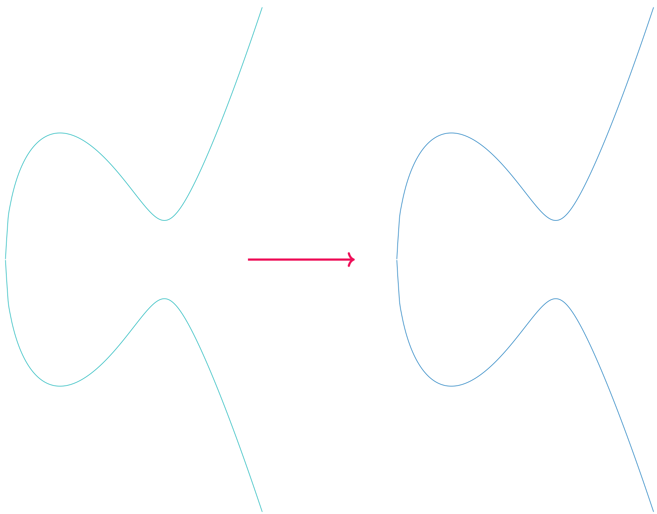
Radical $\sqrt[N]{\text{Vélu}}$ Isogeny Formulae

Thomas Decru

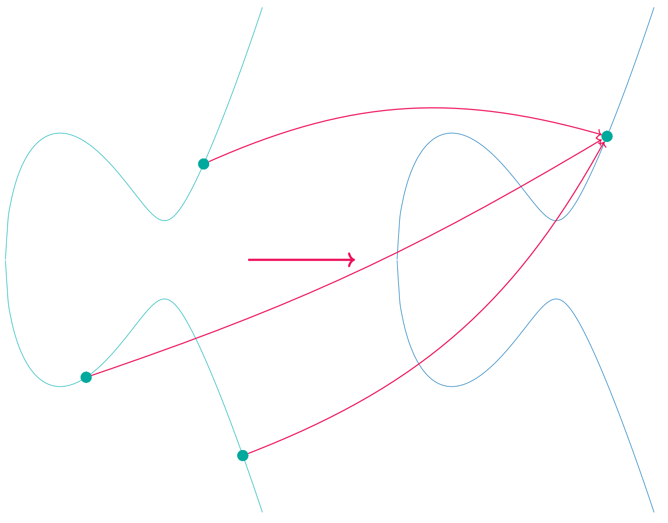
Université Libre de Bruxelles, Belgium

21st of August 2024

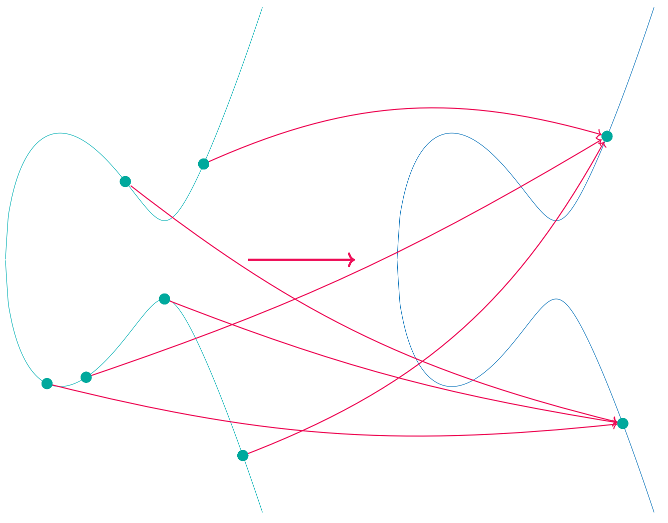
Isogenies



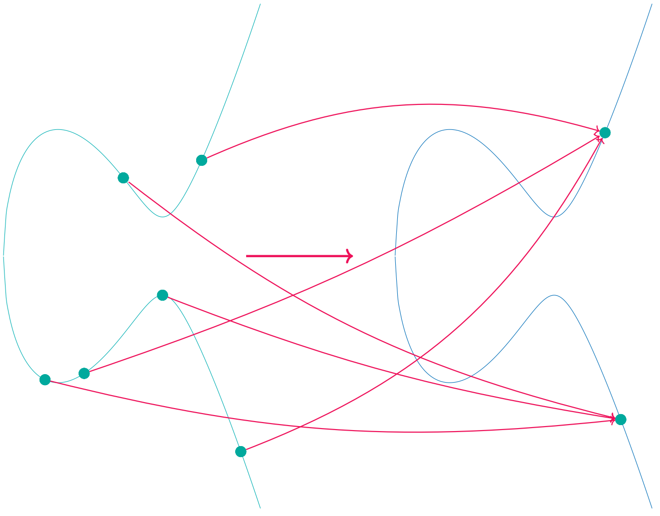
Isogenies



Isogenies

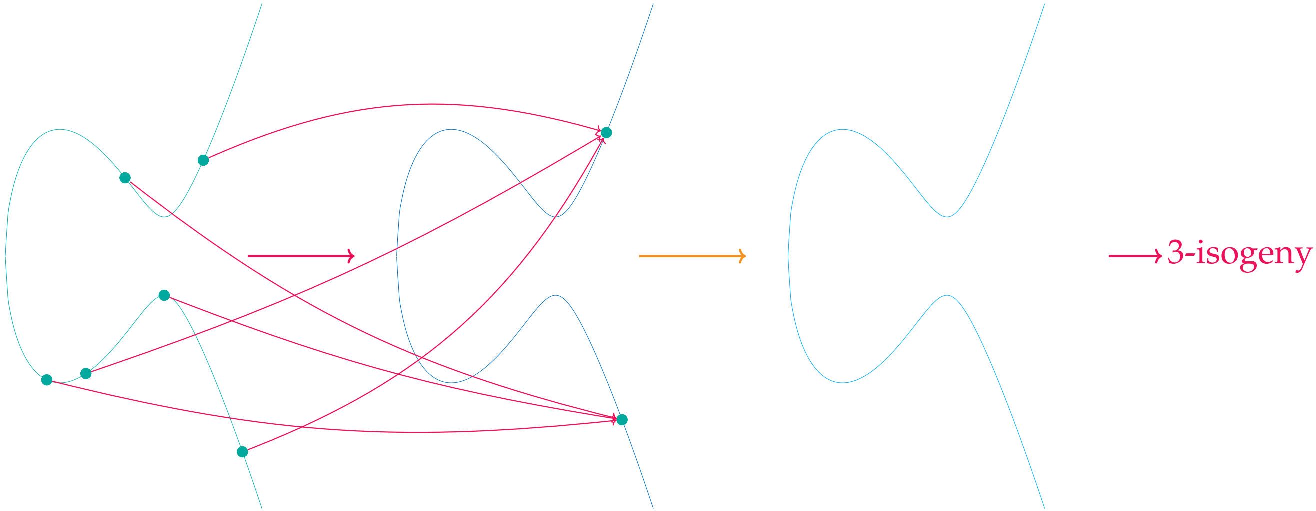


Isogenies

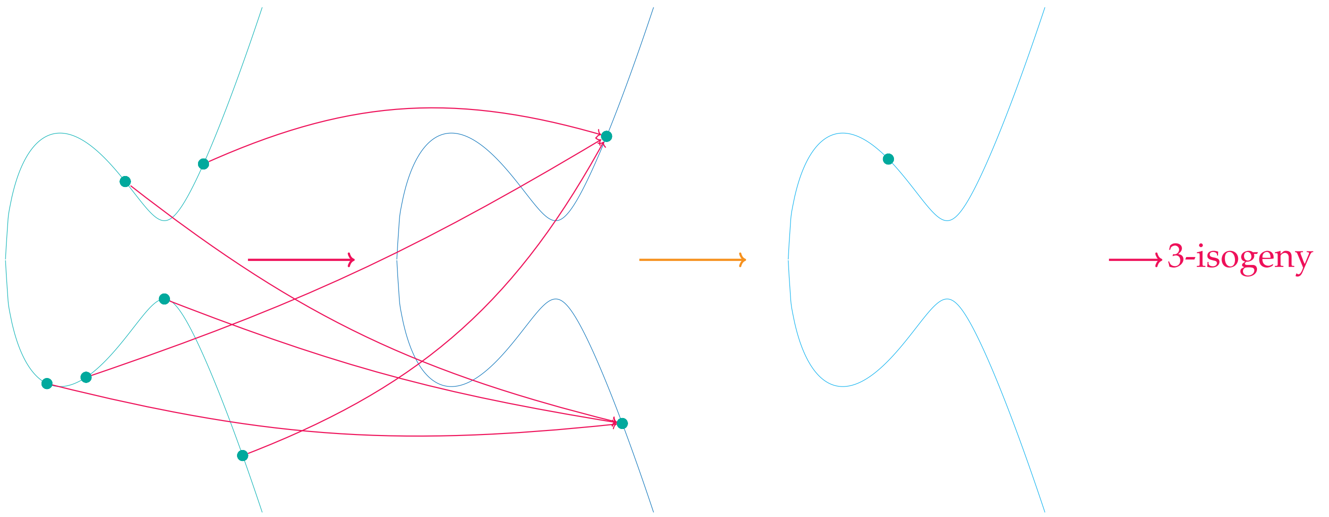


$\longrightarrow$ 3-isogeny

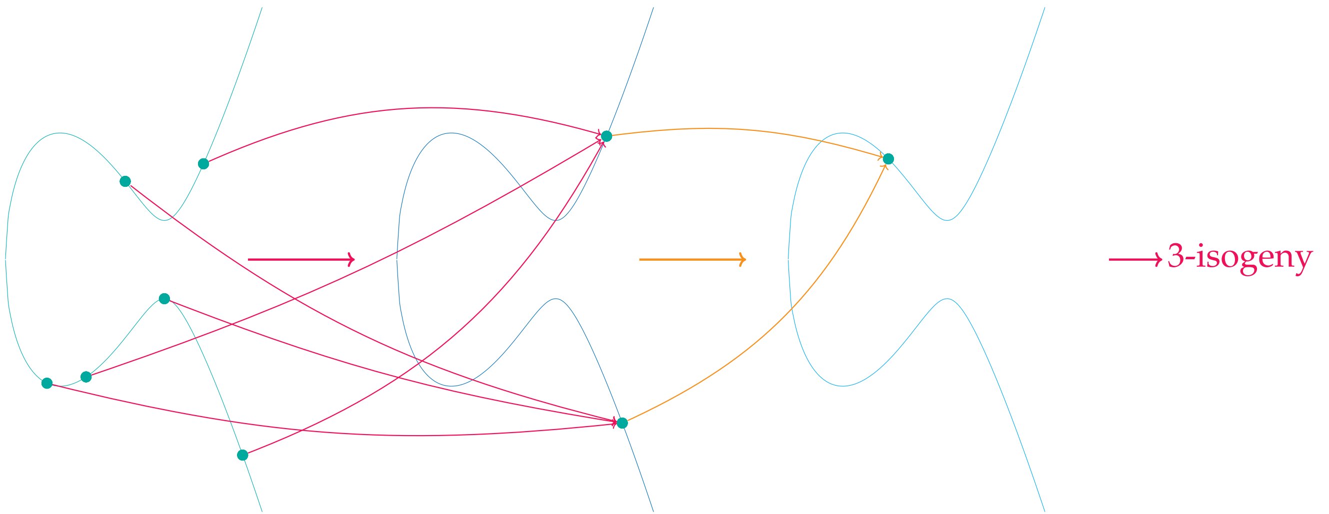
Isogenies



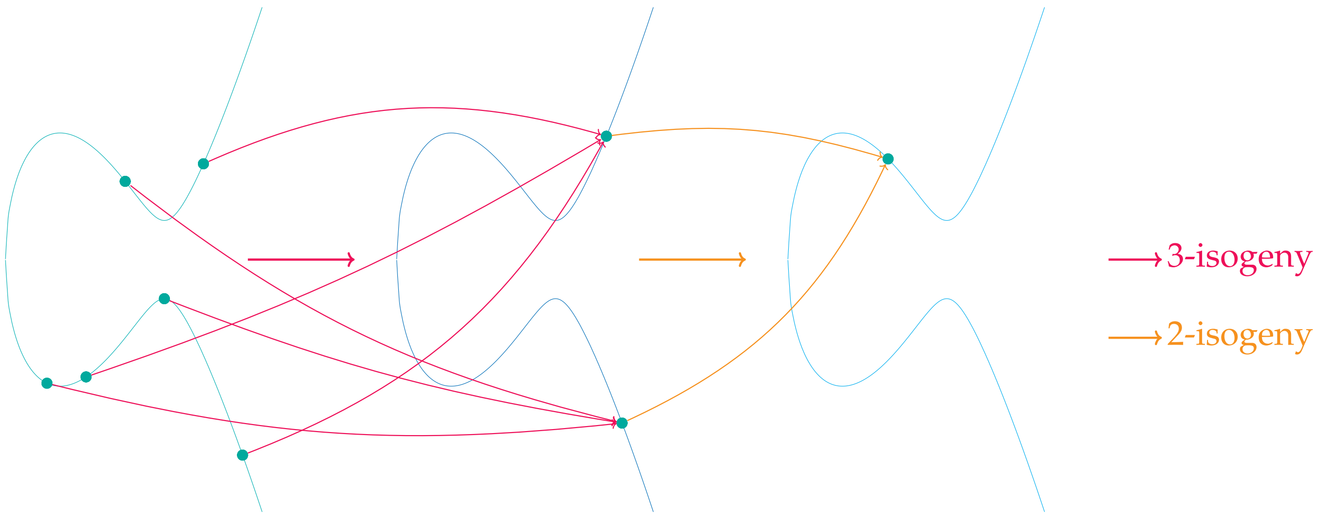
Isogenies



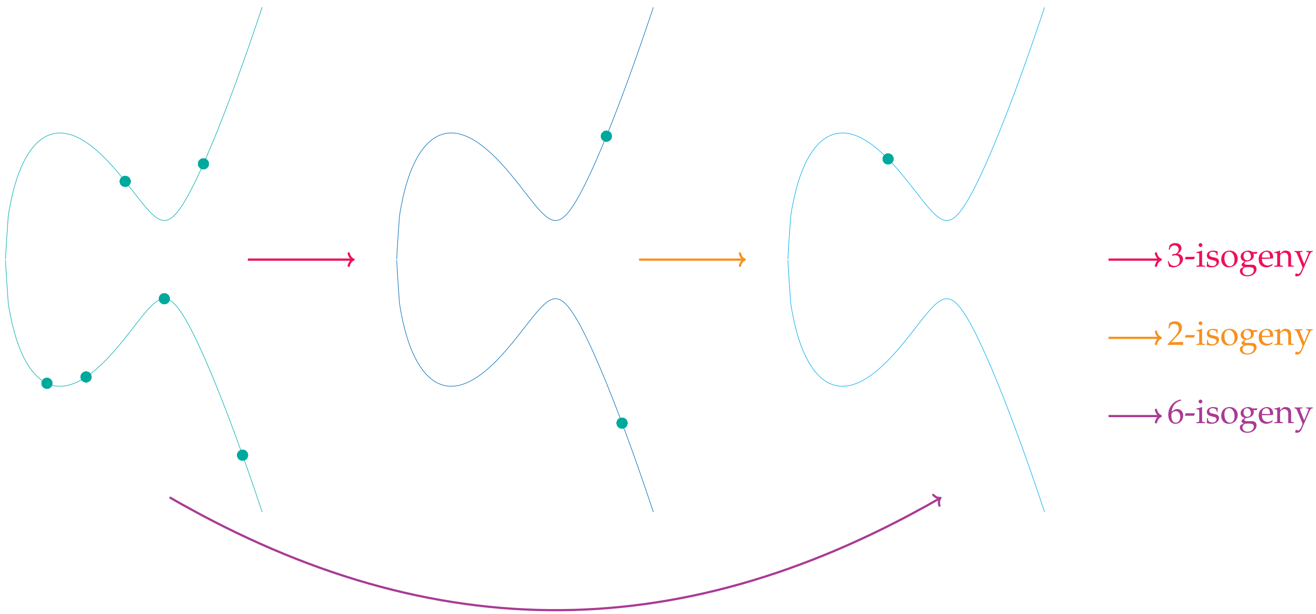
Isogenies



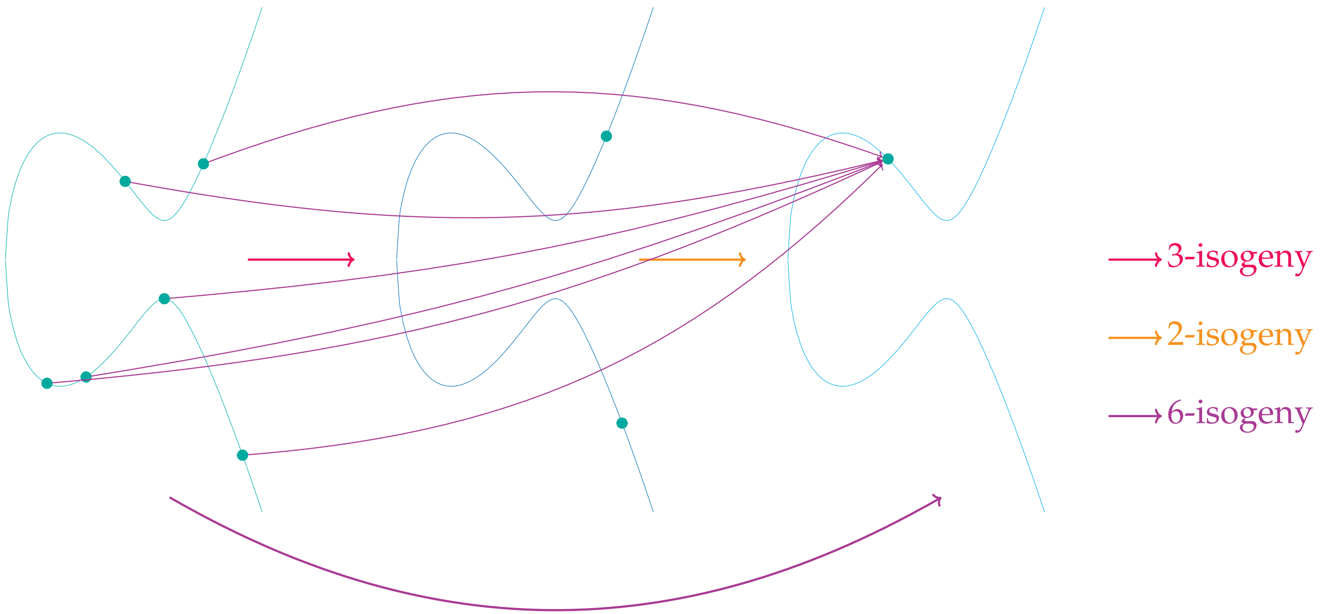
Isogenies



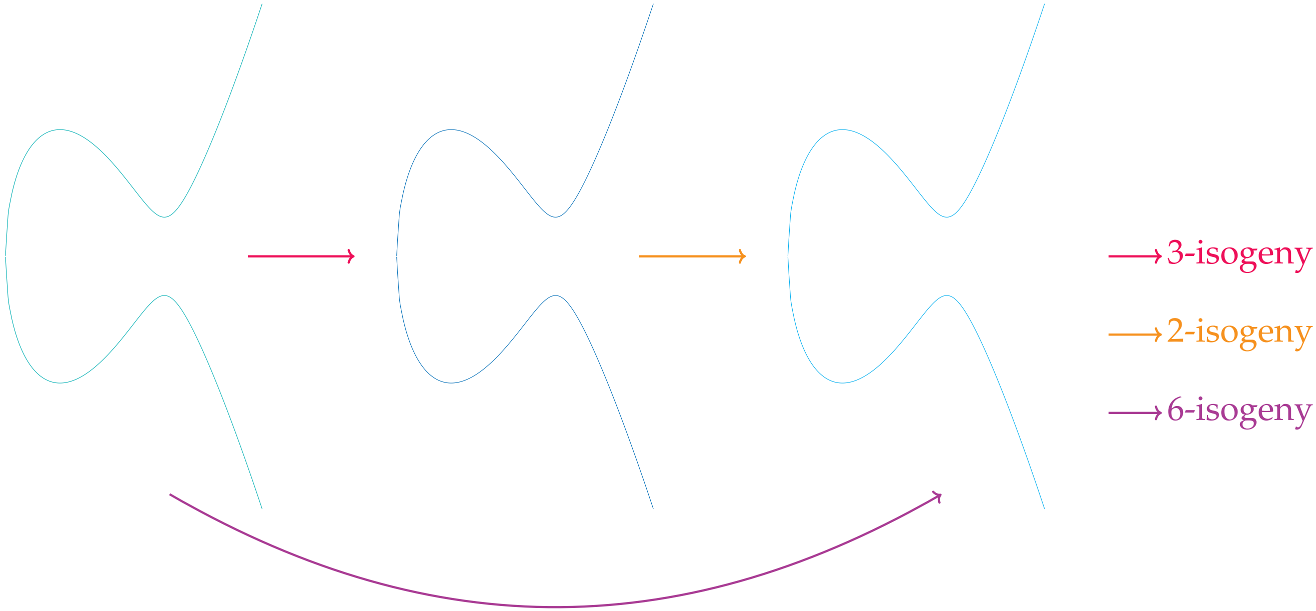
Isogenies



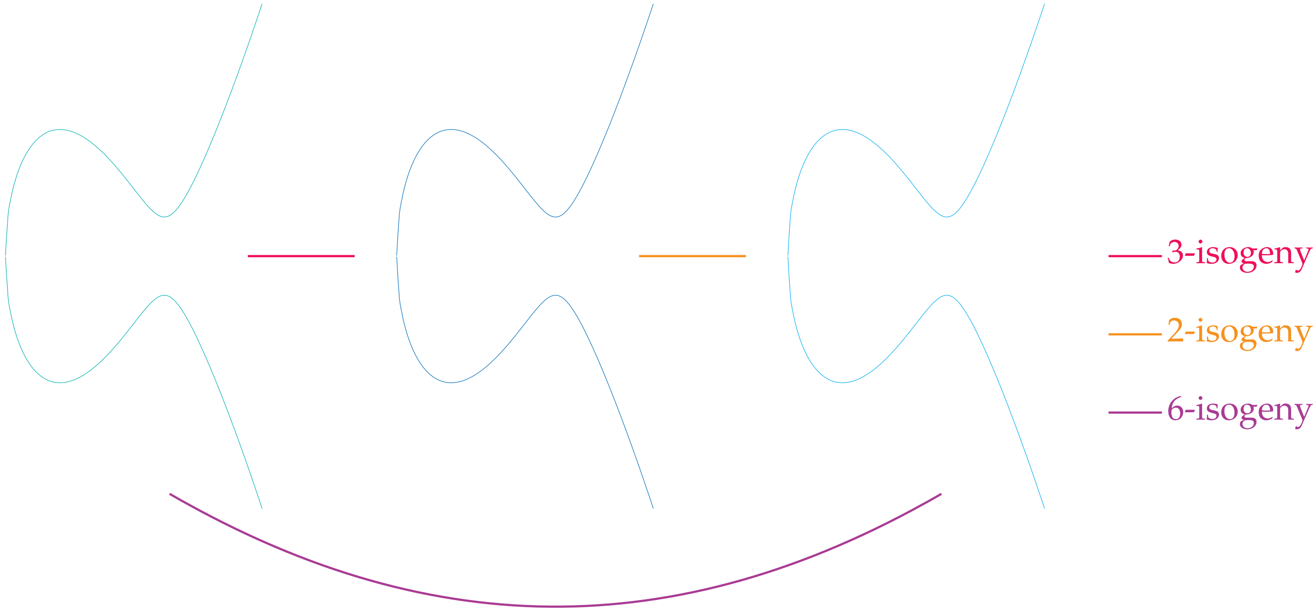
Isogenies



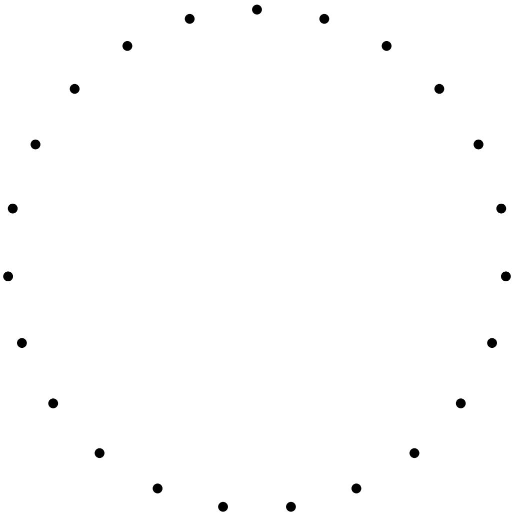
Isogenies



Isogenies

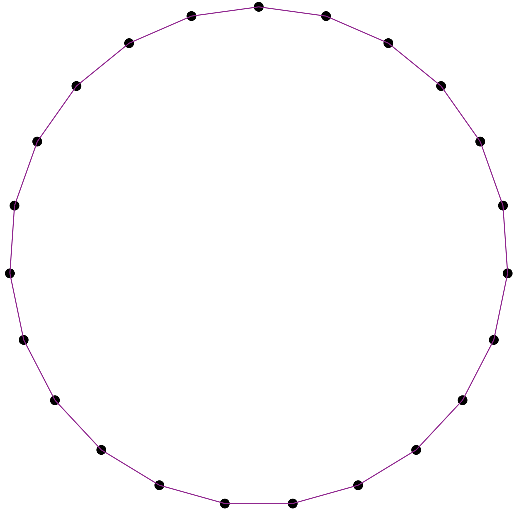


SKETCH OF CSIDH



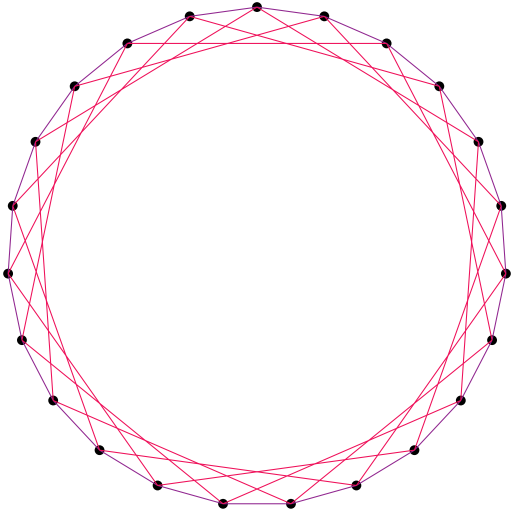
Supersingular elliptic curves over $\mathbb{F}_{647}$ with endomorphism ring $\mathbb{Z}[\sqrt{-647}]$.

Sketch of CSIDH



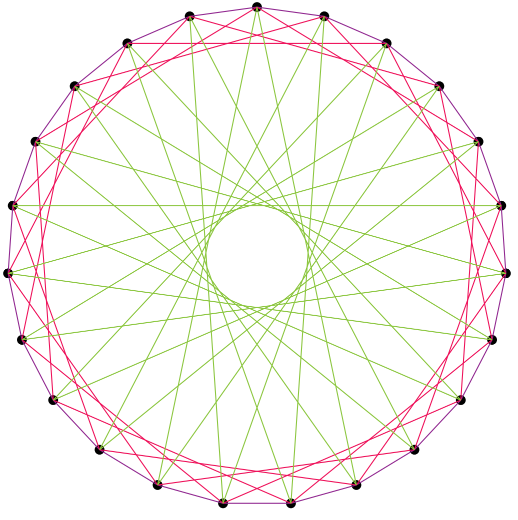
3-isogenies

Sketch of CSIDH



3-isogenies, 5-isogenies

Sketch of CSIDH



3-isogenies, 5-isogenies, 7-isogenies,...

CSIDH

For CSIDH-512 we have

- $p = 4 \cdot \underbrace{3 \cdot 5 \cdot 7 \cdot \ldots 373}_{73 \text{ primes}} \cdot 587 - 1$;
- for each $\ell_i \in \{3, 5, \ldots, 587\}$ we compute at most 5 isogenies of that degree since $11^{74} \approx 2^{255.99}$.

CSIDH

For CSIDH-512 we have

- $p = 4 \cdot \underbrace{3 \cdot 5 \cdot 7 \cdot \ldots 373}_{\text{73 primes}} \cdot 587 - 1;$
- for each $\ell_i \in \{3, 5, \ldots, 587\}$ we compute at most 5 isogenies of that degree since $11^{74} \approx 2^{255.99}$.

Main topic of this talk: how do we compute these ℓ_i-isogenies?

Vélu formulae (classical)

Theorem 1

Let $C = \langle P \rangle$ be a finite subgroup of an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where P is a point of order N, with N odd. Fix a partition $C = \{\mathcal{O}_E\} \cup C^+ \cup C^-$ such that for any $Q \in C^+$ it holds that $-Q \in C^-$. For all $Q \in C^+$ define

$$\begin{aligned}
g_Q^x &= 3x(Q)^2 + 2a_2x(Q) + a_4 - a_1y(Q),\\
g_Q^y &= -2y(Q) - a_1x(Q) - a_3,\\
u_Q &= (g_Q^y)^2, \quad v_Q = 2g_Q^x - a_1g_Q^y\\
v &= \sum_{Q \in C^+} v_Q, \quad w = \sum_{Q \in C^+} (u_Q + x(Q)v_Q).
\end{aligned}$$

Then the separable isogeny φ with domain E and kernel C has codomain

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + (a_4 - 5v)x + a_6 - (a_1^2 + 4a_2) - 7w.$$

Vélu formulae on Montgomery curves

Theorem 2
Let $C = \langle P \rangle$ be a finite subgroup of an elliptic curve

$$E : y^2 = x^3 + a_2 x^2 + x,$$

where P is a point of order N, with N odd. Define

$$\varpi = \prod_{Q \in C \setminus \{\infty\}} x(Q),$$

$$\sigma = \sum_{Q \in C \setminus \{\infty\}} \left(x(Q) - \frac{1}{x(Q)} \right).$$

Then the separable isogeny φ with domain E and kernel C has codomain (up to isomorphism)

$$E' : y^2 = x^3 + \varpi(a_2 - \sigma) x^2 + x.$$

CSIDH-512 ORIGINAL IMPLEMENTATION

For CSIDH-512:

- $\ell_i \in \{3, 5, \ldots, 587\}$ use $\mathcal{O}(\ell_i)$ Vélu formulae.

CSIDH-512 original implementation

For CSIDH-512:

- $\ell_i \in \{3, 5, \ldots, 587\}$ use $\mathcal{O}(\ell_i)$ Vélu formulae.

Remark that

- each isogeny requires sampling an ℓ_i-torsion point (expensive since $\mathcal{O}(\log(p))$);
- trade-off for this can be made by mapping points through isogenies.

Vélu-sqrt formulae

Major breakthrough in computing isogenies: only requires $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ operations!

General idea:

- baby-step giant-step;
- combine with a resultant computation.

Vélu-sqrt formulae

Major breakthrough in computing isogenies: only requires $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ operations!

General idea:

- baby-step giant-step;
- combine with a resultant computation.

For CSIDH-512:

- $\ell_i \in \{3, 5, \ldots, 101\}$ use $\mathcal{O}(\ell_i)$ Vélu formulae;
- $\ell_i \in \{103, 107, \ldots, 587\}$ use $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ Vélu-sqrt formulae.

CSURF AKA RADICAL 2-ISOGENIES

$$E : y^2 = x^3 + Ax^2 + x \qquad \longrightarrow \qquad E' : y^2 = x^3 + \underbrace{2(3 + A(\sqrt{A^2 - 4} - A))}_{:=A'} x^2 + x$$

CSURF AKA RADICAL 2-ISOGENIES

$$E : y^2 = x^3 + Ax^2 + x \qquad \longrightarrow \qquad E' : y^2 = x^3 + \underbrace{2(3 + A(\sqrt{A^2 - 4} - A))}_{:=A'} x^2 + x$$

Cost comparison:

- 2-isogeny: one exponentiation $\alpha^{(p+1)/4} \sim 1.5 \log p$ multiplications by square-and-multiply;
- generating 2-torsion point $\sim 11 \log p$ multiplications in Montgomery ladder.

Radical 3-isogenies

A radical 3-isogeny can be written as

$$E : y^2 + a_1xy + a_3y = x^3 \qquad \longrightarrow \qquad E' : y^2 + \underbrace{(-6\alpha + a_1)}_{:=a_1'}xy + \underbrace{(3a_1\alpha^2 - a_1^2\alpha + 9a_3)}_{:=a_3'}y = x^3$$

where $\alpha = \sqrt[3]{a_3}$.

Radical 5-isogenies

A radical 5-isogeny can be written as

$$E : y^2 + (1-b)xy - by = x^3 - bx^2 \qquad \longrightarrow \qquad E' : y^2 + (1-b')xy - b'y = x^3 - b'x^2$$

where

$$b' = \alpha \frac{\alpha^4 + 3\alpha^3 + 4\alpha^2 + 2\alpha + 1}{\alpha^4 - 2\alpha^3 + 4\alpha^2 - 3\alpha + 1}$$

and $\alpha = \sqrt[5]{b}$.

RADICAL ISOGENIES

	Operation count	Cost relative to 2-isogeny
2-isogeny	**E** + **M**	1
3-isogeny	**E** + 2**M**	1.023
5-isogeny	**E** + 6**M**	1.034
7-isogeny	**E** + 12**M**	1.043
11-isogeny	**E** + 50**M**	1.293
13-isogeny	**E** + 89**M**	1.448
17-isogeny	**E** + 217**M**	1.921
19-isogeny	**E** + 329**M**	2.532

Radical isogenies

	Operation count	Cost relative to 2-isogeny
2-isogeny	**E** + **M**	1
3-isogeny	**E** + 2**M**	1.023
5-isogeny	**E** + 6**M**	1.034
7-isogeny	**E** + 12**M**	1.043
11-isogeny	**E** + 50**M**	1.293
13-isogeny	**E** + 89**M**	1.448
17-isogeny	**E** + 217**M**	1.921
19-isogeny	**E** + 329**M**	2.532

For CSIDH-512:

- $\ell_i \in \{2, 3, 5, \ldots, 19\}$ use radical isogenies;
- $\ell_i \in \{23, 29, \ldots, 101\}$ use $\mathcal{O}(\ell_i)$ Vélu formulae;
- $\ell_i \in \{103, 107, \ldots, 409\}$ use $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ Vélu-sqrt formulae.

Consider

$$E_{b,c} \xrightarrow{\varphi} E' \xrightarrow[\sim]{\iota} E_{b',c'},$$

where

- $E_{b,c}$ and $E_{b',c'}$ are in Tate normal form;
- φ is the isogeny computed with classical Vélu formulae;
- ι is an isomorphism putting E' into Tate normal form.

Radical $\sqrt[N]{\text{élu}}$ isogenies

Define $\varpi_0 = 2$ and for all $i \geq 1$ define

$$\varpi_i = \prod_{k=1}^{i} x(k(0,0)),$$

where we use the conventions $x((0,0)) = 1 = x((0,b))$ and $x(N(0,0)) = b^2$.

Choose

$$t_N((0,0),(0,b)) = \tau_N := -(b^2\varpi_N)^{-1}.$$

Then (conjectured), with $\alpha = \sqrt[N]{\tau_N}$, we have that ι is defined by

$$u = 1 + 3b\sum_{i=1}^{N-2}\varpi_i\alpha^i - \sum_{i=1, i\neq N-3}^{N-1}\varpi_i\varpi_{i+1}\varpi_{i+2}\alpha^{3i},$$

$$s = b\sum_{i=1}^{N-2}\varpi_i\alpha^i - b^3\sum_{i=2}^{N-1}\varpi_{2i}\varpi_{2i+1}\varpi_{N-i-1}\varpi_{N-i}\alpha^{2(N+i)}.$$

Proposition 1

Let $E/\mathbb{F}_q$ be an elliptic curve and $N \geq 5$ an odd integer such that $\gcd(q-1, N) = 1$ and char$(\mathbb{F}_q) \nmid N$, and assume that the formulae for u and s are true. Then the cyclic N^k-isogeny obtained by iteratively mapping $(b, c) \mapsto (b', c')$ can be computed in $(2\log(q) + \mathcal{O}(N))k$ basic $\mathbb{F}_q$-operations.

Proposition 1

Let $E/\mathbb{F}_q$ be an elliptic curve and $N \geq 5$ an odd integer such that $\gcd(q-1, N) = 1$ and char$(\mathbb{F}_q) \nmid N$, and assume that the formulae for u and s are true. Then the cyclic N^k-isogeny obtained by iteratively mapping $(b, c) \mapsto (b', c')$ can be computed in $(2\log(q) + \mathcal{O}(N))k$ basic $\mathbb{F}_q$-operations.

Remarks:

- $2\log(q)$ factor is an upperbound for the exponentiation;
- hidden constant in $\mathcal{O}(N)$ is 16 for **M**.

.

Radical $\sqrt[N]{\text{Vélu}}$ isogenies

For CSIDH-512:

- $\ell_i \in \{2, 3, 5, \ldots, 199\}$ use radical (Vélu) isogenies;
- $\ell_i \in \{211, 223, \ldots, 409\}$ use $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ Vélu-sqrt formulae.

Radical $\sqrt[N]{\text{élu}}$ isogenies

For CSIDH-512:

- $\ell_i \in \{2, 3, 5, \ldots, 199\}$ use radical (Vélu) isogenies;
- $\ell_i \in \{211, 223, \ldots, 409\}$ use $\widetilde{\mathcal{O}}(\sqrt{\ell_i})$ Vélu-sqrt formulae.

Results:

- 35% speedup over previous (limited) radicals in CSIDH-512;
- 64% speedup overall compared to no radicals;
- 64% is stable for larger parameters too.

Further research options

Mathematically:

- Proof?
- Case N even?

Cryptographically:

- Most efficient formulae?
- Constant time version?

ia.cr/2024/878

thomas.decru@ulb.be