European Research Council
Established by the European Commission
anr
ENS DE LYON
cnrs

An introduction to Isogeny-based cryptography

with a view towards understanding SQIsign

Benjamin Wesolowski, CNRS and ENS de Lyon

April 2025, *The SQIparty — a Workshop on Isogeny-Crypto*, Lleida, Spain

The Isogeny problem

what even is an isogeny?

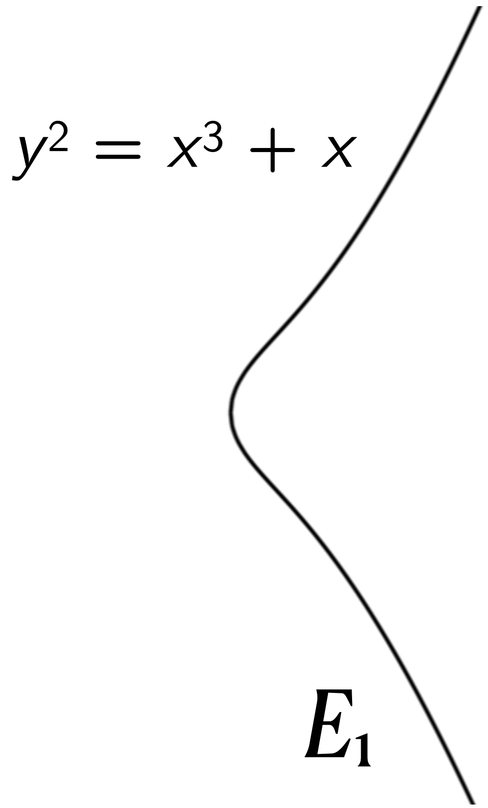
Picture by Beppe Rijs

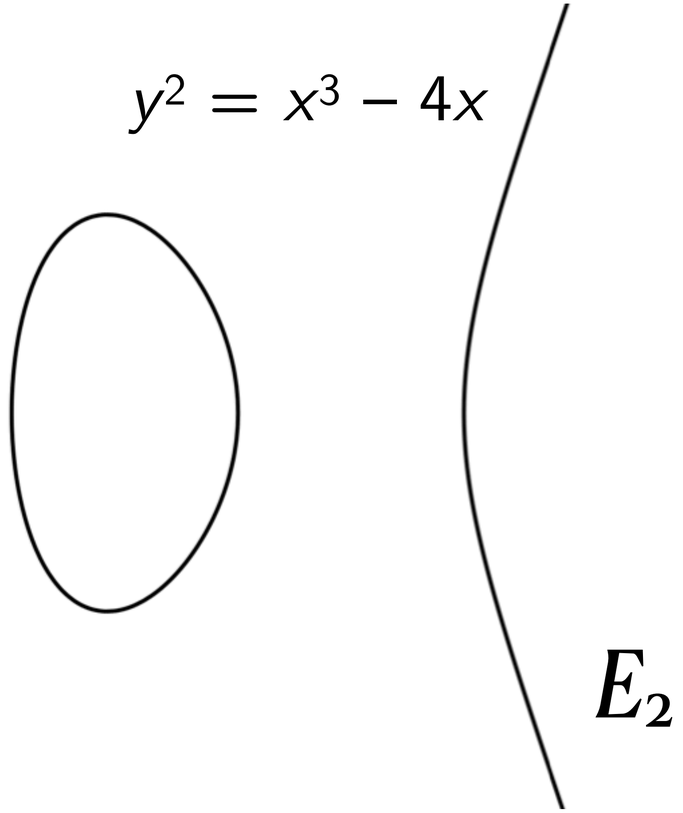
- In crypto, we use elliptic curves over a **finite field**
- Elliptic curves are **groups**: you can add points together!

Elliptic curves

equations of the form

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

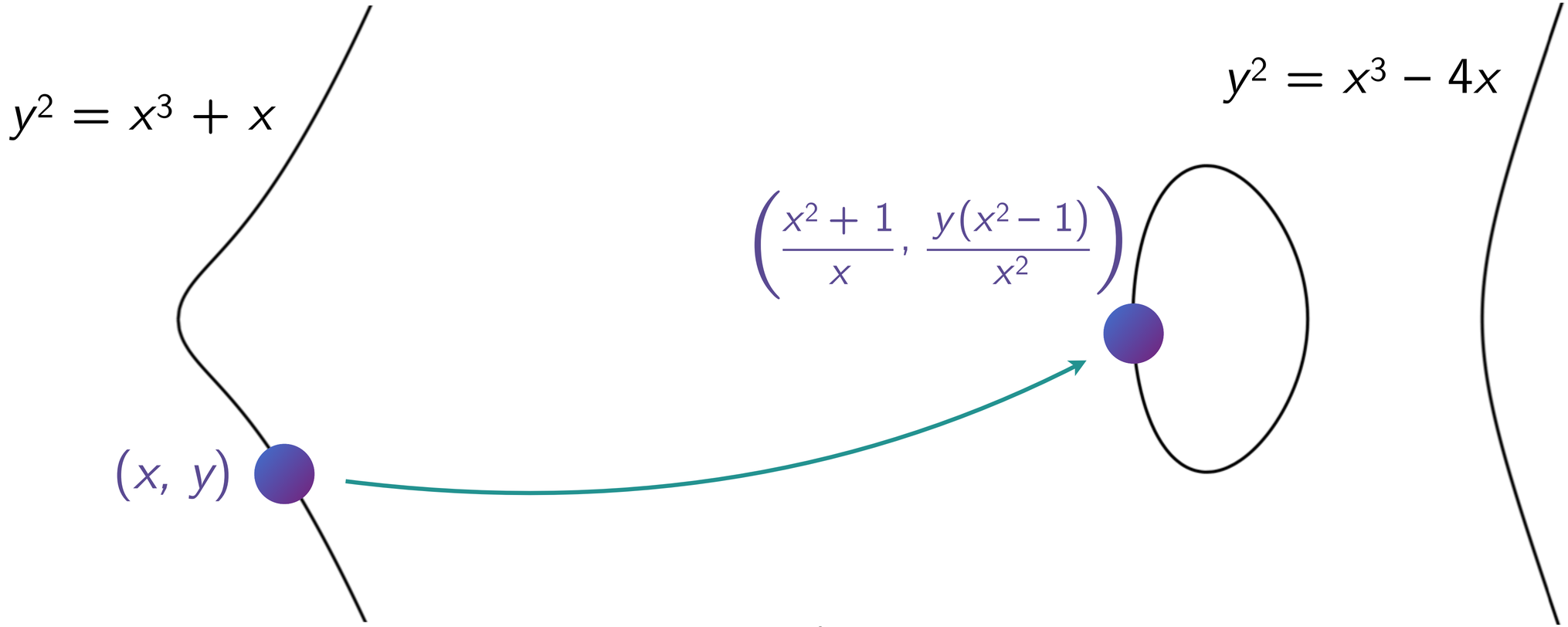




- In crypto, we use elliptic curves over a **finite field**
- Elliptic curves are **groups**: you can add points together!

Elliptic curves

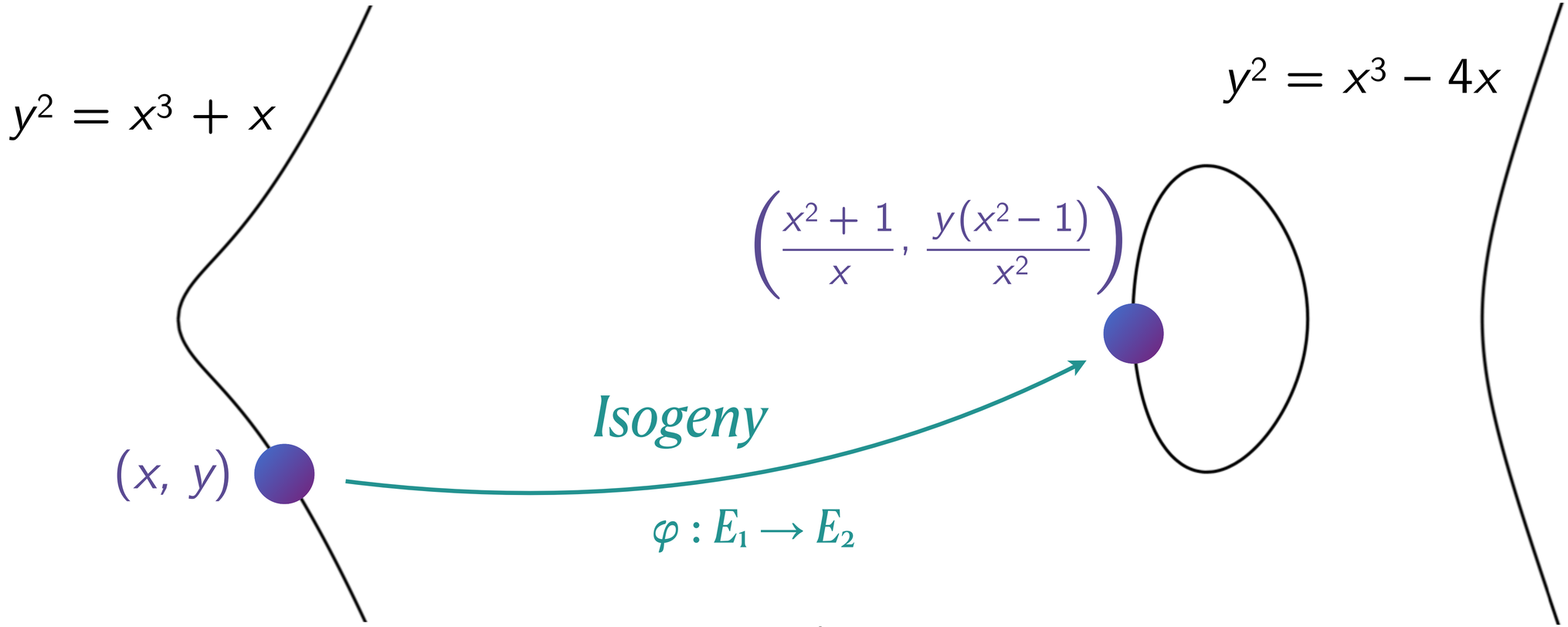
Sometimes, there is a formula to transform solutions from one equation to another



- In crypto, we use elliptic curves over a **finite field**
- Elliptic curves are **groups**: you can add points together!

Elliptic curves

Sometimes, there is a formula to transform solutions from one equation to another

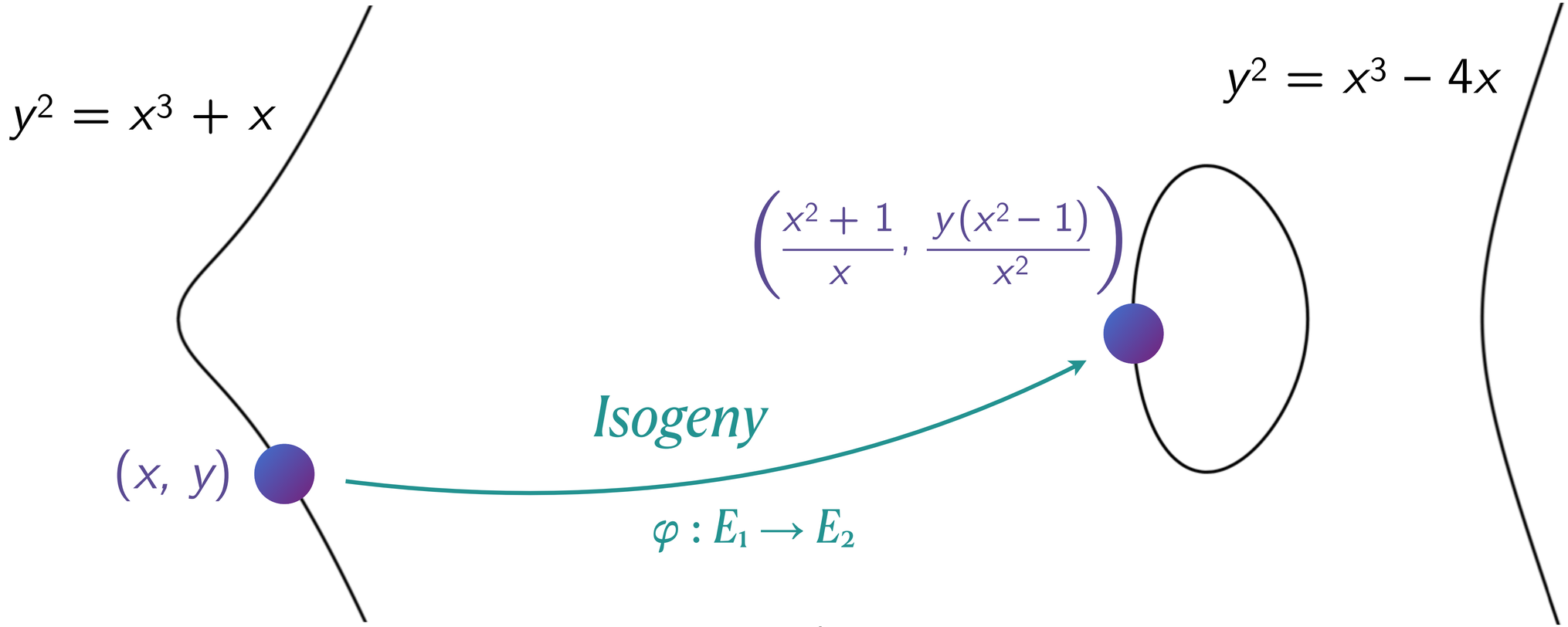


- In crypto, we use elliptic curves over a **finite field**
- Elliptic curves are **groups**: you can add points together!

Elliptic curves

- Isogenies are **group homomorphisms**
- **Degree** = size of kernel

Sometimes, there is a formula to transform solutions from one equation to another

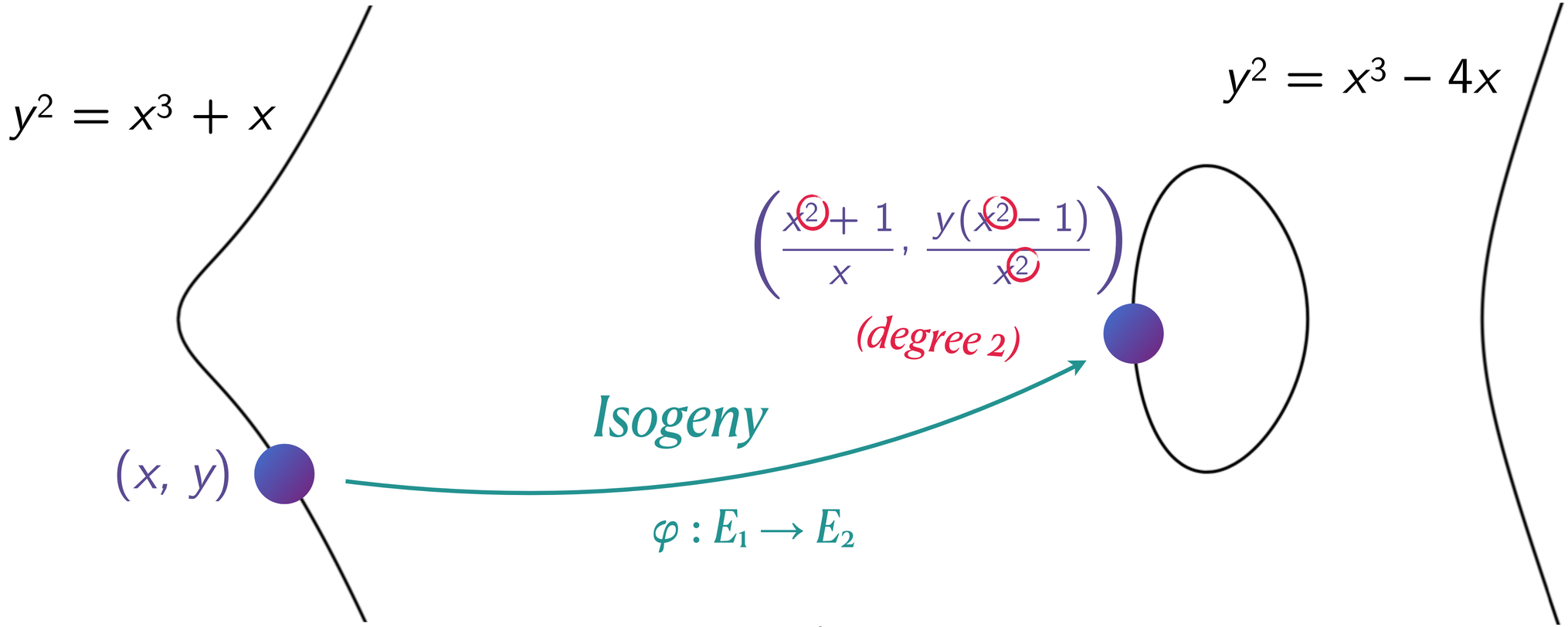


- In crypto, we use elliptic curves over a **finite field**
- Elliptic curves are **groups**: you can add points together!

Elliptic curves

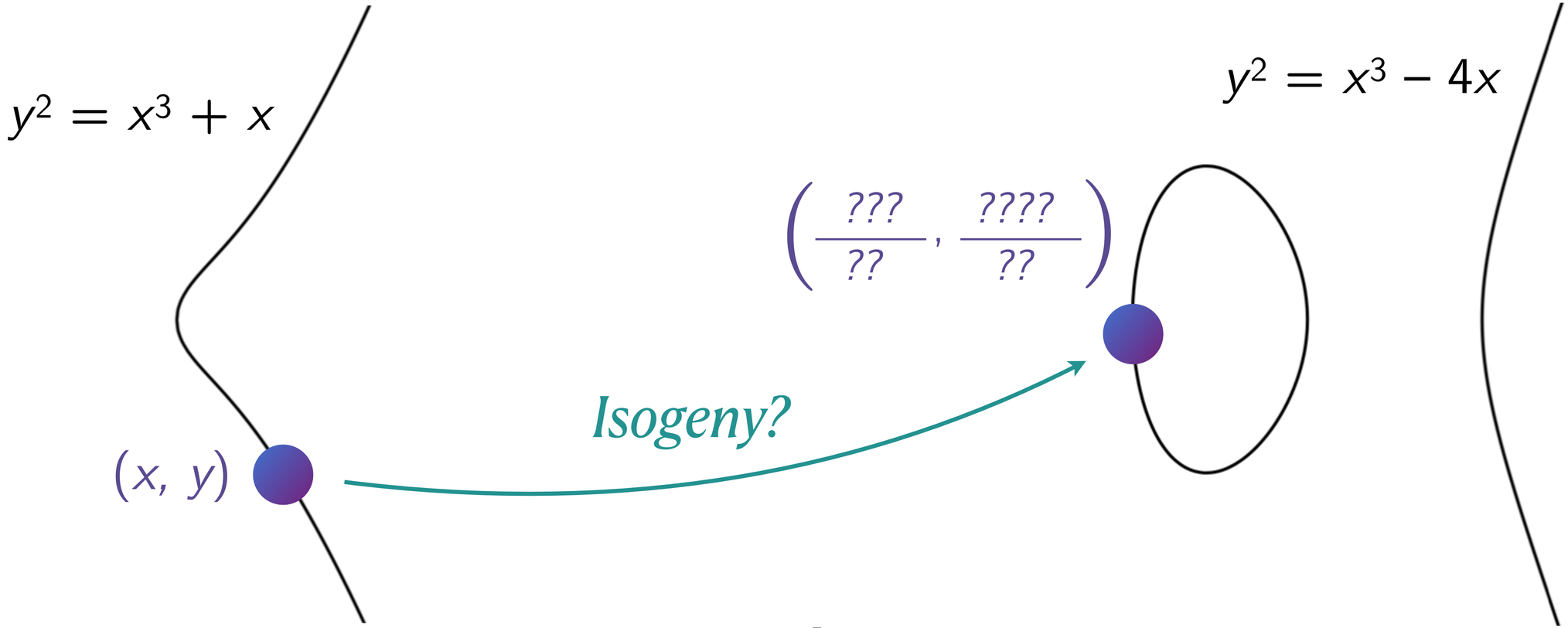
- Isogenies are **group homomorphisms**
- **Degree** = size of kernel

Sometimes, there is a formula to transform solutions from one equation to another



The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$



The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

(degree 2)

fine for small degree...

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

solution routinely has degree $\approx 2^{256}$

(degree 2)

fine for small degree...

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

solution routinely has degree $\approx 2^{256}$

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

(degree 2)

fine for small degree...

- Build "big" isogenies as *formal combinations* of "small" ones

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

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

solution typically has degree $\approx 2^{256}$

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

(degree 2)

fine for small degree...

- Build "big" isogenies as *formal combinations* of "small" ones

$$E_1 \xrightarrow{2} E_2 \xrightarrow{2} E_3 \xrightarrow{2} \dots \xrightarrow{2} E_{257}$$

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

solution typically has degree $\approx 2^{256}$

- The solution φ is an isogeny...
- How to represent an isogeny?

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

(degree 2)

fine for small degree...

- Build "big" isogenies as *formal combinations* of "small" ones

$$E_1 \xrightarrow{2} E_2 \xrightarrow{2} E_3 \xrightarrow{2} \dots \xrightarrow{2} E_{257}$$

degree 2^{256}

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?

$$(x,\ y) \quad \longmapsto \quad \left(\frac{x^2+1}{x},\ \frac{y(x^2-1)}{x^2}\right)$$

solution typically has degree $\approx 2^{256}$

(degree 2)

fine for small degree...

- Build "big" isogenies as *formal combinations* of "small" ones
  - $\varphi \circ \psi$ represented by ('comp', φ, ψ) where φ and ψ are composable
  - $\varphi + \psi$ represented by ('add', φ, ψ) where φ and ψ are both $E_1 \to E_2$

The *Isogeny* problem

Given E_1 and E_2 find an isogeny $\varphi : E_1 \to E_2$

- The solution φ is an isogeny...
- How to represent an isogeny?
  - any **efficient representation**: an encoding which allows one to evaluate $\varphi(P)$ in polynomial time for any P

solution typically has degree $\approx 2^{256}$

Isogeny graph

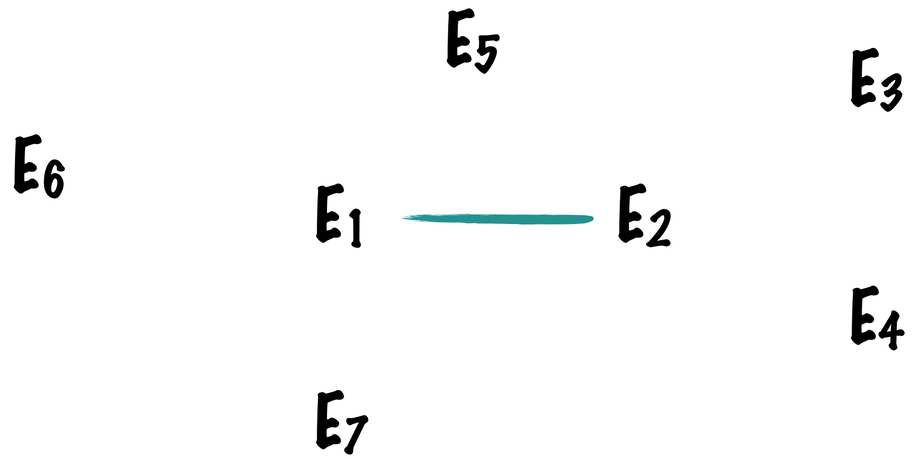
an isogeny of degree 2 = an edge in a graph

Isogeny graph

- **The 2-isogeny graph** (supersingular...)

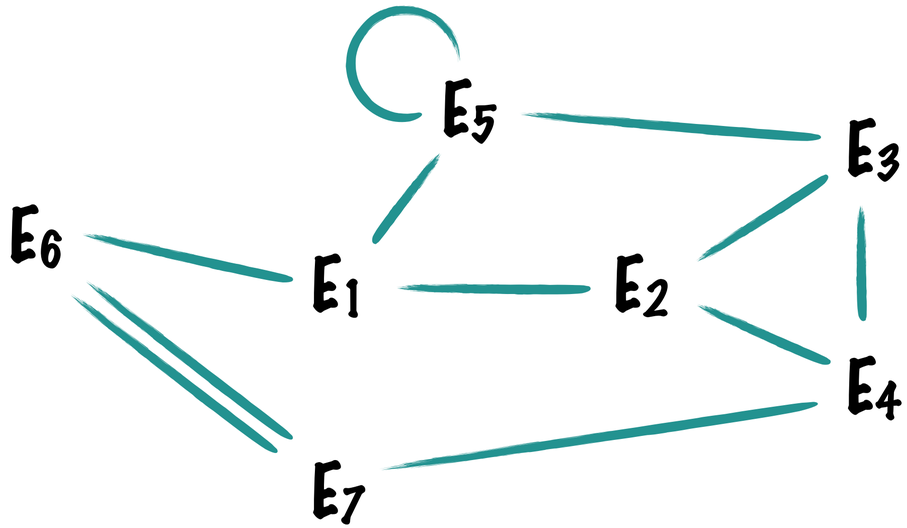
Isogeny graph

- **The 2-isogeny graph** (supersingular...)



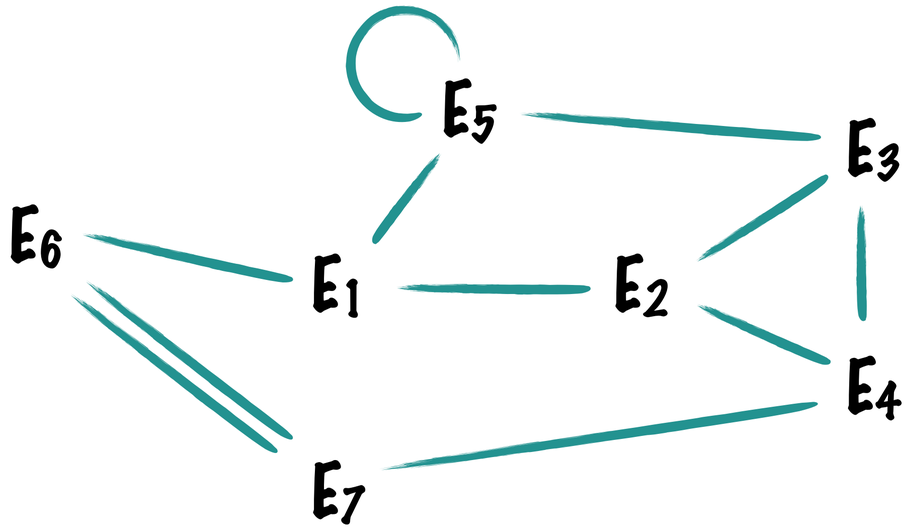
Isogeny graph

- **The 2-isogeny graph** (supersingular...)



Isogeny graph

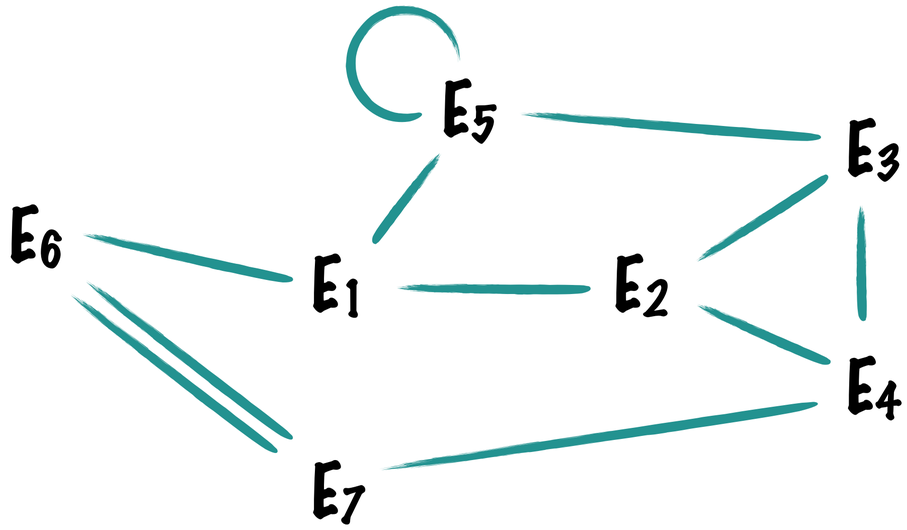
- **The 2-isogeny graph** (supersingular...)



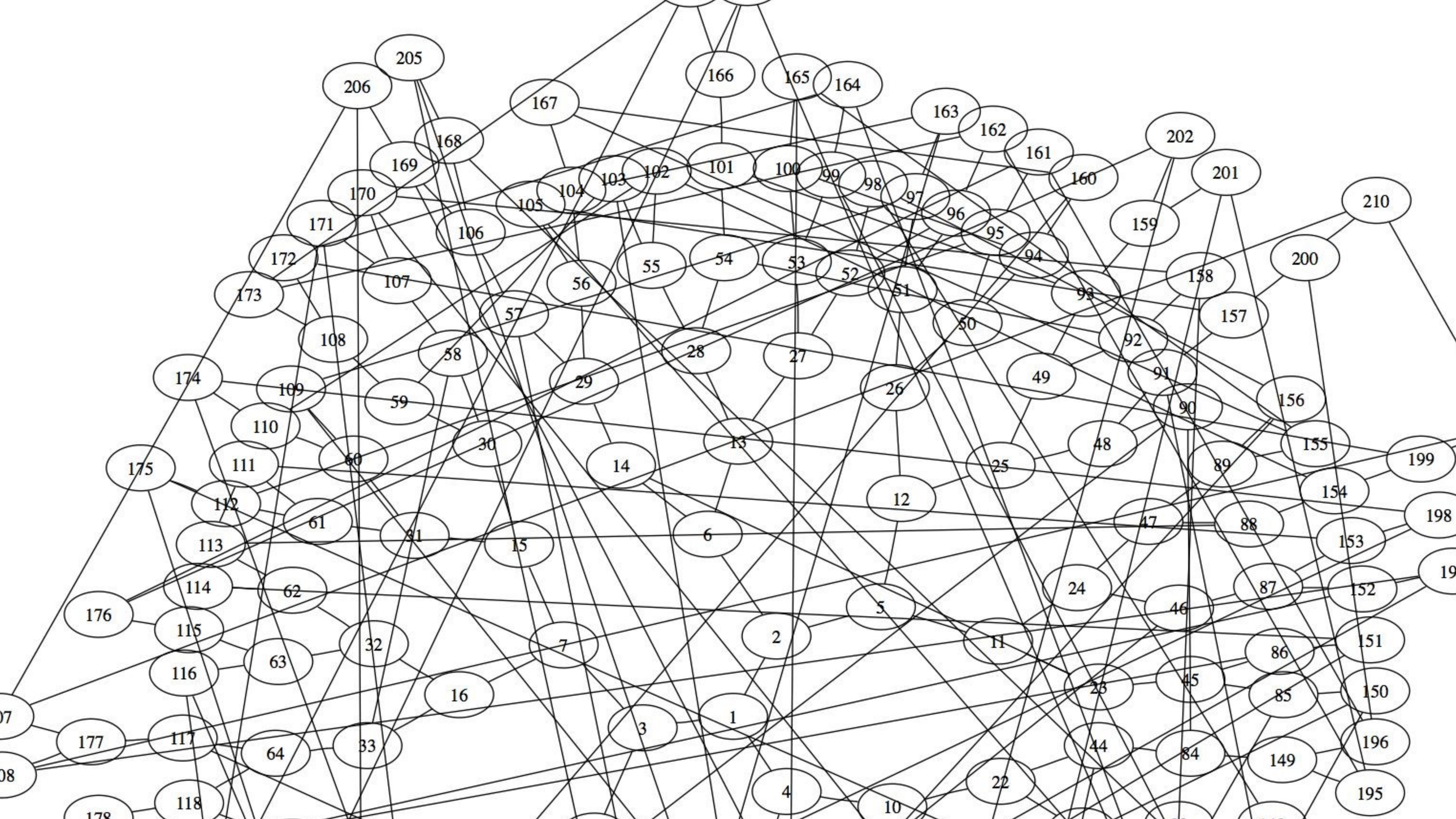
- 3-regular, **connected** (for supersingular curves)

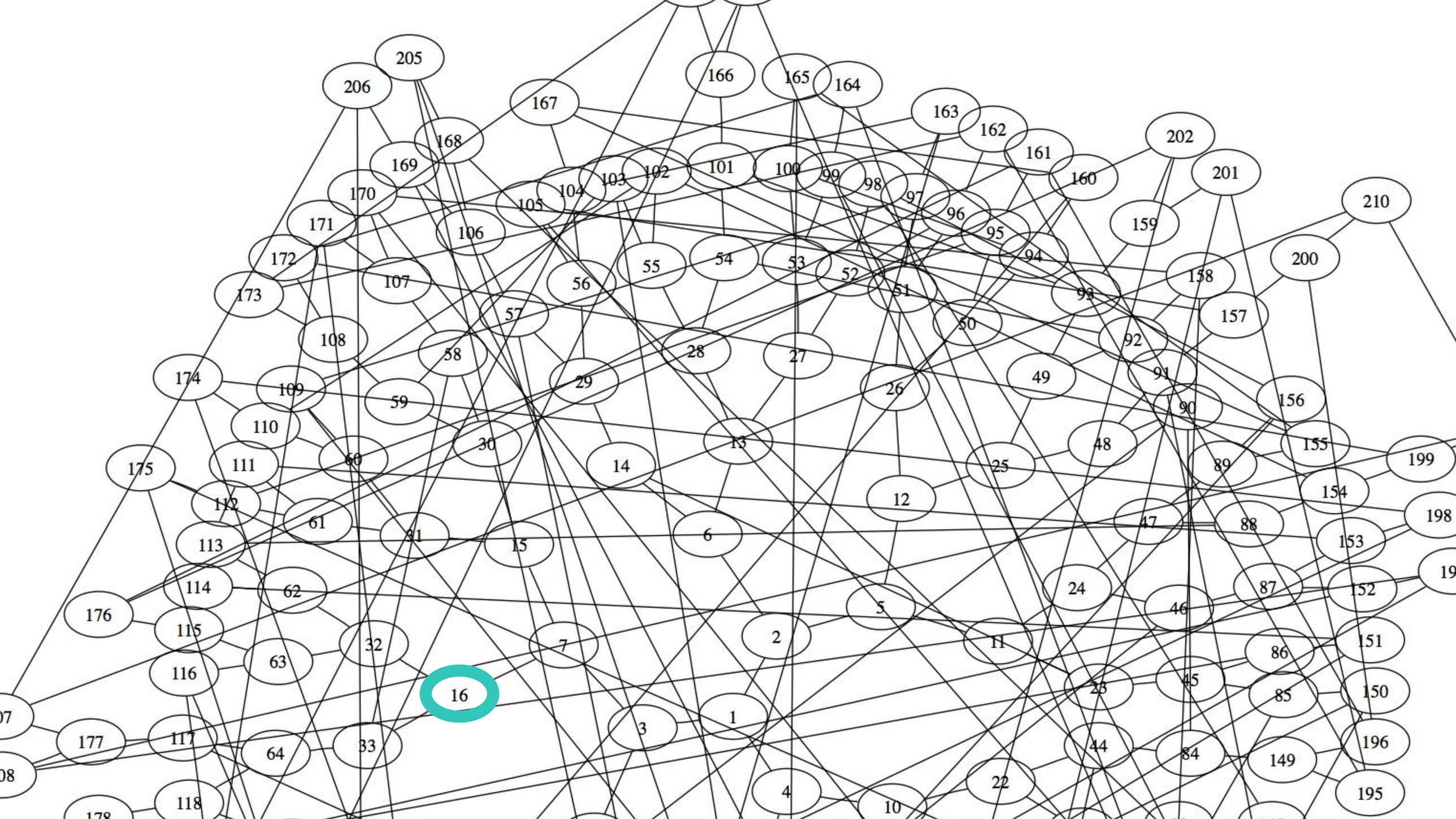
Isogeny graph

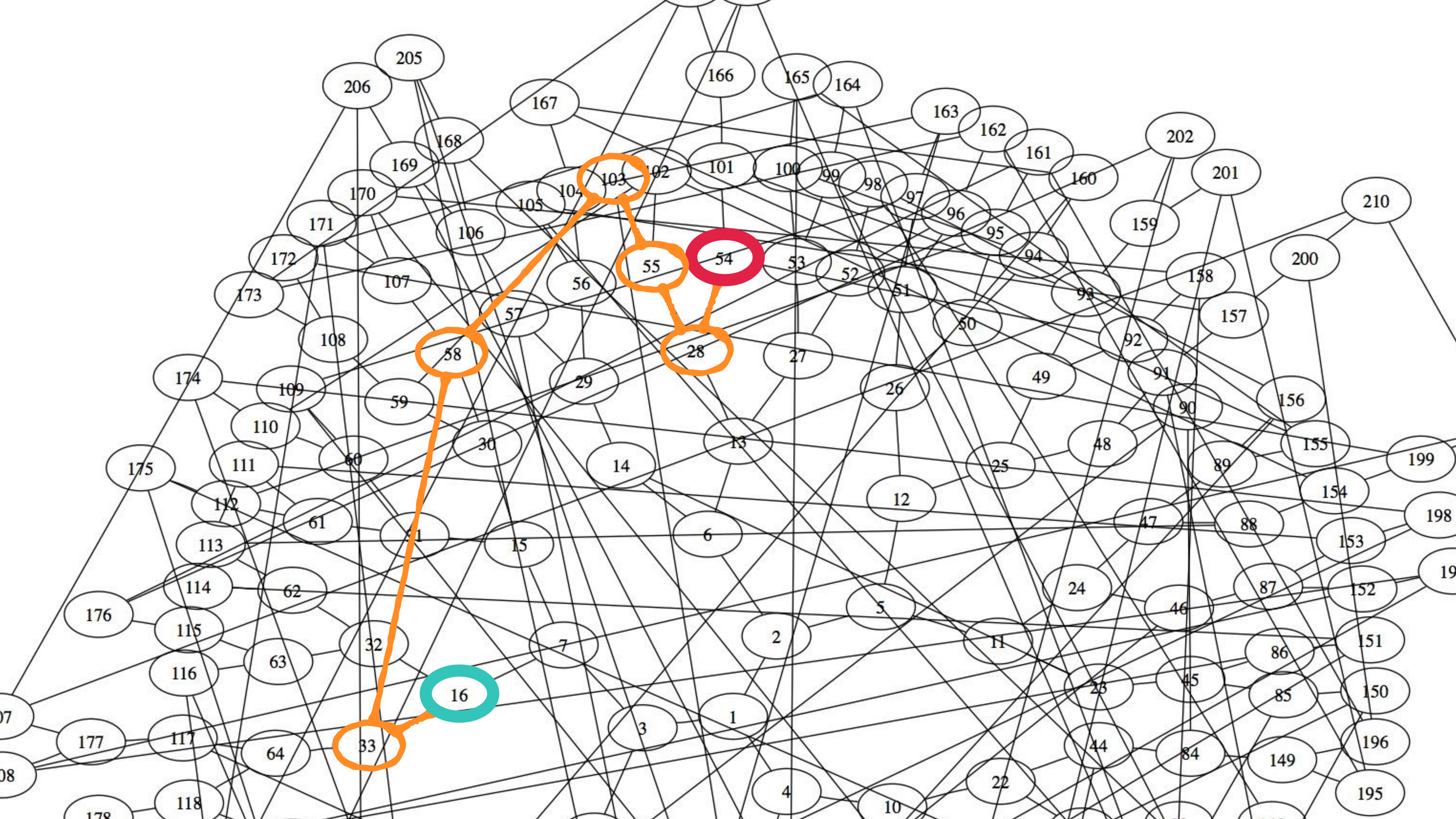
- **The 2-isogeny graph** (supersingular...)

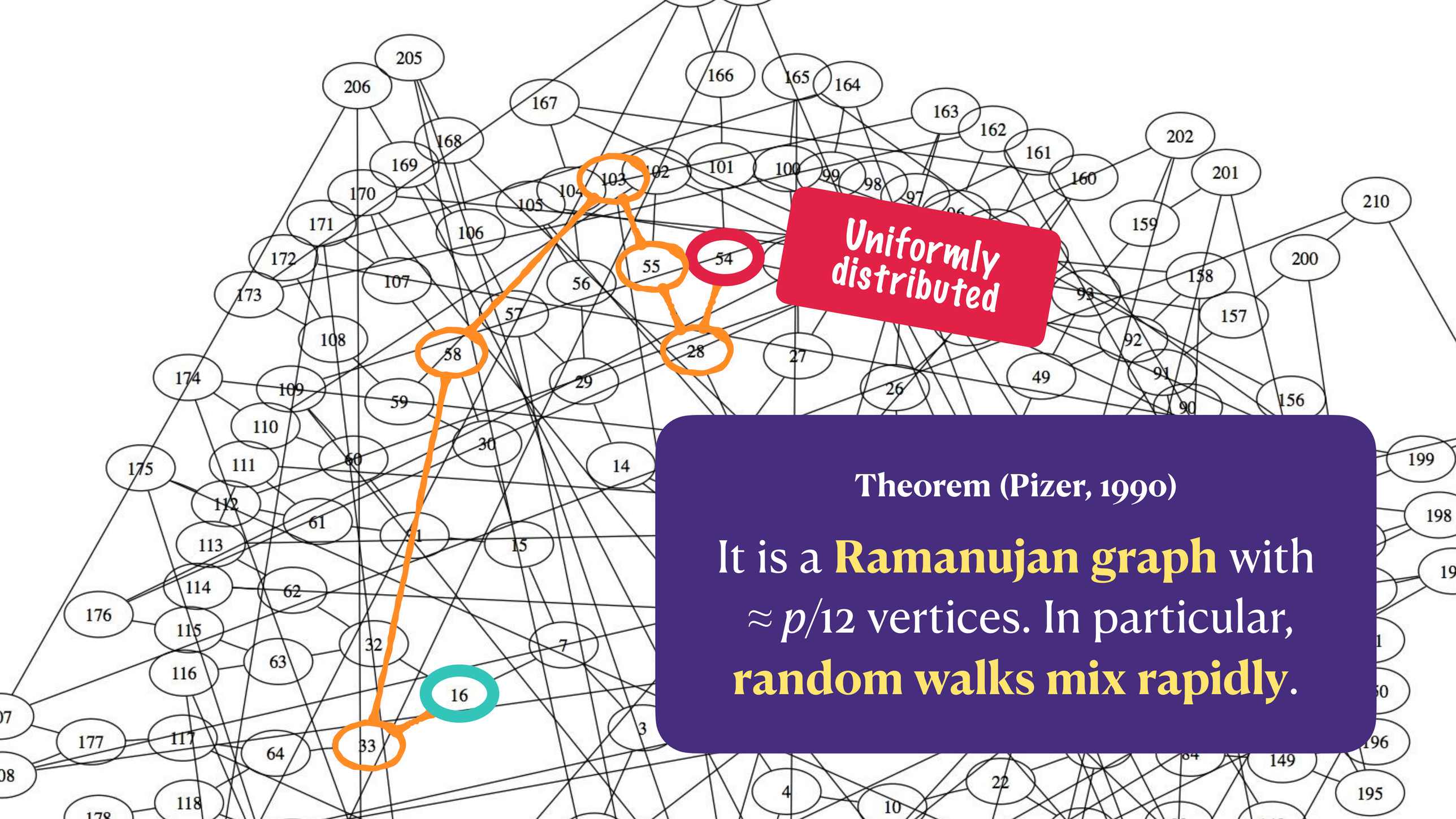


- 3-regular, **connected** (for supersingular curves)
- Paths = isogenies of degree 2^n


205
206
166
165
164
167
163
162
168
161
202
169
160
201
170
104
103
102
101
100
99
98
97
105
96
210
171
106
95
159
172
94
200
55
54
53
52
107
56
158
173
51
93
57
157
50
108
92
58
28
27
174
49
91
109
29
26
59
90
156
110
30
13
48
155
175
111
60
14
25
89
199
112
12
154
61
47
88
198
113
31
15
6
153
114
62
24
87
152
176
5
46
115
2
11
151
32
7
63
86
116
45
23
150
16
85
1
3
177
117
64
33
44
84
196
149
4
22
118
10
195

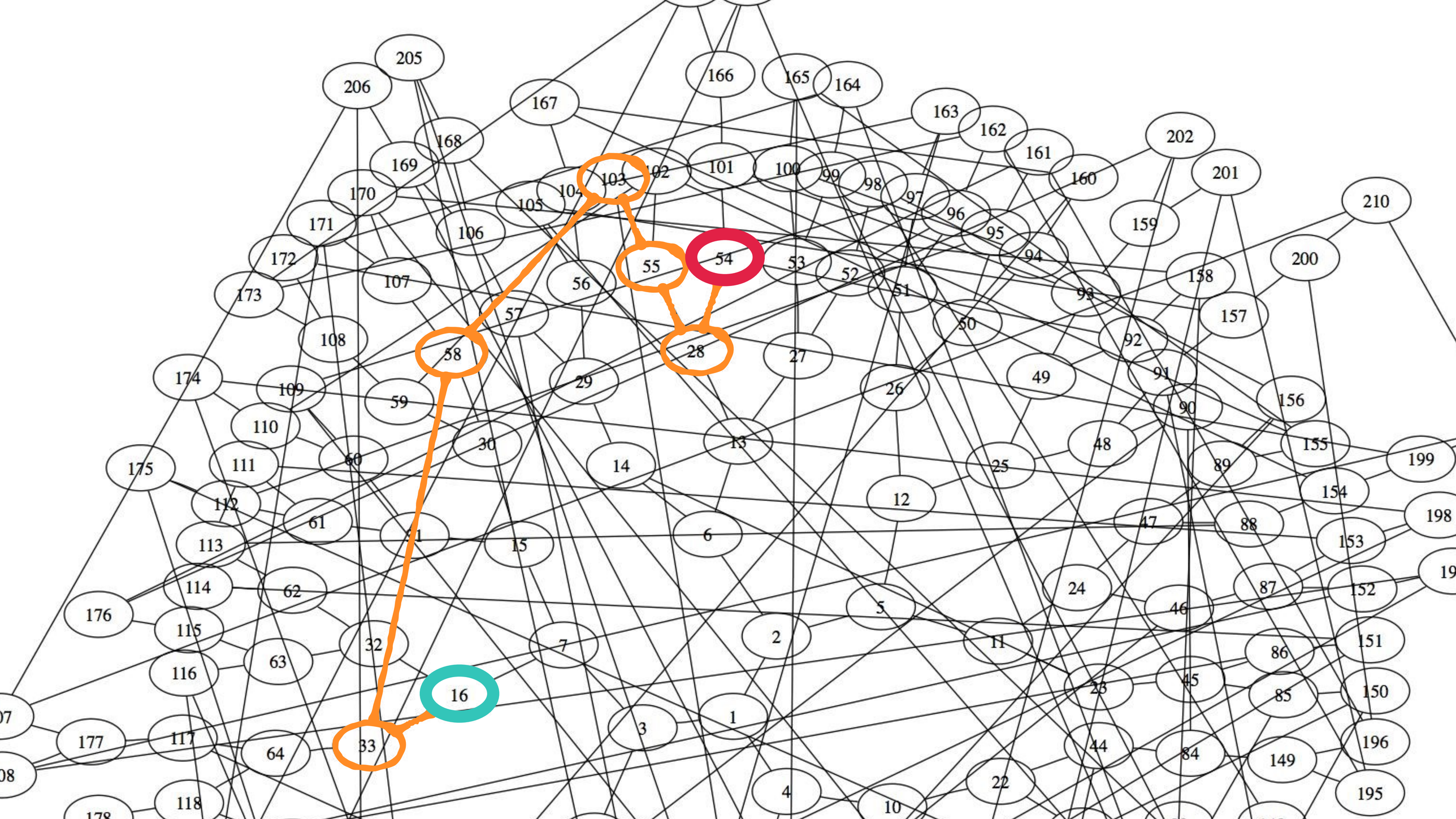

205
206
166
165
164
167
163
162
161
202
168
169
160
201
170
104
103
102
101
100
99
98
97
96
95
210
171
106
105
159
172
55
54
53
52
94
200
107
56
51
158
173
57
50
157
108
58
28
27
92
174
109
59
29
26
49
91
156
110
30
13
48
155
199
175
111
60
14
25
89
154
112
61
12
47
88
198
113
31
15
6
153
114
62
24
87
152
176
115
5
46
63
32
7
2
11
86
151
116
16
45
85
150
1
3
177
117
64
33
44
84
196
149
4
22
118
10
195

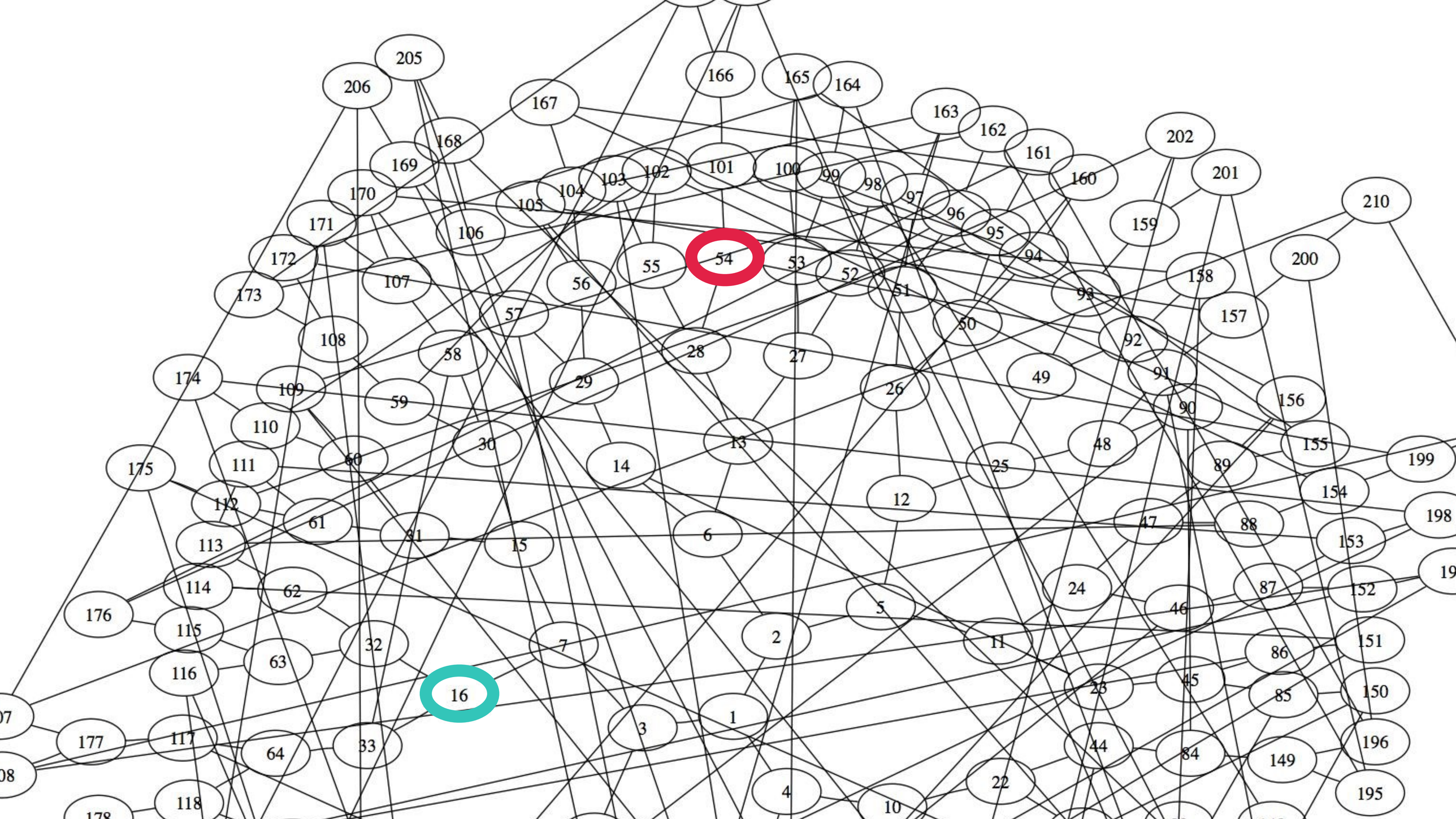

205
206
166
165
164
167
163
162
161
202
168
169
160
201
170
103
102
101
100
99
98
97
96
95
159
210
171
106
105
104
94
172
54
53
52
200
55
158
107
56
51
93
173
57
157
50
108
92
58
28
27
174
49
91
109
29
26
59
90
156
110
30
13
48
155
175
111
60
14
25
89
199
112
12
154
61
47
88
198
113
31
15
6
153
114
62
24
87
152
176
5
46
115
32
7
2
11
86
151
63
116
45
85
150
16
3
1
64
117
44
84
196
177
33
149
118
4
22
195
10

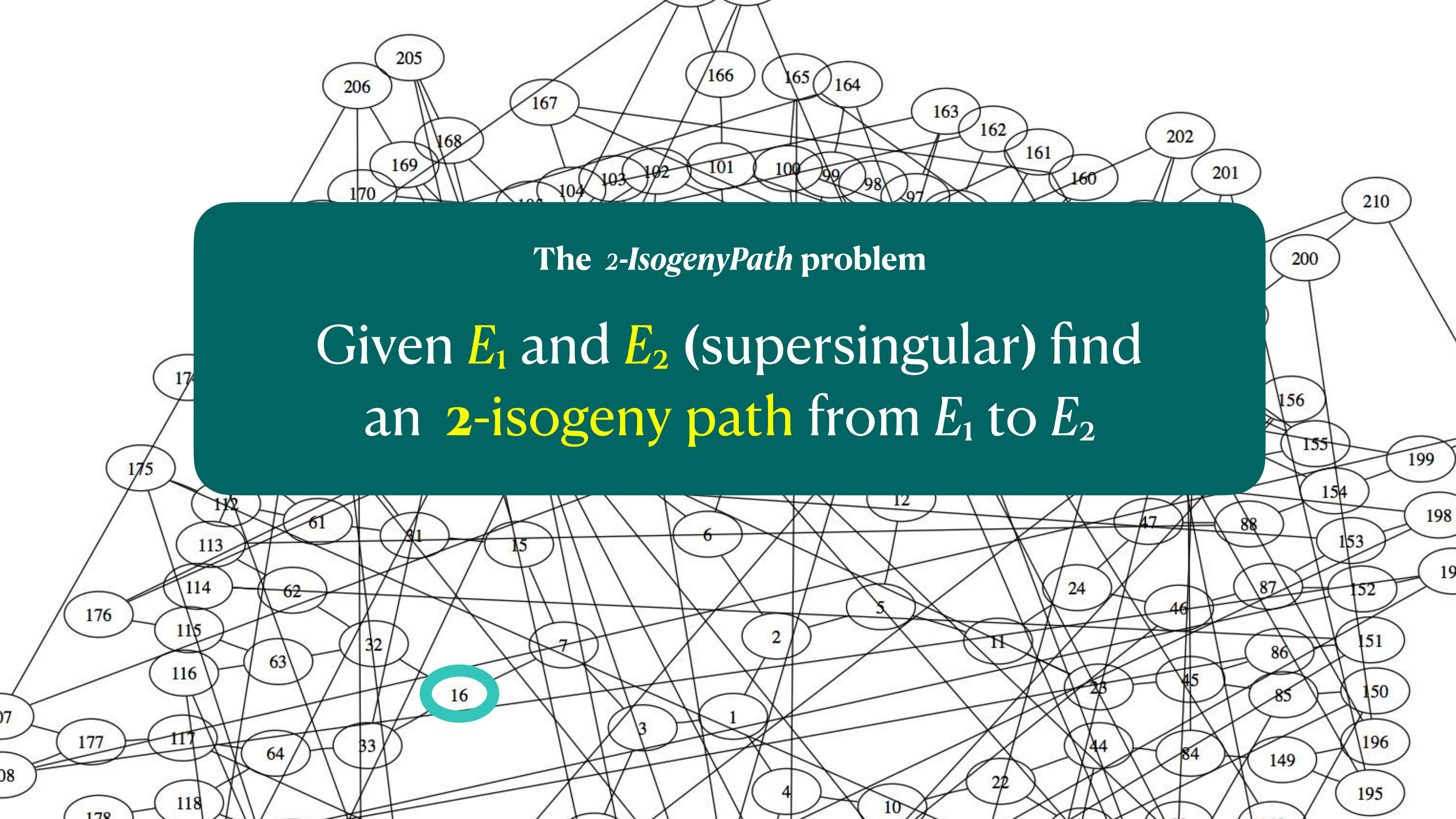


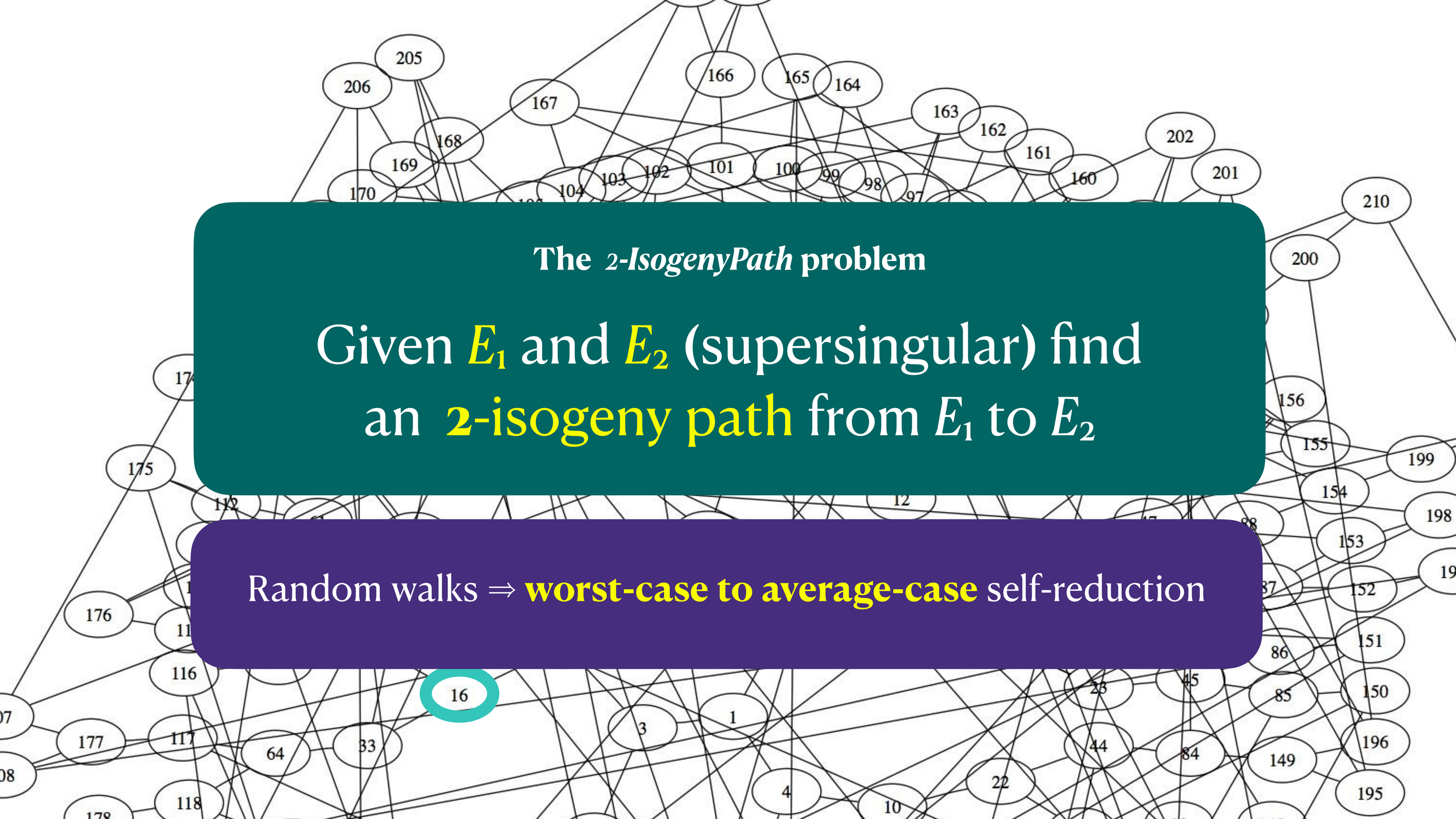
Theorem (Pizer, 1990)

It is a **Ramanujan graph** with $\approx p/12$ vertices. In particular, **random walks mix rapidly**.


205
206
166
165
164
167
163
162
161
202
168
169
160
201
170
103
102
101
100
99
98
97
96
95
159
210
171
106
105
104
94
172
54
53
52
200
55
158
107
56
51
93
173
157
57
50
108
92
58
28
27
174
49
91
109
59
29
26
156
90
110
30
13
48
155
199
175
111
14
25
89
154
60
12
112
61
47
88
198
6
113
31
15
153
114
62
24
87
152
176
5
46
115
32
7
2
11
86
151
63
116
45
85
150
16
3
1
177
117
64
33
44
84
149
196
4
22
118
10
195


205
206
166
165
164
167
163
162
161
202
168
169
160
201
170
104
103
102
101
100
99
98
97
96
95
210
171
106
105
159
172
54
53
52
94
200
55
56
158
107
51
93
173
57
157
50
108
92
58
28
27
174
49
91
109
29
26
59
90
156
110
30
13
48
155
175
111
60
14
25
89
199
112
12
154
61
47
88
198
113
31
15
6
153
114
62
24
87
152
176
5
46
115
32
7
2
11
151
63
86
116
16
23
45
85
150
1
3
177
117
64
33
44
84
196
149
4
22
118
10
195


The 2-IsogenyPath problem
Given E_1 and E_2 (supersingular) find an 2-isogeny path from E_1 to E_2



The *2-IsogenyPath* problem

Given E_1 and E_2 (supersingular) find an **2-isogeny path** from E_1 to E_2

Random walks ⇒ **worst-case to average-case** self-reduction

Interpolation

Representing arbitrary isogenies

Picture by Beppe Rijs

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$

a subgroup of E_1 of order 2^{2n}

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ, the "**interpolation representation**", or "**HD representation** »

HD representation of isogenies

Attacks against SIDH [Eurocrypt 2023: Castryck & Decru, MMPPW, Robert]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Interpolation: **Knowing φ on a few points ⇒ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ, the "**interpolation representation**", or "**HD representation** »

Cost? evaluating an isogeny of degree 2^{2n} in dimension 2, 4 or 8

HD representation of isogenies

Attacks against SIDH [CD23, MMPPW23, Rob23]**:**

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Interpolation: **Knowing φ on a few points $\Rightarrow$ Knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ, the "**interpolation representation**", or "**HD representation**"

Fastest, but requires $2^{2n} - d = a^2$

Cost? evaluating an isogeny of degree 2^{2n} in dimension 2, 4 or 8

HD representation of isogenies

Attacks against SIDH [CD23, MMPPW23, Rob23]:

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Somewhat fast, but requires $2^{2n} - d = a^2 + b^2$

Fastest, but requires $2^{2n} - d = a^2$

Interpolation: **Knowing φ on a few points $\Rightarrow$ knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ, the "**interpolation representation**", or "**HD representation**"

Cost? evaluating an isogeny of degree 2^{2n} in dimension 2, 4 or 8

HD representation of isogenies

Attacks against SIDH [CD23, MMPPW23, Rob23]:

- Let $\varphi : E_1 \to E_2$ of degree d
- Let (P, Q) is a basis of $E_1[2^n]$, with $2^{2n} > 4 \cdot \deg(\varphi)$
- Given $(d, P, Q, \varphi(P), \varphi(Q))$, one can compute $\varphi(R)$ for any $R \in E_1$ in poly. time

a subgroup of E_1 of order 2^{2n}

Somewhat fast, but requires $2^{2n} - d = a^2 + b^2$

Fastest, but requires $2^{2n} - d = a^2$

Very costly, but always works

Interpolation: **Knowing φ on a few points $\Leftrightarrow$ knowing φ everywhere**

Corollary: $(d, P, Q, \varphi(P), \varphi(Q))$ is an efficient representation of φ, the "**interpolation representation**", or "**HD representation**"

Cost? evaluating an isogeny of degree 2^{2n} in dimension 2, 4 or 8

The *Isogeny* problem

Given E_1 and E_2 supersingular, find an isogeny $\varphi : E_1 \to E_2$ in interpolation representation

Isogeny

2-IsogenyPath


trivial
Isogeny
2-IsogenyPath

[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018] / **[W. – FOCS 2021]** + **[Page, W. – Eurocrypt 2024]**

Endomorphisms

and computational problems

Picture by Beppe Rijs

Endomorphism ring

An **endomorphism** of E is an isogeny $\varphi : E \to E$ (or the zero map [0])

Endomorphism ring

An **endomorphism** of E is an isogeny $\varphi : E \to E$ (or the zero map [0])

The **endomorphism ring** of E is $\mathrm{End}(E) = \{\varphi : E \to E\}$

Endomorphism ring

An **endomorphism** of E is an isogeny $\varphi : E \to E$ (or the zero map [0])

The **endomorphism ring** of E is $\mathrm{End}(E) = \{\varphi : E \to E\}$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

Endomorphism ring

An **endomorphism** of E is an isogeny $\varphi : E \to E$ (or the zero map [0])

The **endomorphism ring** of E is $\mathrm{End}(E) = \{\varphi : E \to E\}$

- $\varphi + \psi$ is pointwise addition: $(\varphi + \psi)(P) = \varphi(P) + \psi(P)$
- $\varphi\psi$ is the composition: $(\varphi\psi)(P) = \varphi(\psi(P))$

Multiplication by $m \in \mathbb{Z}$ is an endomorphism

$$[m] : E \to E : P \mapsto P + \ldots + P$$

It forms a subring $\mathbb{Z} \subset \mathrm{End}(E)$

Endomorphism ring

What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...

Endomorphism ring

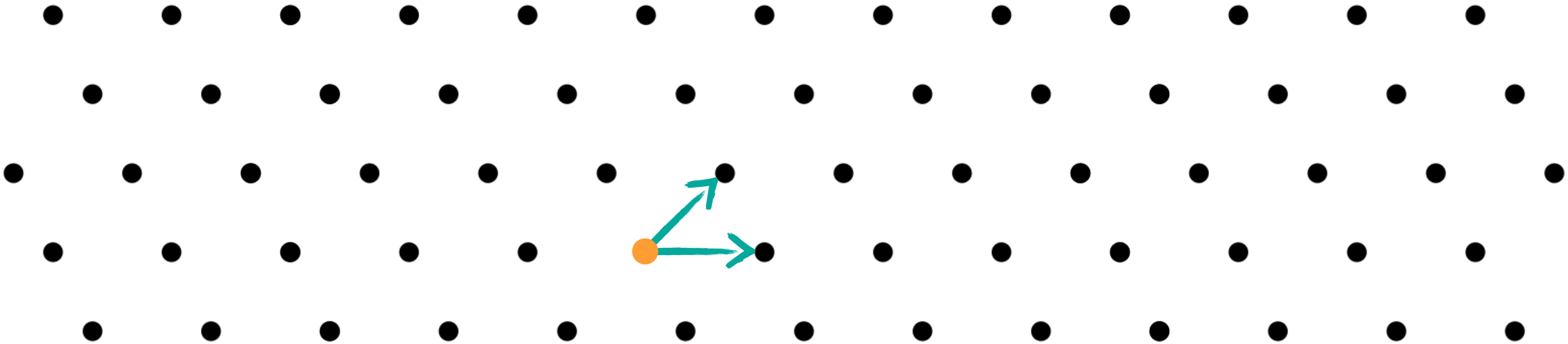
What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4

Endomorphism ring

What is the structure of End(E)?

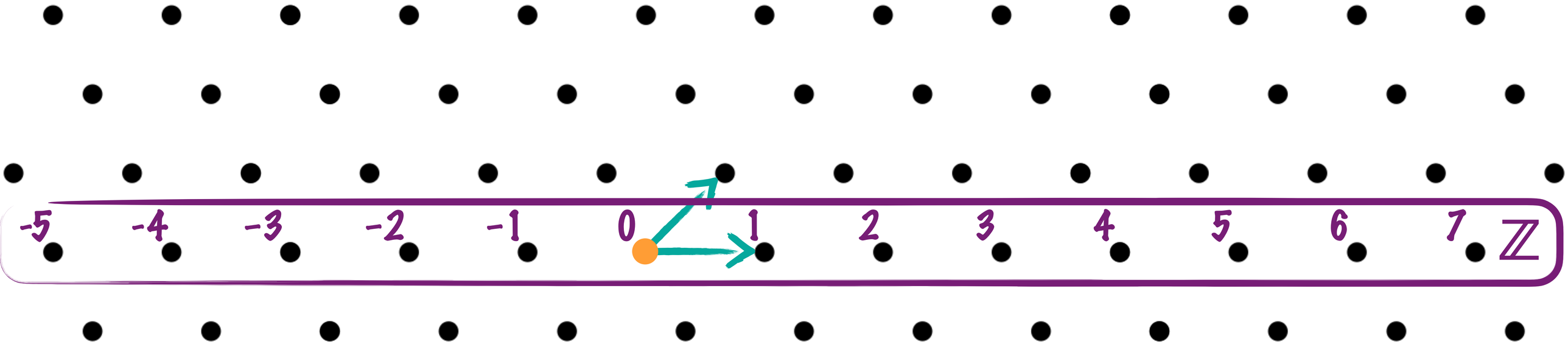
- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4



Endomorphism ring

What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4



Endomorphism ring

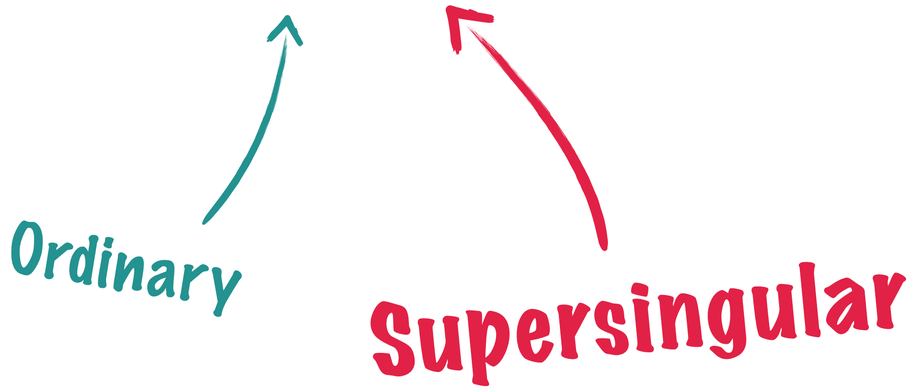
What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4

Endomorphism ring

What is the structure of End(E)?

- It contains $\mathbb{Z} \subset \mathrm{End}(E)$...
- (End(E), +) is a **lattice** of dimension 2 or 4



The endomorphism ring problem

For E **supersingular** $\mathrm{End}(E) = \{\varphi : E \to E\}$ is a lattice of dimension 4

The *EndRing* problem

Given E (supersingular) find 4 generators of the endomorphism ring $\mathrm{End}(E)$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$ $\iota^2 = [-1]$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$ $\iota^2 = [-1]$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$ $\quad \iota\pi = -\pi\iota$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

$\iota^2 = [-1]$

$\iota\pi = -\pi\iota$

$\pi^2 = [-p]$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

$\iota^2 = [-1]$

$\iota\pi = -\pi\iota$

$\pi^2 = [-p]$

$$\mathbf{End}(E_0) \stackrel{?}{=} \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\pi \oplus \mathbb{Z}\iota\pi$$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

$\iota^2 = [-1]$

$\iota\pi = -\pi\iota$

$\pi^2 = [-p]$

$$\textbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

$\iota^2 = [-1]$

$\iota\pi = -\pi\iota$

$\pi^2 = [-p]$

$$\mathbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

EndRing

Quaternion algebra

The **quaternion algebra $B_{p,\infty}$** is the ring (for $p \equiv 3 \pmod 4$)

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\, i \oplus \mathbb{Q}\, j \oplus \mathbb{Q}\, k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

Quaternion algebra

The **quaternion algebra $B_{p,\infty}$** is the ring (for $p \equiv 3 \pmod 4$)

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\, i \oplus \mathbb{Q}\, j \oplus \mathbb{Q}\, k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

End(E) is (isomorphic to) a discrete subrings of $B_{p,\infty}$

Quaternion algebra

The **quaternion algebra $B_{p,\infty}$** is the ring (for $p \equiv 3 \pmod 4$)

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\, i \oplus \mathbb{Q}\, j \oplus \mathbb{Q}\, k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

End(E) is (isomorphic to) a discrete subrings of $B_{p,\infty}$

- End(E) is a **maximal order** in $B_{p,\infty}$

Quaternion algebra

The **quaternion algebra $B_{p,\infty}$** is the ring (for $p \equiv 3 \pmod 4$)

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\, i \oplus \mathbb{Q}\, j \oplus \mathbb{Q}\, k$$

where $i^2 = -1$, $j^2 = -p$, and $k = ij = -ji$

End(E) is (isomorphic to) a discrete subrings of $B_{p,\infty}$

- End(E) is a **maximal order** in $B_{p,\infty}$
- There are **many** maximal orders in $B_{p,\infty}$

Example

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-scalar endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$

$\iota^2 = [-1]$

$\iota\pi = -\pi\iota$

$\pi^2 = [-p]$

$$\mathbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

$$\simeq \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\,\frac{i + j}{2} \oplus \mathbb{Z}\,\frac{1 + ij}{2} \subset B_{p,\infty}$$

EndRing

MaxOrder

One Endomorphism

- We always have $\mathbb{Z} \subset \mathrm{End}(E)$, that part is easy
- Finding any **non-scalar** endomorphism?

One Endomorphism

- We always have $\mathbb{Z} \subset \mathrm{End}(E)$, that part is easy
- Finding any **non-scalar** endomorphism?

The *OneEnd* problem

Given E (supersingular) find ***one*** endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$

Which is hardest? Easiest?

EndRing

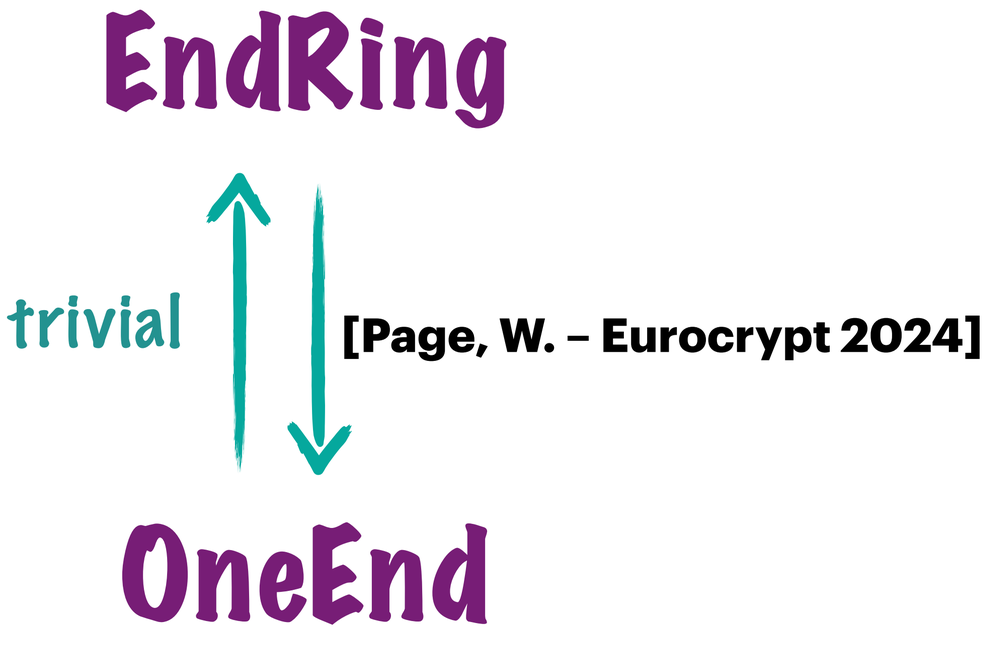
2-IsogenyPath

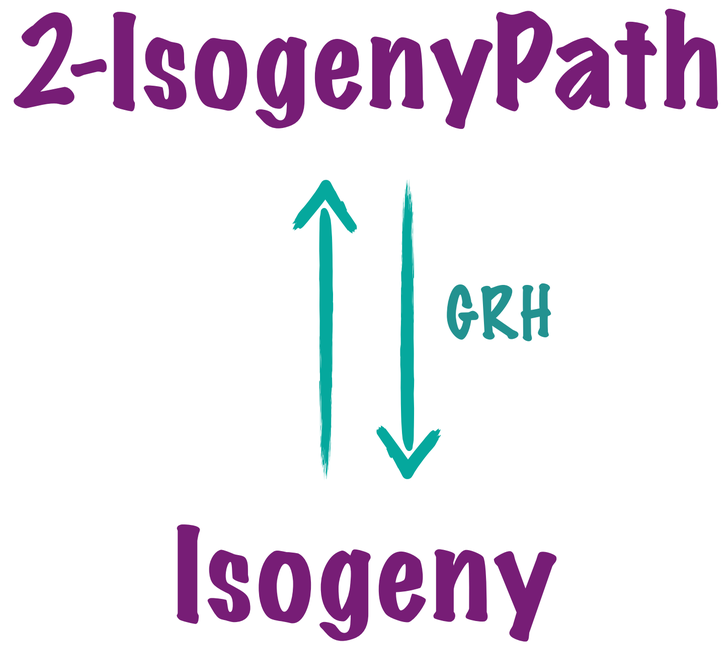
OneEnd

Isogeny

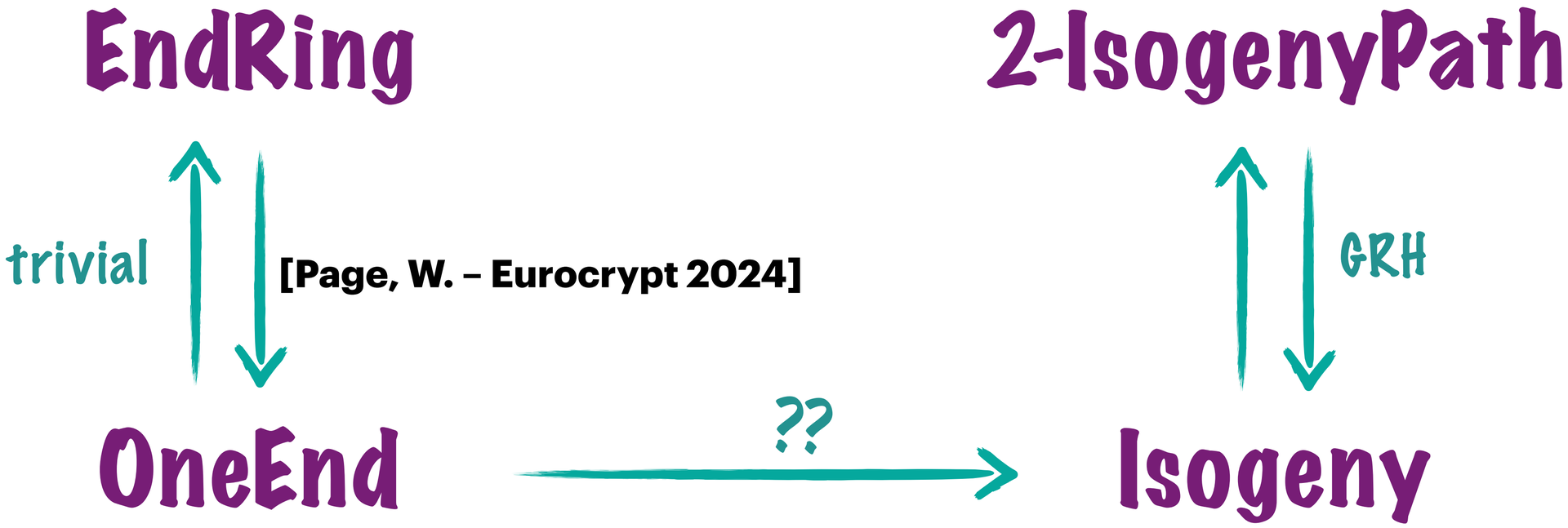
Which is hardest? Easiest?

Which is hardest? Easiest?





Which is hardest? Easiest?



OneEnd reduces to Isogeny

Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

OneEnd reduces to Isogeny

Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

How to find endomorphisms of E:

OneEnd reduces to Isogeny

Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

How to find endomorphisms of *E*:

OneEnd reduces to Isogeny

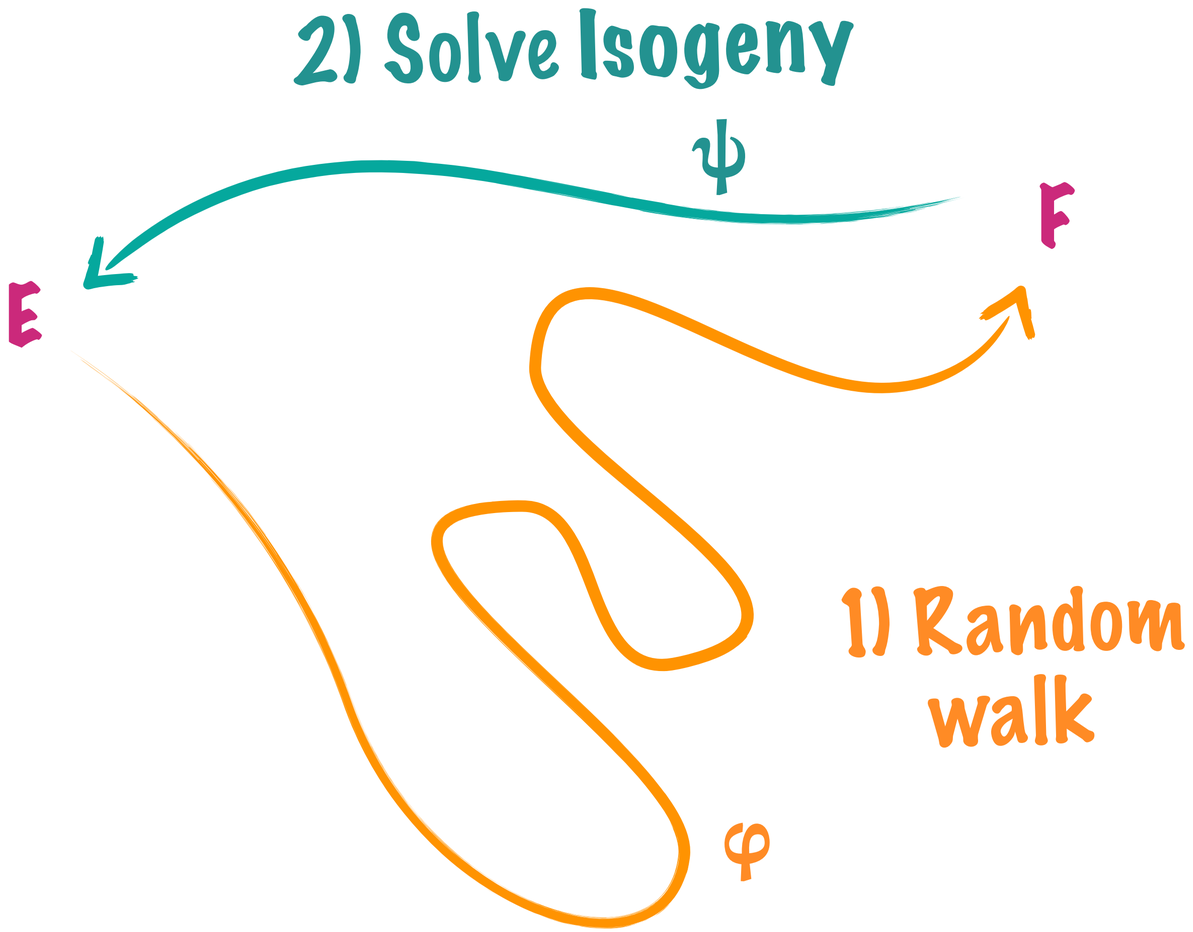
Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

How to find endomorphisms of *E*:

OneEnd reduces to Isogeny

Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

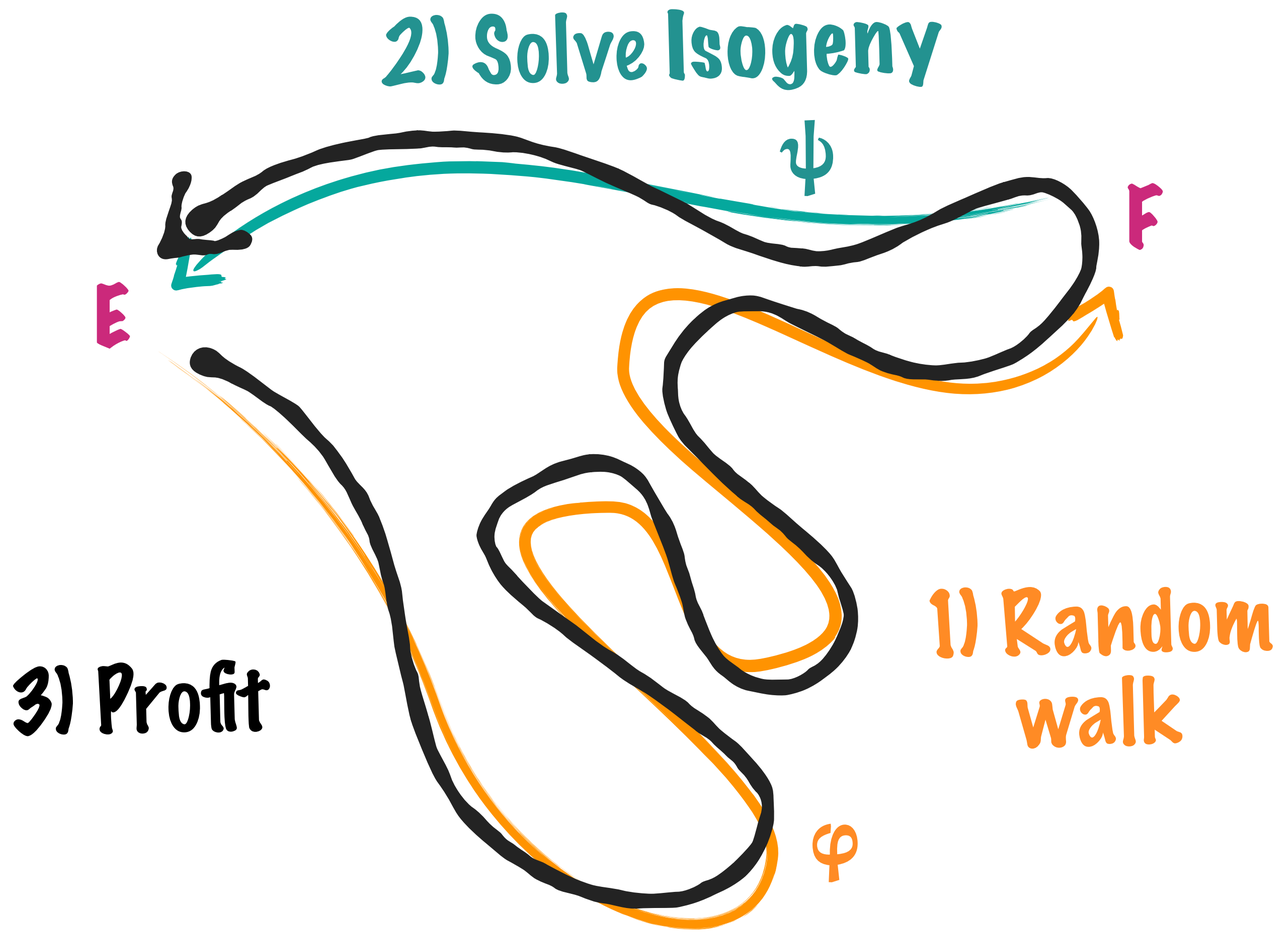
How to find endomorphisms of *E*:



OneEnd reduces to Isogeny

Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

How to find endomorphisms of *E*:

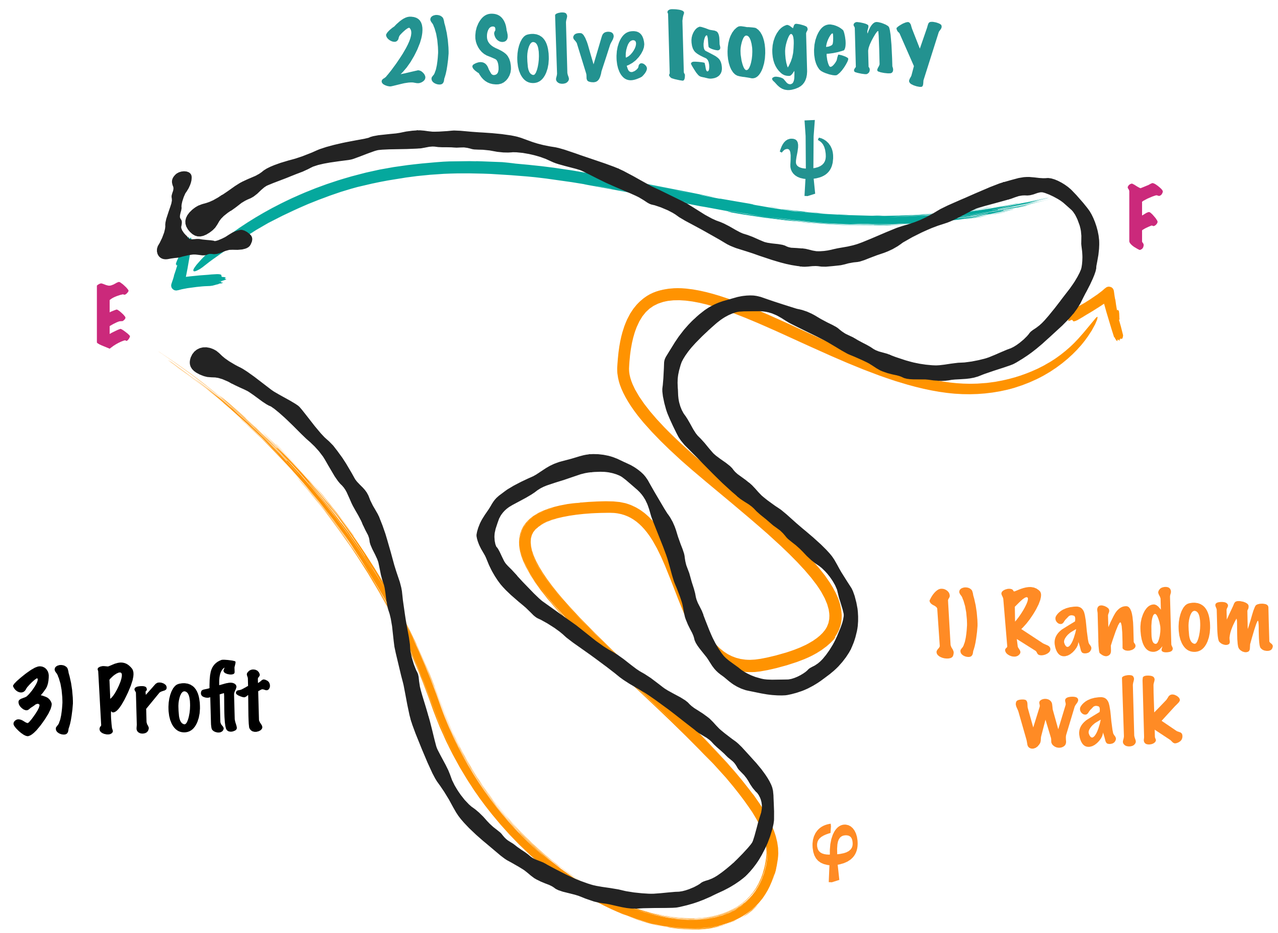


OneEnd reduces to Isogeny

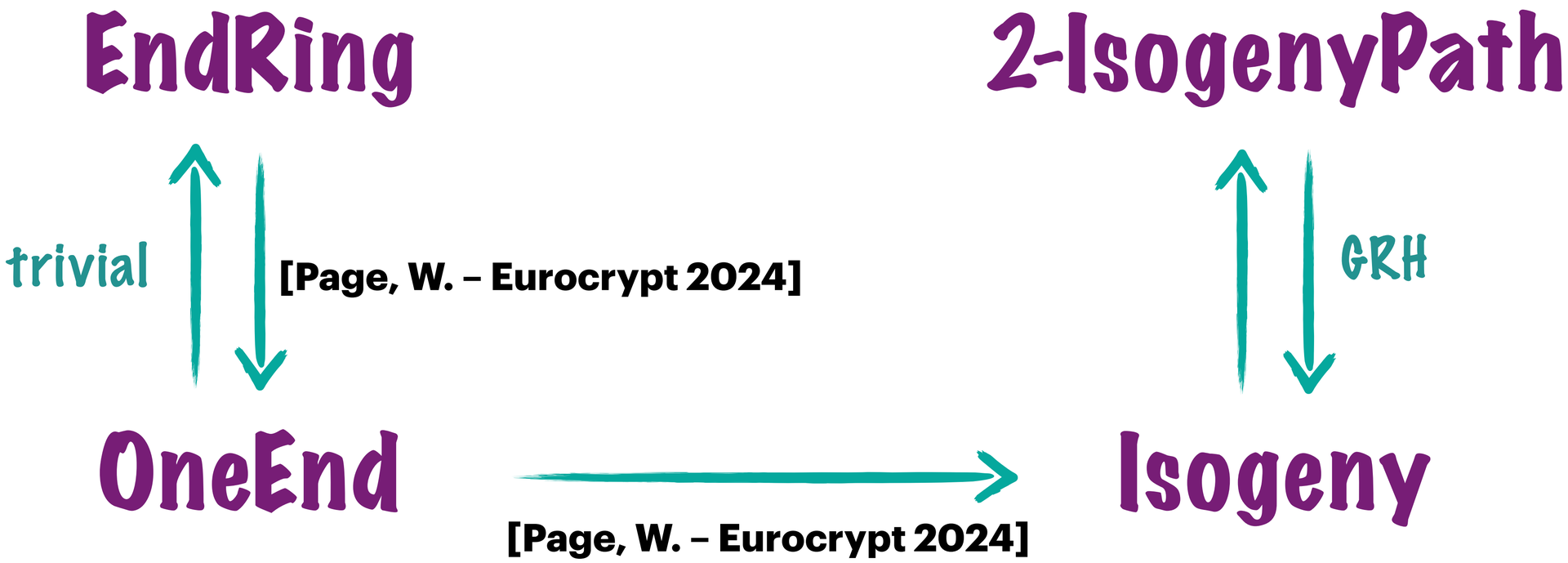
Suppose we can solve **Isogeny**.
Can solve **OneEnd**?

How to find endomorphisms of E:

- If φ is long enough $\psi \circ \varphi \notin \mathbb{Z}$



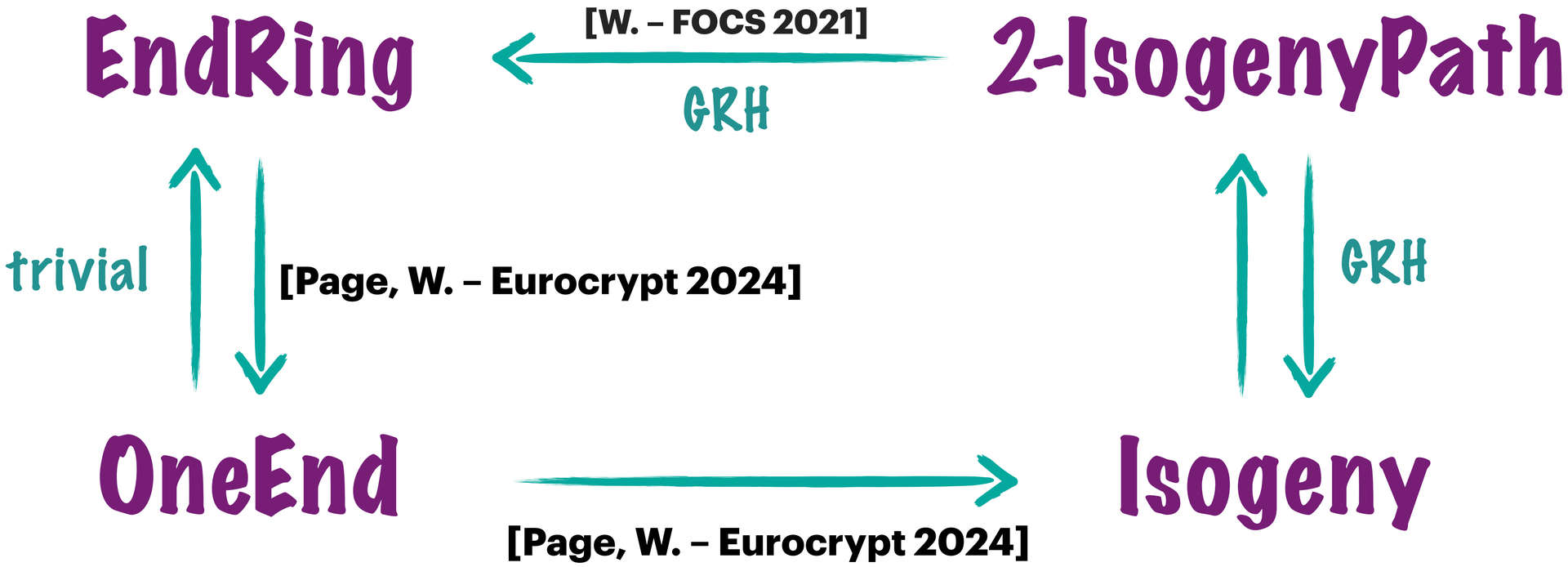
Which is hardest? Easiest?



Earlier heuristic reductions: **[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018]**

Recent unconditional reductions: **[Herlédan Le Merdy, W. – IACR eprint 2025]**

Which is hardest? Easiest?



Earlier heuristic reductions: **[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018]**

Recent unconditional reductions: **[Herlédan Le Merdy, W. – IACR eprint 2025]**

Isogeny World

Quaternion World

Deuring correspondence

Supersingular curves E over $\mathbb{F}_{p2}$
(up to isomorphism)

Maximal orders $\mathcal{O}$ in $B_{p,\infty}$

$\mathcal{O} \simeq \mathbf{End}(E)$

(up to isomorphism)

Isogeny World

Quaternion World

Deuring correspondence

Supersingular curves E over $\mathbb{F}_{p2}$ (up to isomorphism)	Maximal orders $\mathcal{O}$ in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ (up to isomorphism)
Isogenies $\varphi : E \to E'$	$(\mathcal{O},\mathcal{O}')$-ideals I, $\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

Isogeny World

Quaternion World

Deuring correspondence

Isogeny World	Quaternion World
Supersingular curves E over $\mathbb{F}_{p2}$ (up to isomorphism)	Maximal orders $\mathcal{O}$ in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ (up to isomorphism)
Isogenies $\varphi : E \to E'$	$(\mathcal{O},\mathcal{O}')$-ideals I, $\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

Isogeny:

Given E and E',
find $\varphi : E \longrightarrow E'$

Isogeny World

Quaternion World

Deuring correspondence

Isogeny World	Quaternion World
Supersingular curves E over $\mathbb{F}_{p2}$ (up to isomorphism)	Maximal orders $\mathcal{O}$ in $B_{p,\infty}$ $\mathcal{O} \simeq \mathbf{End}(E)$ (up to isomorphism)
Isogenies $\varphi : E \to E'$	$(\mathcal{O},\mathcal{O}')$-ideals I, $\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

Isogeny:

Given E and E',
find $\varphi : E \longrightarrow E'$

Connecting ideal:

Given $\mathcal{O}$ and $\mathcal{O}'$, find
an $(\mathcal{O},\mathcal{O}')$-ideal I

Isogeny World

Quaternion World

Deuring correspondence

Supersingular curves E over $\mathbb{F}_{p^2}$
(up to isomorphism)

Maximal orders $\mathcal{O}$ in $B_{p,\infty}$
$\mathcal{O} \simeq \mathbf{End}(E)$
(up to isomorphism)

Isogenies $\varphi : E \to E'$

$(\mathcal{O},\mathcal{O}')$-ideals I,
$\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

HARD

Isogeny:

Given E and E',
find $\varphi : E \longrightarrow E'$

EASY

Connecting ideal:

Given $\mathcal{O}$ and $\mathcal{O}'$, find
an $(\mathcal{O},\mathcal{O}')$-ideal I

Isogeny World

Quaternion World

Deuring correspondence

Supersingular curves E over $\mathbb{F}_{p^2}$
(up to isomorphism)

Maximal orders $\mathcal{O}$ in $B_{p,\infty}$
$\mathcal{O} \simeq \mathbf{End}(E)$
(up to isomorphism)

Isogenies $\varphi : E \to E'$

$(\mathcal{O},\mathcal{O}')$-ideals I,
$\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

HARD

EndRing/MaxOrder

EASY

Isogeny:

Given E and E',
find $\varphi : E \longrightarrow E'$

Connecting ideal:

Given $\mathcal{O}$ and $\mathcal{O}'$, find
an $(\mathcal{O},\mathcal{O}')$-ideal I

Isogeny World

Quaternion World

Deuring correspondence

Supersingular curves E over $\mathbb{F}_{p2}$
(up to isomorphism)

Maximal orders $\mathcal{O}$ in $B_{p,\infty}$
$\mathcal{O} \simeq \mathbf{End}(E)$
(up to isomorphism)

Isogenies $\varphi : E \to E'$

$(\mathcal{O},\mathcal{O}')$-ideals I,
$\mathcal{O} \simeq \mathbf{End}(E)$ and $\mathcal{O}' \simeq \mathbf{End}(E')$

HARD

EndRing/MaxOrder

EASY

Isogeny:

Given E and E',
find $\varphi : E \to E'$

KLPT, Clapoti...

Connecting ideal:

Given $\mathcal{O}$ and $\mathcal{O}'$, find
an $(\mathcal{O},\mathcal{O}')$-ideal I

EndRing ⇔ Isogeny

EndRing ⇔ Isogeny

[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018] *Supersingular isogeny graphs and endomorphism rings: Reductions and solutions*.

[W. – FOCS 2021] *The supersingular isogeny path and endomorphism ring problems are equivalent*.

EndRing ⇔ Isogeny

End(–) is a GPS that allows you to find your way between supersingular curves:

- given $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$, one can find an isogeny $E_1 \to E_2$ in poly. time

[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018] *Supersingular isogeny graphs and endomorphism rings: Reductions and solutions*.

[W. – FOCS 2021] *The supersingular isogeny path and endomorphism ring problems are equivalent*.

EndRing ⇔ Isogeny

End(–) is a GPS that allows you to find your way between supersingular curves:

- given End(E_1) and End(E_2), one can find an isogeny $E_1 \to E_2$ in poly. time

You can update the GPS coordinates as you travel through isogenies:

- given End(E_1), and a (smooth) isogeny $E_1 \to E_2$, one can find End(E_2) in poly. time

[Eisenträger, Hallgren, Lauter, Morrison, Petit – Eurocrypt 2018] *Supersingular isogeny graphs and endomorphism rings: Reductions and solutions*.

[W. – FOCS 2021] *The supersingular isogeny path and endomorphism ring problems are equivalent*.

EndRing ⇔ Isogeny

End(–) is a GPS that allows you to find your way between supersingular curves:

- given End(E_1) and End(E_2), one can find an isogeny $E_1 \to E_2$ in poly. time

You can update the GPS coordinates as you travel through isogenies:

- given End(E_1), and a (smooth) isogeny $E_1 \to E_2$, one can find End(E_2) in poly. time

For E_1, E_2 supersingular, Hom(E_1, E_2) is a lattice of rank 4

EndRing ⇔ Isogeny

End(–) is a GPS that allows you to find your way between supersingular curves:

- given End(E_1) and End(E_2), one can find ~~an isogeny $E_1 \to E_2$ in poly. time~~ a basis of Hom(E_1, E_2)

You can update the GPS coordinates as you travel through isogenies:

- given End(E_1), and a (smooth) isogeny $E_1 \to E_2$, one can find End(E_2) in poly. time

For E_1, E_2 supersingular, Hom(E_1, E_2) is a lattice of rank 4

EndRing ⇔ Isogeny

End(–) is a GPS that allows you to find your way between supersingular curves:

- given End(E_1) and End(E_2), one can find ~~an isogeny $E_1 \to E_2$ in poly. time~~ a basis of Hom(E_1, E_2)

You can update the GPS coordinates as you travel through isogenies:

- given End(E_1), and a (smooth) isogeny $E_1 \to E_2$, one can find End(E_2) in poly. time

For E_1, E_2 supersingular, Hom(E_1, E_2) is a lattice of rank 4

Computing End(–) ⇔ Computing Hom(–, –)

Key generation

Generating a curve with its endomorphism ring

Picture by Beppe Rijs

Keys

- **Public key**: a supersingular curve E_{pk}
- **Secret key**: a basis of $\text{End}(E_{\text{pk}})$

Keys

- **Public key**: a supersingular curve E_{pk}
- **Secret key**: a basis of $\text{End}(E_{\text{pk}})$

How to generate a random E_{pk} together with $\text{End}(E_{\text{pk}})$?

Keys

- **Public key**: a supersingular curve E_{pk}
- **Secret key**: a basis of $\text{End}(E_{\text{pk}})$

How to generate a random E_{pk} together with $\text{End}(E_{\text{pk}})$?

How to generate even a single supersingular curve?

A special supersingular curve

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

Two non-trivial endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$ $\quad \iota\pi = -\pi\iota$

$$\textbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

A special supersingular curve

Example: $p \equiv 3 \pmod 4$, so $\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha)$ where $\alpha^2 = -1$, and

Consider $E_0 : y^2 = x^3 + x$

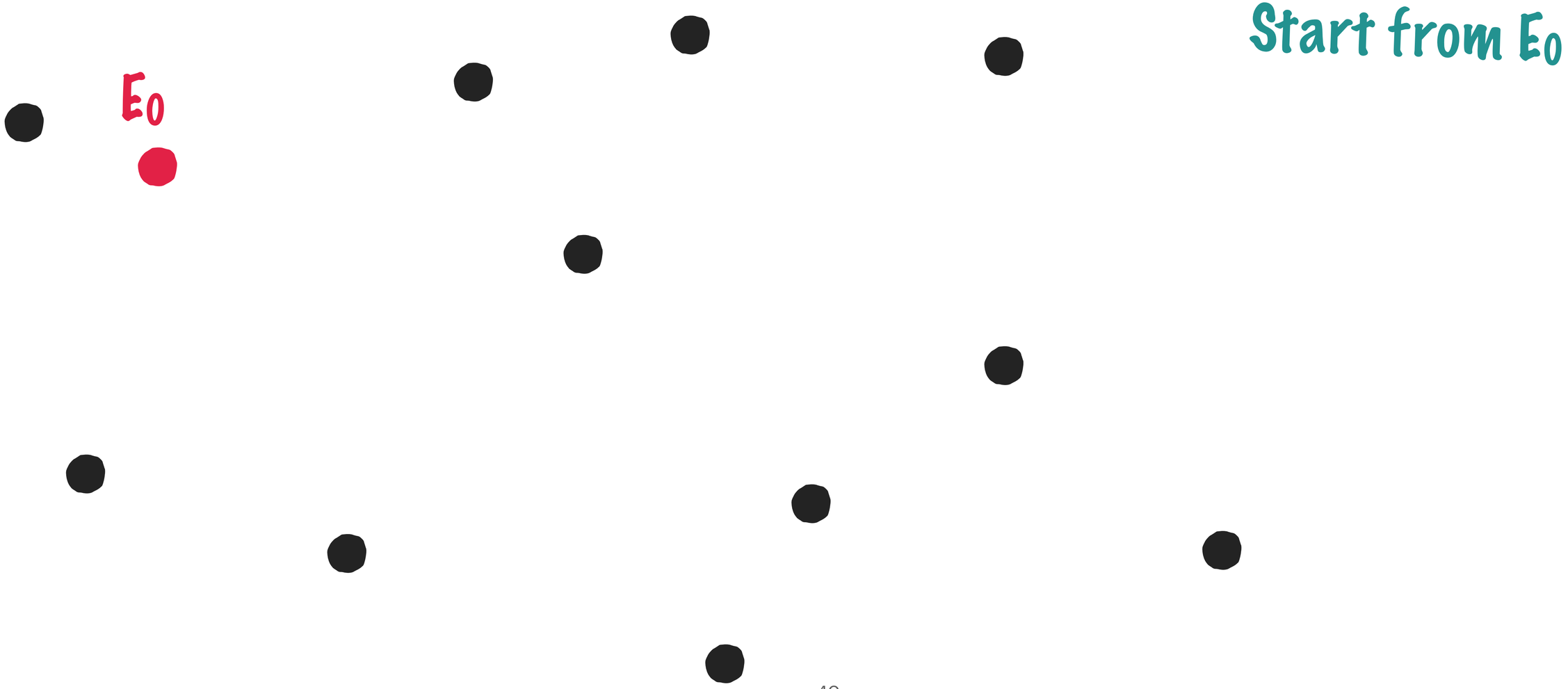
Two non-trivial endomorphisms:

- $\iota : E_0 \to E_0 : (x, y) \mapsto (-x, \alpha y)$ $\quad \iota^2 = [-1]$
- $\pi : E_0 \to E_0 : (x, y) \mapsto (x^p, y^p)$ $\quad \iota\pi = -\pi\iota$

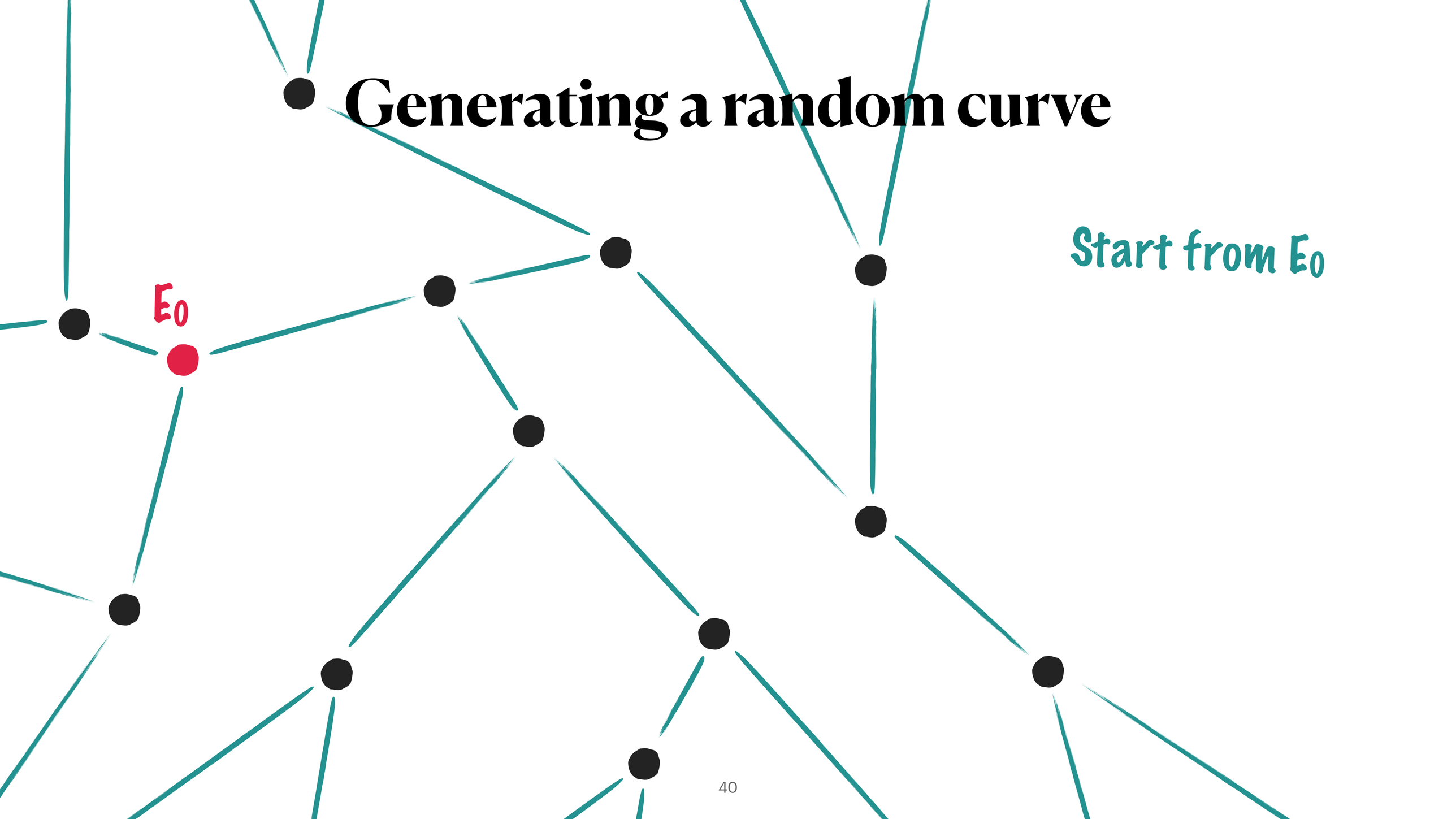
$$\textbf{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\,\frac{\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{1 + \iota\pi}{2}$$

E_0 and End(E_0) is our reference

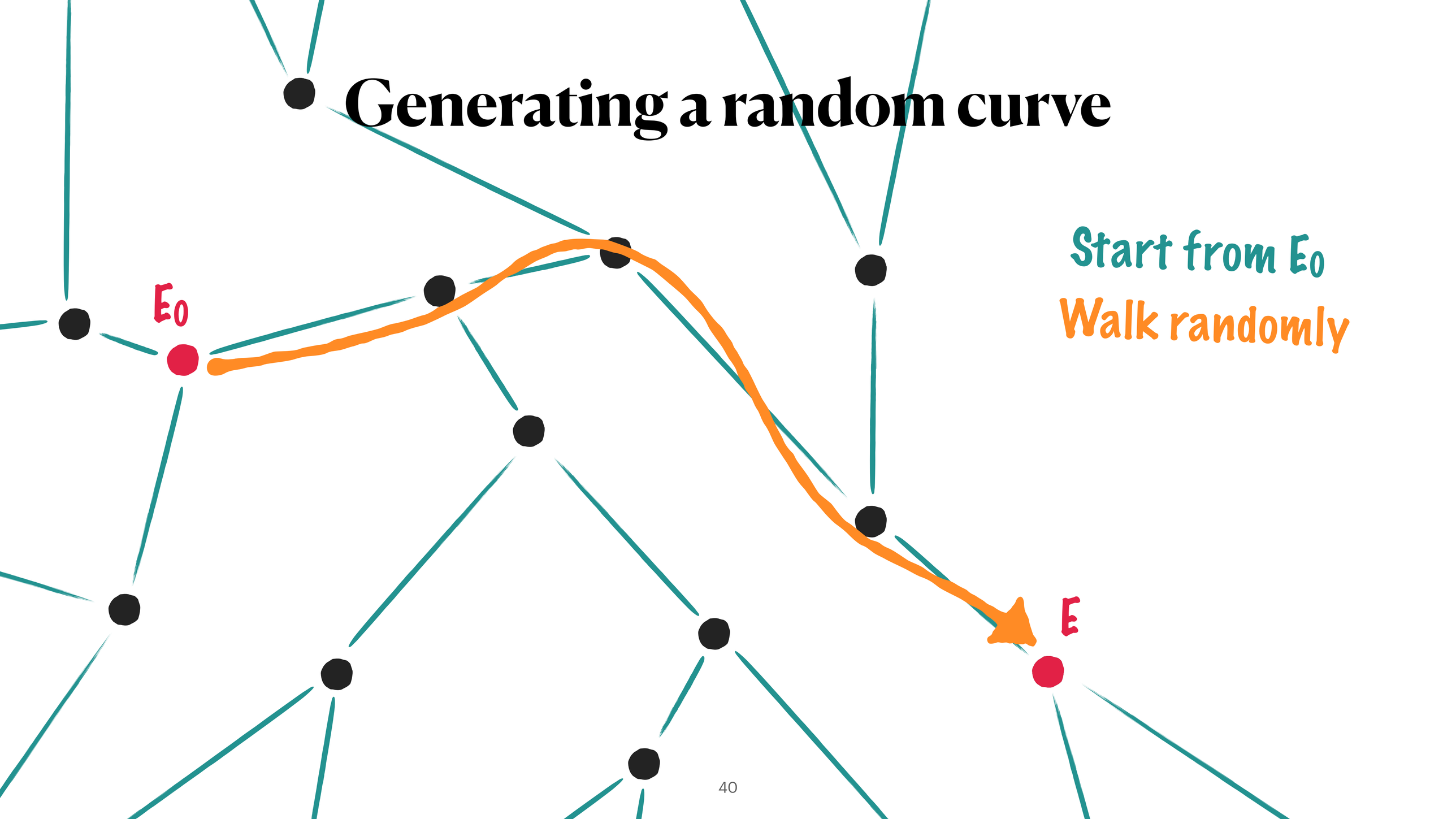
Generating a random curve



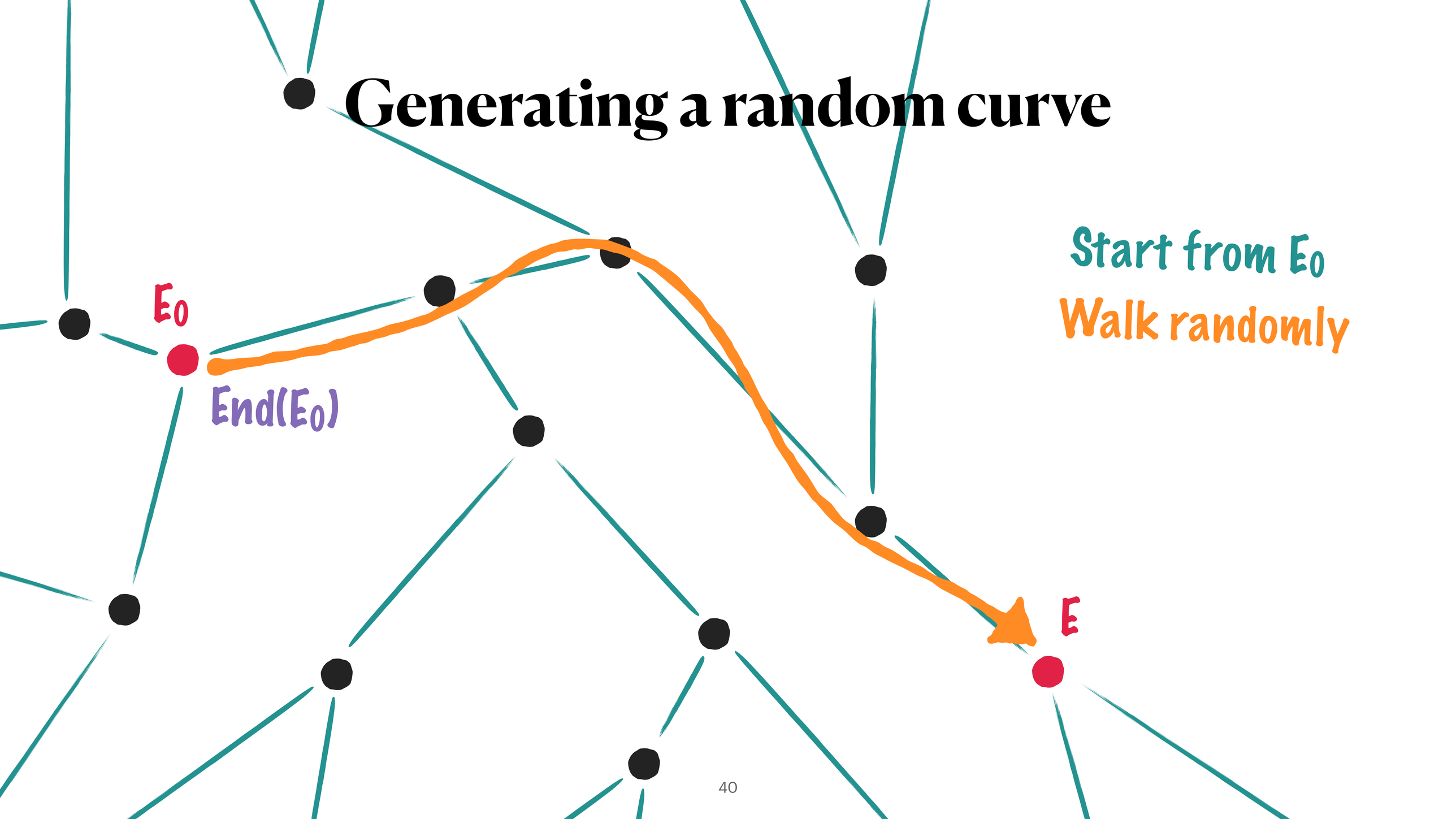
Generating a random curve



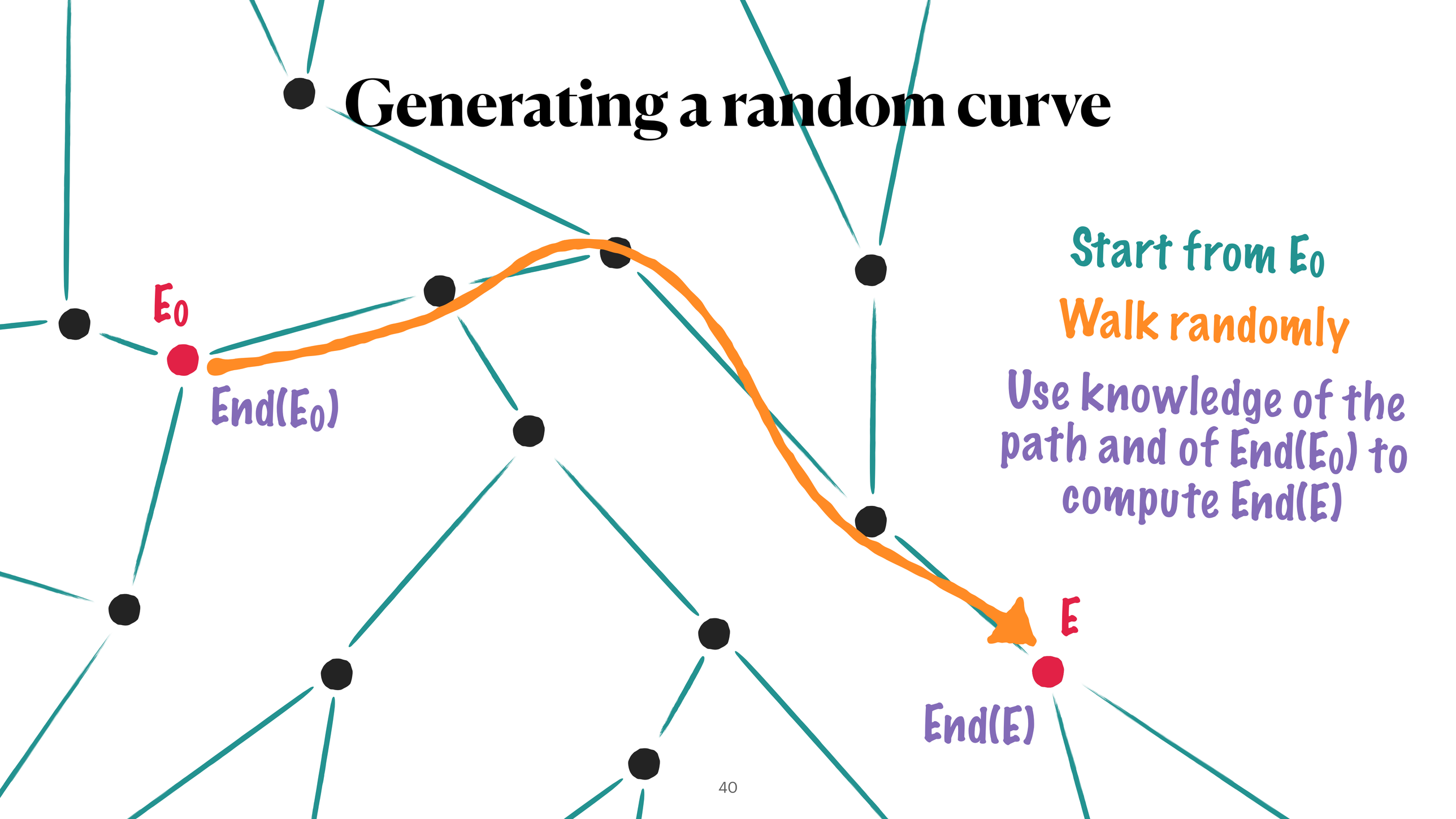
Generating a random curve



Generating a random curve



Generating a random curve



One can generate $(E, \mathrm{End}(E))$ with E uniform