Not Again!

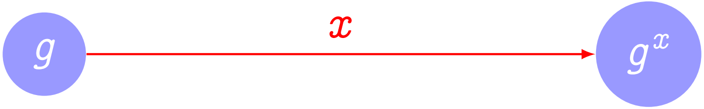
What’s going on in isogeny-based crypto?

Luca De Feo

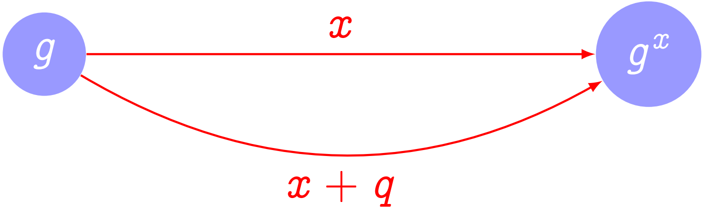
IBM Research Zürich

August 12, 2026, Algebraic Methods in Post-quantum Cryptography, Ohrid

A group



A group



Several generators

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

Several generators

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

Several generators

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

Several generators

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

Several generators

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

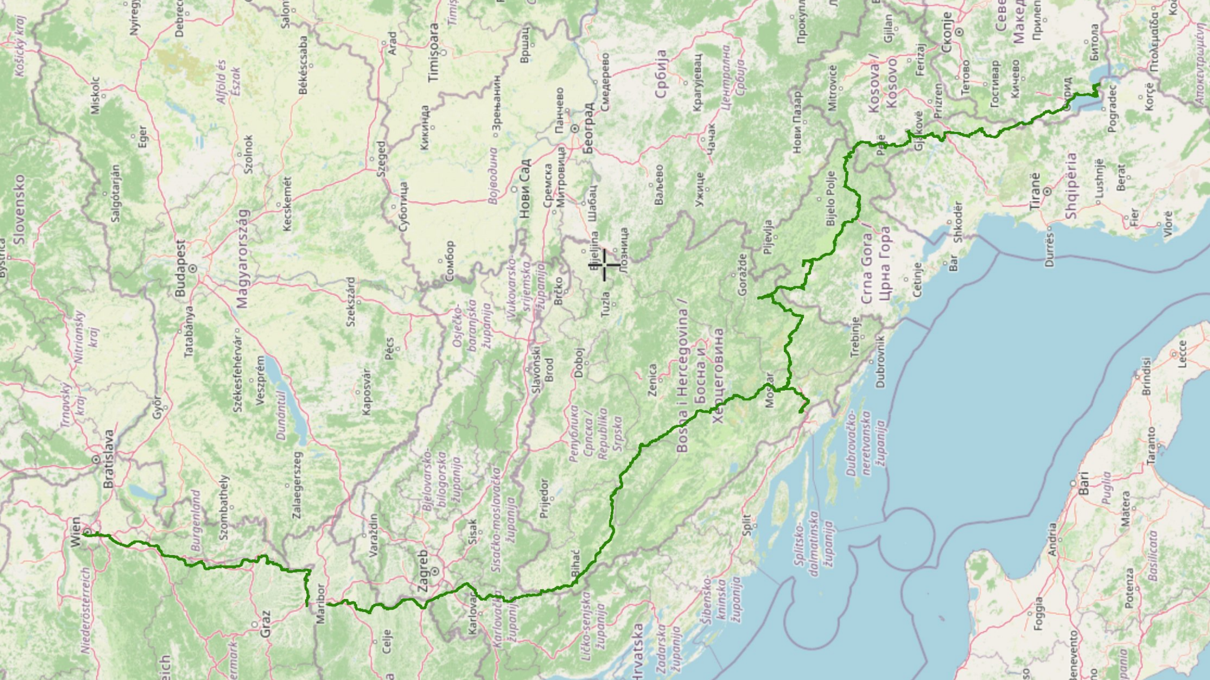
Several generators

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

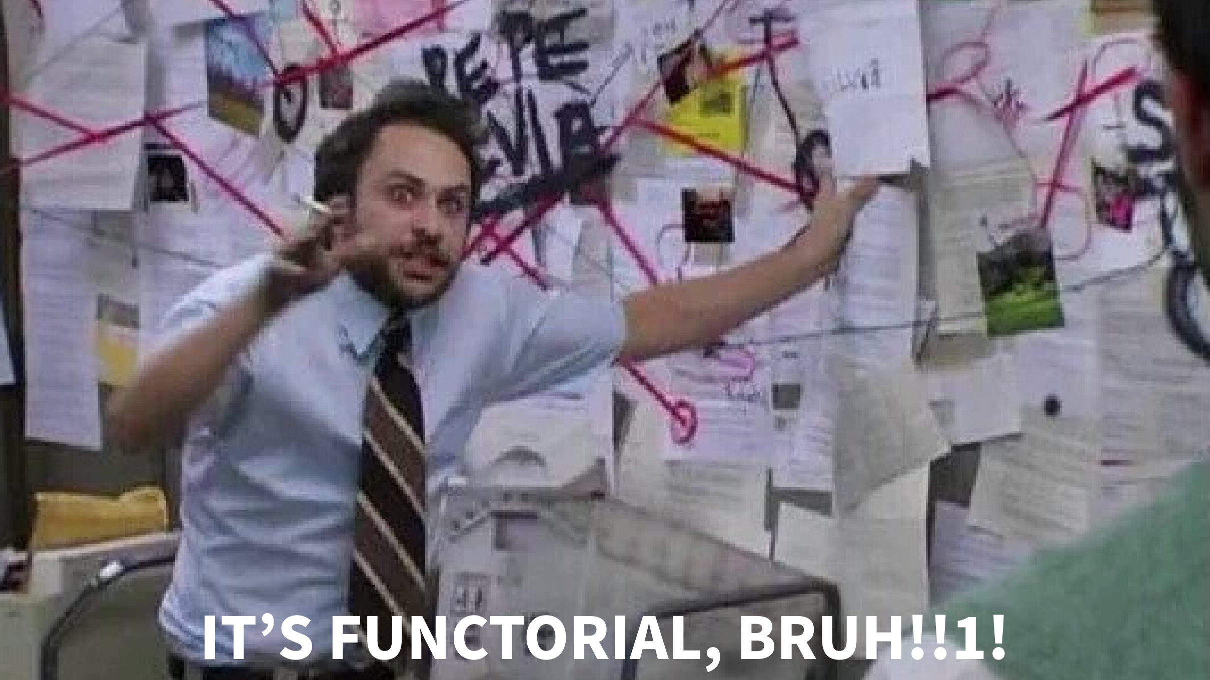
$$\mathbb{Z}^5/\Lambda \longrightarrow G$$

The isogeny problem

The isogeny problem



Wien
Bratislava
Graz
Maribor
Celje
Zagreb
Karlovac
Varaždin
Sisak
Bihać
Prijedor
Slavonski Brod
Doboj
Tuzla
Brčko
Bijeljina
Zenica
Mostar
Split
Dubrovnik
Trebinje
Goražde
Pljevlja
Bijelo Polje
Cetinje
Bar
Shkodër
Tiranë
Durrës
Fier
Vlorë
Berat
Lushnjë
Pogradec
Korçë
Prizren
Pejë
Gjakovë
Ferizaj
Mitrovicë
Kosova / Kosovo
Crna Gora
Црна Гора
Shqipëria
Bosna i Hercegovina /
Босна и Херцеговина
Republika Srpska
Република Српска
Hrvatska
Budapest
Magyarország
Győr
Szombathely
Zalaegerszeg
Veszprém
Székesfehérvár
Tatabánya
Kaposvár
Pécs
Szekszárd
Kecskemét
Szolnok
Eger
Miskolc
Salgótarján
Debrecen
Békéscsaba
Szeged
Arad
Timişoara
Београд
Нови Сад
Суботица
Сомбор
Зрењанин
Кикинда
Панчево
Смедерево
Шабац
Лозница
Ваљево
Ужице
Чачак
Крагујевац
Србија
Нови Пазар
Скопје
Тетово
Гостивар
Кичево
Битола
Прилеп
Охрид
Bari
Brindisi
Lecce
Taranto
Matera
Potenza
Foggia
Andria
Puglia
Basilicata
Burgenland
Niederösterreich
Slovensko
Vojvodina
Војводина
Dunántúl
Trnavský kraj
Nitriansky kraj
Košický kraj
Alföld és Észak
Bjelovarsko-bilogorska županija
Sisačko-moslavačka županija
Karlovačka županija
Ličko-senjska županija
Zadarska županija
Šibensko-kninska županija
Splitsko-dalmatinska županija
Dubrovačko-neretvanska županija
Osječko-baranjska županija
Vukovarsko-srijemska županija


IT’S FUNCTORIAL, BRUH!!1!

Algebra $\circlearrowright$ Geometry

Isogenies

$$y^2 = x^3 + 1 \xrightarrow{\varphi} y^2 = x^3 - x$$

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

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

Isogenies

$$y^2 = x^3 + 1 \xrightarrow{\quad\varphi\quad} y^2 = x^3 - x$$

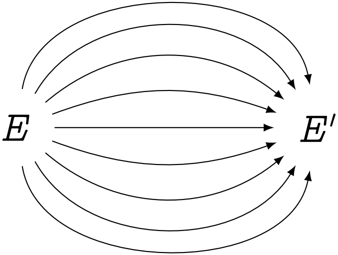
Algebraic morphisms: $\left(\dfrac{5x^2 + 5x + 4}{x + 1},\quad y\dfrac{2x^2 + 4x - 4}{x^2 + 2x + 1}\right)$

$\longmapsto$ Interpolation

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

$\longmapsto$ Groups ***of*** morphisms

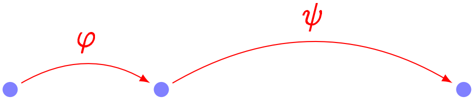
“Classes” of isogenies



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

Degree

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



- A measure of "size";

Degree

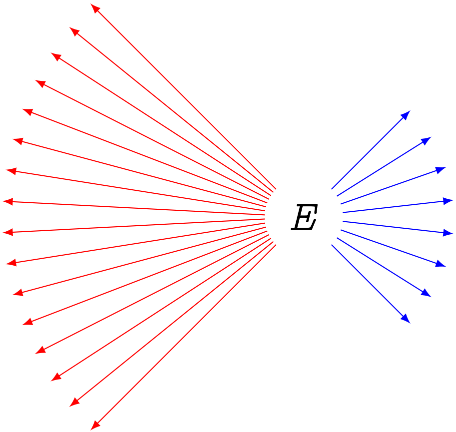
$$\deg(\varphi) \in \mathbb{N}^+$$

$$\bullet \xrightarrow{\varphi} \bullet \xrightarrow{\psi} \bullet$$

- A measure of “size”;
- Multiplicative.

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

The larger the degree, the more isogenies



Lattices of isogenies

$$\begin{tikzcd} E' & E \arrow[l, bend right, "\varphi"'] \arrow[l, bend left, "\psi"] \end{tikzcd}$$

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

Lattices of isogenies

$$\begin{tikzcd} E' & & E \arrow[ll, bend right, "\varphi"'] \arrow[ll, dashed, "\varphi + \psi"'] \arrow[ll, bend left, "\psi"] \end{tikzcd}$$

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

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

Lattices of isogenies

$$\begin{tikzcd}
E' & & E \arrow[ll, bend right, "\varphi"'] \arrow[ll, dashed, "{\color{red}a}\varphi + {\color{red}b}\psi"'] \arrow[ll, bend left, "\psi"]
\end{tikzcd}$$

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

$$({\color{red}a}\varphi + {\color{red}b}\psi)(P) := [{\color{red}a}]\varphi(P) + [{\color{red}b}]\psi(P)$$

Lattices of isogenies

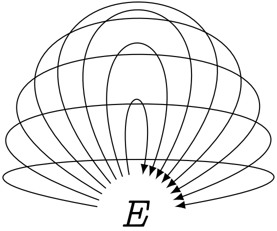
$$\begin{tikzcd}[column sep=huge] E' & E \arrow[l, bend right, "\varphi"'] \arrow[l, dashed, "{\color{red}a}\varphi + {\color{red}b}\psi"'] \arrow[l, bend left, "\psi"] \end{tikzcd}$$

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

$$({\color{red}a}\varphi + {\color{red}b}\psi)(P) := [{\color{red}a}]\varphi(P) + [{\color{red}b}]\psi(P)$$

- $\deg(a\varphi) = a^2 \deg(\varphi)$,
- $\left|\deg(\varphi+\psi) - \deg(\varphi) - \deg(\psi)\right| \le 2\sqrt{\deg(\varphi)\deg(\psi)}$,
- 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

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

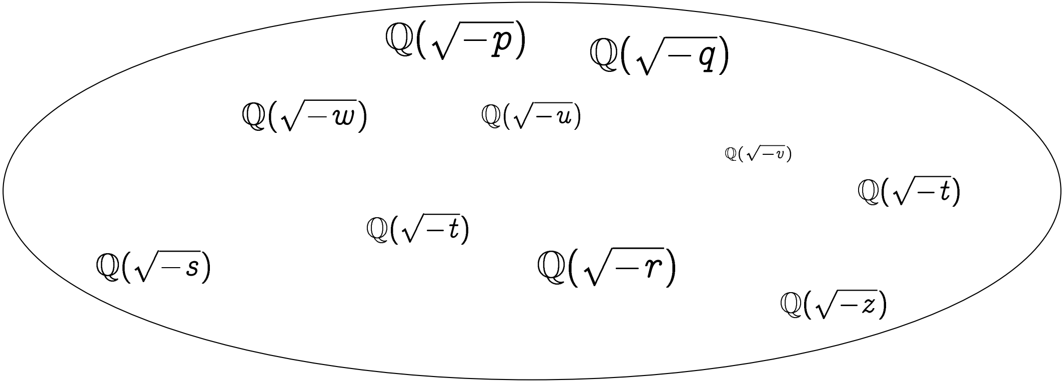
Quadratic imaginary field

Endomorphism rings

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

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

Endomorphism rings



Quaternion algebra

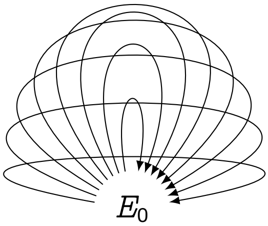
$$i^2 = -p \qquad j^2 = -q \qquad ij = -ji$$

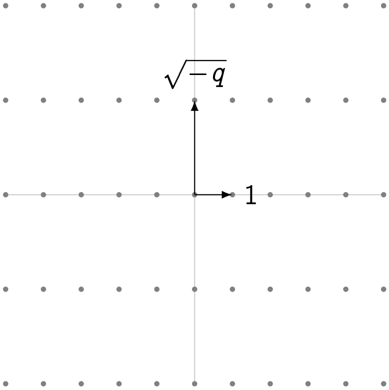
Orders

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

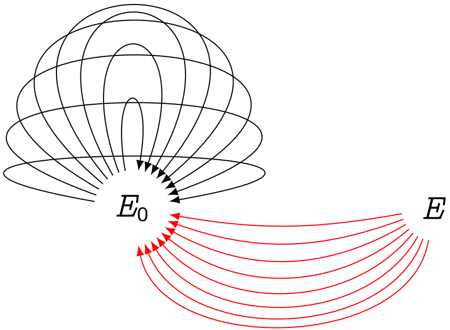
Order type:

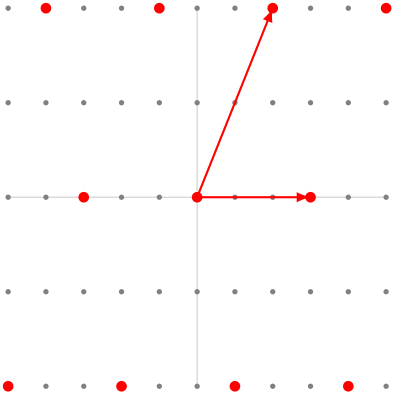
$$\mathcal{O} \simeq \alpha\mathcal{O}\alpha^{-1}$$



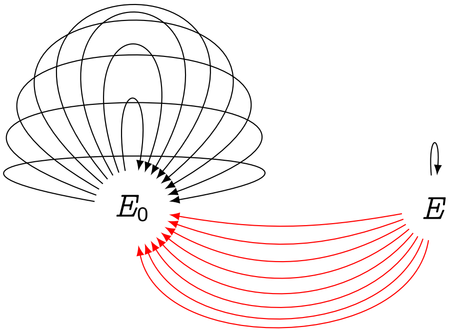


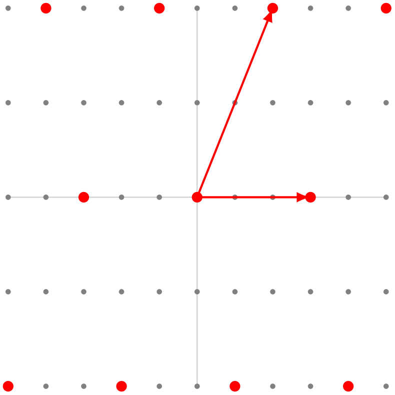
$\mathbb{Z}[\sqrt{-q}]$



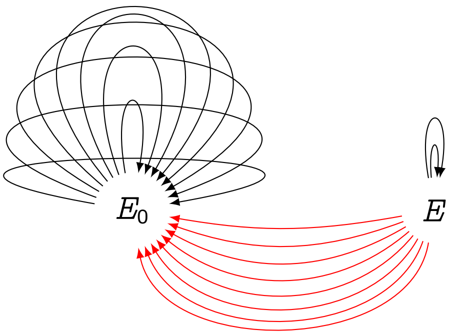


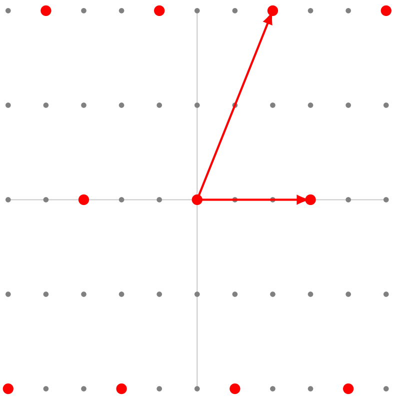
$\mathbb{Z}[\sqrt{-q}]$



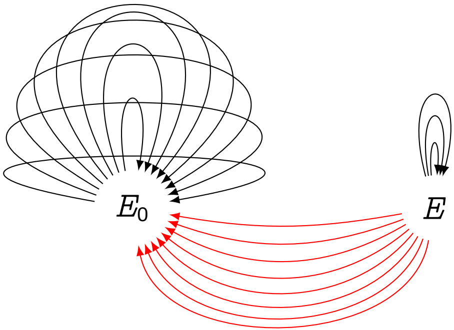


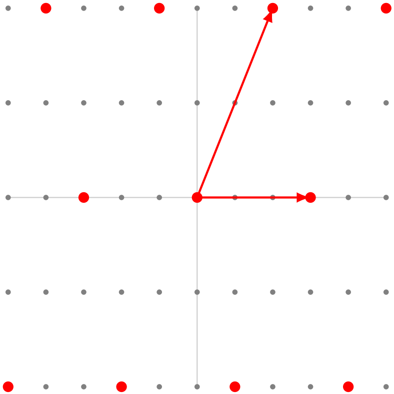
$\mathbb{Z}[\sqrt{-q}]$



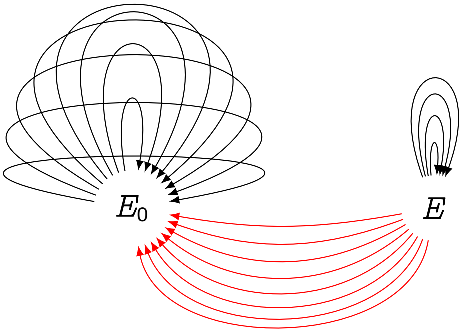


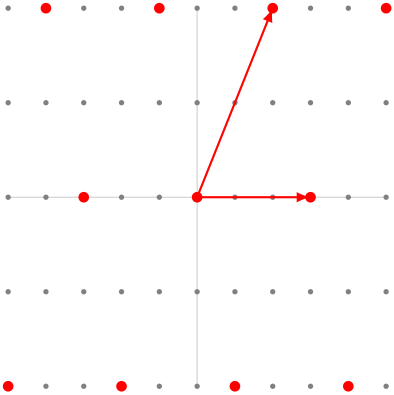
$\mathbb{Z}[\sqrt{-q}]$



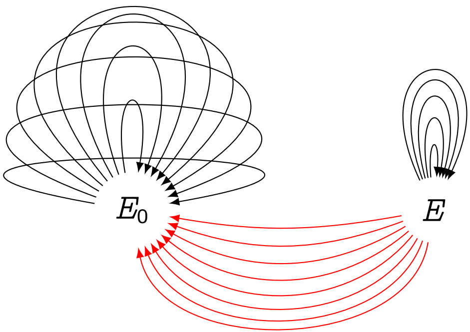


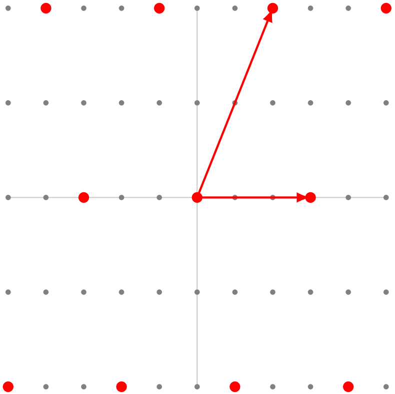
$\mathbb{Z}[\sqrt{-q}]$



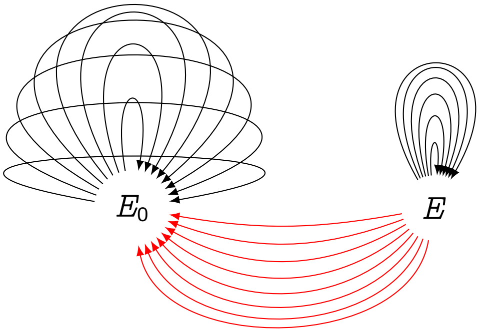


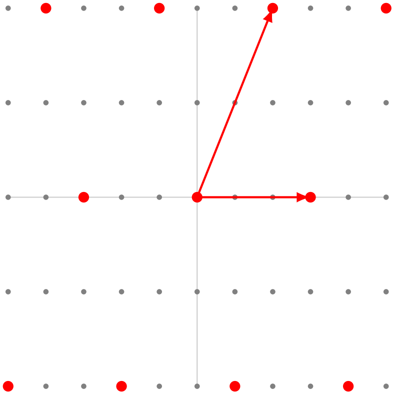
$$\mathbb{Z}[\sqrt{-q}]$$



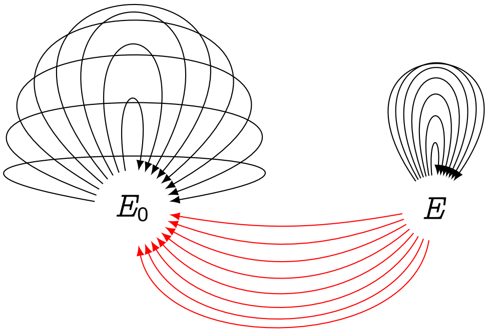


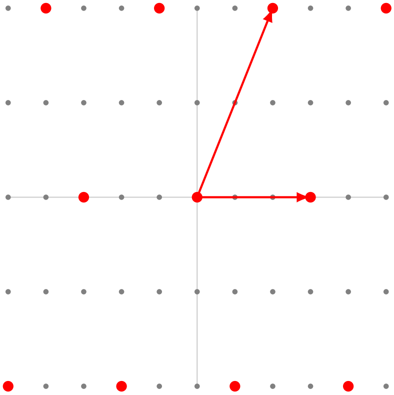
$\mathbb{Z}[\sqrt{-q}]$



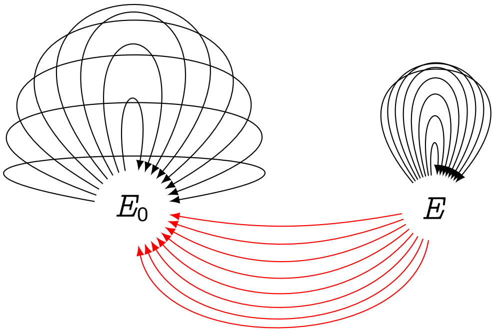


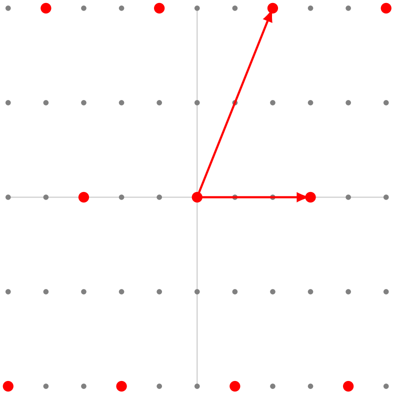
$$\mathbb{Z}[\sqrt{-q}]$$



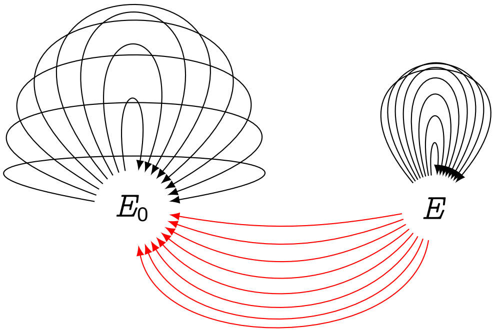


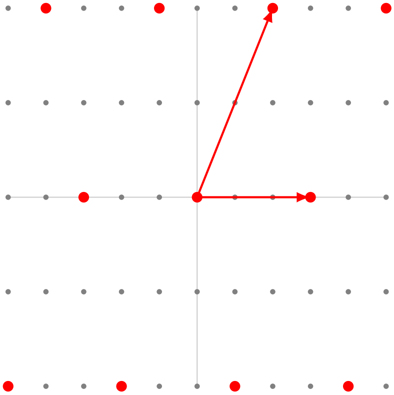
$\mathbb{Z}[\sqrt{-q}]$





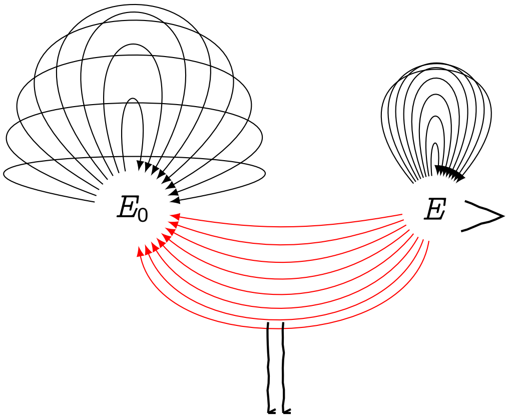
$\mathbb{Z}[\sqrt{-q}]$

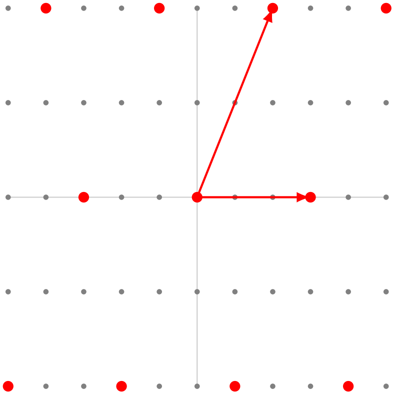




$\mathbb{Z}[\sqrt{-q}]$

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

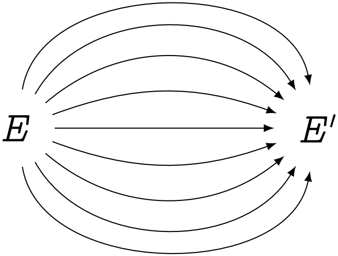




$\mathbb{Z}[\sqrt{-q}]$

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

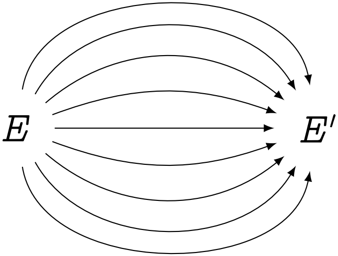
homset



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

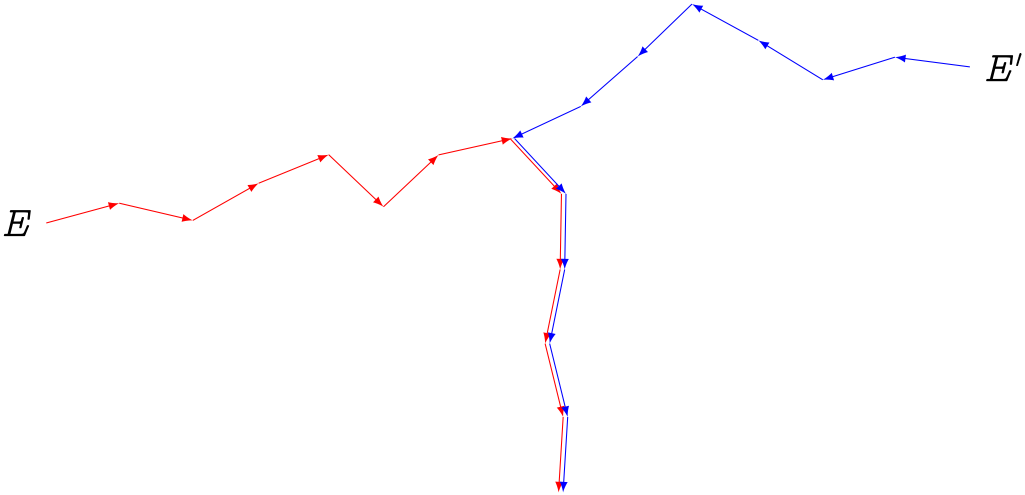
Given a random supersingular curve E, compute a basis of $\mathrm{End}(E)$.

$$\Longleftrightarrow$$

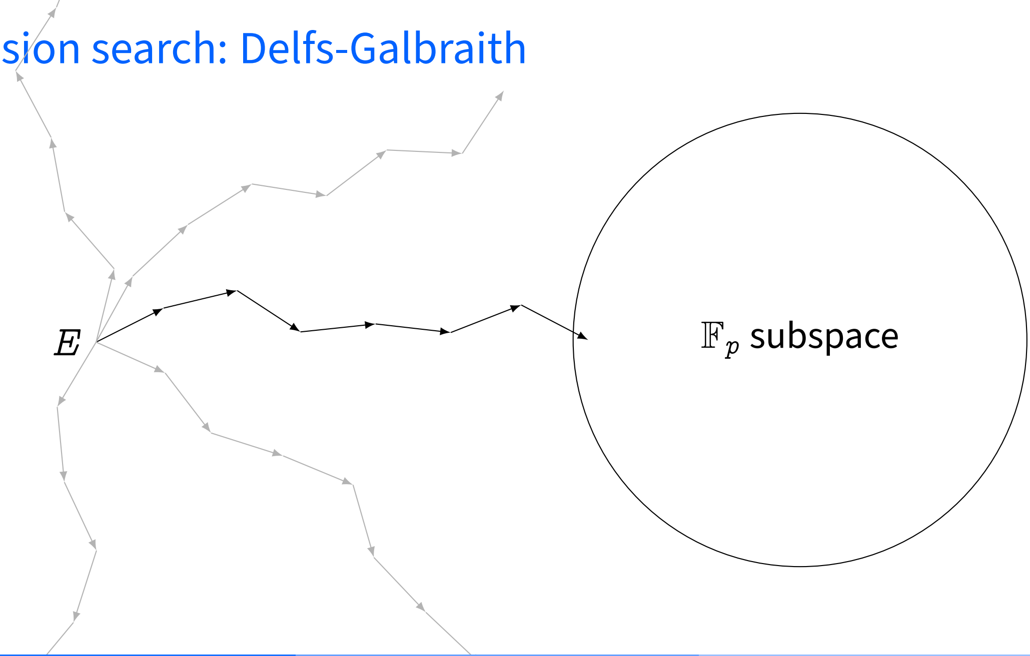
Given random supersingular curves E, E', compute an isogeny $E \to E'$.

Both problems are random self-reducible

Collision search: Galbraith



Collision search: Delfs-Galbraith



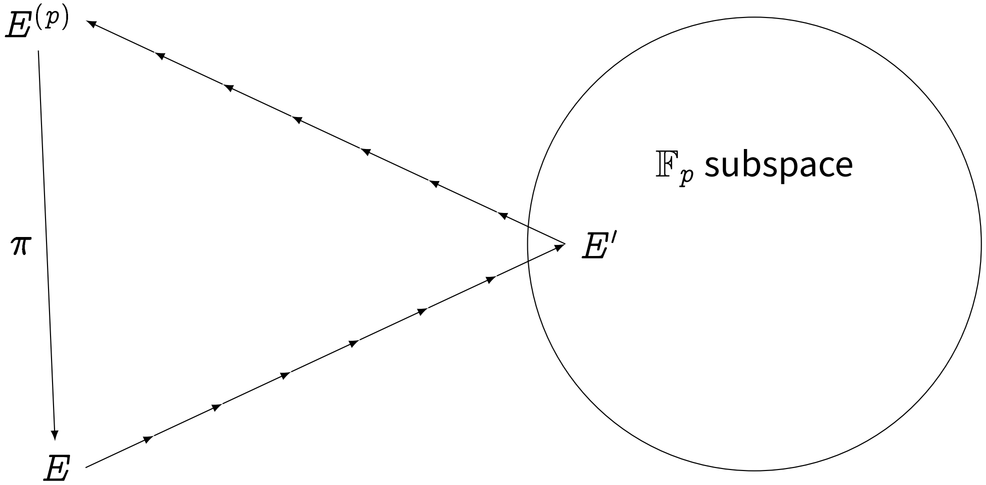
Frobenius

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

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

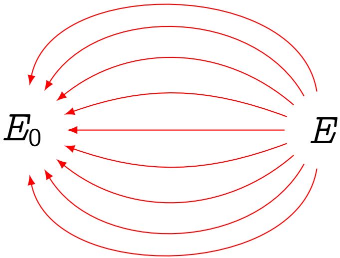
$$\begin{aligned} \pi : E &\longrightarrow E^{(p)} \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

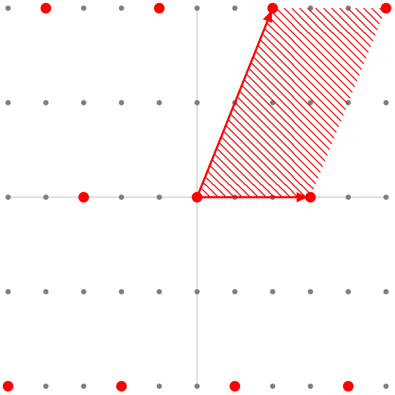
Reflections



Geometry of numbers

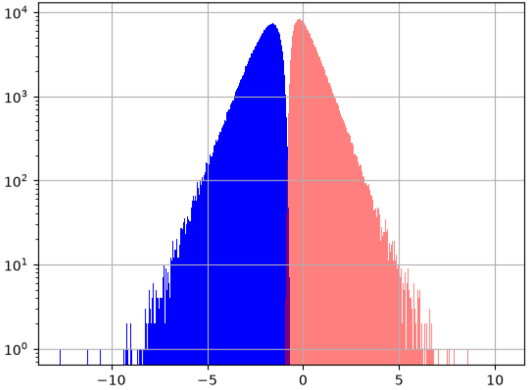
discriminant = covolume = p



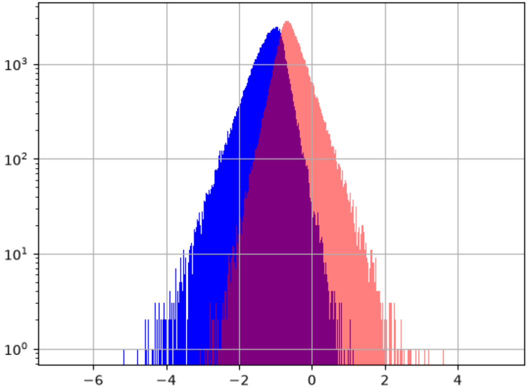


Gaussian heuristic $\Rightarrow$ $d_1 \approx d_2 \approx d_3 \approx d_4 \approx \sqrt{p}$

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?

$$E \xrightarrow{\deg\varphi \approx \sqrt{p}} E'$$

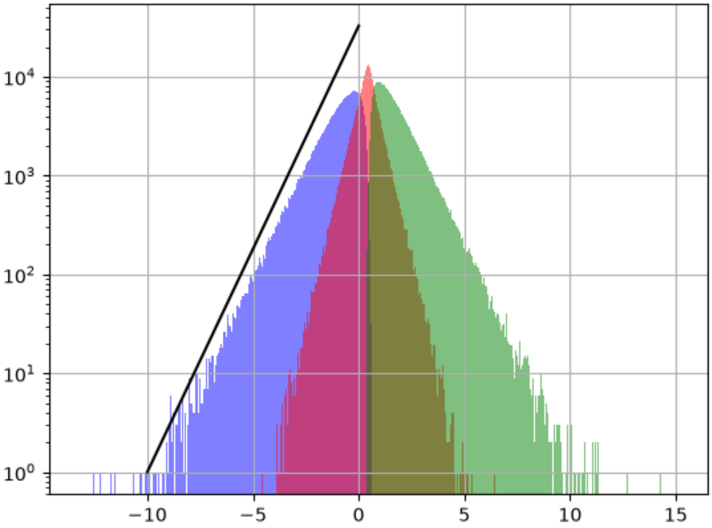
- $O(n)$ isogenies of degree n from E
- $\Rightarrow O(n^2)$ isogenies of degree $\leq n$ from E

How hard is it to find a short isogeny?

$$E \xrightarrow{\qquad p^{1/4} \qquad}\xleftarrow{\qquad p^{1/4} \qquad} E'$$

- $O(n)$ 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

$$
\begin{tikzcd}
 & \mathrm{Hom}(E_1^{(p)}, E_2) \arrow[dl] & \\
\mathrm{Hom}(E_1, E_2) \arrow[dr] \arrow[rr, phantom, "\#"] & & \mathrm{Hom}(E_1^{(p)}, E_2^{(p)}) \arrow[ul] \\
 & \mathrm{Hom}(E_1, E_2^{(p)}) \arrow[ur] &
\end{tikzcd}
$$

Transference

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

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

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

Transference

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

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

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

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

$$1, d_1, d_2, d_3 \qquad d_1^*, d_2^*, d_3^*, d_4^*$$

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

Wesolowski's attack

$$E \xrightarrow{\quad p^{1/3} \quad} E^{(p)}$$

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

Wesolowski's attack

$$E \xrightarrow{\quad p^{1/6} \quad} \; \xleftarrow{\quad p^{1/6} \quad} E^{(p)}$$

- $O(n)$ 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 $O(p^{1/3})$.

Wesolowski's attack

$$\begin{tikzcd} E \arrow[r, "p^{1/6}"] \arrow[rr, bend right, dash, "\pi"'] & {} & E^{(p)} \arrow[l, "p^{1/6}"'] \end{tikzcd}$$

- $O(n)$ 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 $O(p^{1/3})$.

Thank you

`https://defeo.lu/`

@luca_defeo@ioc.exchange

@bsky.defeo.lu