Setting the Stage: Isogeny-Based Cryptography

Rank-one tensor completion (SIAGA 1, 2017)

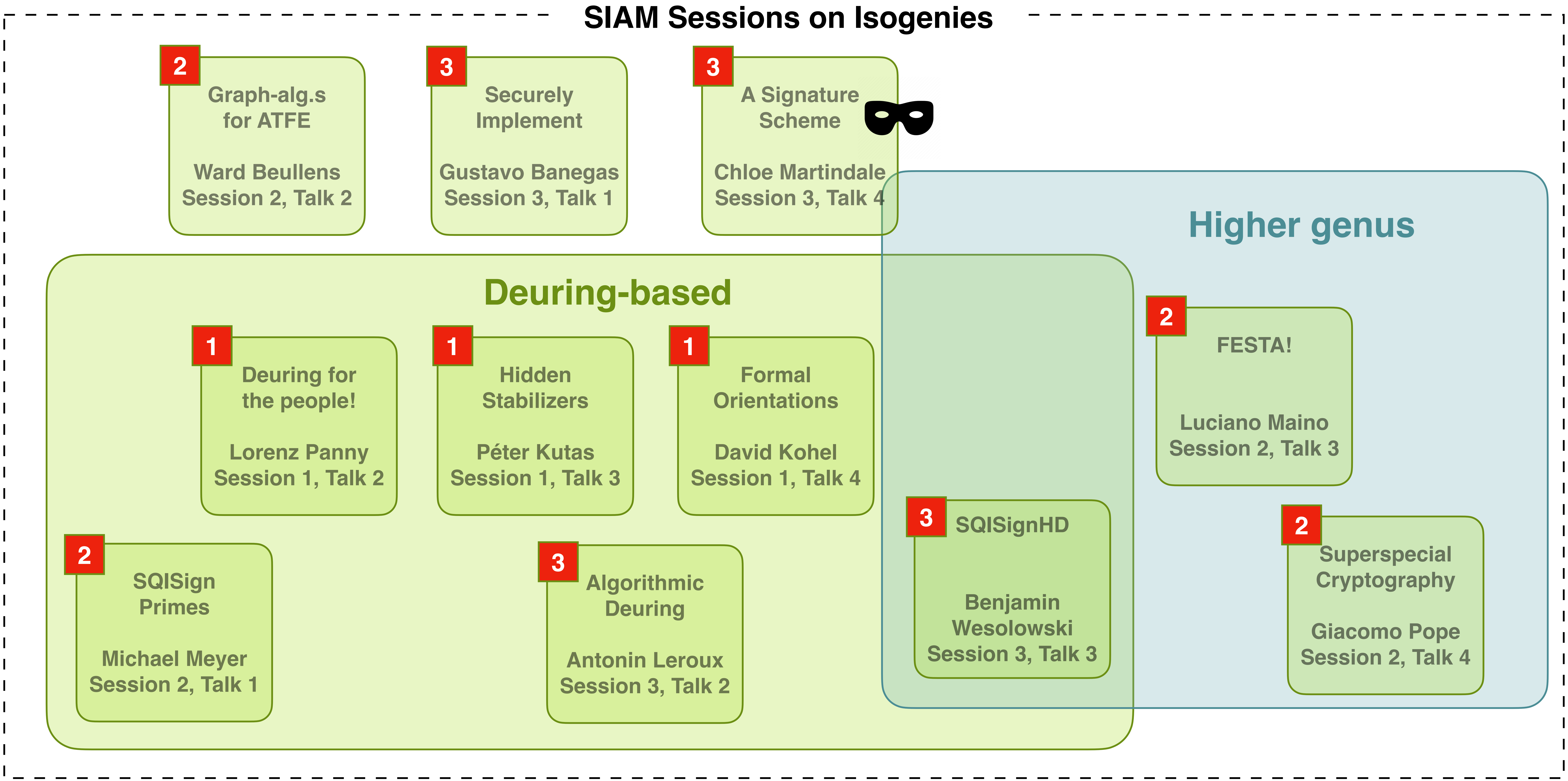
Monika Trimoska and Krijn Reijnders

SIAM AG - Applications of Isogenies in Cryptography

July 13th, 2023

Radboud University

A rough overview on the three sessions



SIAM Sessions on Isogenies

2 Graph-alg.s for ATFE
Ward Beullens
Session 2, Talk 2

3 Securely Implement
Gustavo Banegas
Session 3, Talk 1

3 A Signature Scheme
Chloe Martindale
Session 3, Talk 4

Higher genus

Deuring-based

1 Deuring for the people!
Lorenz Panny
Session 1, Talk 2

1 Hidden Stabilizers
Péter Kutas
Session 1, Talk 3

1 Formal Orientations
David Kohel
Session 1, Talk 4

2 FESTA!
Luciano Maino
Session 2, Talk 3

3 SQISignHD
Benjamin Wesolowski
Session 3, Talk 3

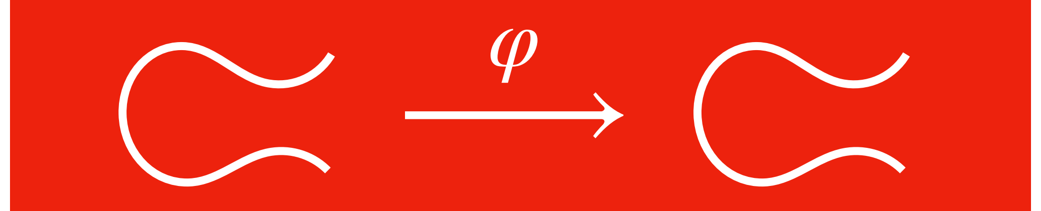
2 SQISign Primes
Michael Meyer
Session 2, Talk 1

3 Algorithmic Deuring
Antonin Leroux
Session 3, Talk 2

2 Superspecial Cryptography
Giacomo Pope
Session 2, Talk 4

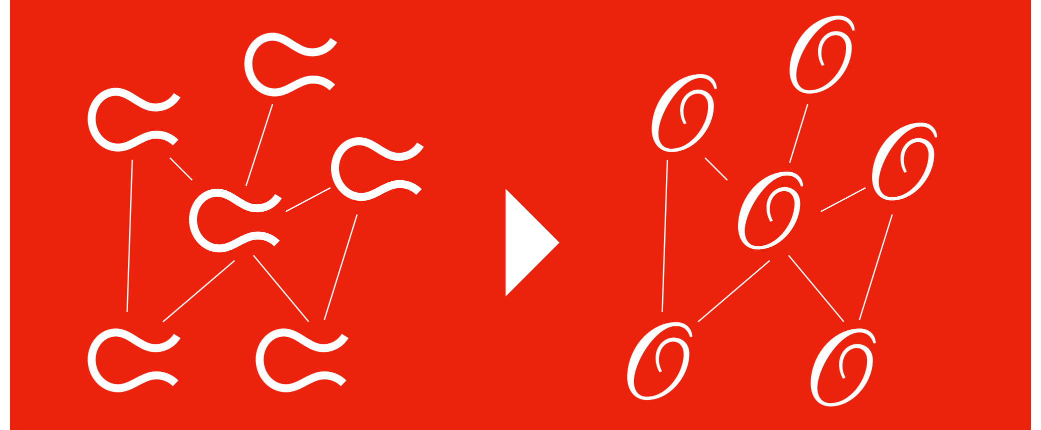
Setting the stage: going over the basics

1



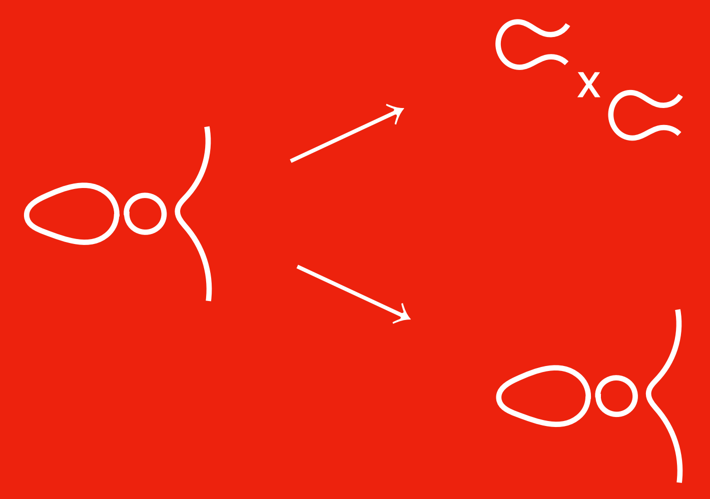
Isogenies

2



The Deuring Correspondence

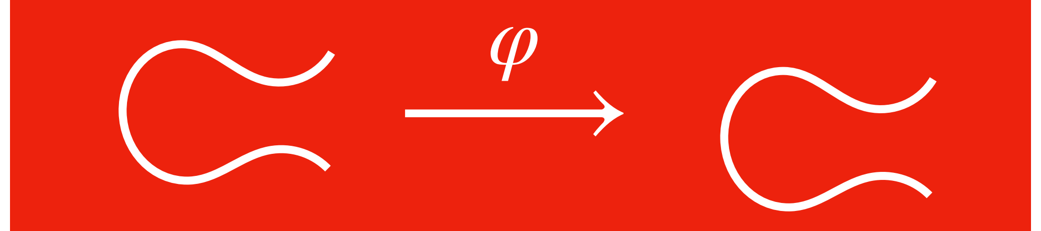
3



Isogenies in dimension 2

Isogenies 101

1



Isogenies

Elliptic curve

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

$$E \xrightarrow{\varphi} E'$$

Another curve

$E' : y^2 = x^3 - 3x + 3$

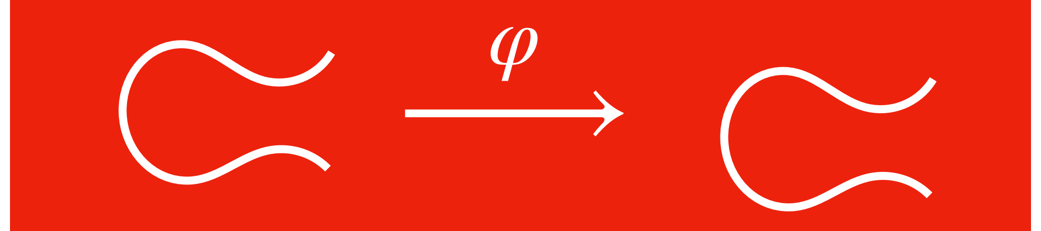
$P, Q \in E$

Isogeny

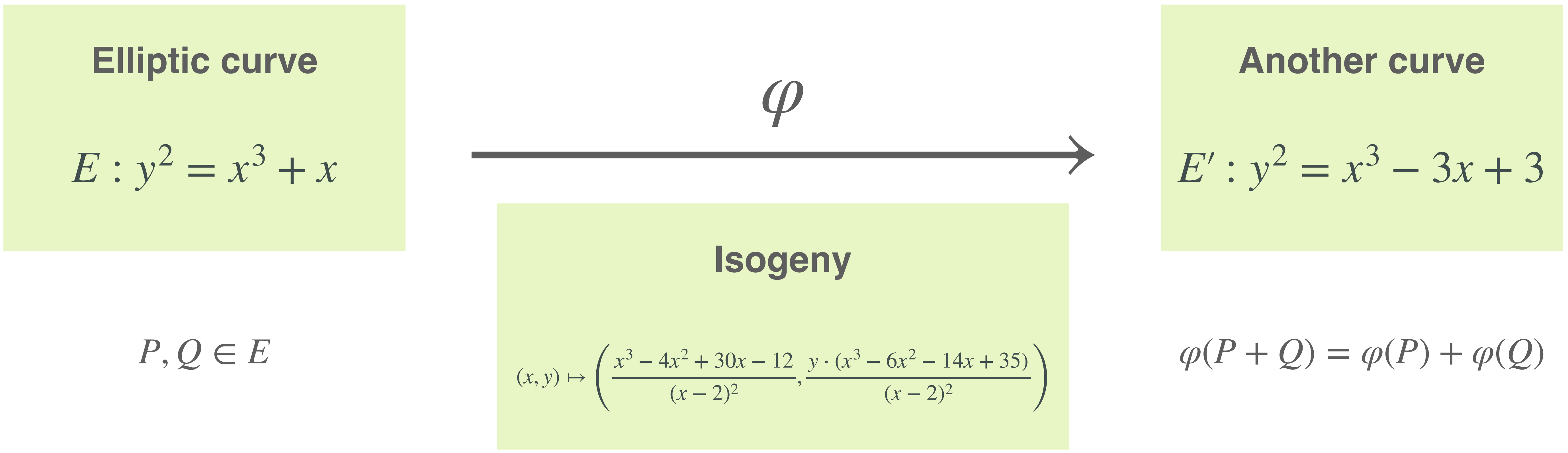
$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

1



Isogenies



Elliptic curve

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

$$E \xrightarrow{\varphi} E'$$

Another curve

$E' : y^2 = x^3 - 3x + 3$

$P, Q \in E$

Isogeny

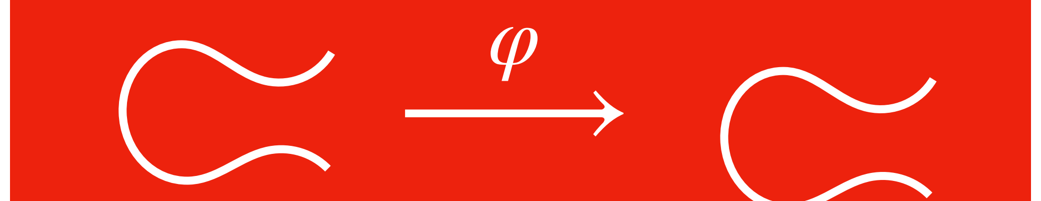
$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

Endomorphism

$\varphi : E \to E$

1



Isogenies

Elliptic curve

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

$$\xrightarrow{\varphi}$$

Another curve

$$E' : y^2 = x^3 - 3x + 3$$

$$P, Q \in E$$

Isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

Endomorphism

$$\varphi : E \to E$$

1

$$[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$$

2

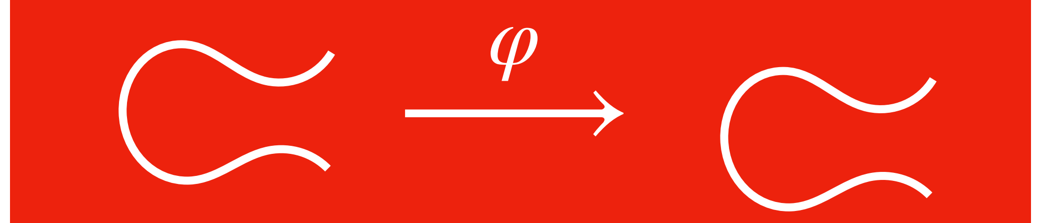
$$\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$$

1
2

Ordinary elliptic curve

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$$

1



Isogenies

Elliptic curve

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

$$\xrightarrow{\varphi}$$

Another curve

$E' : y^2 = x^3 - 3x + 3$

Isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

$P, Q \in E$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

Endomorphism

$\varphi : E \to E$

1 $[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

2 $\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

? other endomorphisms?

$\varphi : E \to E$

1
2

Ordinary elliptic curve

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

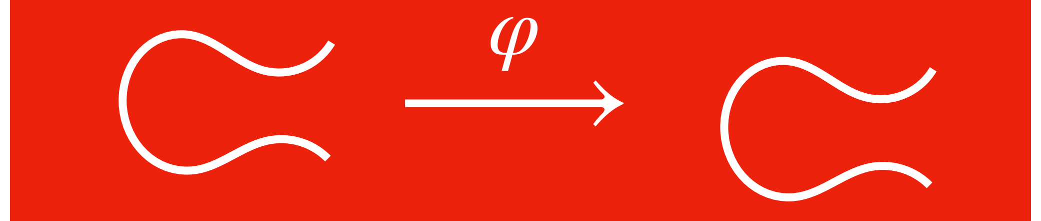
1
2
3
4

Supersingular elliptic curve

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathcal{B}_{p,\infty}$

1



Isogenies

Elliptic curve

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

$P, Q \in E$

$$\xrightarrow{\varphi}$$

Isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{y \cdot (x^3 - 6x^2 - 14x + 35)}{(x-2)^2} \right)$$

Another curve

$E' : y^2 = x^3 - 3x + 3$

$\varphi(P + Q) = \varphi(P) + \varphi(Q)$

Endomorphism

$\varphi : E \to E$

1

$[N] : E \to E, \quad P \mapsto \underbrace{P + \ldots + P}_{N \text{ times}}$

2

$\pi : E \to E, \quad (x, y) \mapsto (x^q, y^q)$

?

other endomorphisms?

$\varphi : E \to E$

1 2

Ordinary elliptic curve

$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$

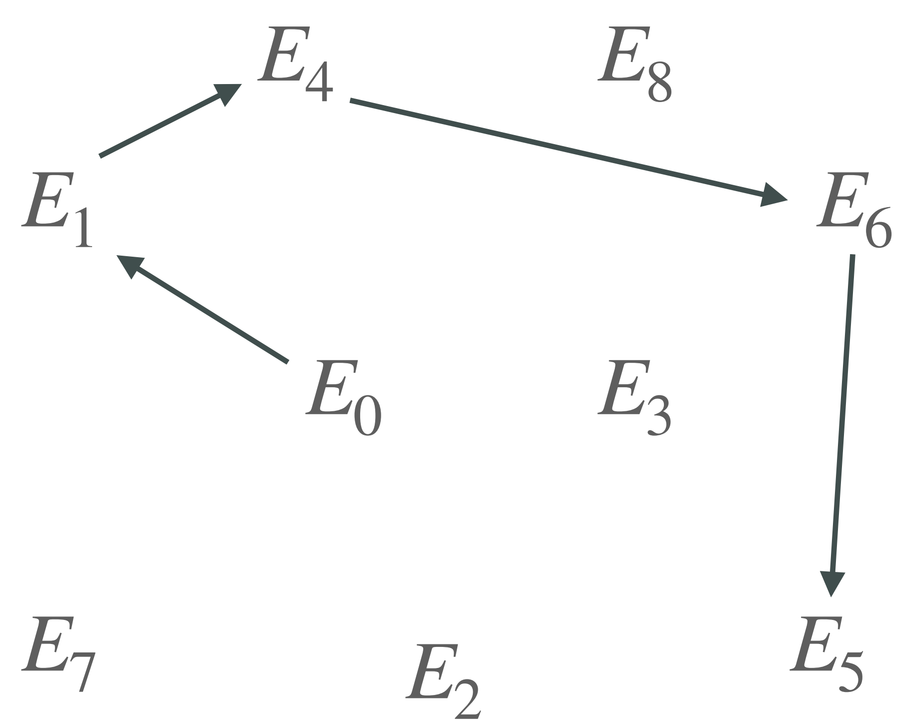
1 2 3 4

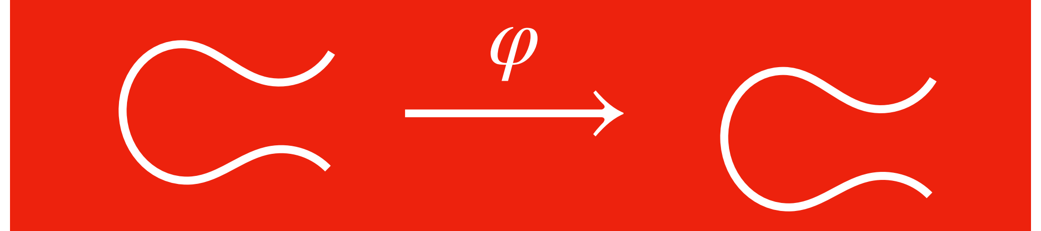
Supersingular elliptic curve

non-commutative maximal order

$\mathrm{End}(E) \subseteq \mathscr{B}_{p,\infty}$

isogeny-based crypto

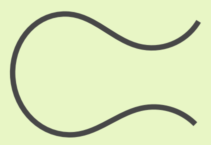




Isogenies

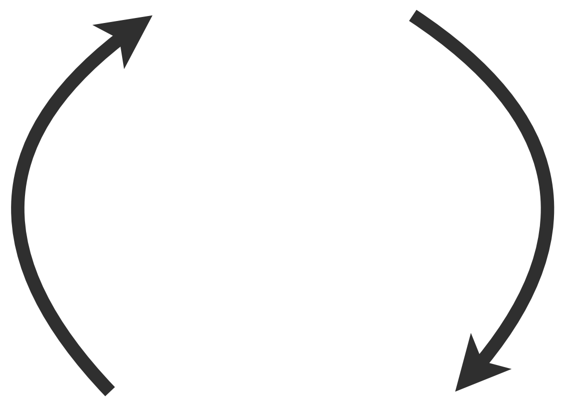
EndRing Problem

Given: a supersingular curve E



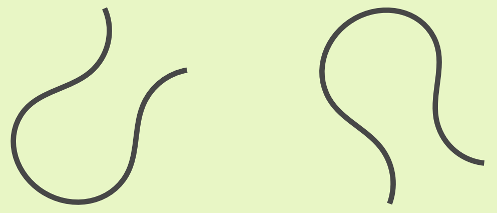
Find: a basis of $\mathrm{End}(E)$:

$$\mathrm{End}(E) = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \mathbb{Z}\alpha_3 \oplus \mathbb{Z}\alpha_4$$



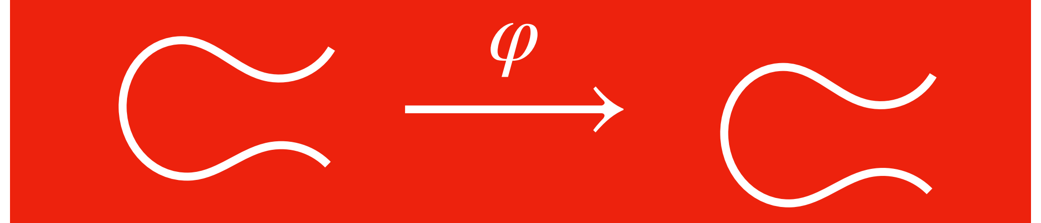
Isogeny Path Problem

Given: two supersingular curves E and E'



Find: an isogeny φ from E to E'

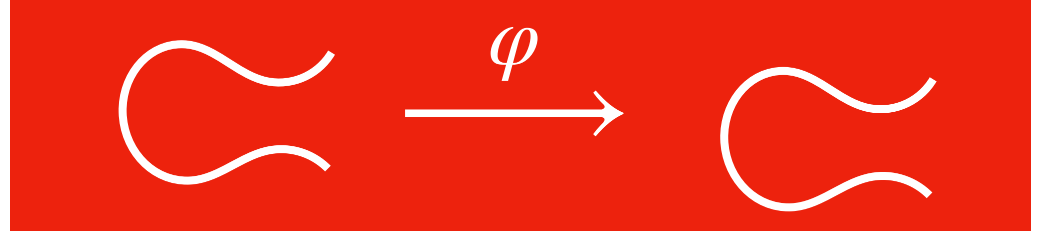
1



Isogenies

$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

1

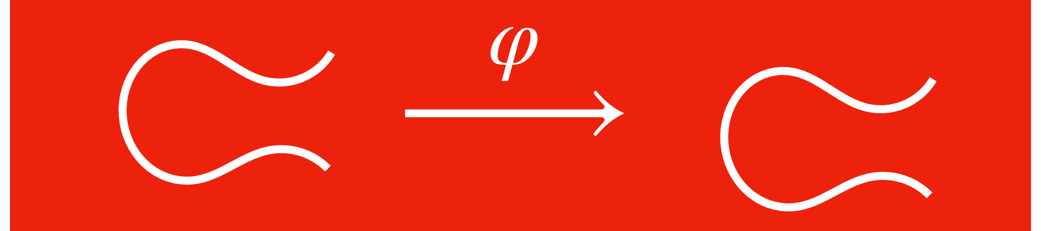


Isogenies

$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ ≋ ❤

1



Isogenies

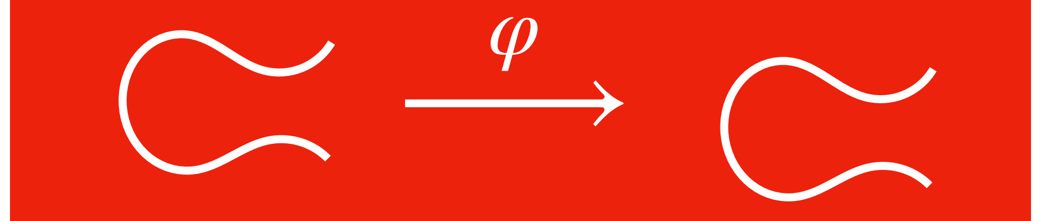
$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ ≋ ❤

Action of the class group

$$\star : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) \to \mathrm{Ell}_{\mathcal{O}}(p)$$
$$(\mathfrak{a}, E) \mapsto \mathfrak{a} \star E$$

1



Isogenies

$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

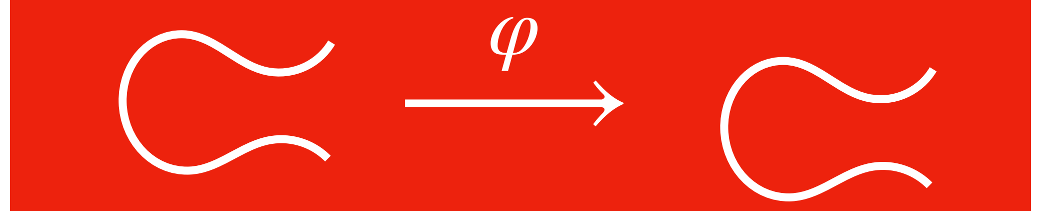
$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ ≋ ❤

Action of the class group

The ideal class group of $\mathcal{O}$
(It is a finite abelian group)

Set of $\mathcal{O}$-oriented
elliptic curves

$$\star : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) \to \mathrm{Ell}_{\mathcal{O}}(p)$$
$$(\mathfrak{a}, E) \mapsto \mathfrak{a} \star E$$



$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ ≋ ❤

Action of the class group

The ideal class group of $\mathcal{O}$
(It is a finite abelian group)

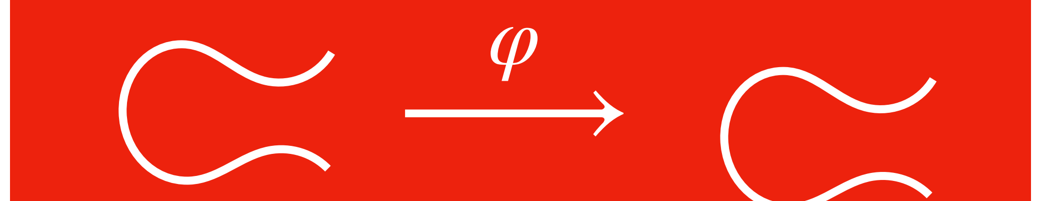
Set of $\mathcal{O}$-oriented
elliptic curves

$$\star : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) \to \mathrm{Ell}_{\mathcal{O}}(p)$$
$$(\mathfrak{a}, E) \mapsto \mathfrak{a} \star E$$

→ $\mathfrak{b} \star (\mathfrak{a} \star E) = (\mathfrak{b}\mathfrak{a}) \star E$

→ $e \star E = E$

1



Isogenies

$\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E)\backslash\mathbb{Z}$
is a subring of dimension 2
(a quadratic subring)

CSIDH

$\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ ≋ ❤

Action of the class group

The ideal class group of $\mathcal{O}$
(It is a finite abelian group)

Set of $\mathcal{O}$-oriented
elliptic curves

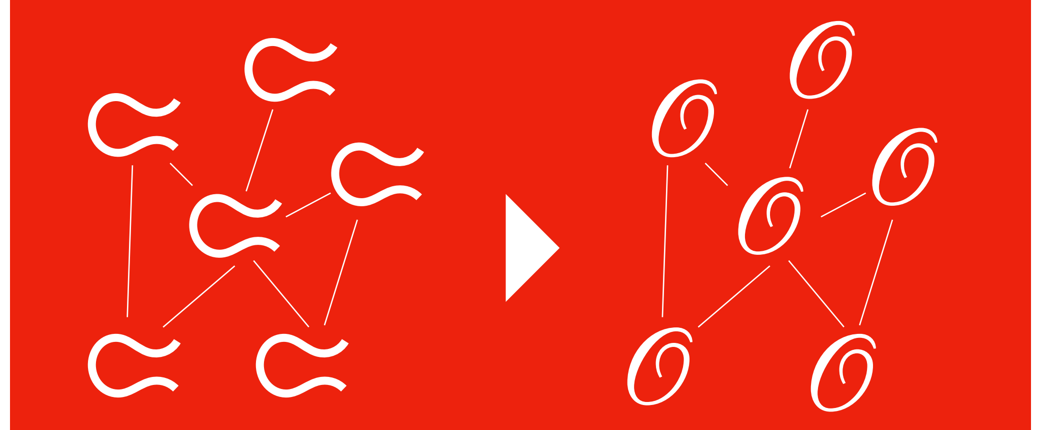
$$\star : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) \to \mathrm{Ell}_{\mathcal{O}}(p)$$
$$(\mathfrak{a}, E) \mapsto \mathfrak{a} \star E$$

→ $\mathfrak{b} \star (\mathfrak{a} \star E) = (\mathfrak{b}\mathfrak{a}) \star E$

→ $e \star E = E$

Deuring 101

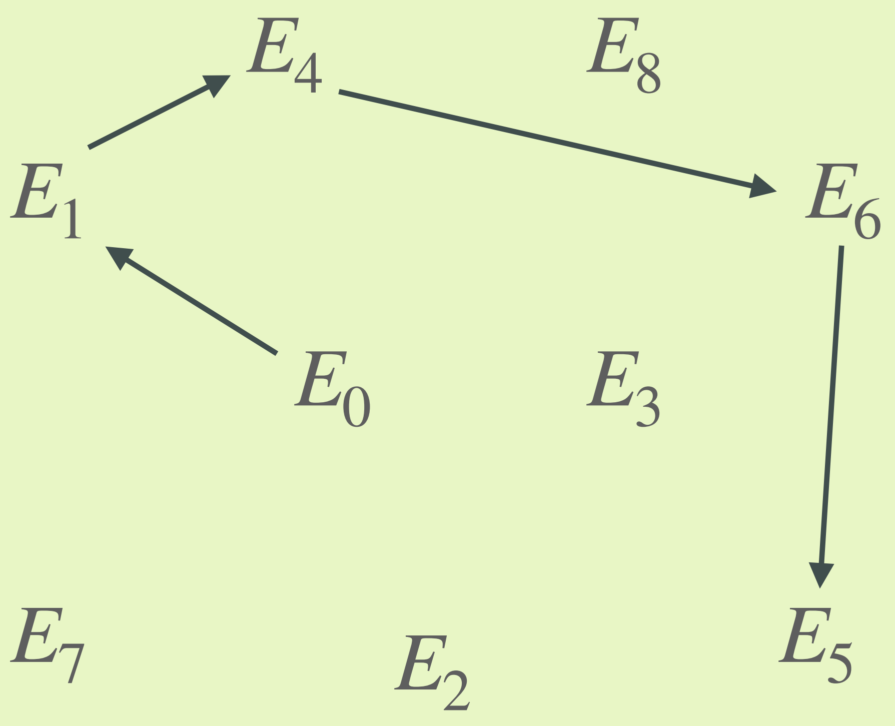
2



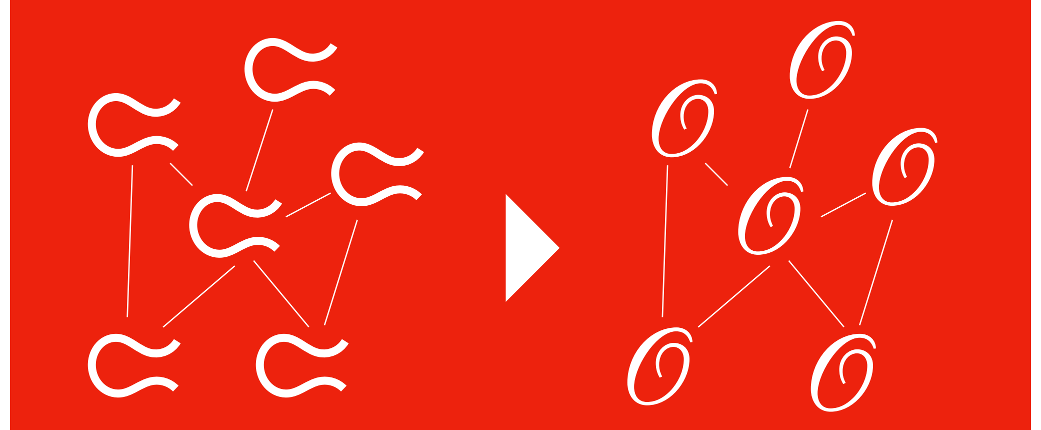
The Deuring Correspondence

Deuring correspondence

world of supersingular curves



2

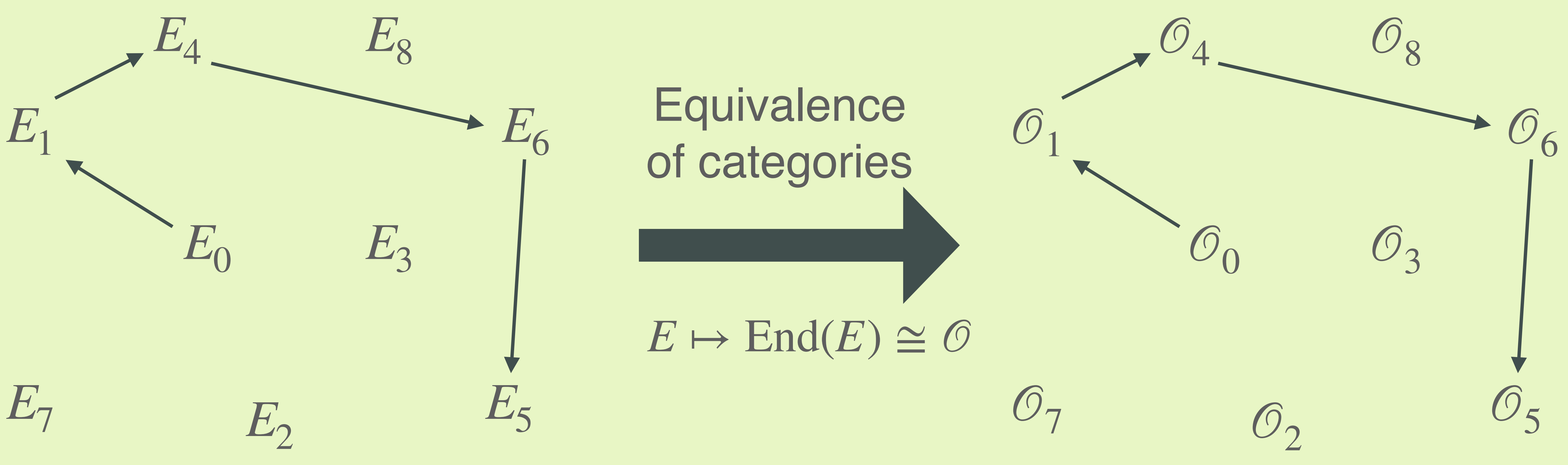


The Deuring Correspondence

Deuring correspondence

world of supersingular curves

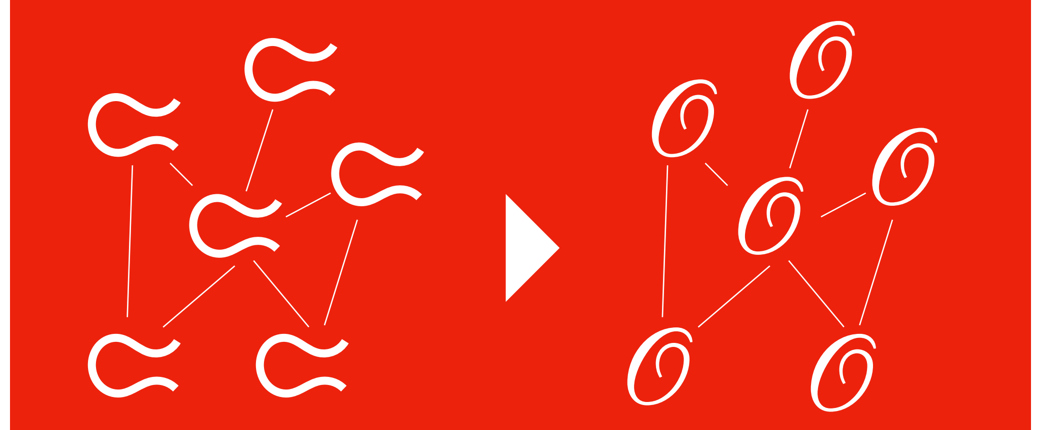
world of maximal orders



Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

2

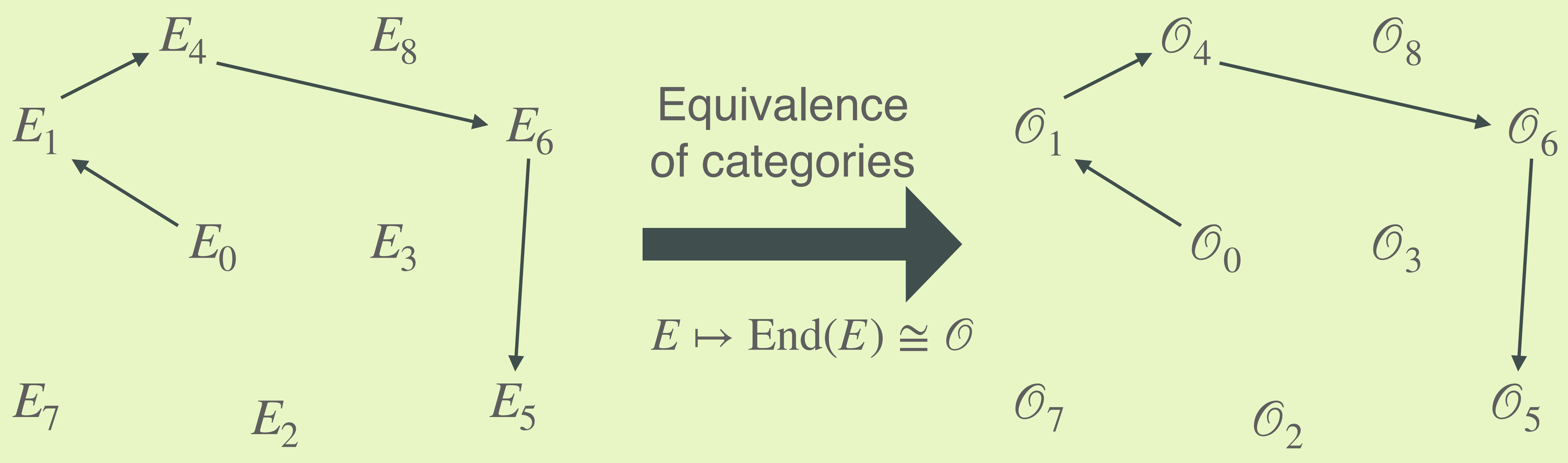


The Deuring Correspondence

Deuring correspondence

world of supersingular curves

world of maximal orders

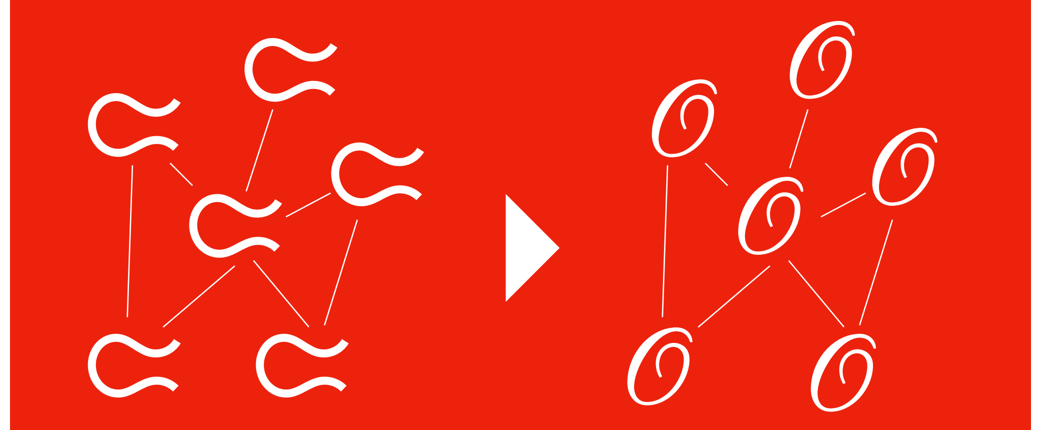


Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

curve-order dictionary

supersingular curves	quaternion orders

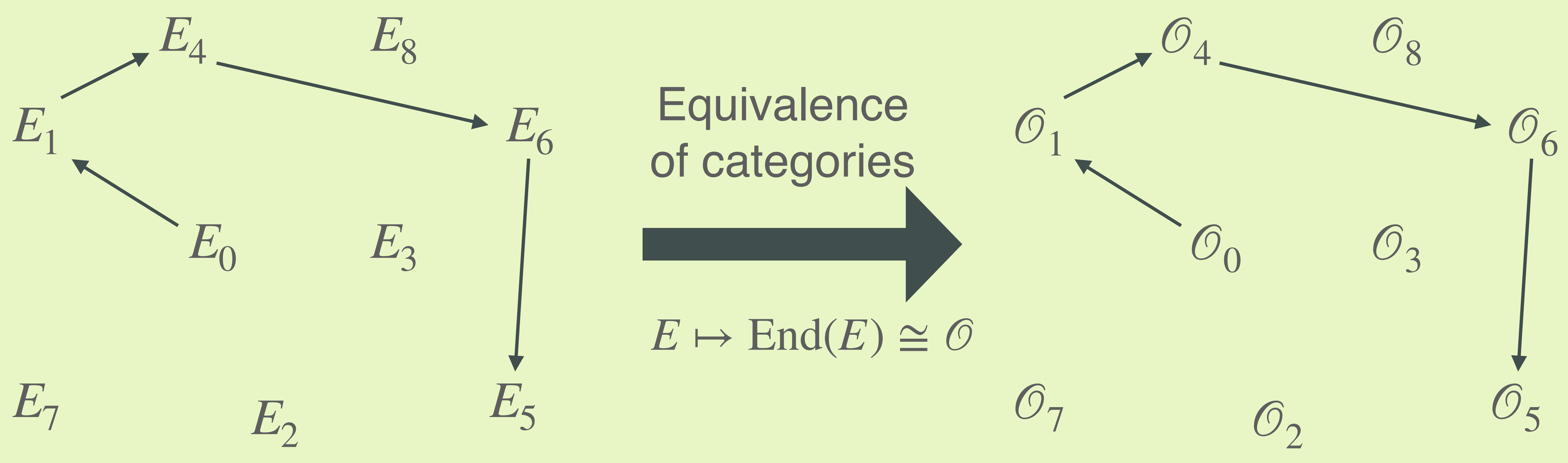


The Deuring Correspondence

Deuring correspondence

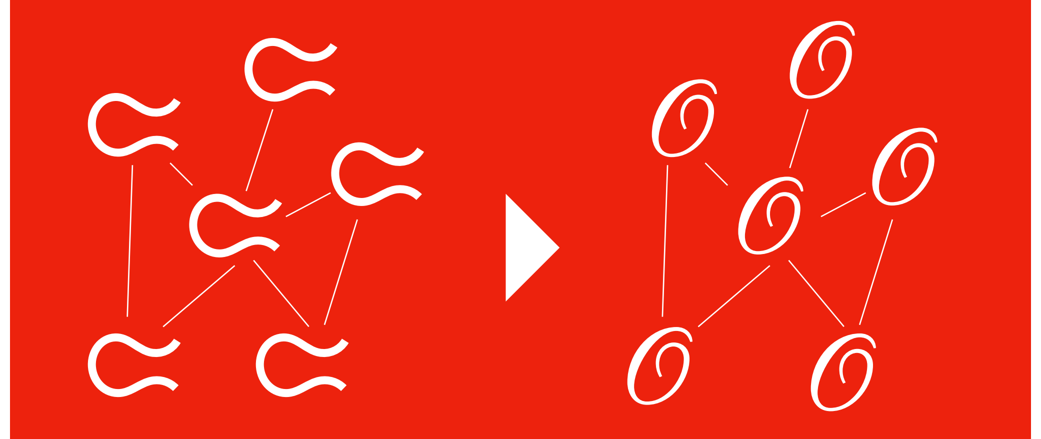
world of supersingular curves

world of maximal orders



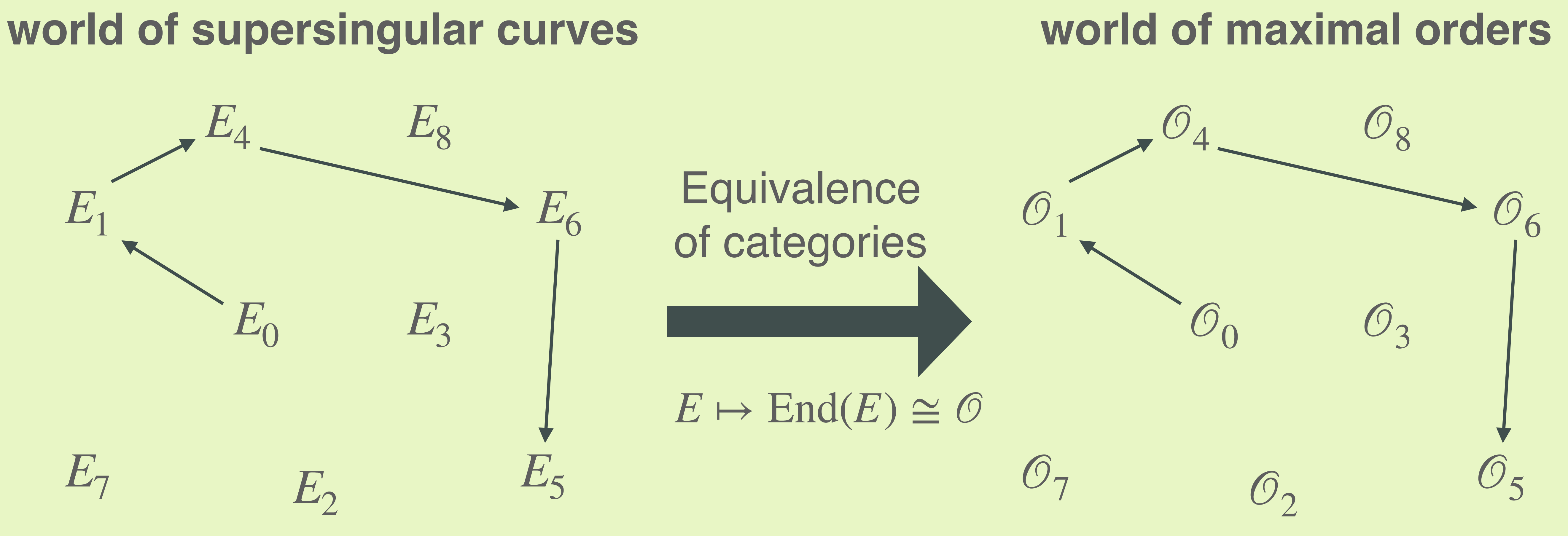
curve-order dictionary

supersingular curves	quaternion orders
curve E	maximal order $\mathcal{O}$



The Deuring Correspondence

Deuring correspondence



world of supersingular curves

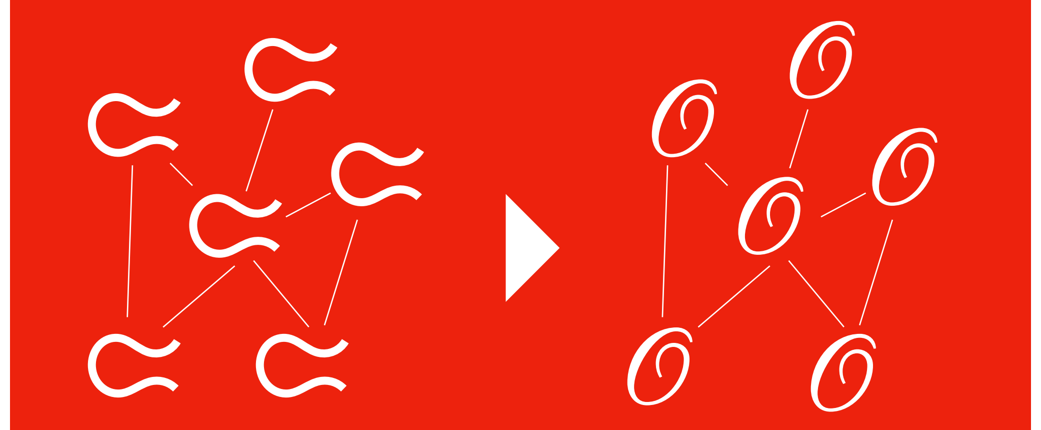
world of maximal orders

Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

curve-order dictionary

supersingular curves	quaternion orders
curve E	maximal order $\mathcal{O}$
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal

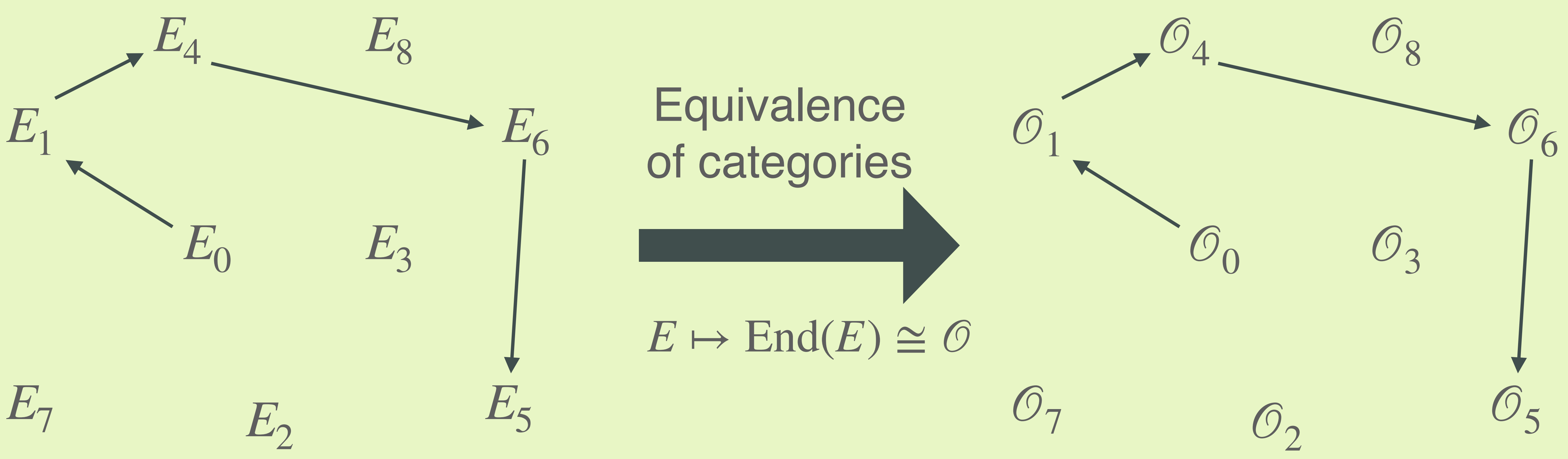


The Deuring Correspondence

Deuring correspondence

world of supersingular curves

world of maximal orders



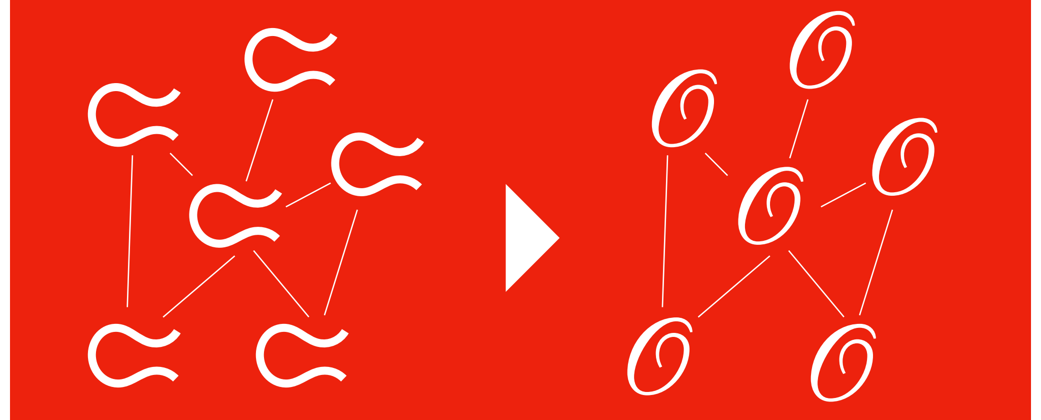
Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

curve-order dictionary

supersingular curves	quaternion orders
curve E	maximal order $\mathcal{O}$
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset \mathcal{O}$

2

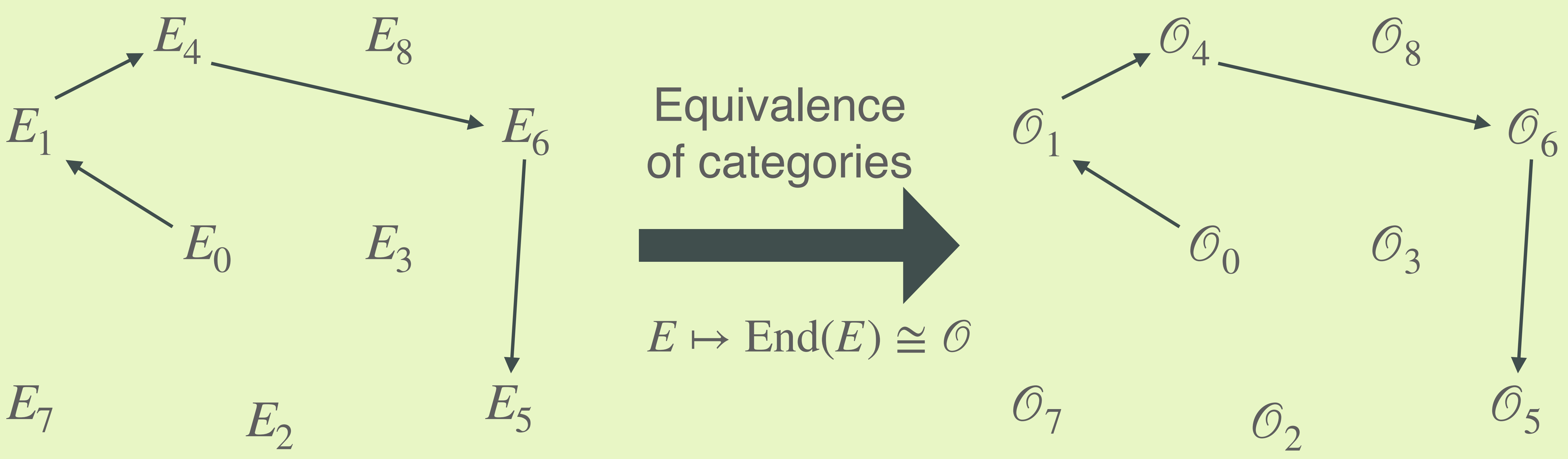


The Deuring Correspondence

Deuring correspondence

world of supersingular curves

world of maximal orders



Equivalence of categories

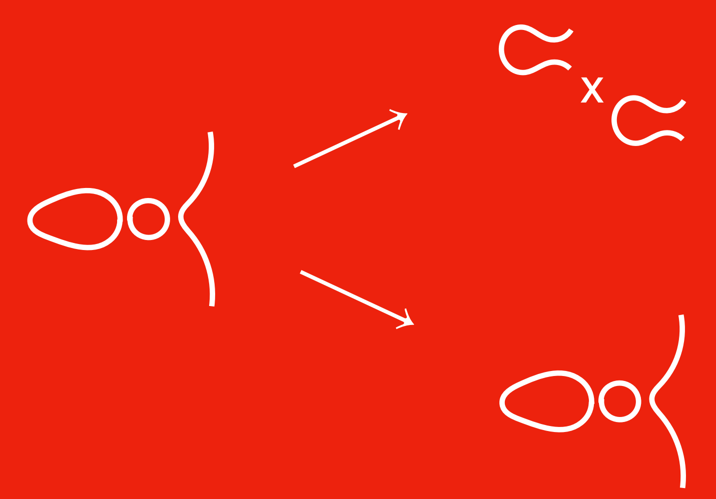
$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

curve-order dictionary

supersingular curves	quaternion orders
curve E	maximal order $\mathcal{O}$
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset \mathcal{O}$
and this continues for the *degree*, the *dual*, *equivalence*, *composition*…	and this continues for the *norm*, the *dual*, *equivalence, multiplication*…

Genus 2
101

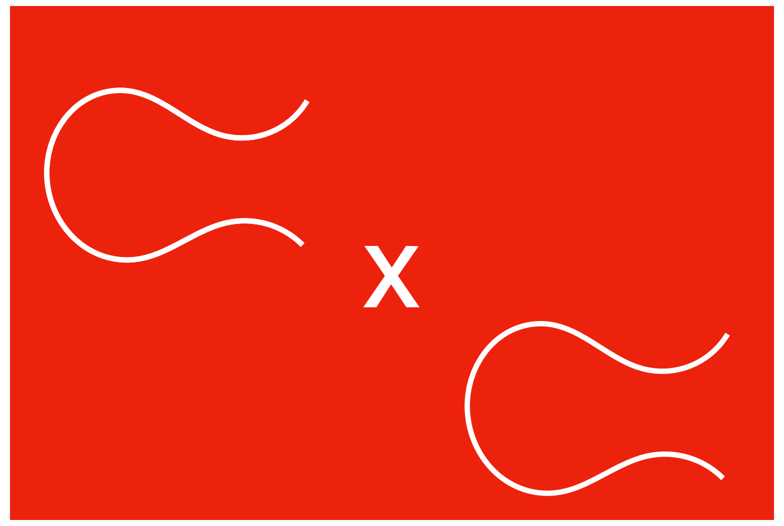
3



Isogenies in dimension 2

A

superspecial (principally polarised) abelian surfaces

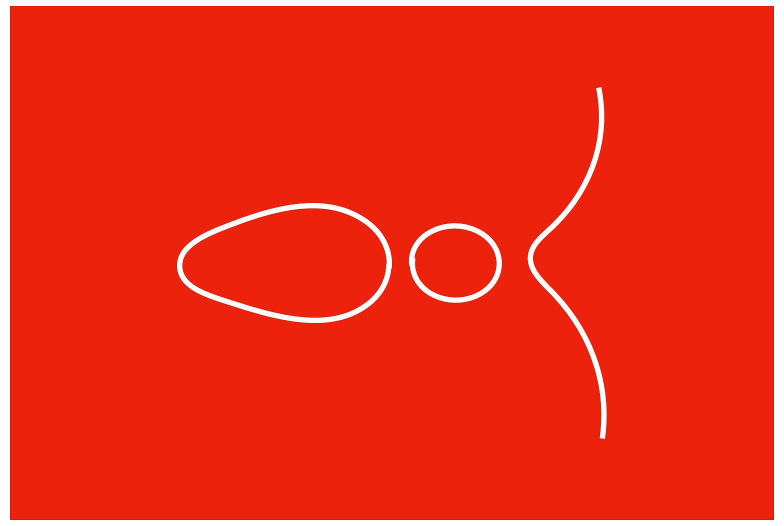


Products of elliptic curves $E \times E'$

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

$\times$

$E' : y^2 = x^3 - 3x + 3$

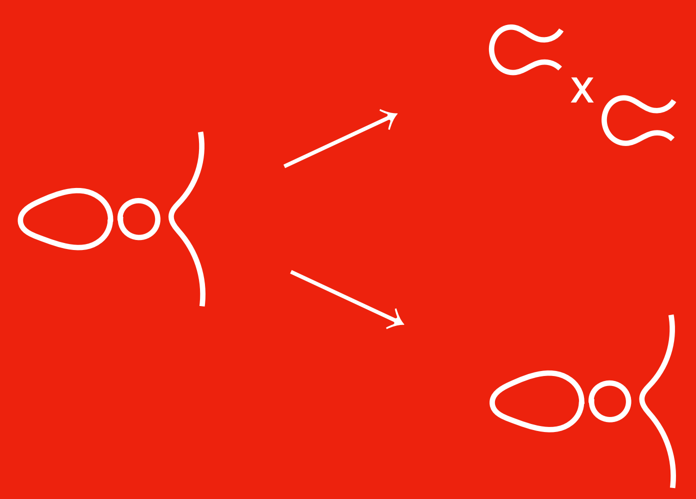


Jacobians of genus-2 curves

$C : y^2 = f(x),$

$\deg f = 5$ or $\deg f = 6$

$E' : y^2 = x^5 + 1184x^3 + 1846x^2 + 956x + 560$



Group law on genus-2 curve over the reals

$$(P_1 + P_2) \oplus (Q_1 + Q_2) = R_1 + R_2$$

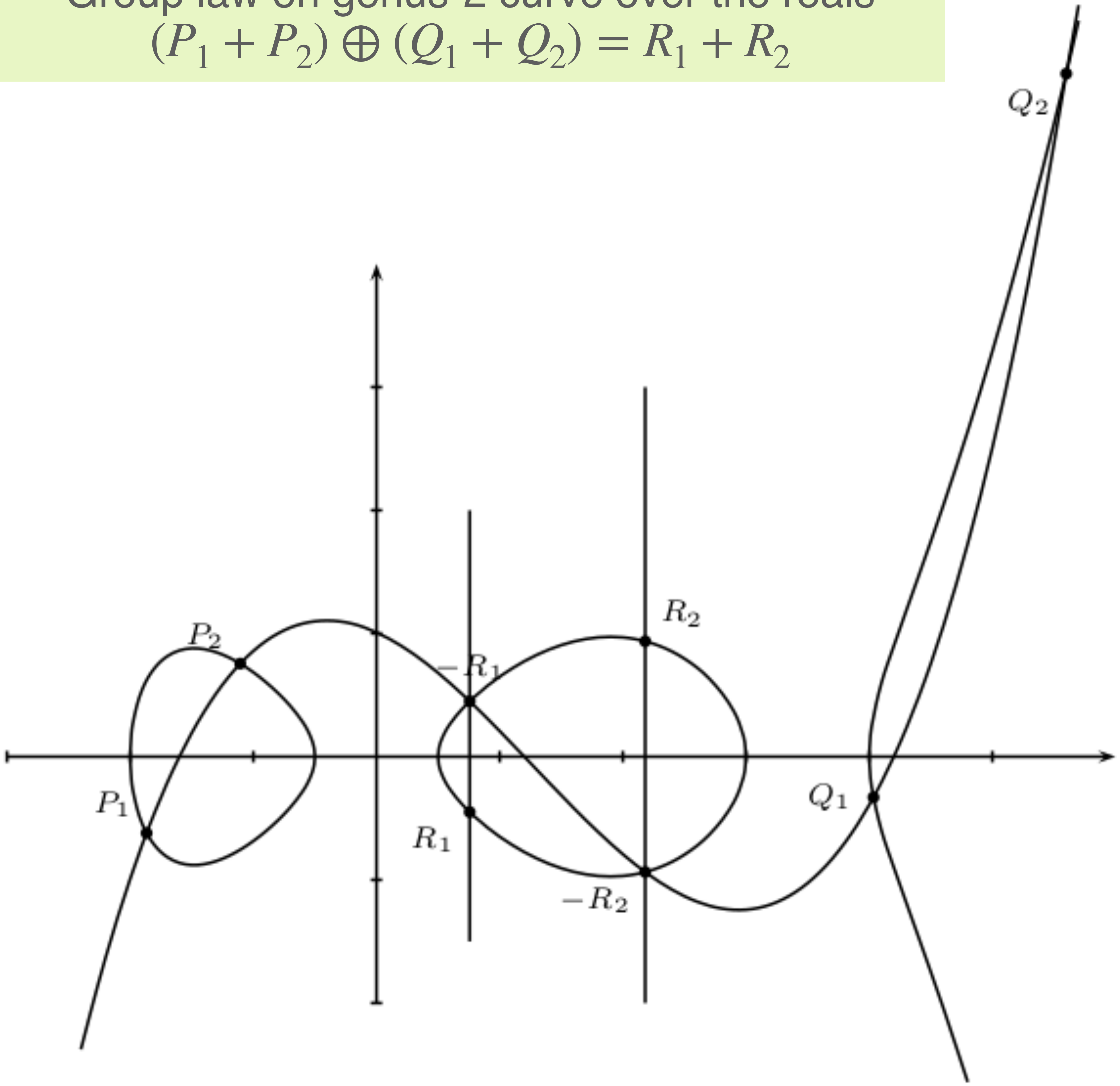
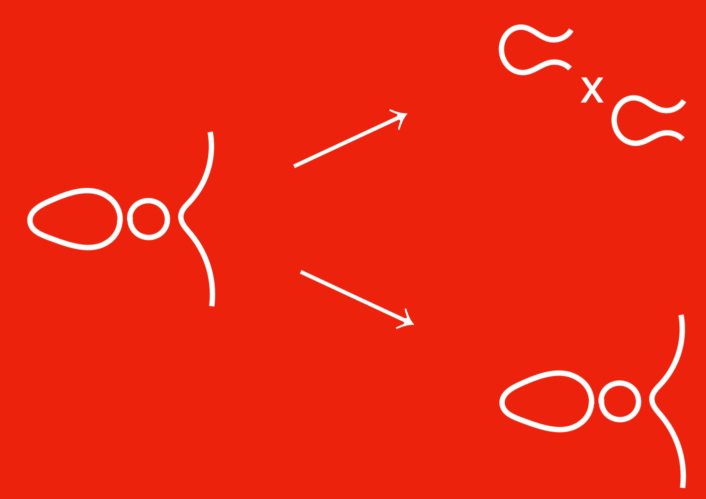


Fig. 14.1 from the Handbook of Elliptic and Hyperelliptic Curve Cryptography



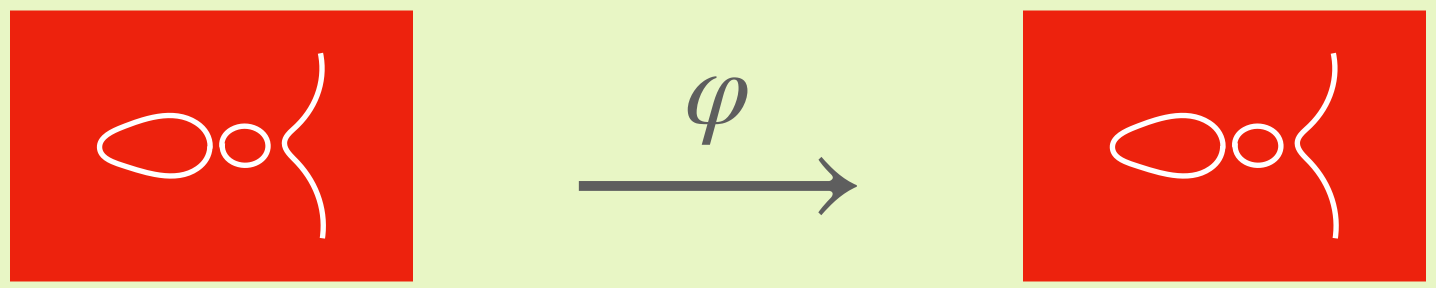
Isogenies in dimension 2

(N, N) - isogeny

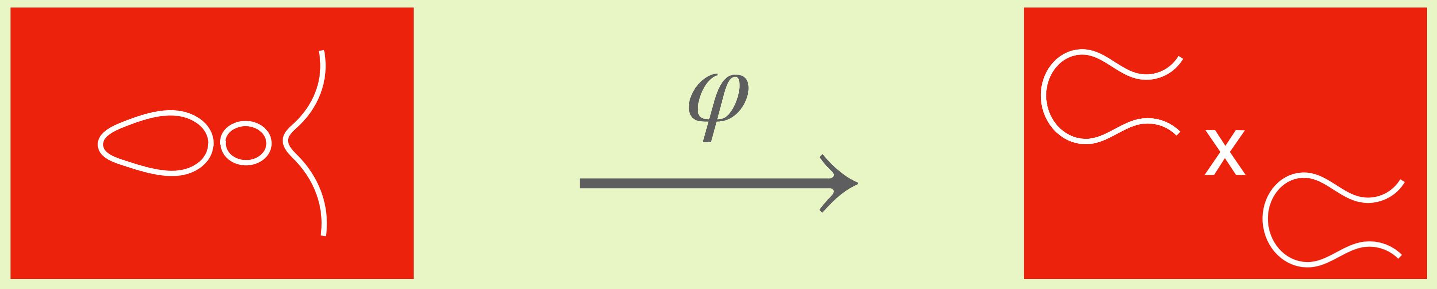
$$\begin{tikzcd} A \arrow[r, "\varphi"] & A' \end{tikzcd}$$

kernel of φ is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$

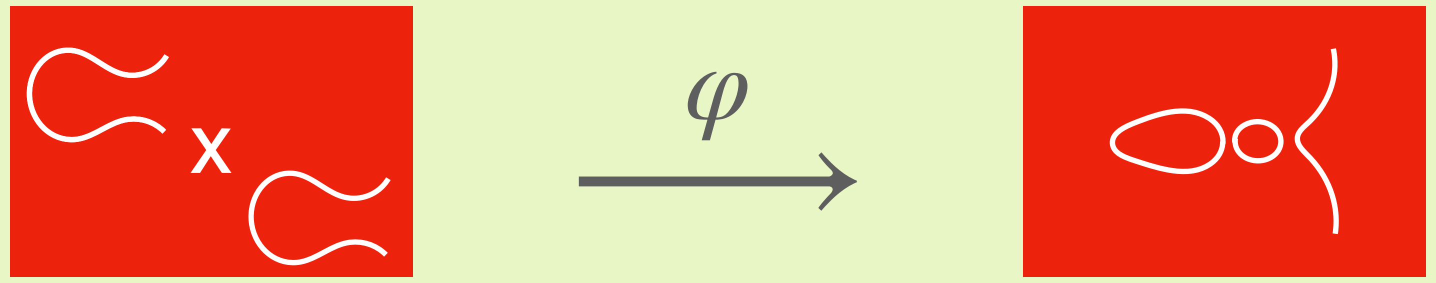
1) $J(C) \to J(C')$



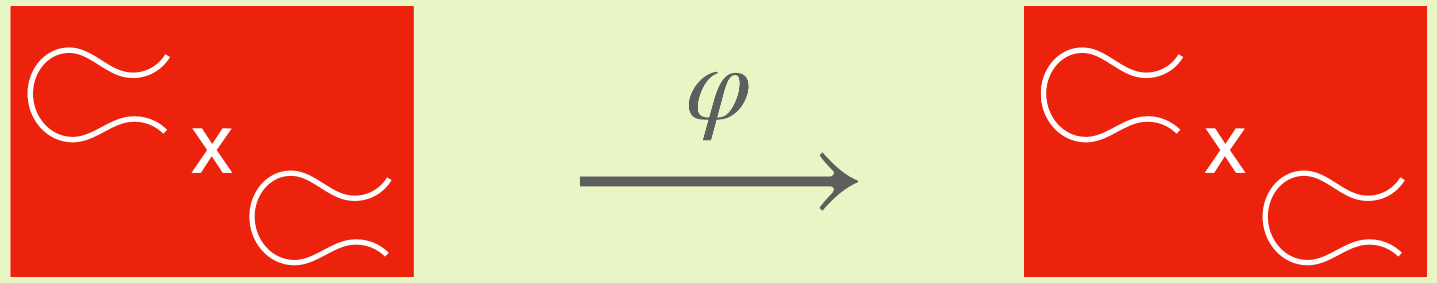
2) $J(C) \to E_1' \times E_2'$



3) $E_1 \times E_2 \to J(C')$



4) $E_1 \times E_2 \to E_1' \times E_2'$



Isogenies in dimension 2

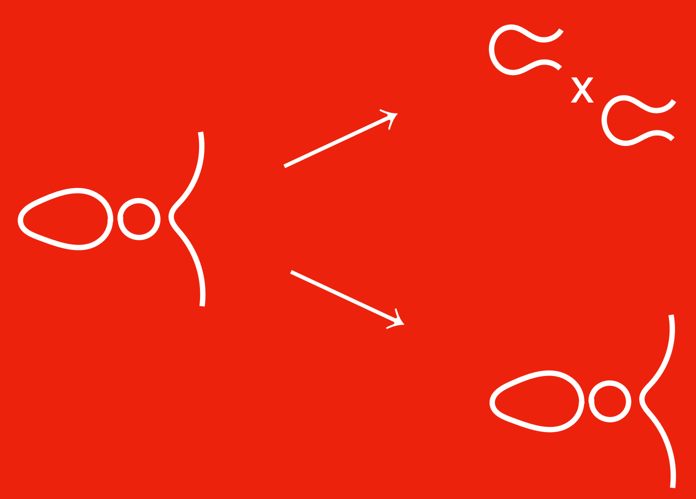
Isogeny diamond configuration

$$\begin{tikzcd} E_0 \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & E_1 = E_0/H_1 \arrow[d, "\gamma'"'] \\ E_2 = E_0/H_2 \arrow[r, "\varphi'"] & E_3 \end{tikzcd}$$

- $\gamma' \circ \varphi = \varphi' \circ \gamma$
- $\varphi \circ \hat{\gamma} = \widehat{\gamma'} \circ \varphi'$
- $\gamma \circ \hat{\varphi} = \widehat{\varphi'} \circ \gamma'$
- $\hat{\varphi} \circ \varphi = [\#H_1]$
- $\hat{\gamma} \circ \gamma = [\#H_2]$

*See also: Kani for beginners - S. Galbraith

3



Isogenies in dimension 2

Isogeny diamond configuration

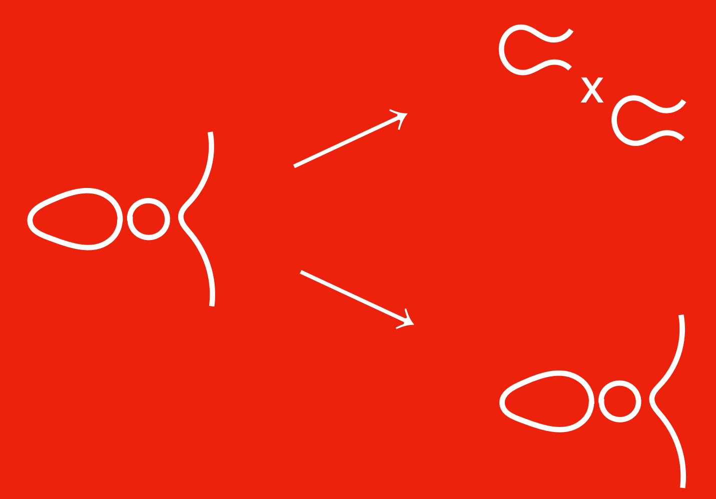
$$\begin{tikzcd}
E_0 \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & E_1 = E_0/H_1 \arrow[d, "\gamma'"'] \\
E_2 = E_0/H_2 \arrow[r, "\varphi'"] & E_3
\end{tikzcd}$$

$$\rho : E_2 \times E_1 \to E_0 \times E_3$$
$$\rho(X, Y) = (\hat{\gamma}(X) + \hat{\varphi}(Y), \varphi'(X) - \gamma'(Y))$$

- $\gamma' \circ \varphi = \varphi' \circ \gamma$
- $\varphi \circ \hat{\gamma} = \widehat{\gamma'} \circ \varphi'$
- $\gamma \circ \hat{\varphi} = \widehat{\varphi'} \circ \gamma'$
- $\hat{\varphi} \circ \varphi = [\#H_1]$
- $\hat{\gamma} \circ \gamma = [\#H_2]$

*See also: Kani for beginners - S. Galbraith

3



Isogenies in dimension 2

Isogeny diamond configuration

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & E_1 = E_0/H_1 \arrow[d, "\gamma'"'] \\
E_2 = E_0/H_2 \arrow[r, "\varphi'"] & E_3
\end{tikzcd}$$

$$\rho : E_2 \times E_1 \to E_0 \times E_3$$
$$\rho(X, Y) = (\hat{\gamma}(X) + \hat{\varphi}(Y), \varphi'(X) - \gamma'(Y))$$

- $\gamma' \circ \varphi = \varphi' \circ \gamma$
- $\varphi \circ \hat{\gamma} = \hat{\gamma}' \circ \varphi'$
- $\gamma \circ \hat{\varphi} = \hat{\varphi}' \circ \gamma'$
- $\hat{\varphi} \circ \varphi = [\#H_1]$
- $\hat{\gamma} \circ \gamma = [\#H_2]$

$\#H_1 + \#H_2$

↳ ρ is an (N, N)-isogeny with kernel $H = \langle (P_2, P_1), (Q_2, Q_1) \rangle$

$\downarrow$

$(P_1, Q_1) = (\varphi(P_0), \varphi(Q_0))$

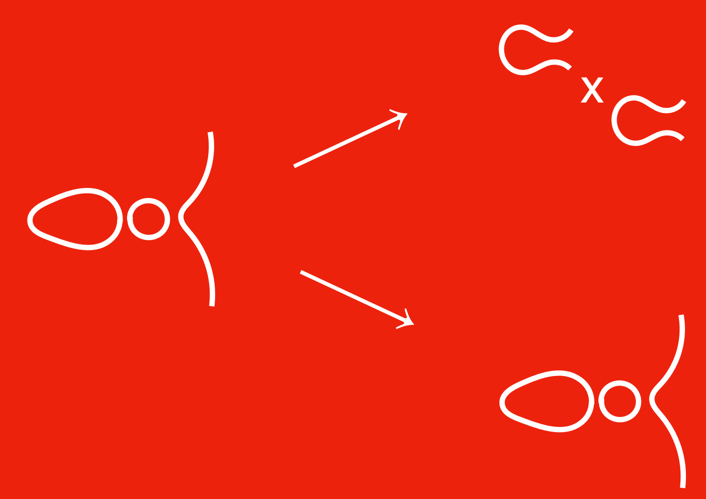
$(P_2, Q_2) = (\gamma(P_0), \gamma(Q_0))$

$\downarrow$

$\{P_0, Q_0\}$ is a basis for $E_0[N]$

*See also: Kani for beginners - S. Galbraith

3



Isogenies in dimension 2

Isogeny diamond configuration

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & E_1 = E_0/H_1 \arrow[d, "\gamma'"'] \\
E_2 = E_0/H_2 \arrow[r, "\varphi'"] & E_3
\end{tikzcd}$$

$$\rho : E_2 \times E_1 \to E_0 \times E_3$$
$$\rho(X, Y) = (\hat{\gamma}(X) + \hat{\varphi}(Y), \varphi'(X) - \gamma'(Y))$$

- $\gamma' \circ \varphi = \varphi' \circ \gamma$
- $\varphi \circ \hat{\gamma} = \hat{\gamma'} \circ \varphi'$
- $\gamma \circ \hat{\varphi} = \hat{\varphi'} \circ \gamma'$
- $\hat{\varphi} \circ \varphi = [\#H_1]$
- $\hat{\gamma} \circ \gamma = [\#H_2]$

$\#H_1 + \#H_2$

↳ ρ is an (N, N)-isogeny with kernel $H = \langle (P_2, P_1), (Q_2, Q_1) \rangle$

↓

$(P_1, Q_1) = (\varphi(P_0), \varphi(Q_0))$

$(P_2, Q_2) = (\gamma(P_0), \gamma(Q_0))$

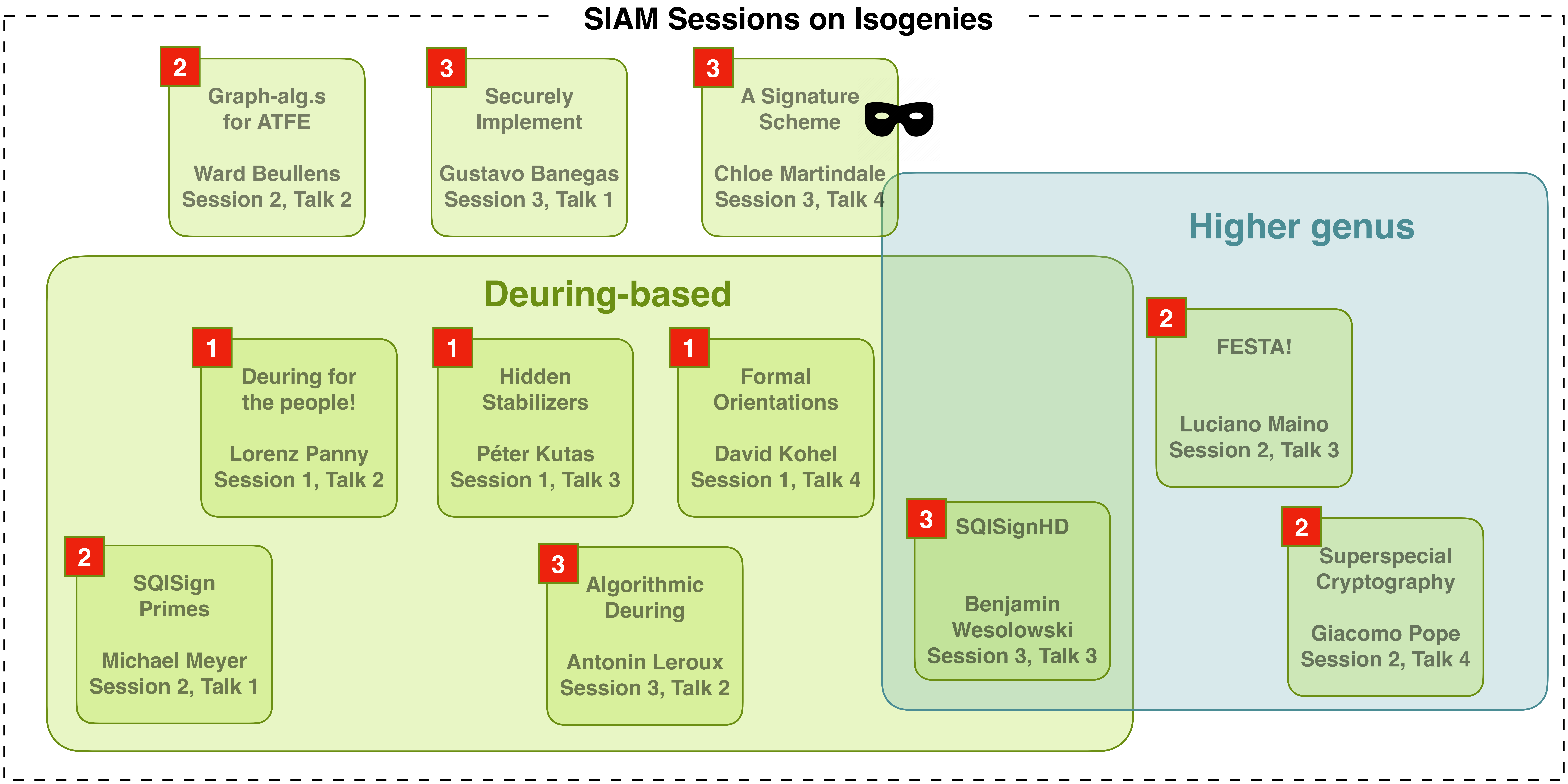
↓

$\{P_0, Q_0\}$ is a basis for $E_0[N]$

↳ $E_2 \times E_1 / H$ is not likely to be a product of elliptic curves

*See also: Kani for beginners - S. Galbraith

A rough overview on the three sessions



SIAM Sessions on Isogenies

2 Graph-alg.s for ATFE

Ward Beullens
Session 2, Talk 2

3 Securely Implement

Gustavo Banegas
Session 3, Talk 1

3 A Signature Scheme

Chloe Martindale
Session 3, Talk 4

Higher genus

Deuring-based

1 Deuring for the people!

Lorenz Panny
Session 1, Talk 2

1 Hidden Stabilizers

Péter Kutas
Session 1, Talk 3

1 Formal Orientations

David Kohel
Session 1, Talk 4

2 FESTA!

Luciano Maino
Session 2, Talk 3

2 SQISign Primes

Michael Meyer
Session 2, Talk 1

3 Algorithmic Deuring

Antonin Leroux
Session 3, Talk 2

3 SQISignHD

Benjamin Wesolowski
Session 3, Talk 3

2 Superspecial Cryptography

Giacomo Pope
Session 2, Talk 4

Thanks for your attention!

Enjoy our sessions!