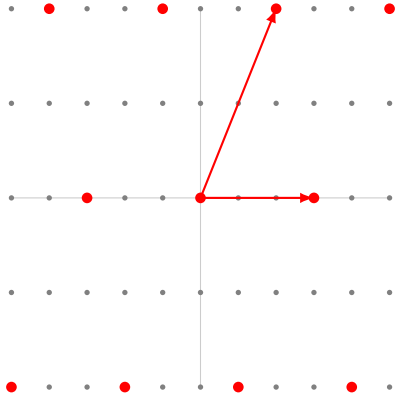
$\mathbb{Z}[\sqrt{-q}]$



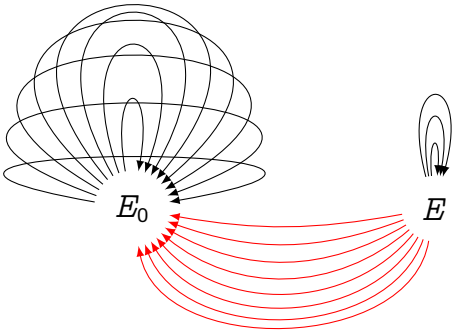


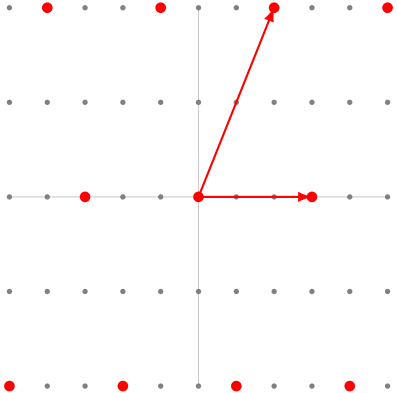
$\mathbb{Z}[\sqrt{-q}]$



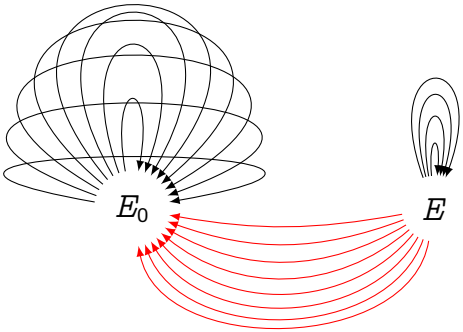


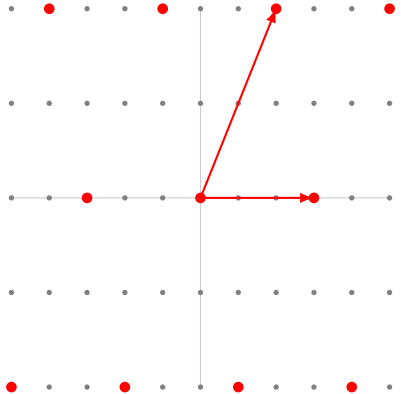
$\mathbb{Z}[\sqrt{-q}]$



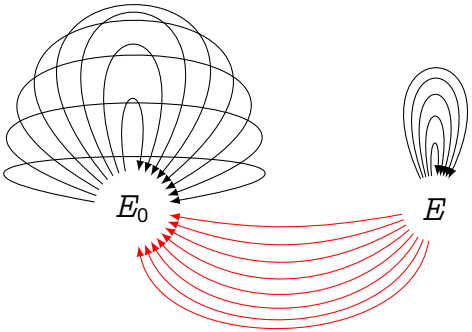


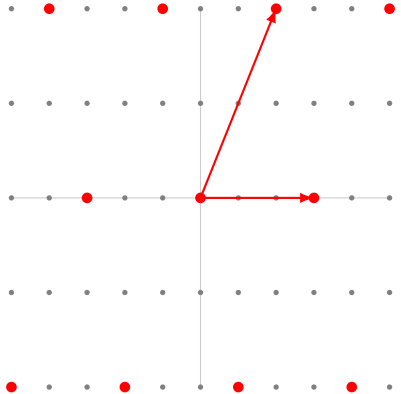
$\mathbb{Z}[\sqrt{-q}]$



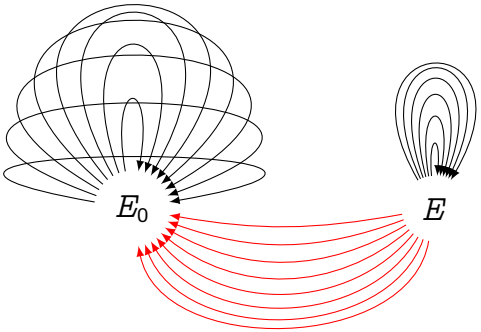


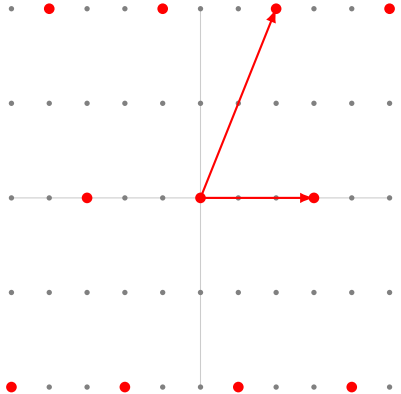
$\mathbb{Z}[\sqrt{-q}]$



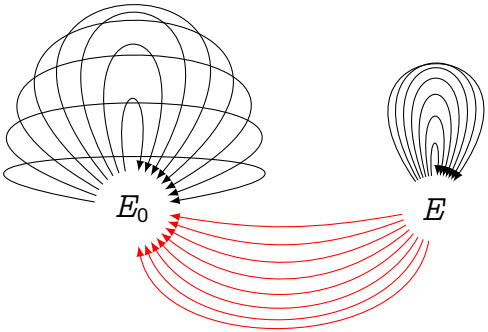


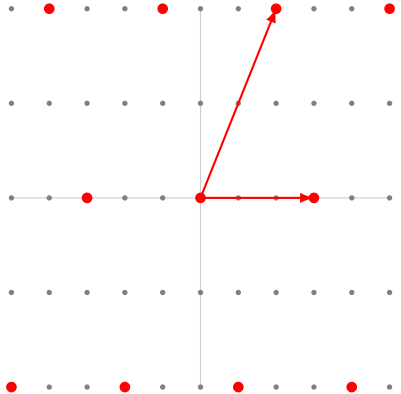
$\mathbb{Z}[\sqrt{-q}]$



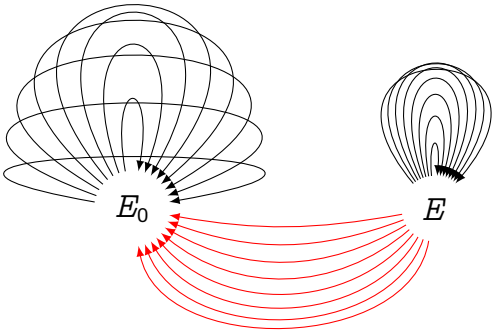


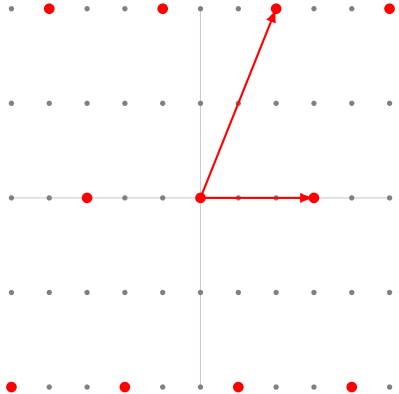
$\mathbb{Z}[\sqrt{-q}]$



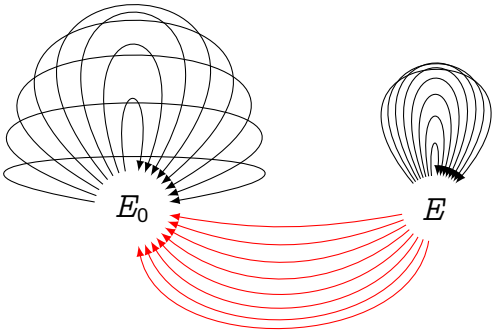


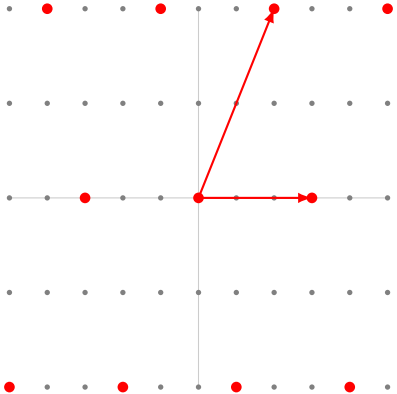
$\mathbb{Z}[\sqrt{-q}]$





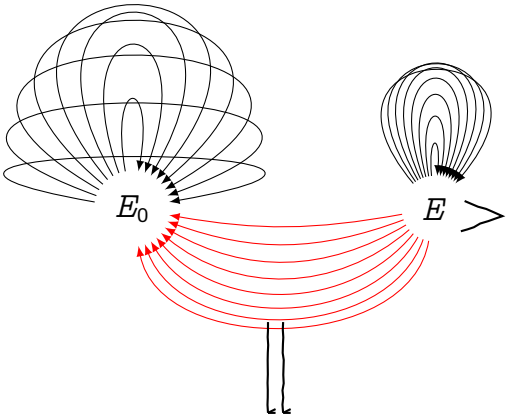
$\mathbb{Z}[\sqrt{-q}]$

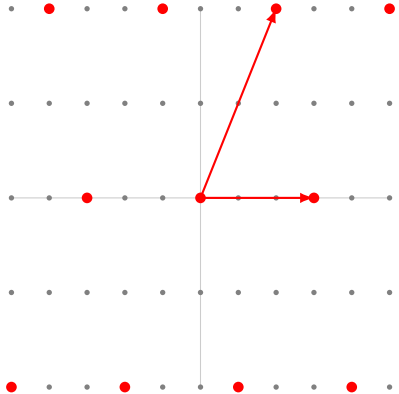




$\mathbb{Z}[\sqrt{-q}]$

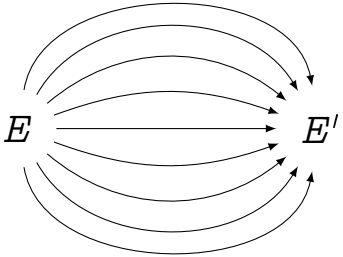
Deuring: $\mathrm{End}(E_0)$ sublattices $\leftrightarrow$ homsets $\leftrightarrow$ curves isogenous to E_0.





Deuring: $\mathrm{End}(E_0)$ sublattices $\leftrightarrow$ homsets $\leftrightarrow$ curves isogenous to E_0.

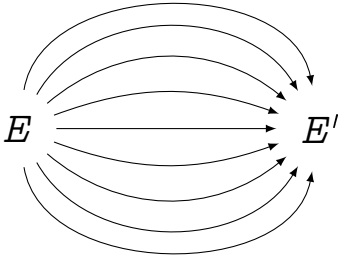
homset



lattice (class)

$$\begin{pmatrix} 13 & 3 & 4 & 1 \\ 0 & 13 & 14 & 0 \\ 0 & 0 & 31 & 9 \\ 0 & 0 & 0 & 173 \end{pmatrix}$$

homset



lattice (class)

$$\begin{pmatrix} 13 & 3 & 4 & 1 \\ 0 & 13 & 14 & 0 \\ 0 & 0 & 31 & 9 \\ 0 & 0 & 0 & 173 \end{pmatrix}$$

degree

norm

The supersingular space

- $\approx \frac{p}{12}$ curves defined over $\mathbb{F}_{p^2}$
- of which $\sim \sqrt{p}$ curves defined over $\mathbb{F}_p$
- Connected by ℓ-isogenies for any choice of $\ell > 1$

The endomorphism ring problem

Given a random supersingular curve E, compute a basis of $\mathrm{End}(E)$.

$\Leftrightarrow$

Given random supersingular curves E, E', compute an isogeny $E \to E'$.

The endomorphism ring problem

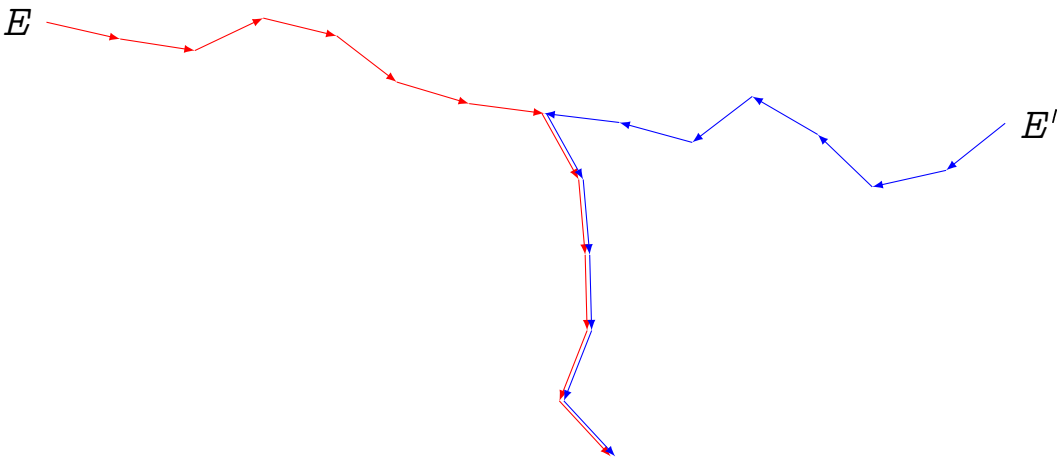
Given a random supersingular curve E, compute a basis of $\mathrm{End}(E)$.

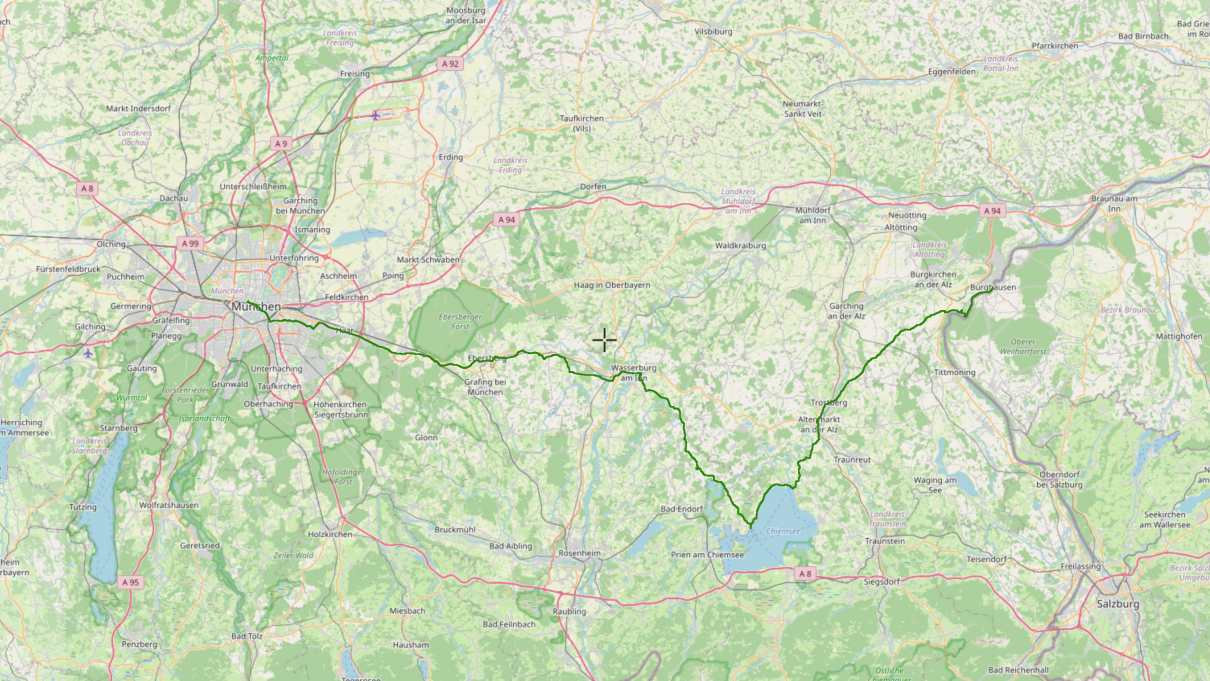
$\Leftrightarrow$

Given random supersingular curves E, E', compute an isogeny $E \to E'$.

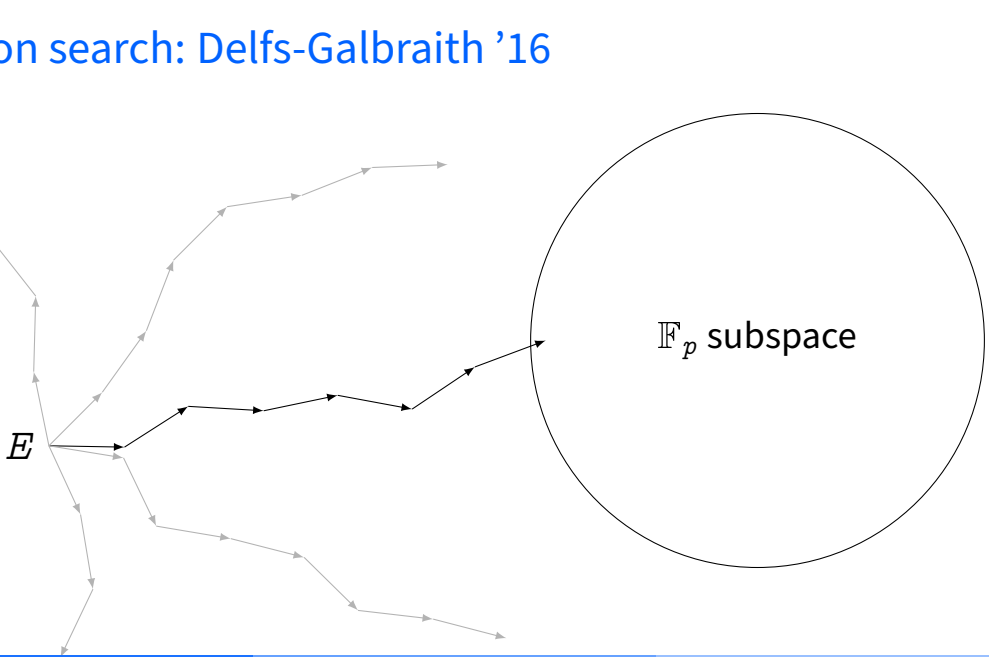
Both problems are random self-reducible

Collision search: Galbraith ’99




Moosburg an der Isar
Landkreis Freising
Ampertal
Freising
A 92
Vilsbiburg
Pfarrkirchen
Bad Birnbach
Landkreis Rottal-Inn
Eggenfelden
Markt Indersdorf
Landkreis Dachau
A 9
Taufkirchen (Vils)
Neumarkt-Sankt Veit
Erding
Landkreis Erding
A 8
Dachau
Unterschleißheim
Garching bei München
Ismaning
Dorfen
Landkreis Mühldorf am Inn
Mühldorf am Inn
Neuötting
Altötting
A 94
Braunau am Inn
Olching
A 99
Unterföhring
Markt Schwaben
Waldkraiburg
Landkreis Altötting
Fürstenfeldbruck
Puchheim
Aschheim
Poing
Burgkirchen an der Alz
Burghausen
München
Haag in Oberbayern
Germering
Feldkirchen
Garching an der Alz
Gilching
Gräfelfing
Ebersberger Forst
Bezirk Braunau
Planegg
Ebersberg
Mättighofen
Wasserburg am Inn
Oberer Weilhartforst
Gauting
Unterhaching
Grafing bei München
Tittmoning
Würmtal
Grünwald
Taufkirchen
Forstenrieder Park
Oberhaching
Höhenkirchen-Siegertsbrunn
Isarlandschaft
Trostberg
Starnberg
Altenmarkt an der Alz
Landkreis Starnberg
Glonn
Traunreut
Hofoldinger Forst
Waging am See
Oberndorf bei Salzburg
Tutzing
Wolfratshausen
Bad Endorf
Landkreis Traunstein
Seekirchen am Wallersee
Holzkirchen
Bruckmühl
Chiemsee
Traunstein
Geretsried
Bad Aibling
Rosenheim
Prien am Chiemsee
Teisendorf
Zeller Wald
A 95
A 8
Siegsdorf
Freilassing
Salzburg
Miesbach
Bad Feilnbach
Raubling
Bad Tölz
Penzberg
Hausham
Bad Reichenhall

Collision search: Delfs-Galbraith ’16



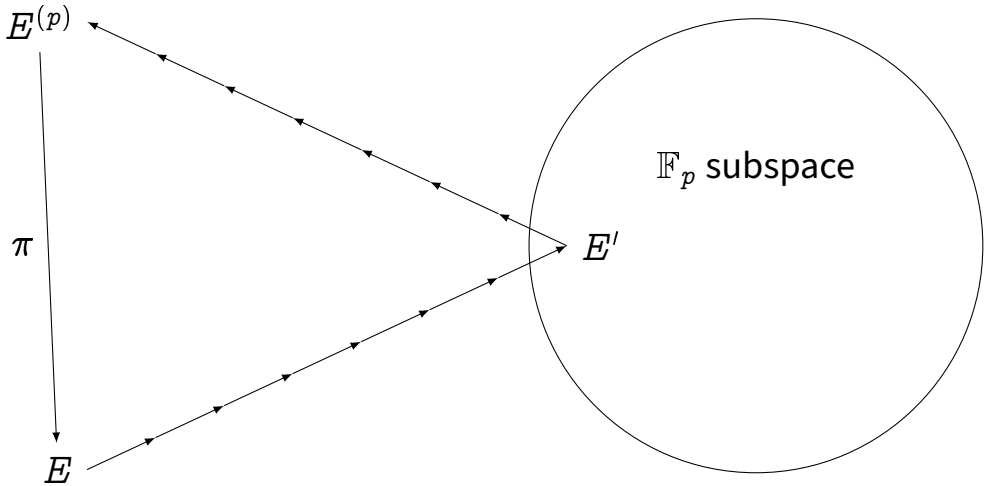
Frobenius

$$E : y^2 = x^3 + ax + b$$

$$E^{(p)} : y^2 = x^3 + a^p x + b^p$$

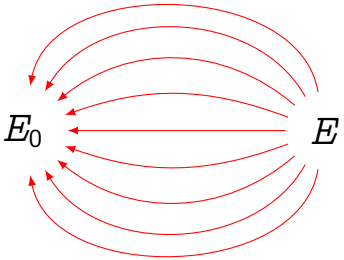
$$\pi : E \longrightarrow E^{(p)}$$
$$(x, y) \longmapsto (x^p, y^p)$$

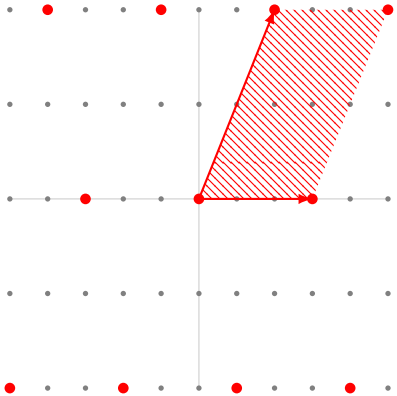
Reflections (Chenu-Smith ’21)



Geometry of numbers

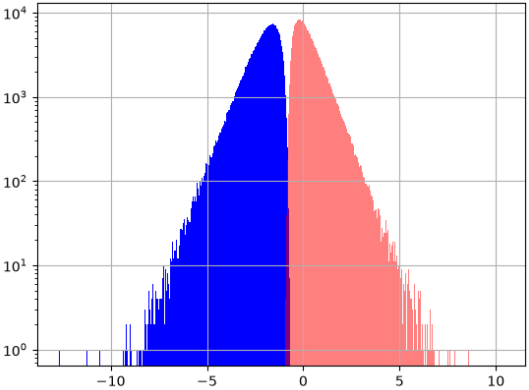
discriminant = covolume = p



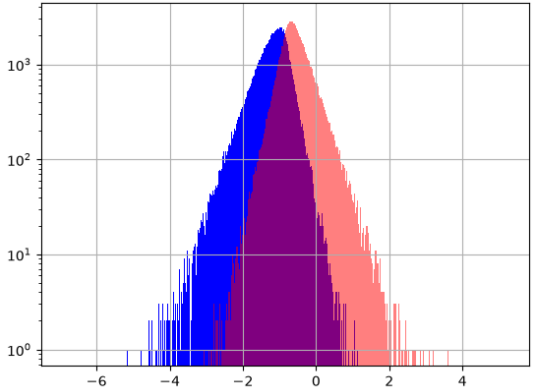


Gaussian heuristic $\Rightarrow$ $d_1 \approx d_2 \approx d_3 \approx d_4 \approx \sqrt{p}$

Squared minima of random $\mathrm{Hom}(E, E')$, log scale

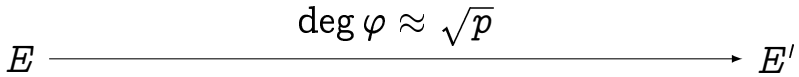


1st and 4th minimum



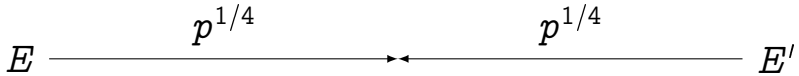
2nd and 3rd minimum

How hard is it to find a short isogeny? (Folklore)



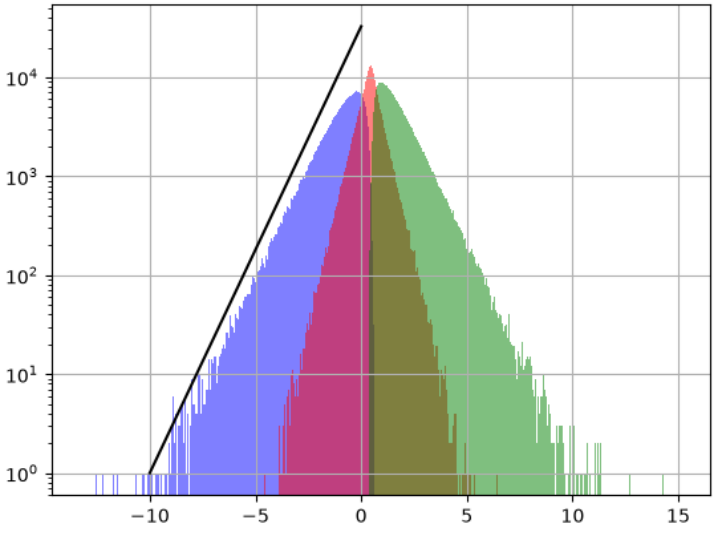
- $O(n)$ isogenies of degree n from E
- $\Rightarrow O(n^2)$ isogenies of degree $\leq n$ from E

How hard is it to find a short isogeny? (Folklore)

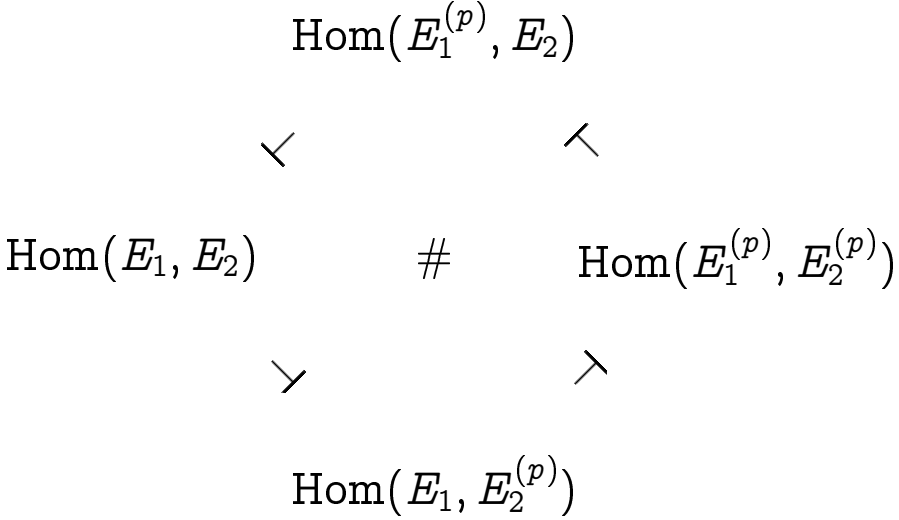


- $O(n)$ isogenies of degree n from E
- $\Rightarrow$ $O(n^2)$ isogenies of degree $\leq n$ from E
- $\Rightarrow$ If we're lucky, we can meet-in-the-middle at cost $O(\sqrt{p})$.

Minima of endomorphism rings



Duality


$\mathrm{Hom}(E_1^{(p)}, E_2)$
$\mathrm{Hom}(E_1, E_2)$
#
$\mathrm{Hom}(E_1^{(p)}, E_2^{(p)})$
$\mathrm{Hom}(E_1, E_2^{(p)})$

Transference

$\mathrm{Hom}(E_1, E_2)$

d_1, d_2, d_3, d_4

$\mathrm{Hom}(E_1, E_2^{(p)})$

$d_1^*, d_2^*, d_3^*, d_4^*$

$$d_1 d_4^* \approx d_2 d_3^* \approx d_3 d_2^* \approx d_4 d_1^* \approx p$$

Transference

$\mathrm{Hom}(E_1, E_2)$

d_1, d_2, d_3, d_4

$\mathrm{Hom}(E_1, E_2^{(p)})$

$d_1^*, d_2^*, d_3^*, d_4^*$

$$d_1 d_4^* \approx d_2 d_3^* \approx d_3 d_2^* \approx d_4 d_1^* \approx p$$

$\mathrm{End}(E)$

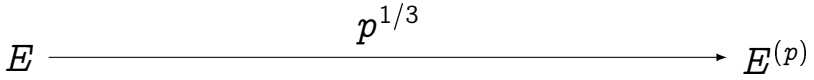
$1, d_2, d_3, d_4$

$\mathrm{Hom}(E, E^{(p)})$

$d_1^*, d_2^*, d_3^*, d_4^*$

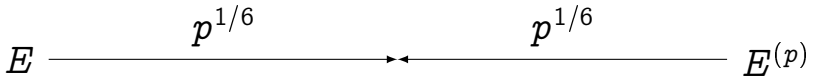
$$d_4^* \approx d_2 d_3^* \approx d_3 d_2^* \approx d_4 d_1^* \approx p$$

Wesolowski's attack '26



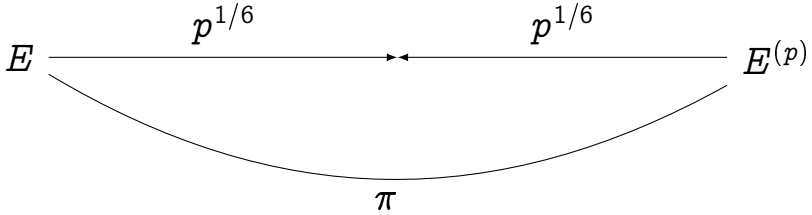
- $O(n)$ isogenies of degree n from E
- $\Rightarrow O(n^2)$ isogenies of degree $\leq n$ from E

Wesolowski's attack '26



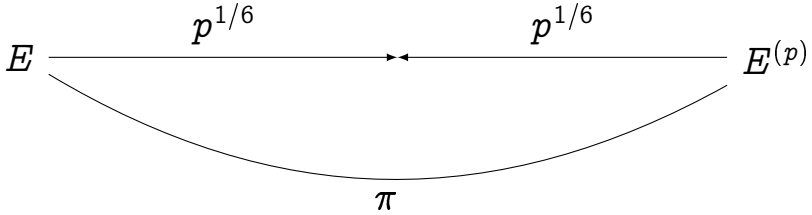
- $O(n)$ isogenies of degree n from E
- $\Rightarrow$ $O(n^2)$ isogenies of degree $\leq n$ from E
- $\Rightarrow$ If we're lucky, we can meet-in-the-middle at cost $O(p^{1/3})$ time

Wesolowski's attack '26



- $O(n)$ isogenies of degree n from E
- $\Rightarrow$ $O(n^2)$ isogenies of degree $\leq n$ from E
- $\Rightarrow$ If we're lucky, we can meet-in-the-middle at cost $O(p^{1/3})$ time

Wesolowski's attack '26



- $O(n)$ isogenies of degree n from E
- $\Rightarrow$ $O(n^2)$ isogenies of degree $\leq n$ from E
- $\Rightarrow$ If we're lucky, we can meet-in-the-middle at cost $O(p^{1/3})$ time **and memory!**

How to cost Wesolowski's attack?

Invariant: $T^2 M = \tilde{O}(p)$ via

- van Oorschot–Wiener
- "going under" (Chenu-Smith)

At constant memory: $T = \tilde{O}(\sqrt{p})$

With memory bound w: $T = \tilde{O}(\sqrt{p/w})$

SQIsign Round 3

	old p	new p	memory	$\sqrt{p/w}$	PK	Sig
	bits		*bound*	*bits*	*bytes*	
NIST-I	**250.3**	325.6	2^{80}	**245.6**	83	200
NIST-III	**382.0**	504.8	2^{120}	**384.8**	129	306
NIST-V	**504.8**	668.1	2^{160}	**508.1**	169	406

SQIsign Round 3

	old p	new p	memory	$\sqrt{p/w}$	PK	Sig
	bits		*bound*	*bits*	*bytes*	
NIST-I	**250.3**	325.6	2^{80}	**245.6**	83	200
NIST-III	**382.0**	504.8	2^{120}	**384.8**	129	306
NIST-V	**504.8**	668.1	2^{160}	**508.1**	169	406

	Key Gen.	Signing	Verification
	Mcycles		
NIST-I	32.2	93.9	12.1
NIST-III	102.1	320.3	31.5
NIST-V	214.5	674.7	77.6

Thank you

https://defeo.lu/

 @luca_defeo@ioc.exchange

 @bsky.defeo.lu