Supersingular isogenies in cryptography

Craig Costello

Summer School on Real-World Crypto and Privacy
June 15, 2018
Šibenik, Croatia

Microsoft® Research

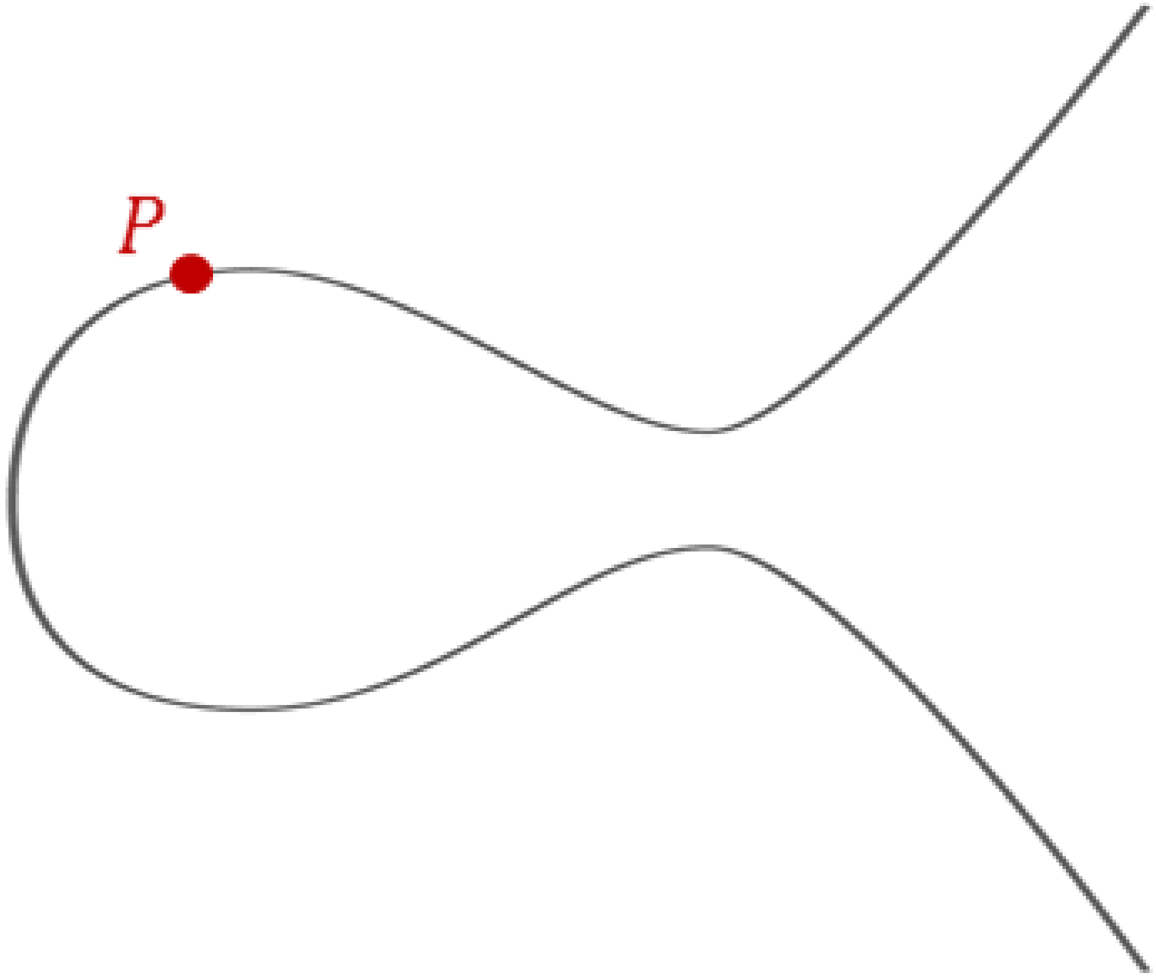
Part 1: Motivation

Part 2: Preliminaries

Part 3: SIDH

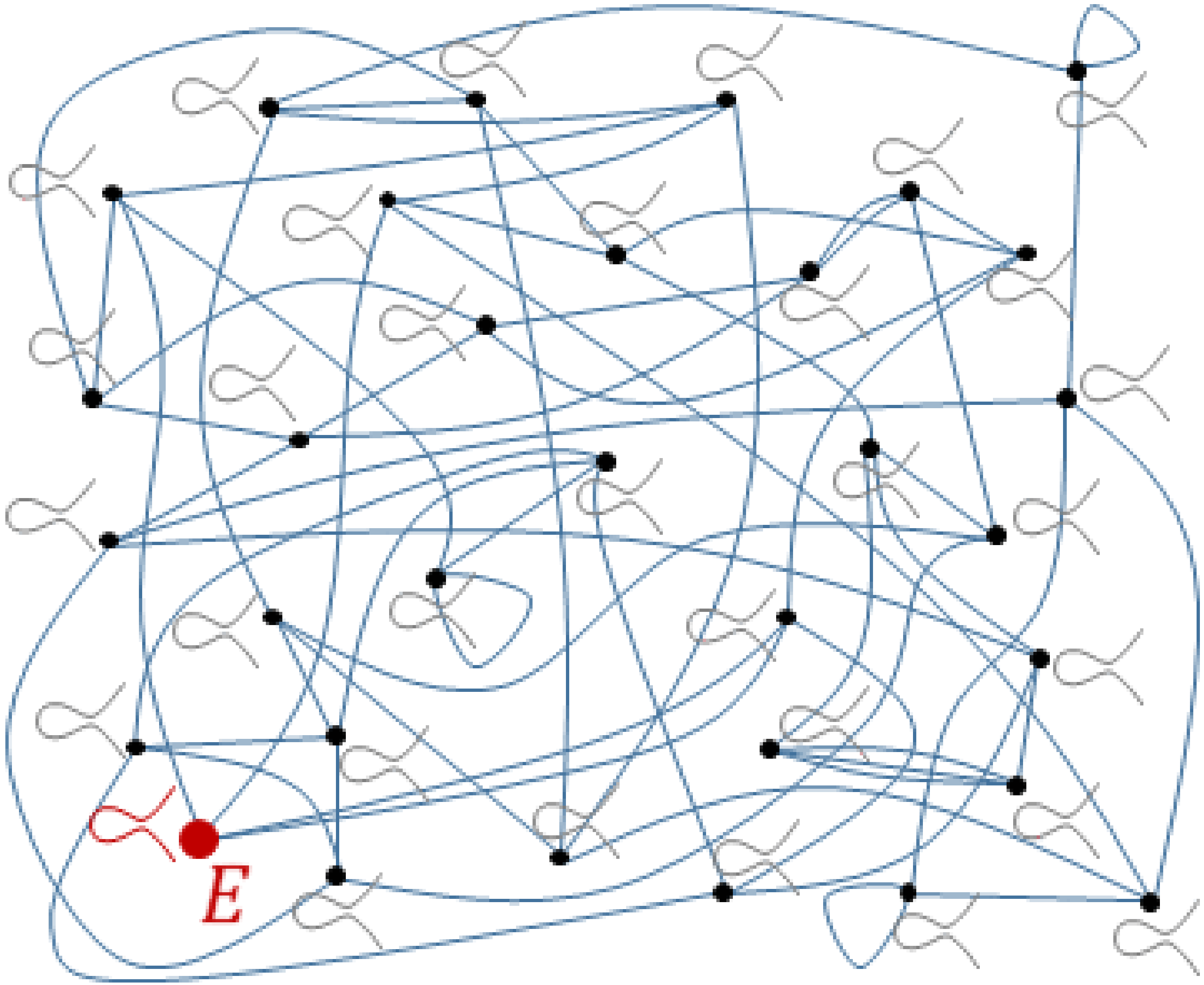
Recall Monday's talk: pre-quantum ECC

$$P, k \mapsto [k]P$$



GIF: Wouter Castryck

Today's talk: post-quantum ECC



W. Castryck (GIF): "Elliptic curves are dead: long live elliptic curves" https://www.esat.kuleuven.be/cosic/?p=7404

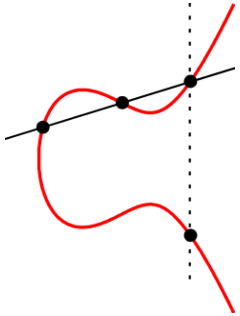
Diffie-Hellman instantiations

$\mathbb{Z}_q$

$g^a \bmod q$

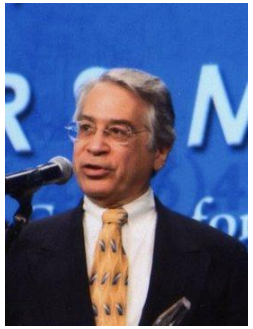
$g^b \bmod q$

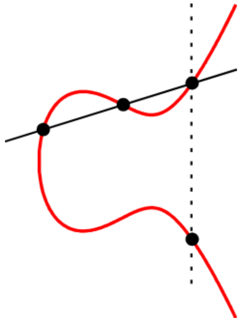
$\mathbb{Z}_q$

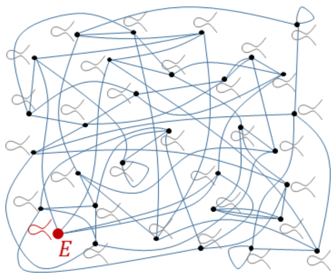


$[a]P$

$[b]P$

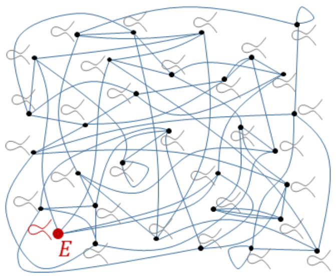






$\phi_A(E)$

$\phi_B(E)$



Diffie-Hellman instantiations

	DH	ECDH	SIDH
Elements	integers g modulo prime	points P in curve group	curves E in isogeny class
Secrets	exponents x	scalars k	isogenies ϕ
computations	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $E, \phi(E)$ find ϕ

Part 1: Motivation

Part 2: Preliminaries

Part 3: SIDH

Extension fields

To construct degree n extension field $\mathbb{F}_{q^n}$ of a finite field $\mathbb{F}_q$, take $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ where $f(\alpha) = 0$ and $f(x)$ is irreducible of degree n in $\mathbb{F}_q[x]$.

Example: for any prime $p \equiv 3 \bmod 4$, can take $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ where $i^2 + 1 = 0$

Elliptic Curves and j-invariants

- Recall that every elliptic curve E over a field K with $\mathbf{char}(K) > 3$ can be defined by
$$E : y^2 = x^3 + ax + b,$$
where $a, b \in K$, $4a^3 + 27b^2 \neq 0$

- For any extension K'/K, the set of K'-rational points forms a group with identity
- The j-invariant $j(E) = j(a,b) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$ determines isomorphism class over $\overline{K}$

- E.g., E': $y^2 = x^3 + au^2x + bu^3$ is isomorphic to E for all $u \in K^*$

- Recover a curve from j: e.g., set $a = -3c$ and $b = 2c$ with $c = j/(j - 1728)$

Example

Over $\mathbb{F}_{13}$, the curves

$$E_1 : y^2 = x^3 + 9x + 8$$

and

$$E_2 : y^2 = x^3 + 3x + 5$$

are isomorphic, since

$$j(E_1) = 1728 \cdot \frac{4 \cdot 9^3}{4 \cdot 9^3 + 27 \cdot 8^2} = 3 = 1728 \cdot \frac{4 \cdot 3^3}{4 \cdot 3^3 + 27 \cdot 5^2} = j(E_2)$$

An isomorphism is given by

$$\psi \ : E_1 \to E_2 , \qquad (x, y) \mapsto (10x, 5y),$$
$$\psi^{-1} : E_2 \to E_1 , \qquad (x, y) \mapsto (4x, 8y),$$

noting that $\psi(\infty_1) = \infty_2$

Torsion subgroups

- The multiplication-by-n map:

$$n : E \to E, \qquad P \mapsto [n]P$$

- The n-torsion subgroup is the kernel of $[n]$

$$E[n] = \{P \in E(\bar{K}) : \ [n]P = \infty\}$$

- Found as the roots of the n^{th} division polynomial ψ_n

- If $\mathbf{char}(K)$ doesn't divide n, then

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n$$

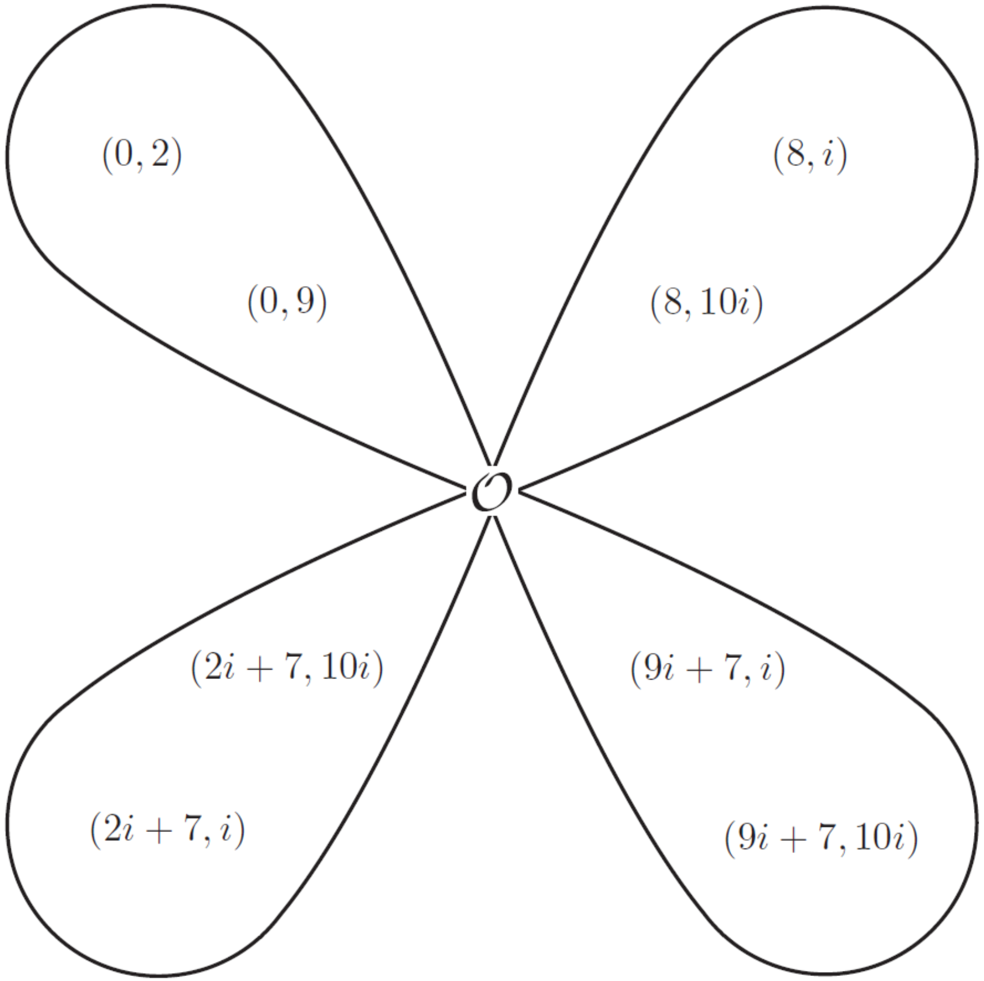
Example ($n = 3$)

- Consider $E/\mathbb{F}_{11}: y^2 = x^3 + 4$ with $\#E(\mathbb{F}_{11}) = 12$

- 3-division polynomial $\psi_3(x) = 3x^4 + 4x$ partially splits as $\psi_3(x) = x(x+3)\left(x^2 + 8x + 9\right)$

- Thus, $x = 0$ and $x = -3$ give 3-torsion points. The points $(0,2)$ and $(0,9)$ are in $E(\mathbb{F}_{11})$, but the rest lie in $E(\mathbb{F}_{11^2})$

- Write $\mathbb{F}_{11^2} = \mathbb{F}_{11}(i)$ with $i^2 + 1 = 0$.
  $\psi_3(x)$ splits over $\mathbb{F}_{11^2}$ as
  $\psi_3(x) = x(x+3)(x+9i+4)(x+2i+4)$



- Observe $E[3] \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$, i.e., 4 cyclic subgroups of order 3

Subgroup isogenies

- **Isogeny:** morphism (rational map)

$$\phi : E_1 \to E_2$$

  that preserves identity, i.e. $\phi(\infty_1) = \infty_2$

- Degree of (separable) isogeny is number of elements in kernel, same as its degree as a rational map

- Given finite subgroup $\boldsymbol{G} \in \boldsymbol{E_1}$, there is a unique curve $\boldsymbol{E_2}$ and isogeny $\boldsymbol{\phi : E_1 \to E_2}$ (up to isomorphism) having kernel $\boldsymbol{G}$. Write $\boldsymbol{E_2 = \phi(E_1) = E_1/\langle G\rangle}$.

Subgroup isogenies: special cases

- Isomorphisms are a *special case of isogenies* where the kernel is trivial

$$\phi : E_1 \to E_2, \quad \ker(\phi) = \infty_1$$

- Endomorphisms are a *special case of isogenies* where the domain and co-domain are the same curve

$$\phi : E_1 \to E_1, \quad \ker(\phi) = G, \quad |G| > 1$$

- Perhaps think of isogenies as a generalization of either/both: isogenies allow non-trivial kernel and allow different domain/co-domain

- Isogenies are *almost* isomorphisms

Velu's formulas

Given any finite subgroup of G of E, we may form a **quotient isogeny**

$$\phi: E \to E' = E/G$$

with kernel G using Velu's formulas

Example: $E : y^2 = (x^2 + b_1 x + b_0)(x - a)$. The point $(a, 0)$ has order 2; the quotient of E by $\langle(a,0)\rangle$ gives an isogeny

$$\phi : E \to E' = E/\langle(a,0)\rangle,$$

where

$$E' : y^2 = x^3 + \left(-(4a + 2b_1)\right)x^2 + \left(b_1^2 - 4b_0\right)x$$

And where ϕ maps (x, y) to

$$\left(\frac{x^3-(a-b_1)x^2-(b_1a-b_0)x-b_0a}{x-a}, \frac{\left(x^2-(2a)x-(b_1a+b_0)\right)y}{(x-a)^2}\right)$$

Velu's formulas

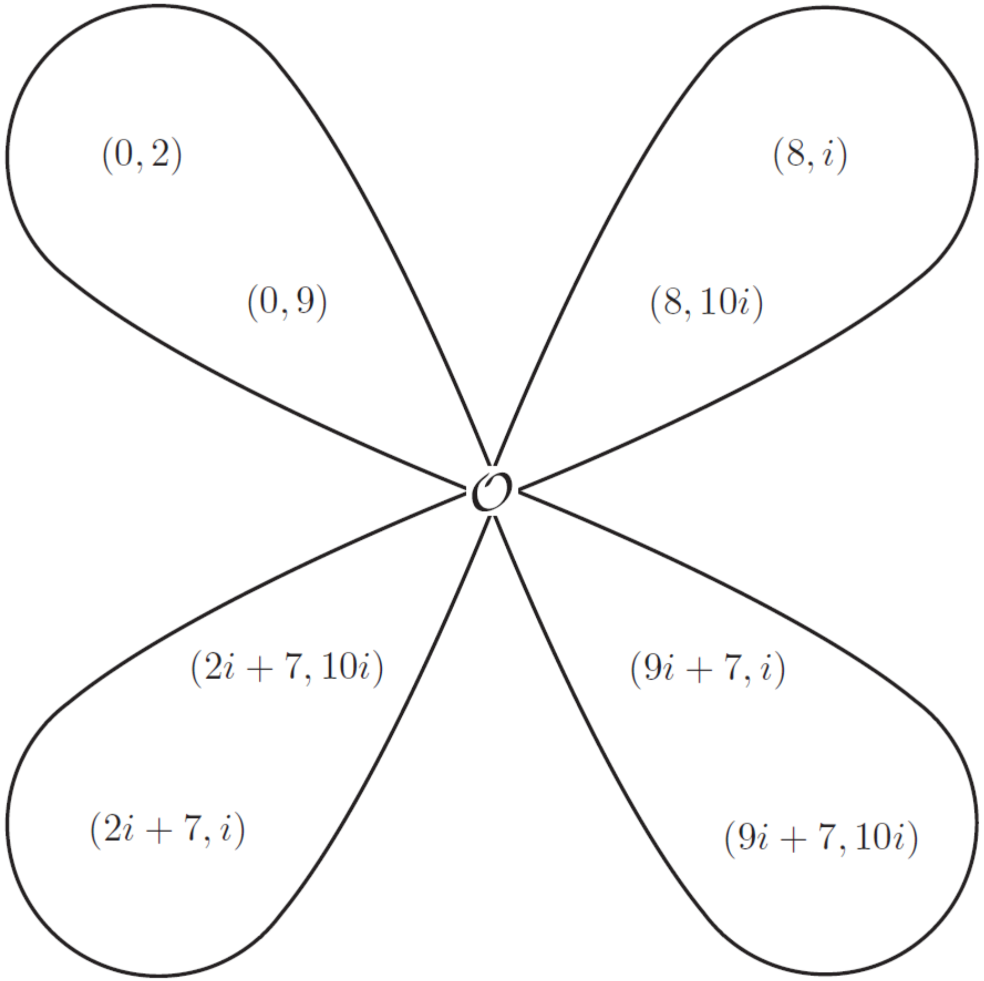
Given curve coefficients $\boldsymbol{a}, \boldsymbol{b}$ for $\boldsymbol{E}$, and **all** of the $\boldsymbol{x}$-coordinates $\boldsymbol{x_i}$ of the subgroup $\boldsymbol{G} \in \boldsymbol{E}$, Velu's formulas output $\boldsymbol{a}', \boldsymbol{b}'$ for $\boldsymbol{E}'$, and the map

$$\phi : \ E \rightarrow E',$$
$$(x, y) \mapsto \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)} \right)$$

Example, cont.

$G = E[3]$

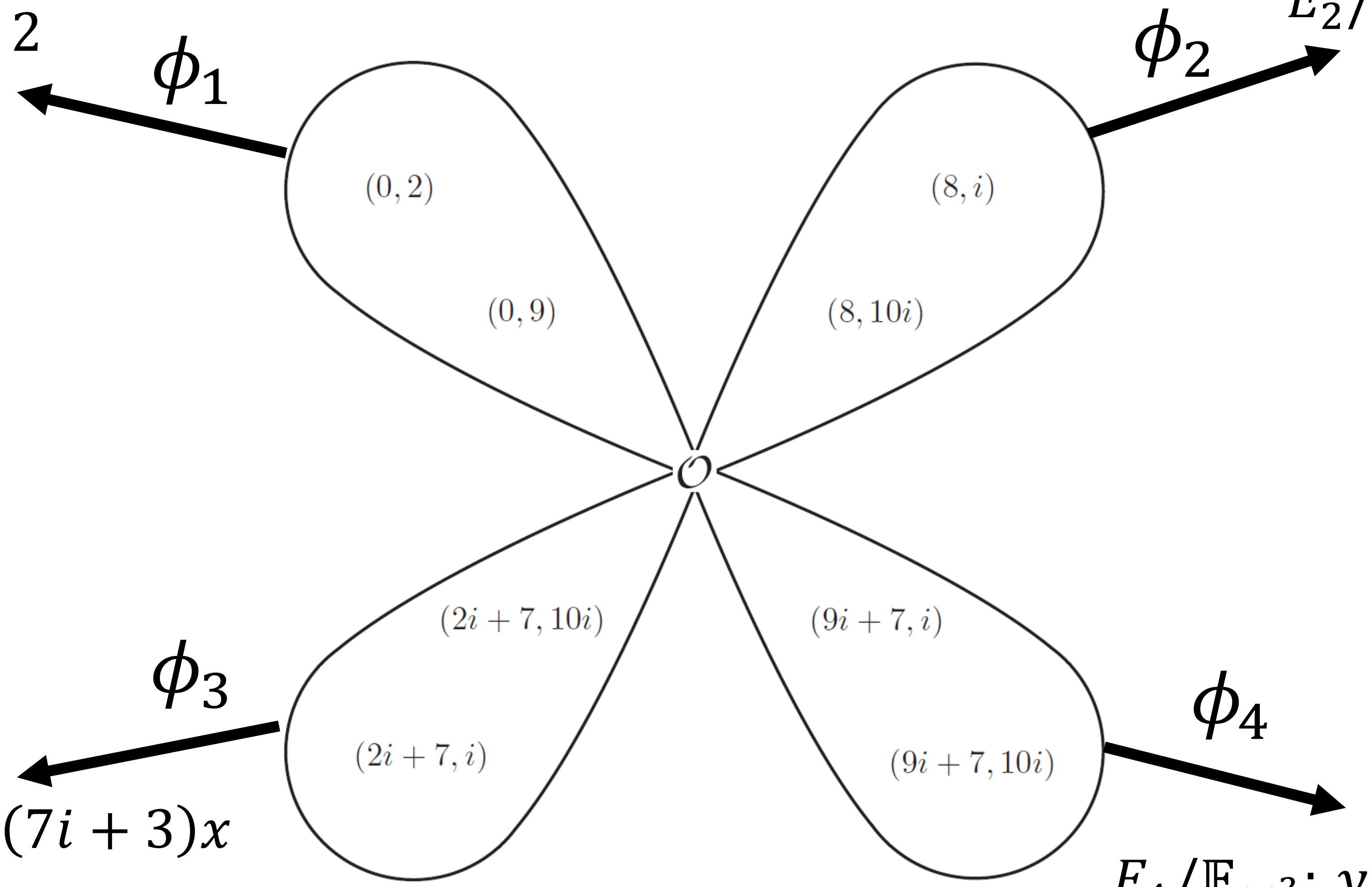
- Recall $E/\mathbb{F}_{11}: y^2 = x^3 + 4$ with $\#E(\mathbb{F}_{11}) = 12$
- Consider $[3] : E \to E$, the multiplication-by-3 endomorphism
- $G = \mathbf{ker}([3])$, which is not cyclic
- Conversely, given the subgroup G, the unique isogeny ϕ with $\mathbf{ker}(\phi) = G$ turns out to be the endormorphism $\phi = [3]$
- But what happens if we instead take G as one of the cyclic subgroups of order 3?



Example, cont. $E/\mathbb{F}_{11}: y^2 = x^3 + 4$

$E_1/\mathbb{F}_{11}: y^2 = x^3 + 2$

$E_2/\mathbb{F}_{11}: y^2 = x^3 + 5x$



$E_3/\mathbb{F}_{11^2}: y^2 = x^3 + (7i + 3)x$

$E_4/\mathbb{F}_{11^2}: y^2 = x^3 + (4i + 3)x$

Isomorphisms and isogenies

- Fact 1: E_1 and E_2 isomorphic iff $j(E_1) = j(E_2)$
- Fact 2: E_1 and E_2 isogenous iff $\#E_1 = \#E_2$ (Tate)
- Fact 3: $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$ (Hasse)

Upshot for fixed q

$O(\sqrt{q})$ isogeny classes

$O(q)$ isomorphism classes

Supersingular curves

- $E/\mathbb{F}_q$ with $q = p^n$ supersingular iff $E[p] = \{\infty\}$
- Fact: all supersingular curves can be defined over $\mathbb{F}_{p^2}$
- Let S_{p^2} be the set of supersingular j-invariants

Theorem: $\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + b, \quad b \in \{0,1,2\}$

The supersingular isogeny graph

- We are interested in the set of supersingular curves (up to isomorphism) over a specific field

- Thm (Mestre): all supersingular curves over $\mathbb{F}_{p^2}$ in same isogeny class

- Fact (see previous slides): for every prime $\boldsymbol{\ell}$ not dividing $\boldsymbol{p}$, there exists $\boldsymbol{\ell}+\mathbf{1}$ isogenies of degree $\boldsymbol{\ell}$ originating from any supersingular curve

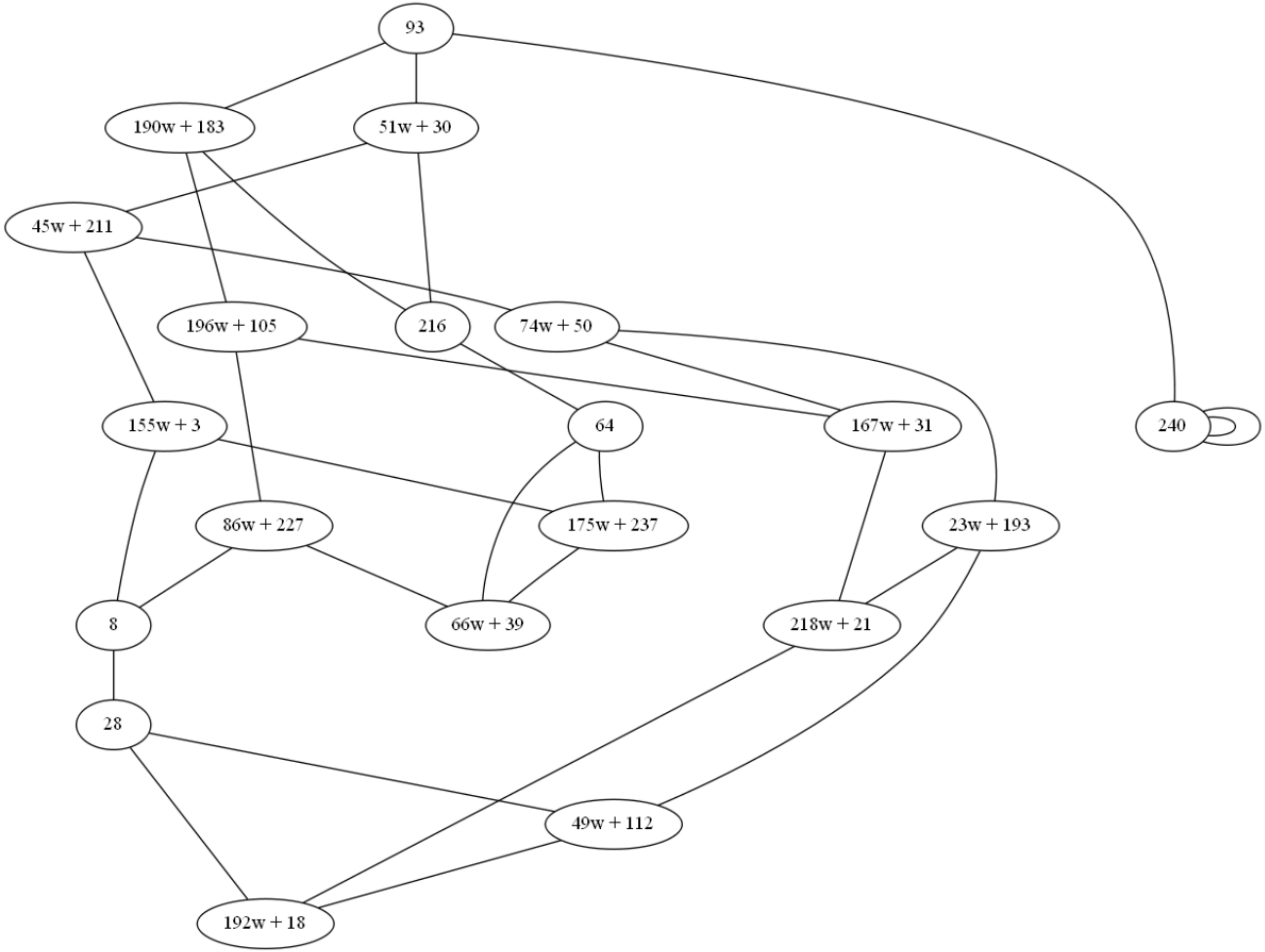
Upshot: immediately leads to $(\ell+1)$ directed regular graph $X(S_{p^2},\ell)$

E.g. a supersingular isogeny graph

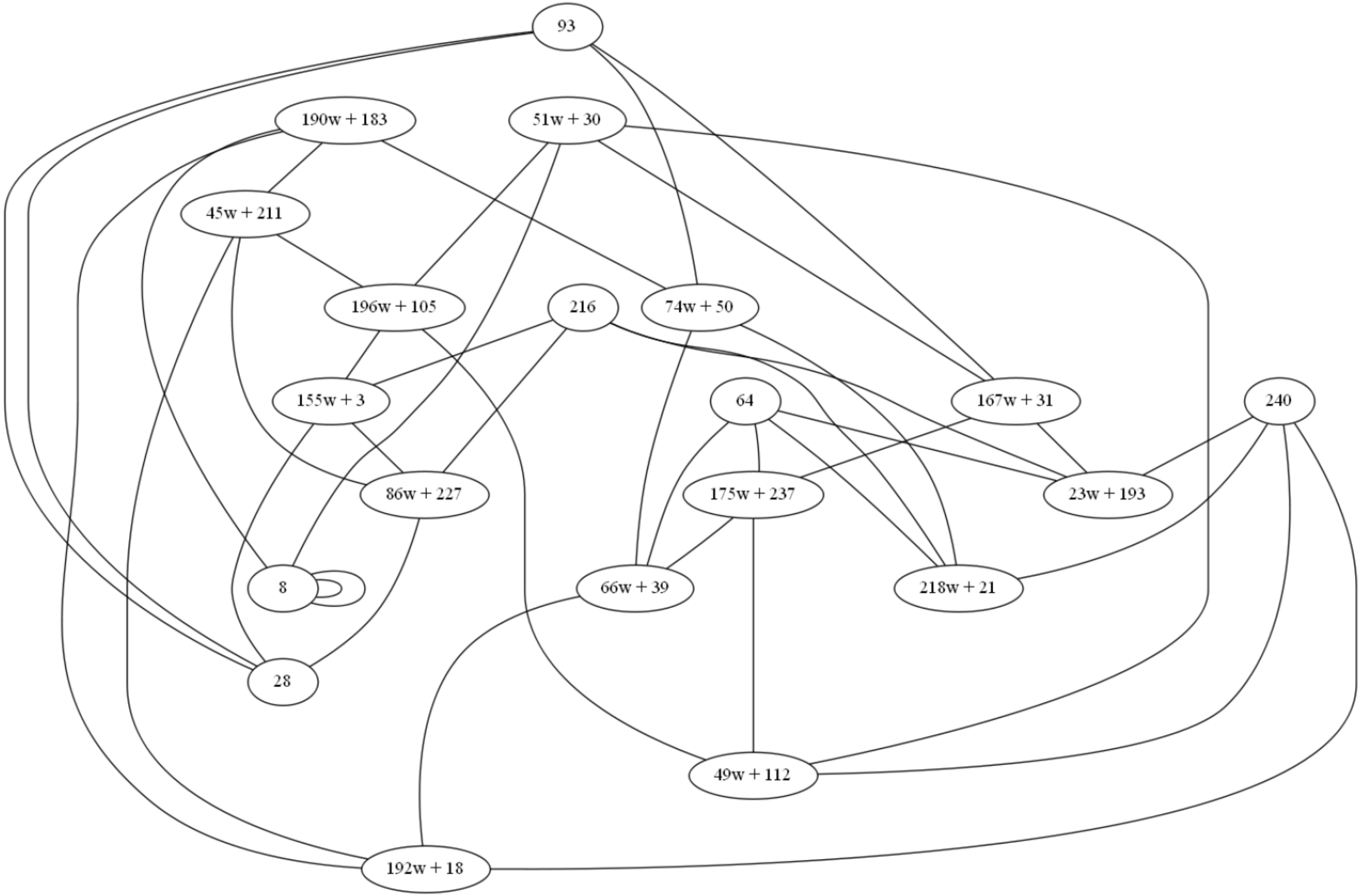
- Let $p = 241$, $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 - 3x + 7)$
- $\#S_{p^2} = 20$
- $S_{p^2} = \{93,\ 51w + 30,\ 190w + 183,\ 240,\ 216,\ 45w + 211,\ 196w + 105,\ 64,\ 155w + 3,\ 74w + 50,\ 86w + 227,\ 167w + 31,\ 175w + 237,\ 66w + 39,\ 8,\ 23w + 193,\ 218w + 21,\ 28,\ 49w + 112,\ 192w + 18\}$

Credit to Fre Vercauteren for example and pictures…

Supersingular isogeny graph for $\ell = 2$: $X(S_{241^2}, 2)$



Supersingular isogeny graph for $\ell = 3$: $X(S_{241^2}, 3)$



Supersingular isogeny graphs are Ramanujan graphs

Rapid mixing property: Let $\boldsymbol{S}$ be any subset of the vertices of the graph $\boldsymbol{G}$, and $\boldsymbol{x}$ be any vertex in $\boldsymbol{G}$. A “long enough” random walk will land in $\boldsymbol{S}$ with probability at least $\frac{|\boldsymbol{S}|}{2|\boldsymbol{G}|}$.

See De Feo, Jao, Plut (Prop 2.1) for precise formula describing what's “long enough”

Part 1: Motivation

Part 2: Preliminaries

Part 3: SIDH

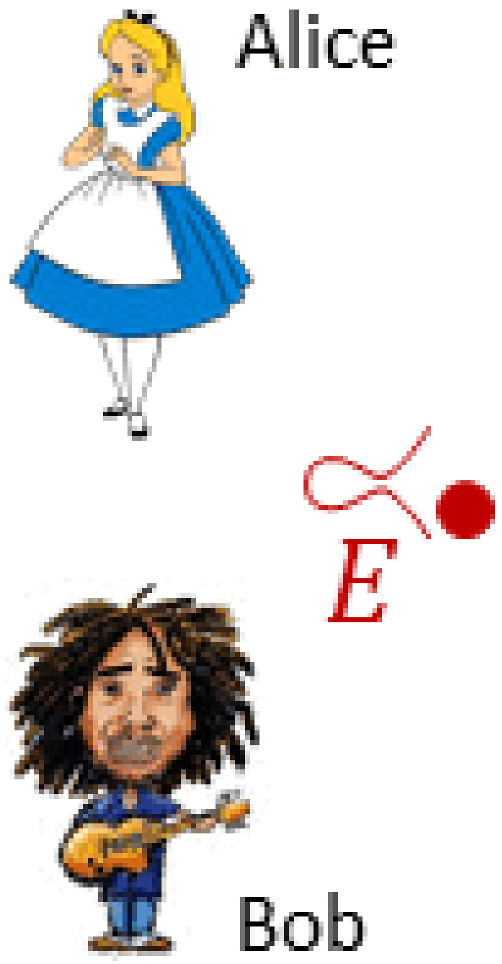
SIDH: history

- **1999:** Couveignes gives talk "Hard homogenous spaces" (eprint.iacr.org/2006/291)
- **2006 (OIDH)**: Rostovsev and Stolbunov propose ordinary isogeny DH
- **2010 (OIDH break)**: Childs-Jao-Soukharev give quantum subexponential alg.
- **2011 (SIDH)**: Jao and De Feo choose supersingular curves

Crucial difference: supersingular (i.e., non-ordinary) endomorphism ring is not commutative (resists 2010 attack)

⚠ WARNING

DO NOT BE DETERRED BY THE WORD SUPERSINGULAR

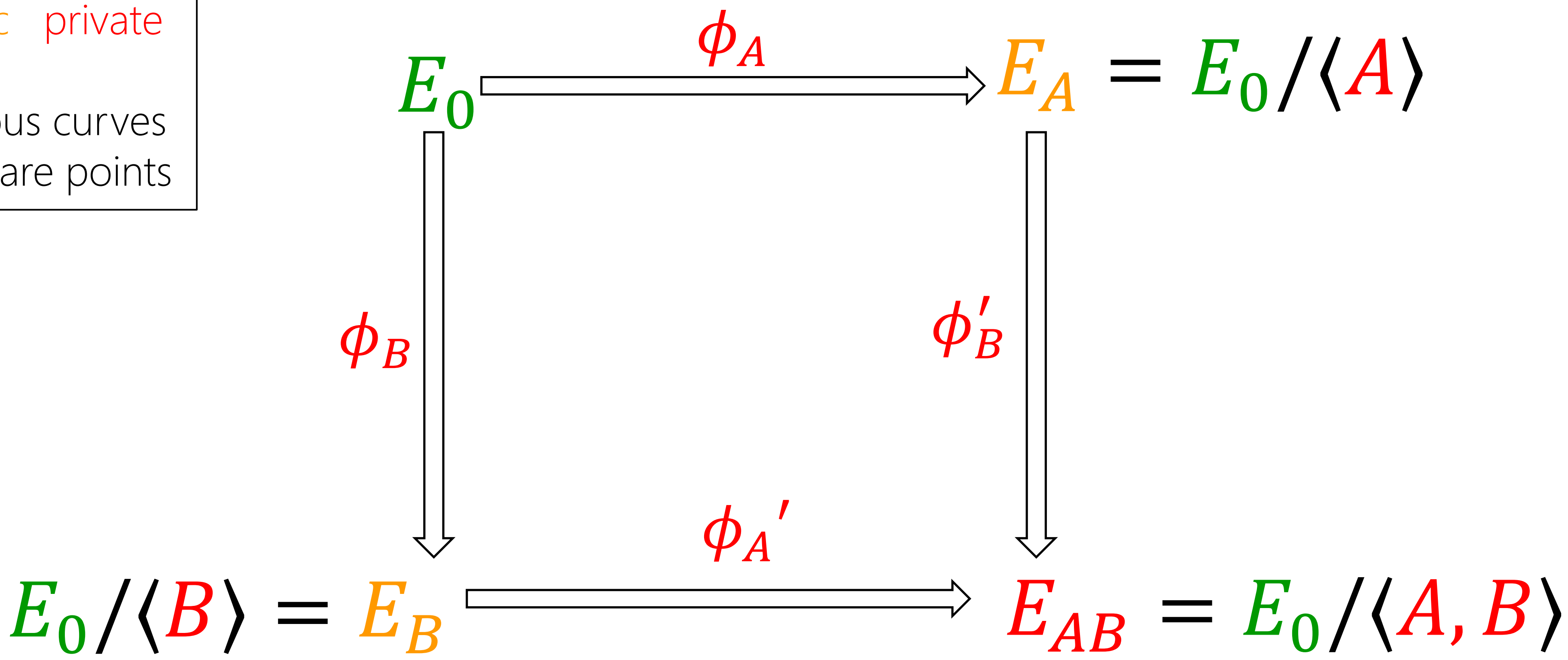


W. Castryck (GIF): "Elliptic curves are dead: long live elliptic curves" https://www.esat.kuleuven.be/cosic/?p=7404

SIDH: in a nutshell

params public private

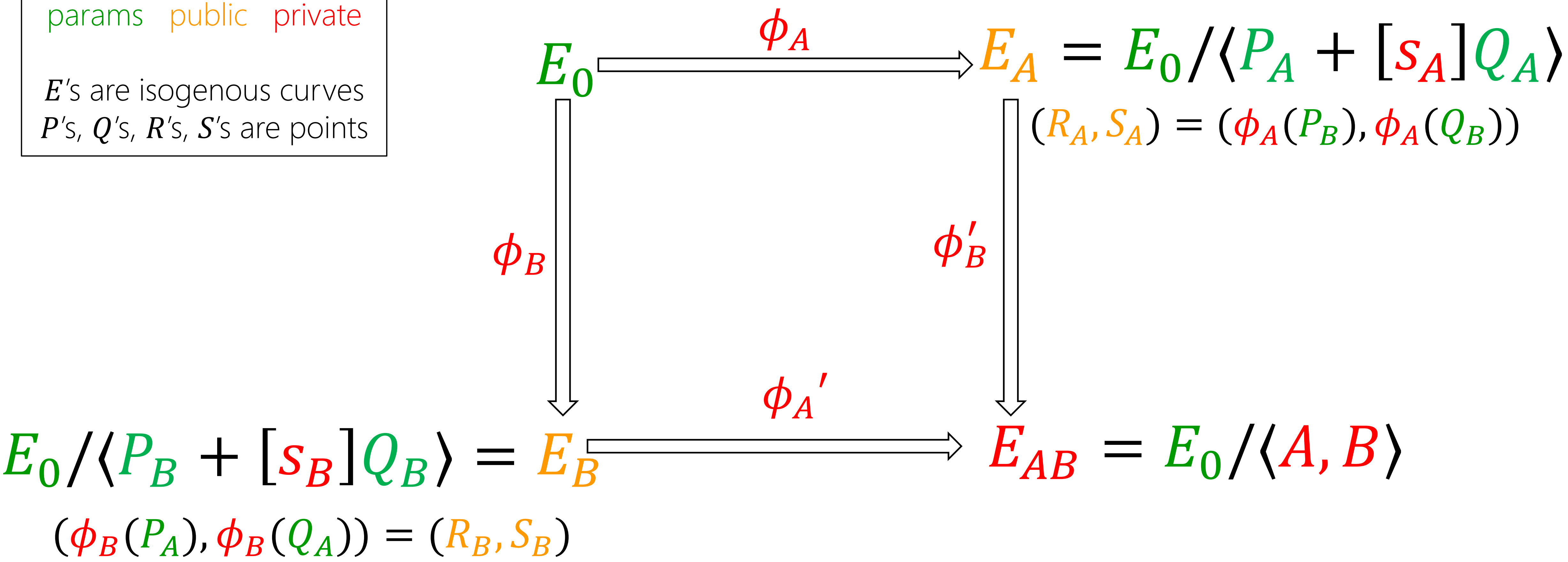
E's are isogenous curves
P's, Q's, R's, S's are points



SIDH: in a nutshell

params public private

E's are isogenous curves
P's, Q's, R's, S's are points



Key: Alice sends her isogeny evaluated at Bob's generators, and vice versa

$$E_A/\langle R_A + [s_B]S_A \rangle \cong E_0/\langle P_A + [s_A]Q_A \, , P_B + [s_B]Q_B \rangle \cong E_B/\langle R_B + [s_A]S_B \rangle$$

Exploiting smooth degree isogenies

- Computing isogenies of prime degree $\boldsymbol{\ell}$ at least $\boldsymbol{O(\ell)}$, e.g., Velu's formulas need the whole kernel specified

- We (obviously) need exp. set of kernels, meaning exp. sized isogenies, which we can't compute unless they're smooth

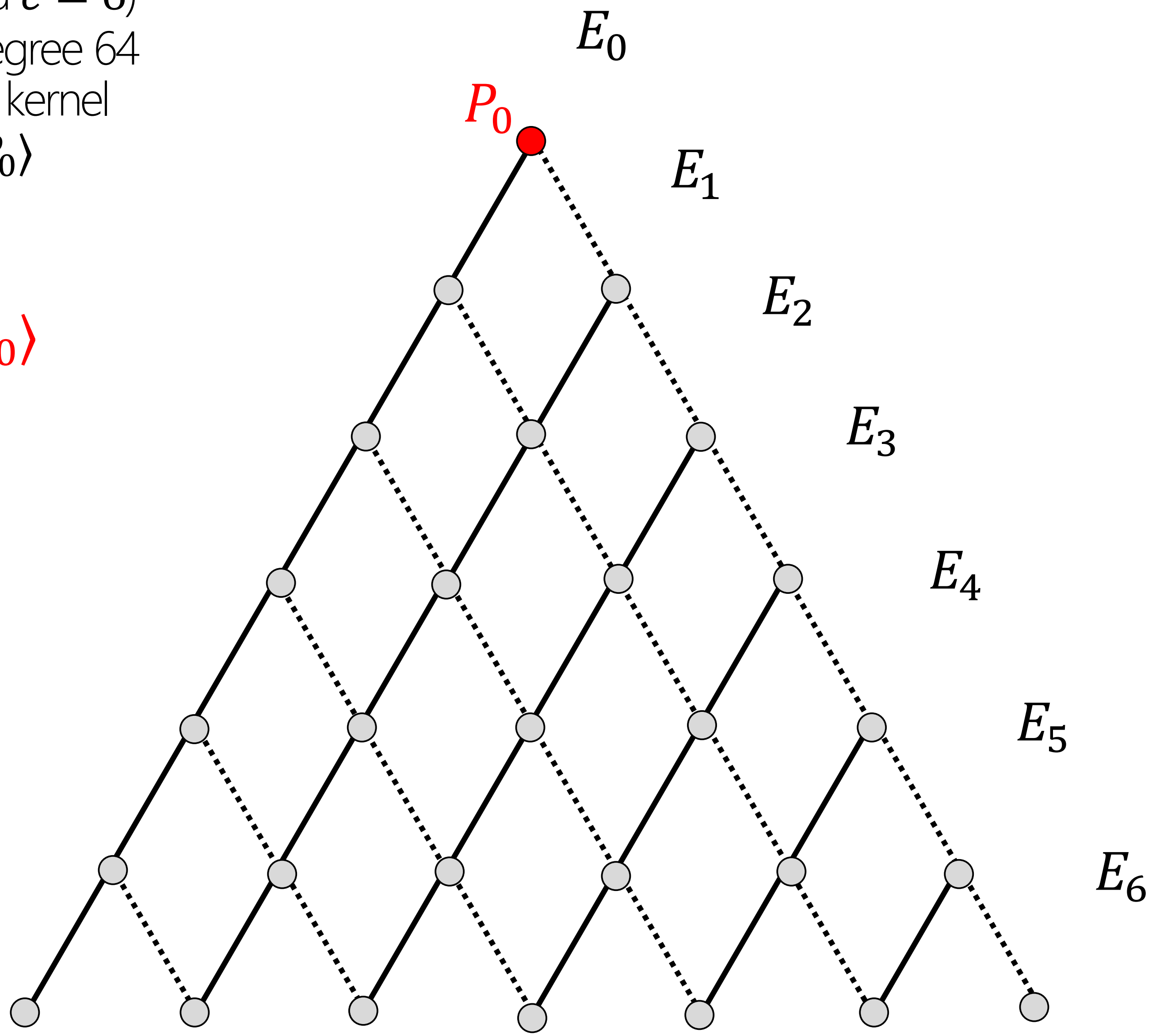
- Here (for efficiency/ease) we will only use isogenies of degree $\boldsymbol{\ell^e}$ for $\boldsymbol{\ell} \in \{2,3\}$

- In SIDH: Alice does $\mathbf{2}$-isogenies, Bob does $\mathbf{3}$-isogenies

Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

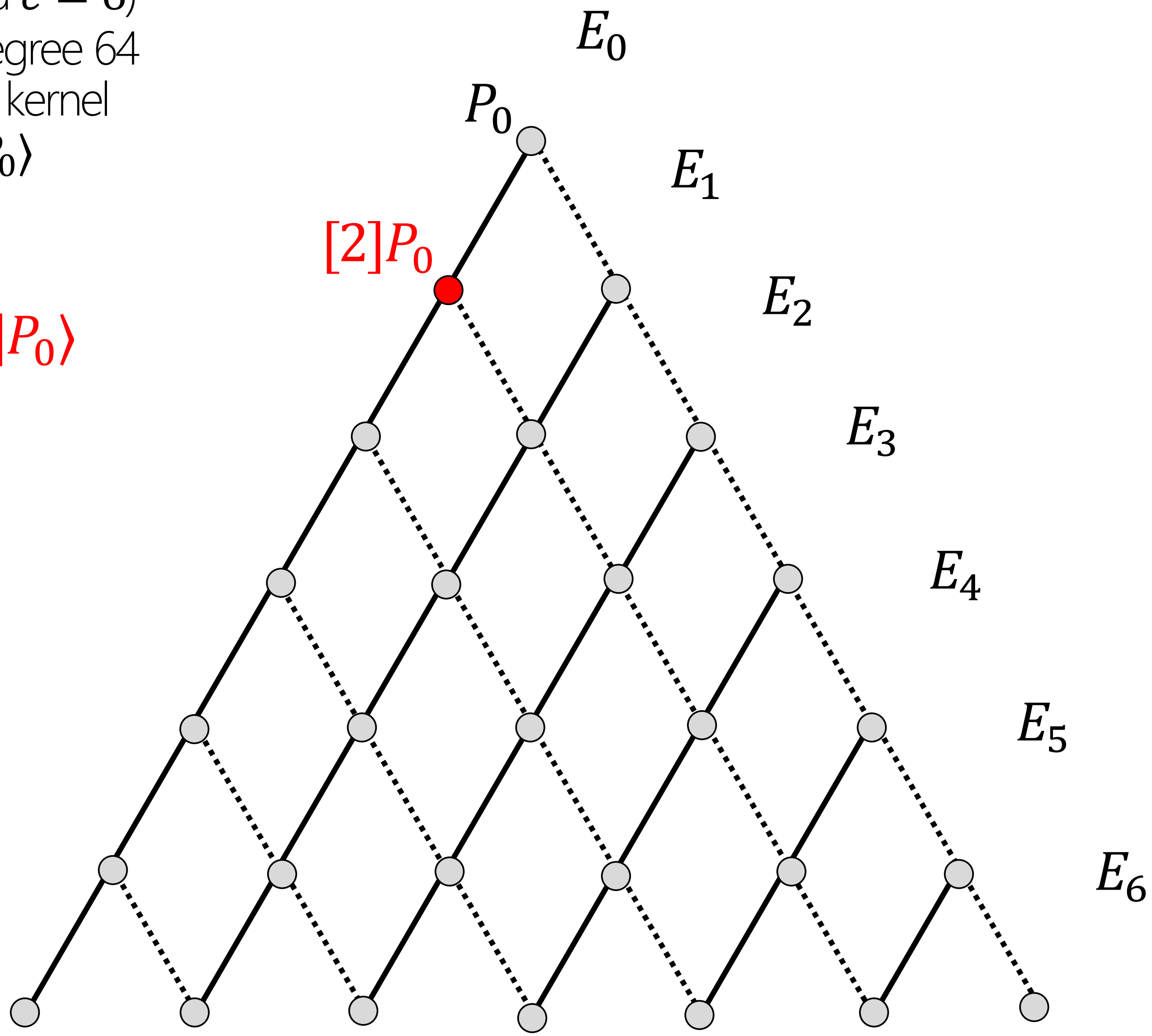
$E_6 = E_0 / \langle P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

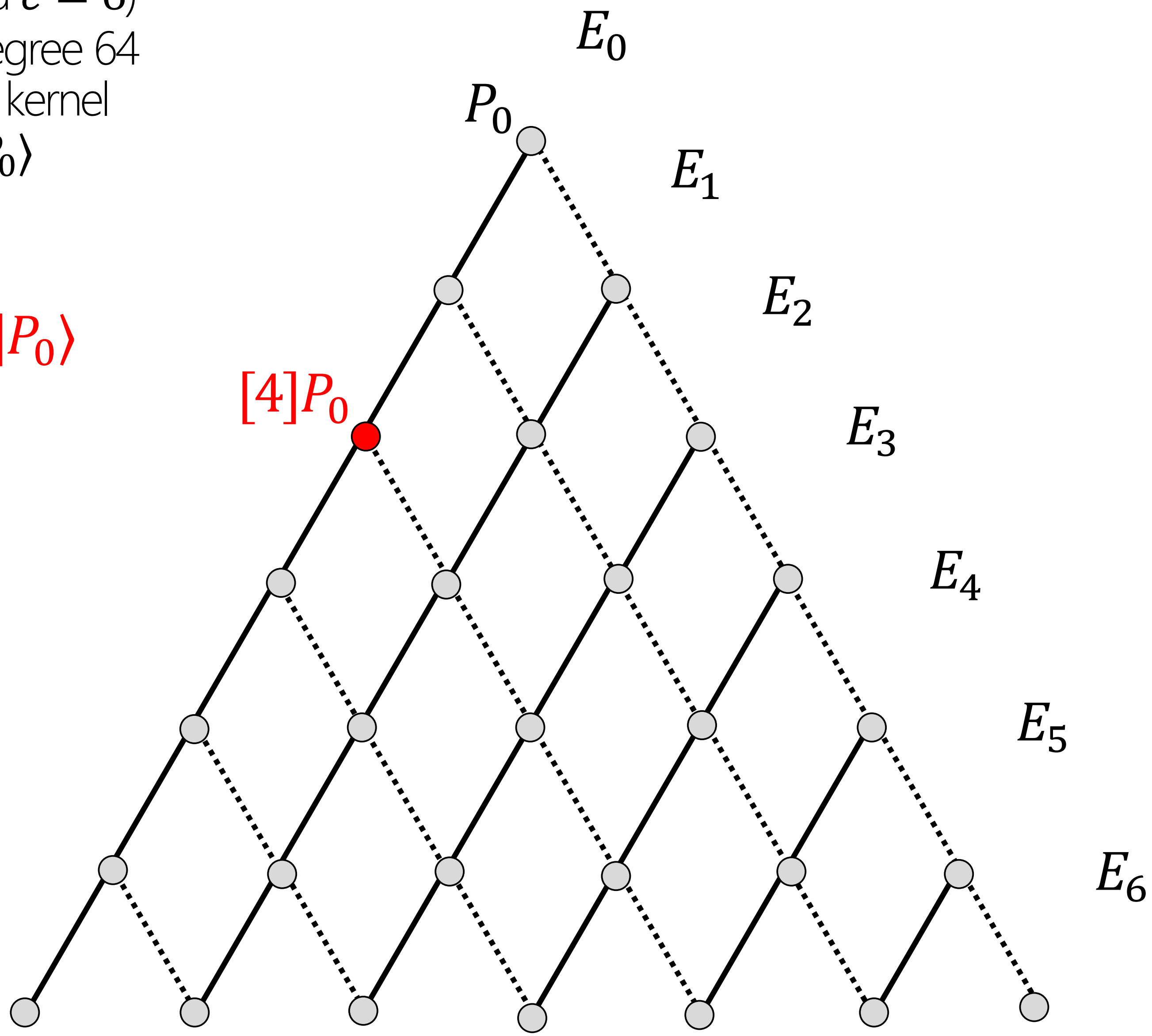
$E_5 = E_0 / \langle [2]P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

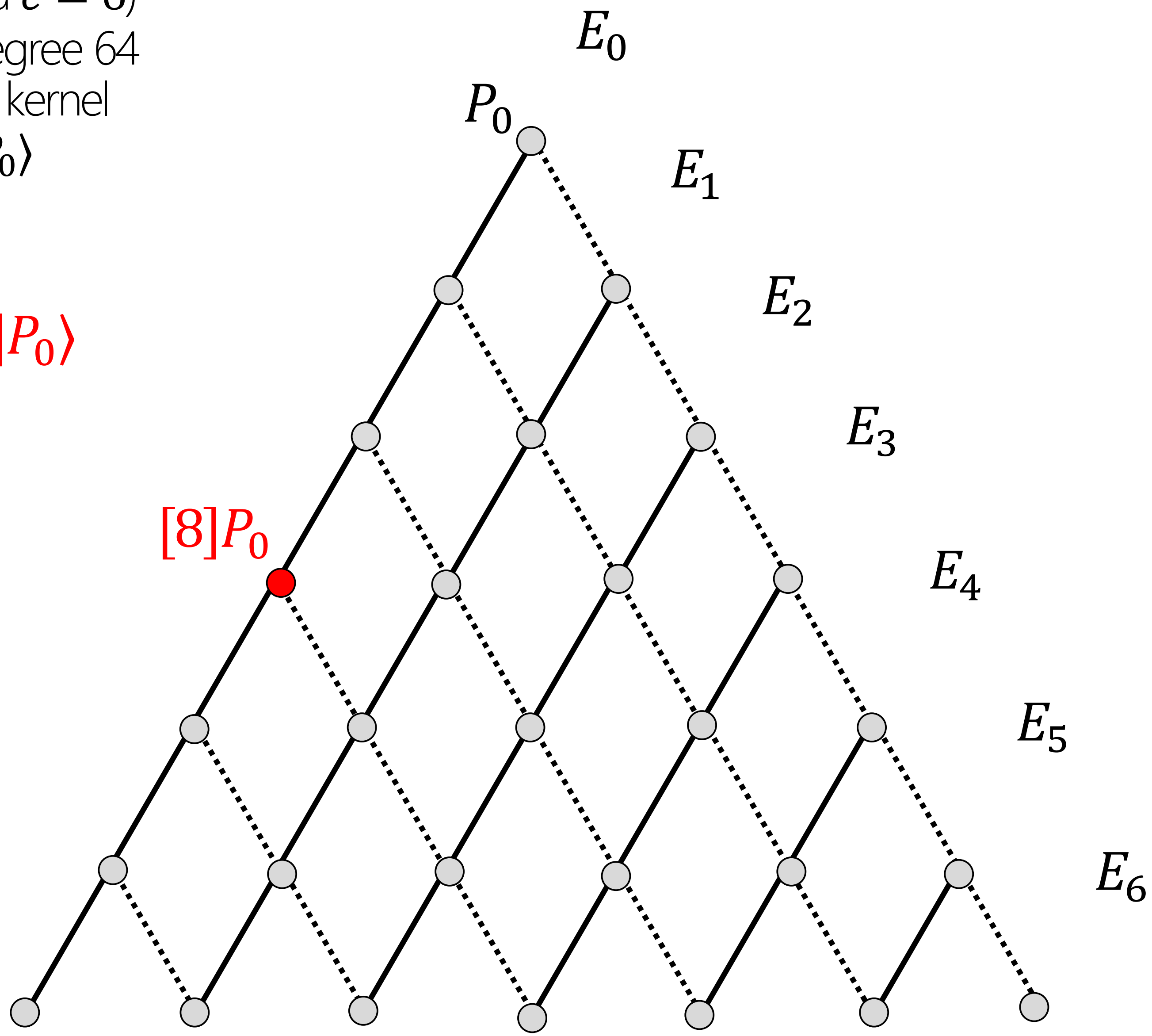
$E_4 = E_0 / \langle [4]P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : \ E_0 \rightarrow E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

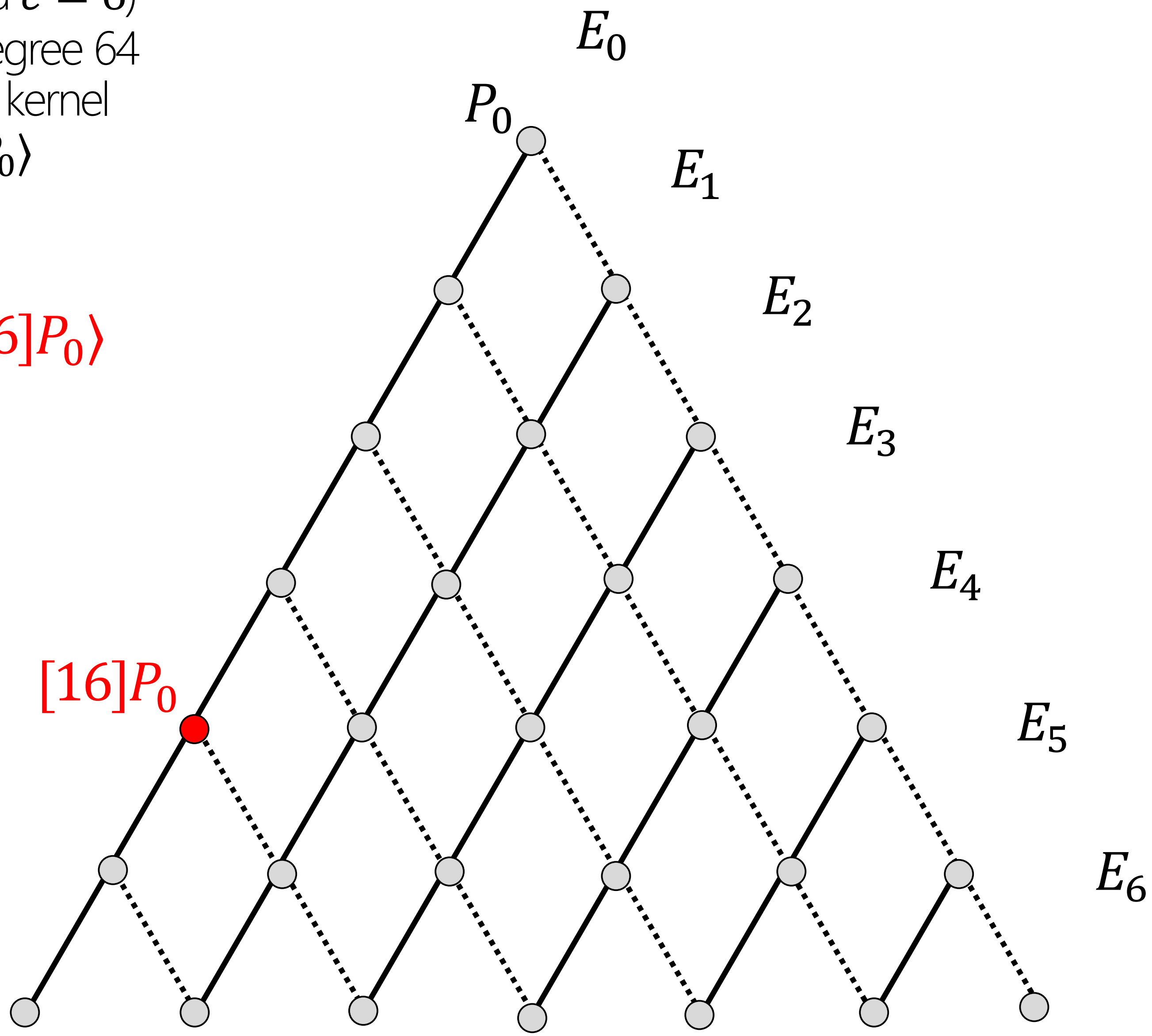
$E_3 = E_0/\langle [8]P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_2 = E_0 / \langle [16]P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)

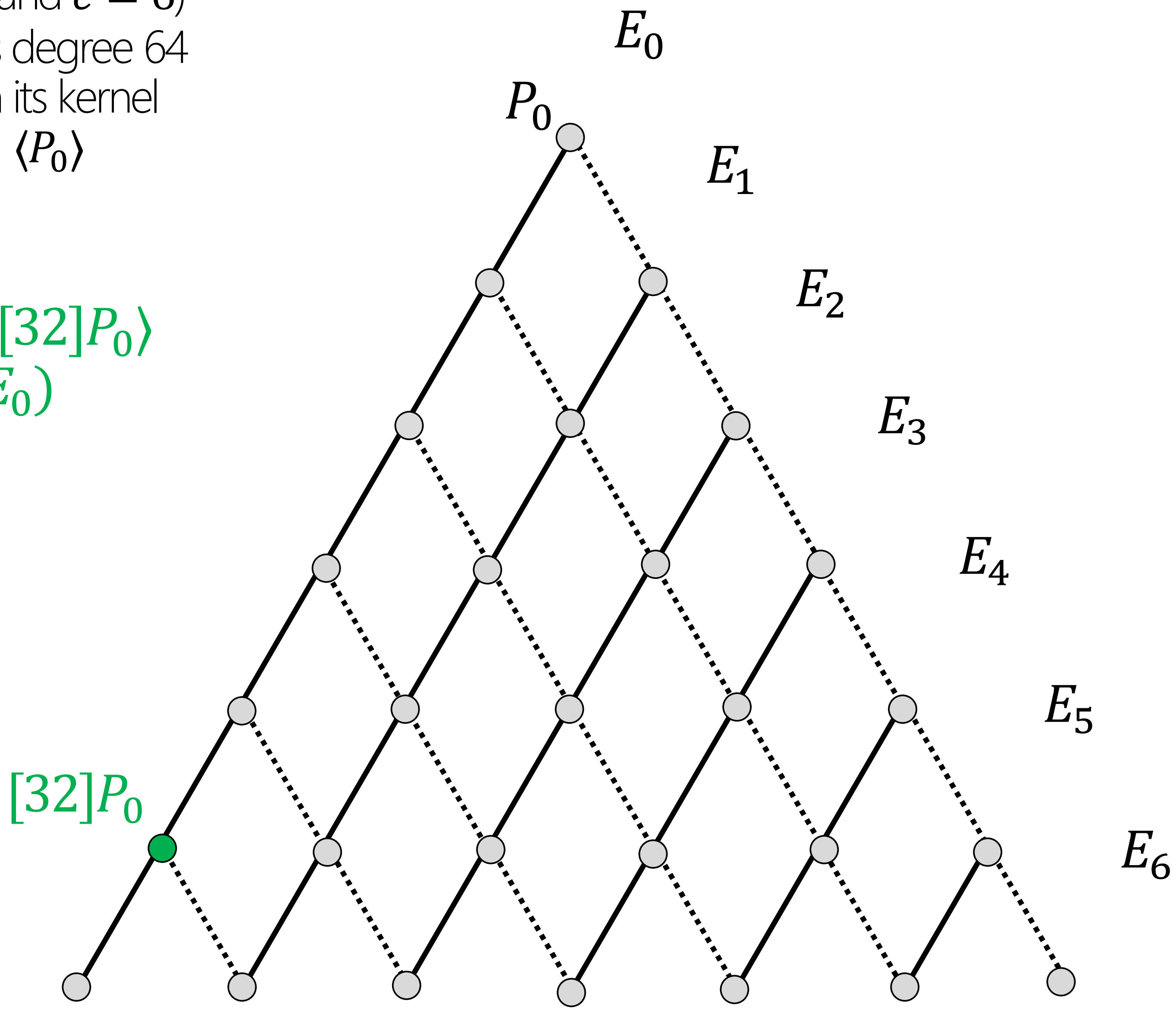
$\phi : E_0 \to E_6$ is degree 64

64 elements in its kernel

$\ker(\phi) = \langle P_0 \rangle$

$E_1 = E_0 / \langle [32]P_0 \rangle$

$= \phi_0(E_0)$

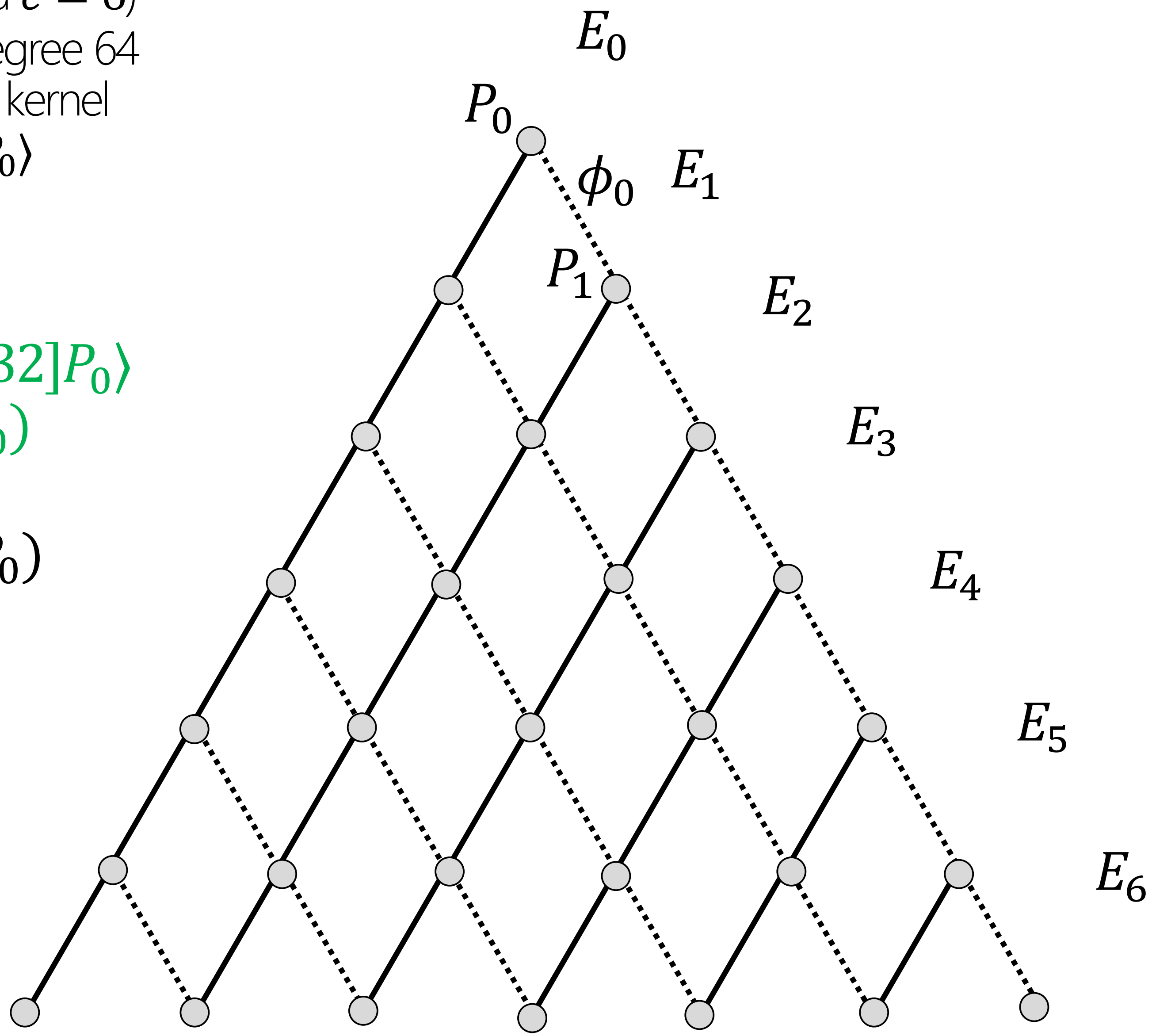


Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_1 = E_0 / \langle [32]P_0 \rangle$
$= \phi_0(E_0)$

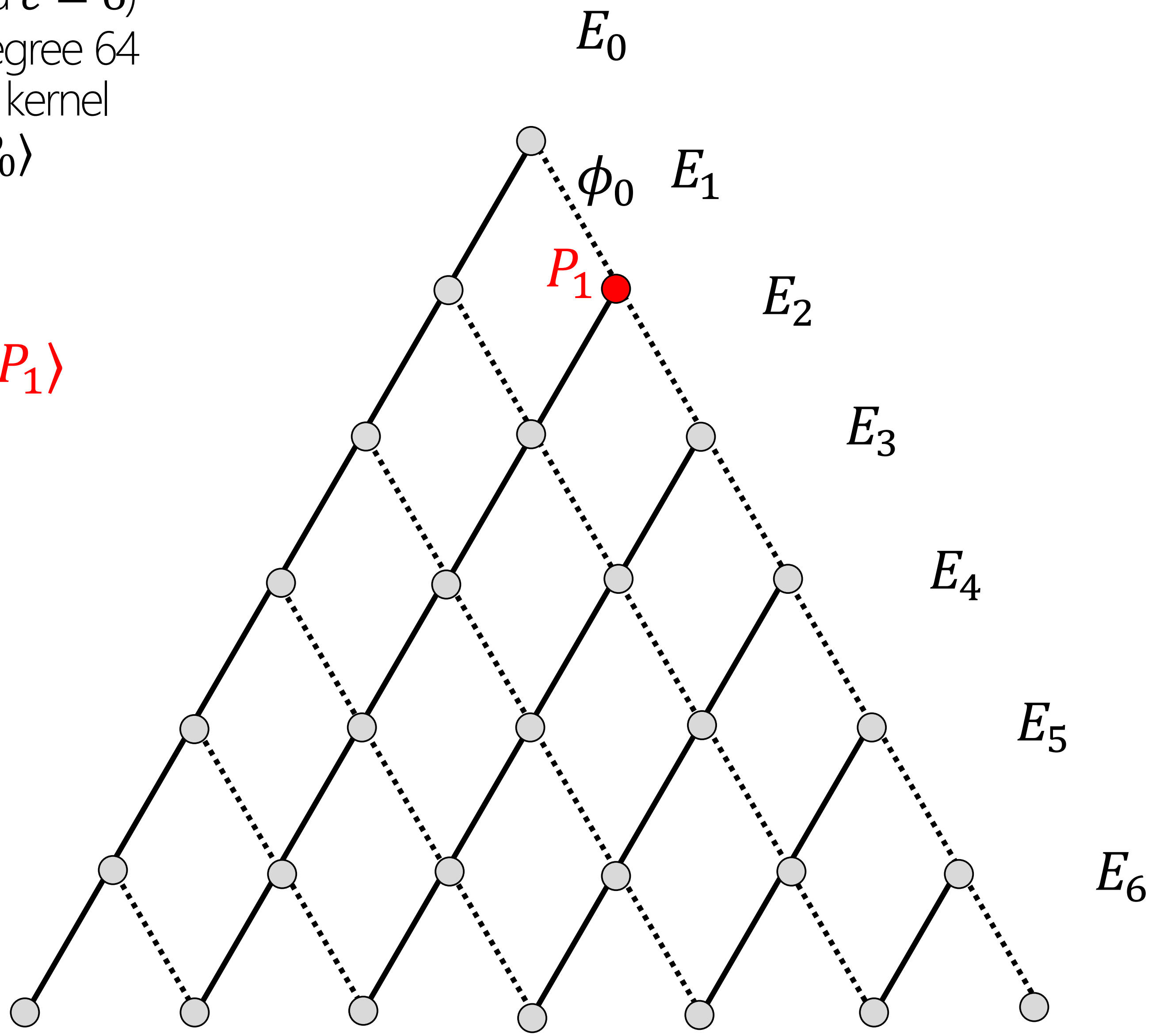
$P_1 = \phi_0(P_0)$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

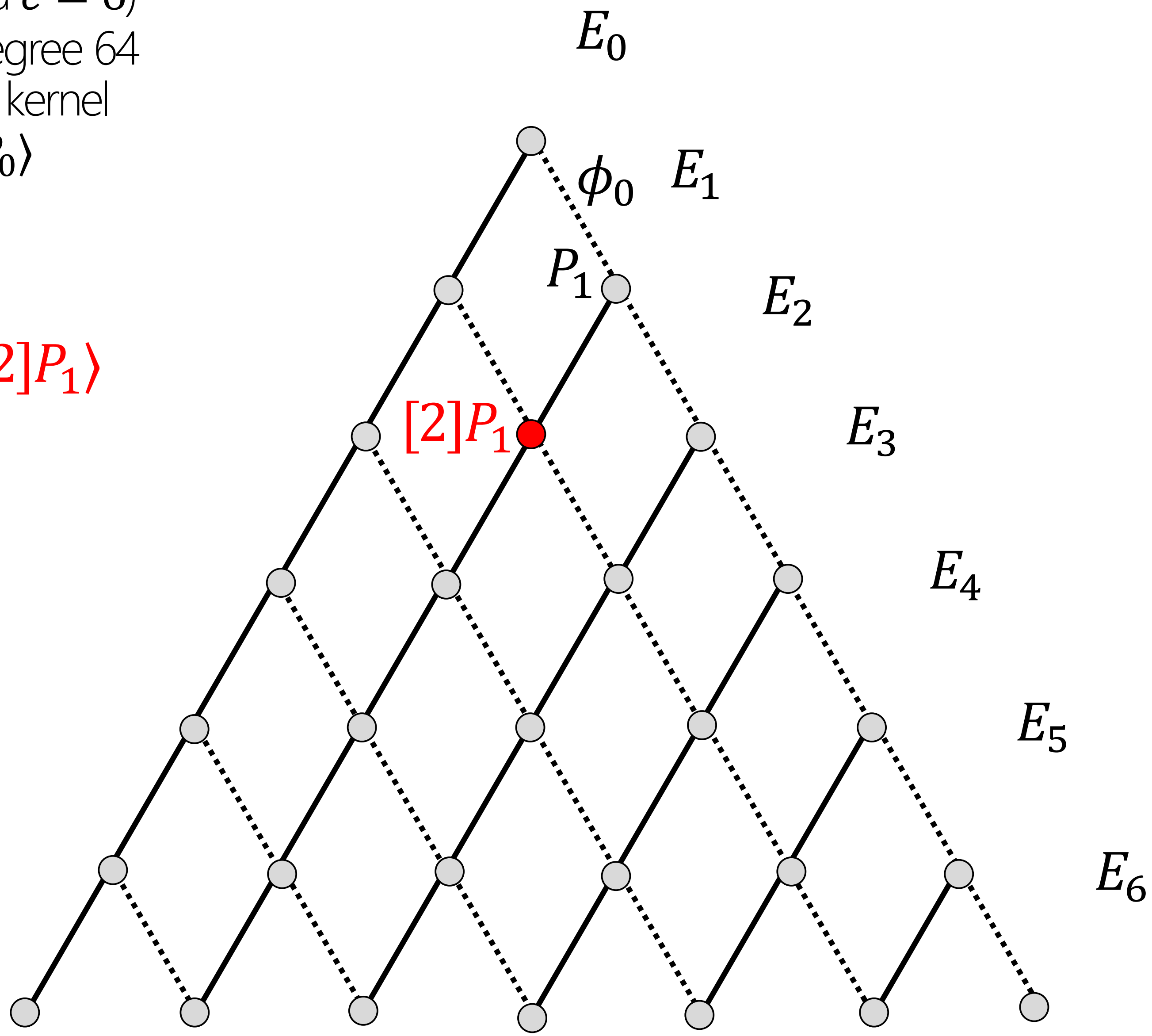
$E_6 = E_1 / \langle P_1 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \rightarrow E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

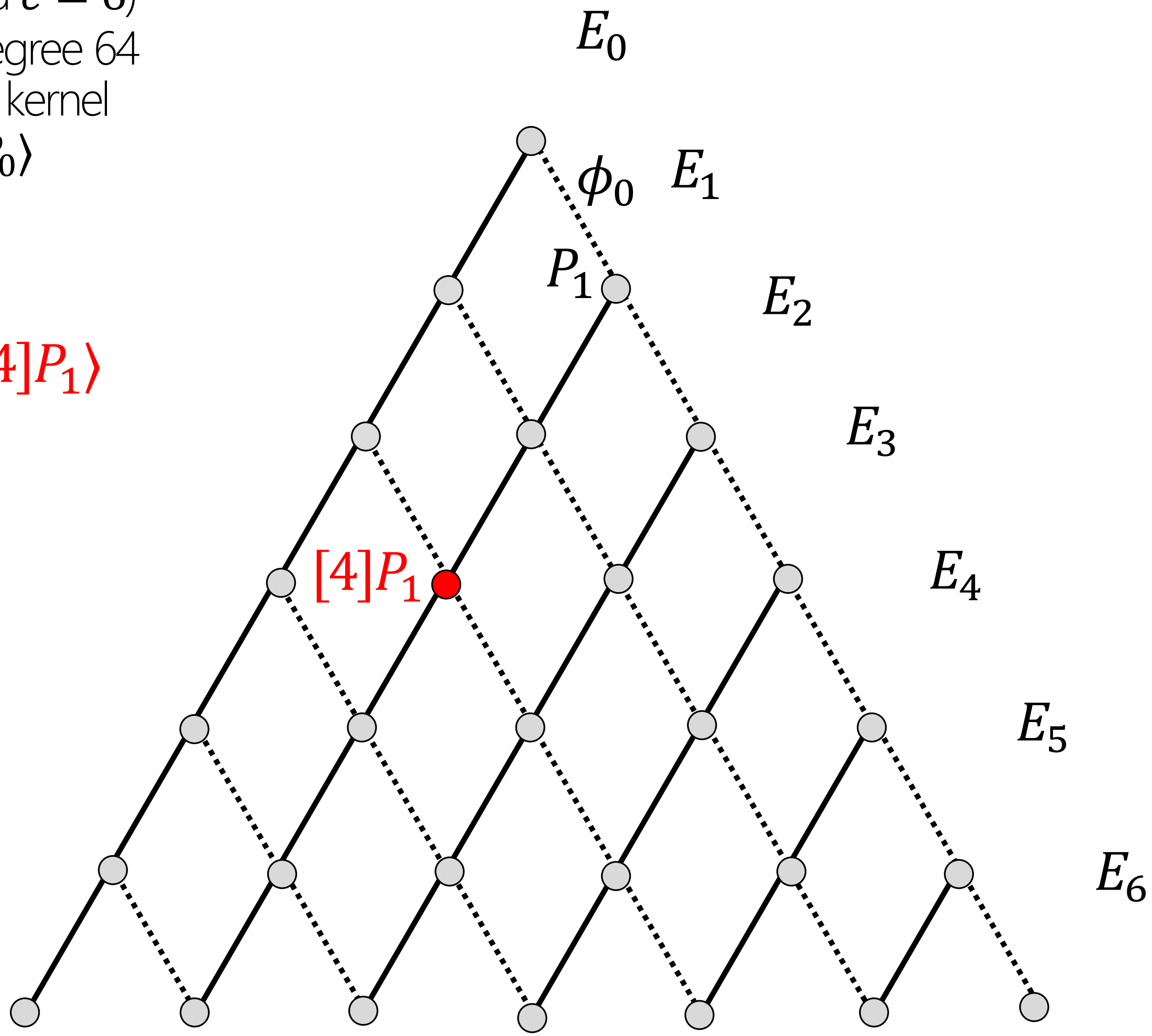
$E_5 = E_1/\langle [2]P_1 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : \ E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

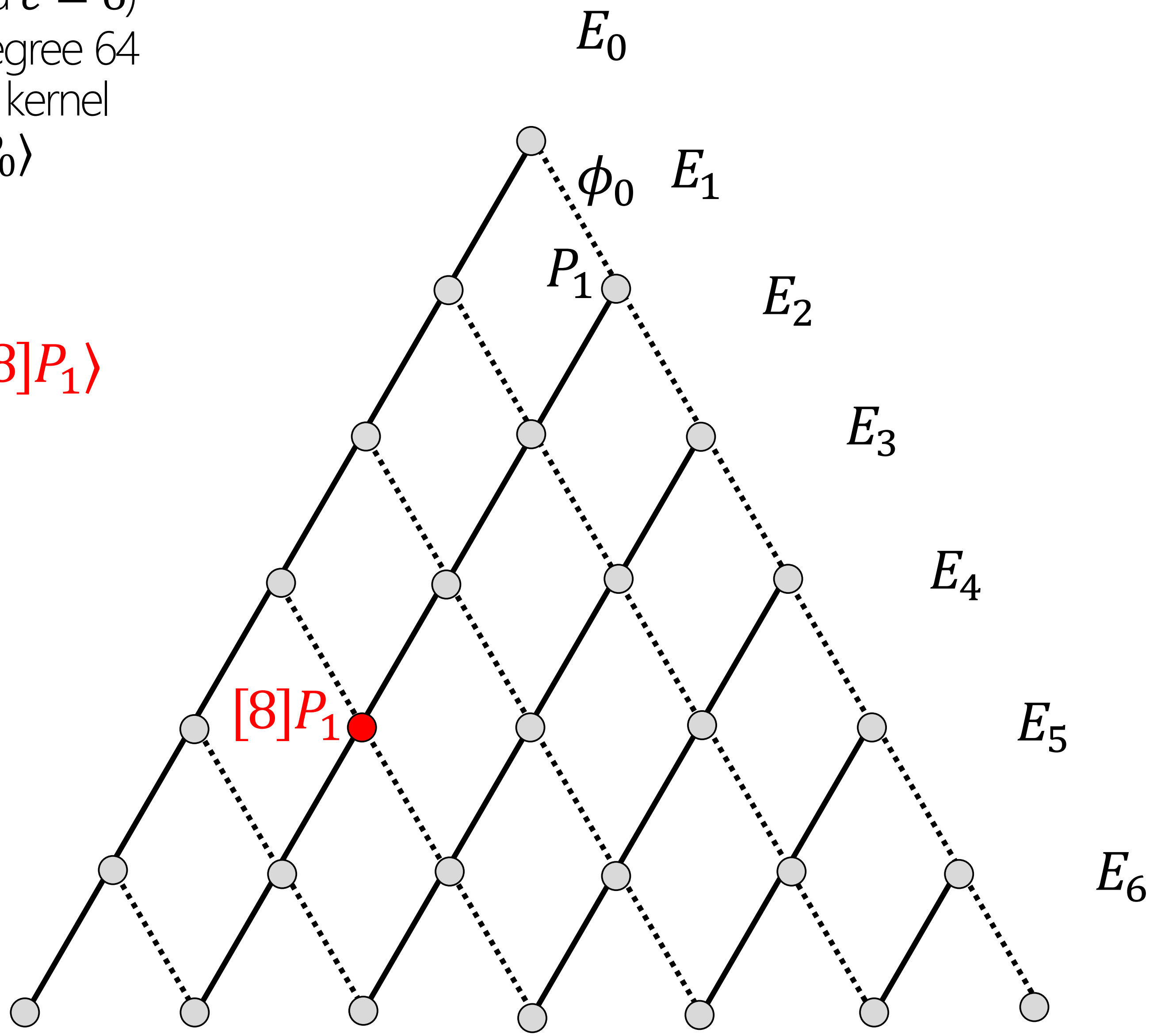
$E_4 = E_1 / \langle [4] P_1 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

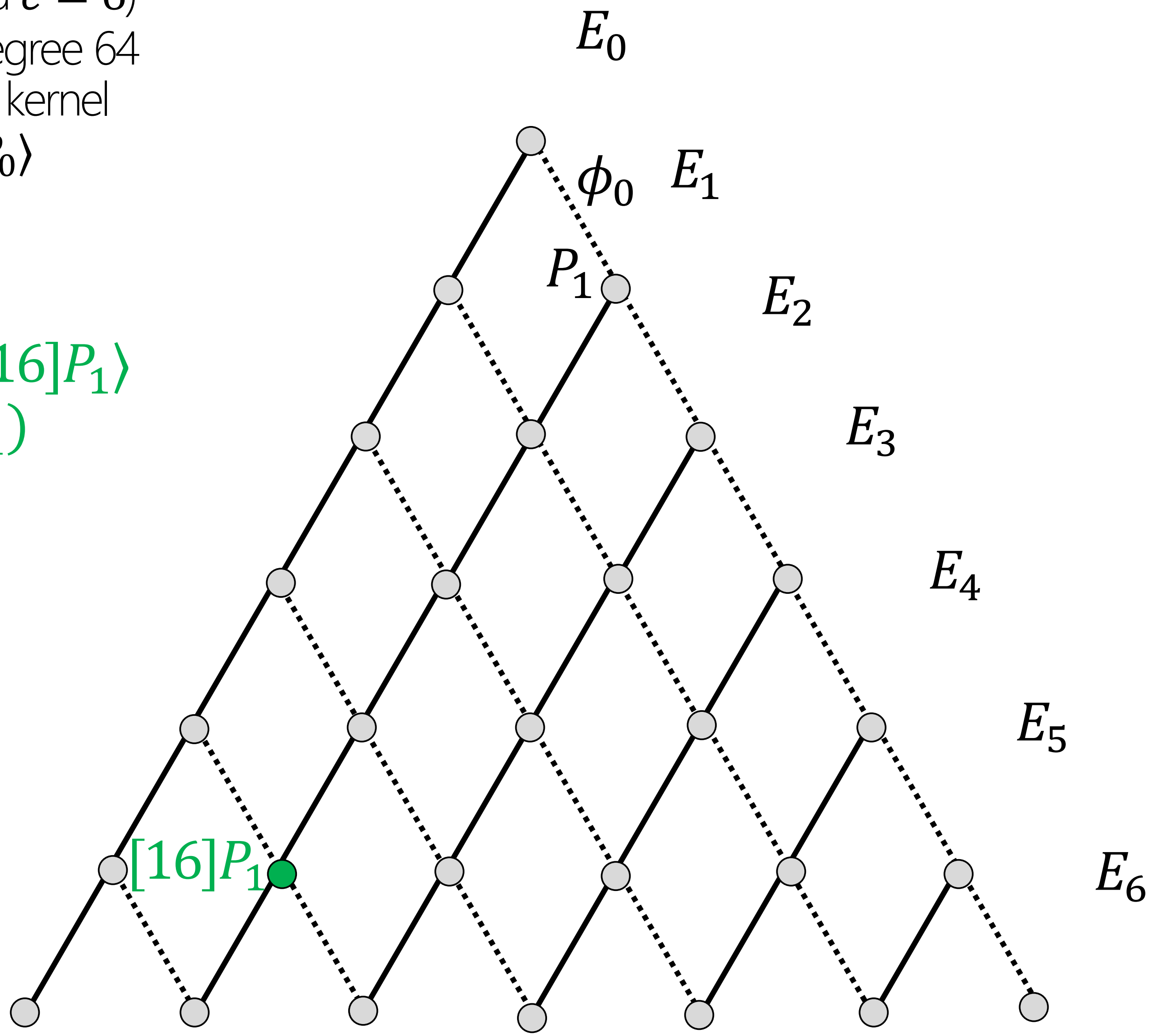
$E_3 = E_1 / \langle [8] P_1 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_2 = E_1/\langle [16]P_1 \rangle$
$= \phi_1(E_1)$

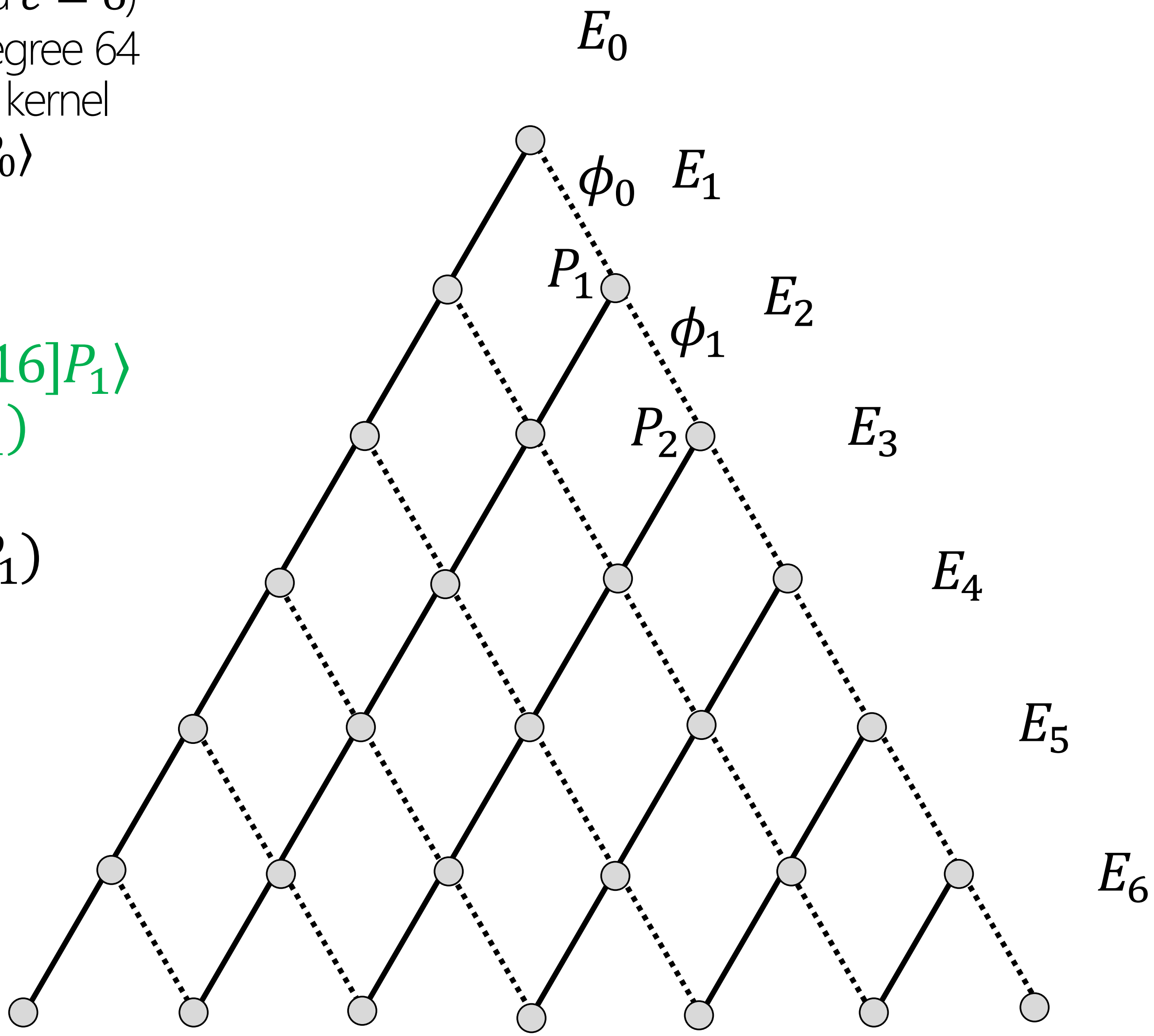


Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$$E_2 = E_1/\langle [16]P_1 \rangle = \phi_1(E_1)$$

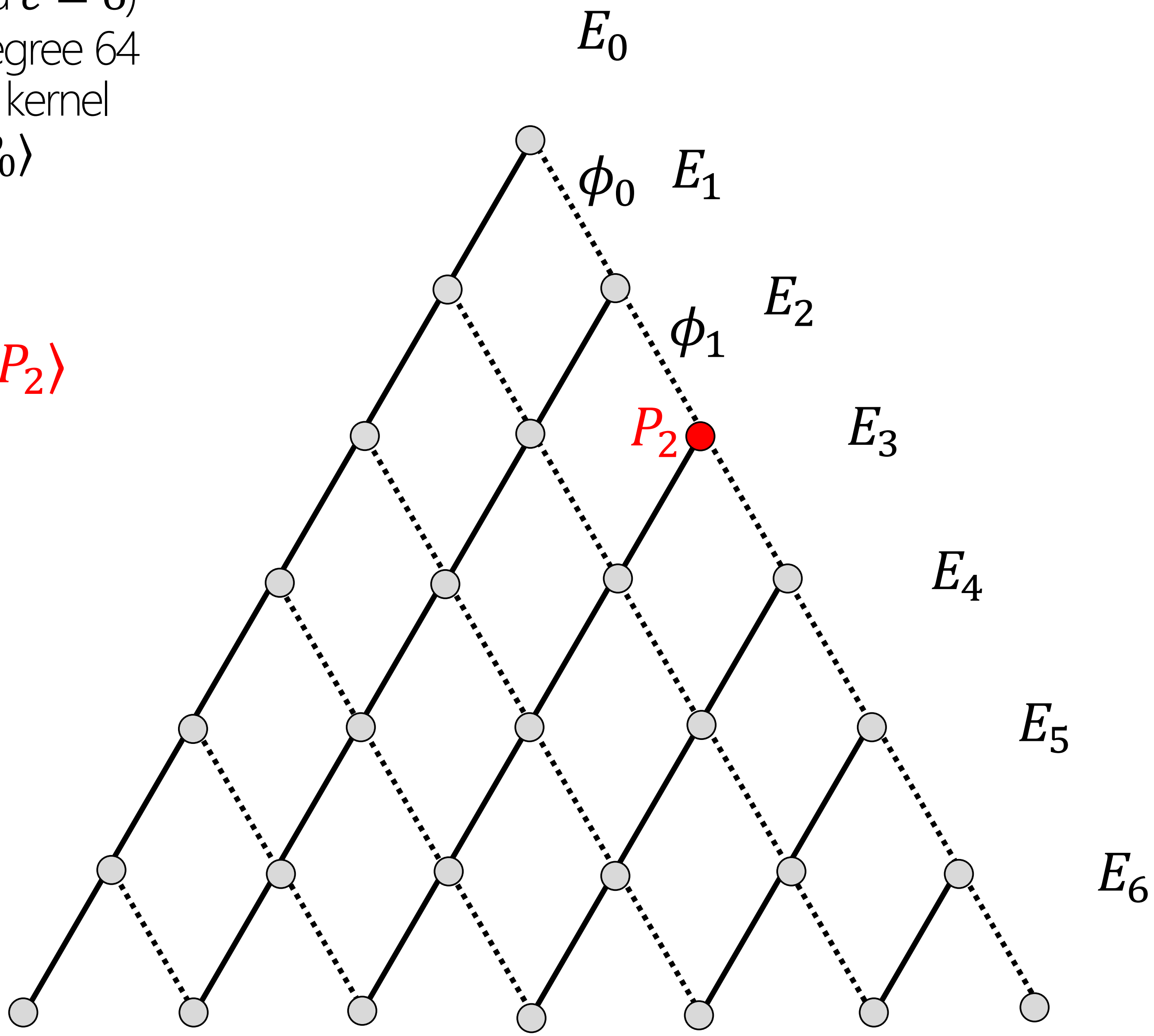
$$P_2 = \phi_1(P_1)$$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \rightarrow E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_6 = E_2 / \langle P_2 \rangle$



Computing ℓ^e degree isogenies

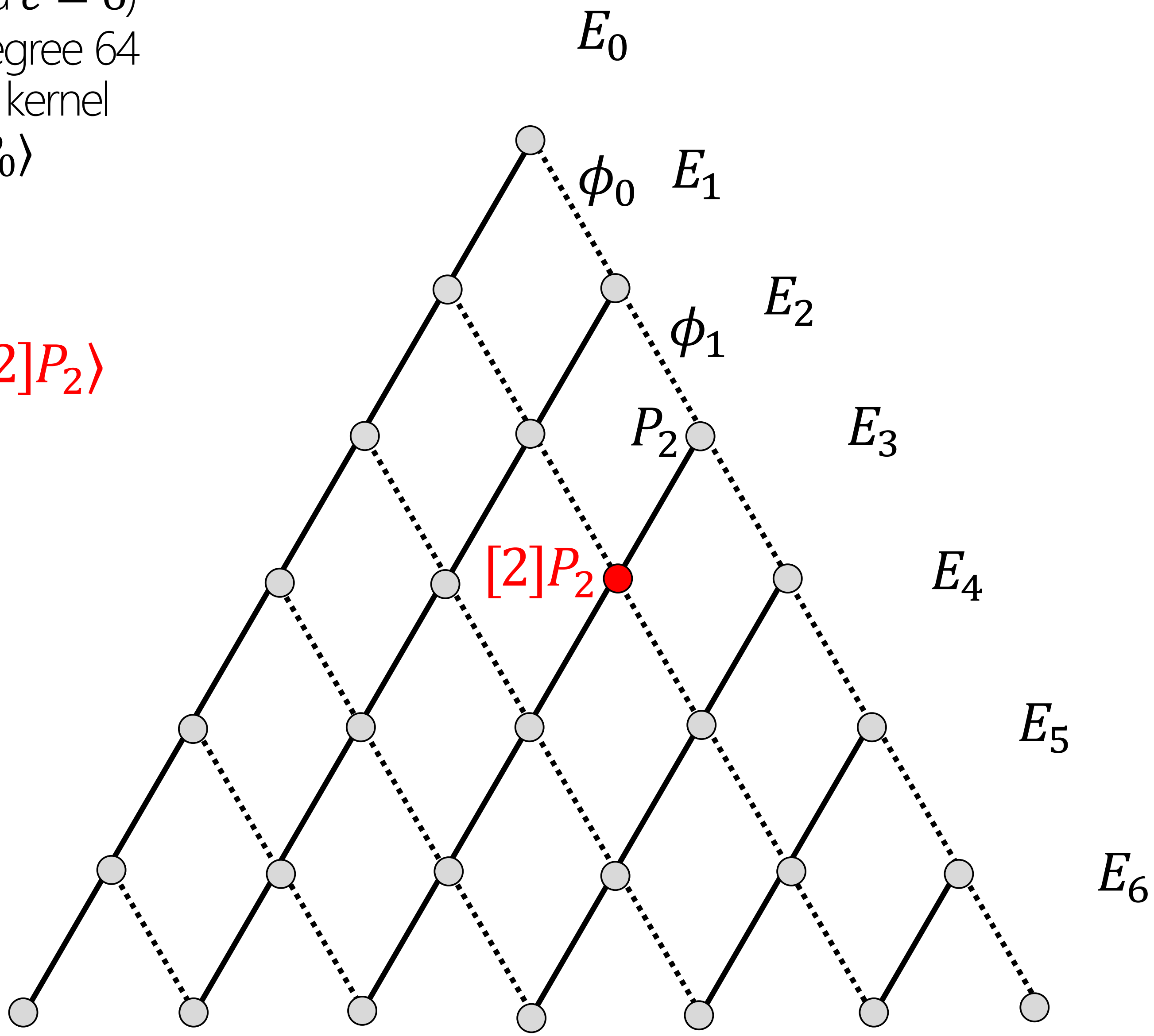
(suppose $\ell = 2$ and $e = 6$)

$\phi: \ E_0 \to E_6$ is degree 64

64 elements in its kernel

$\ker(\phi) = \langle P_0 \rangle$

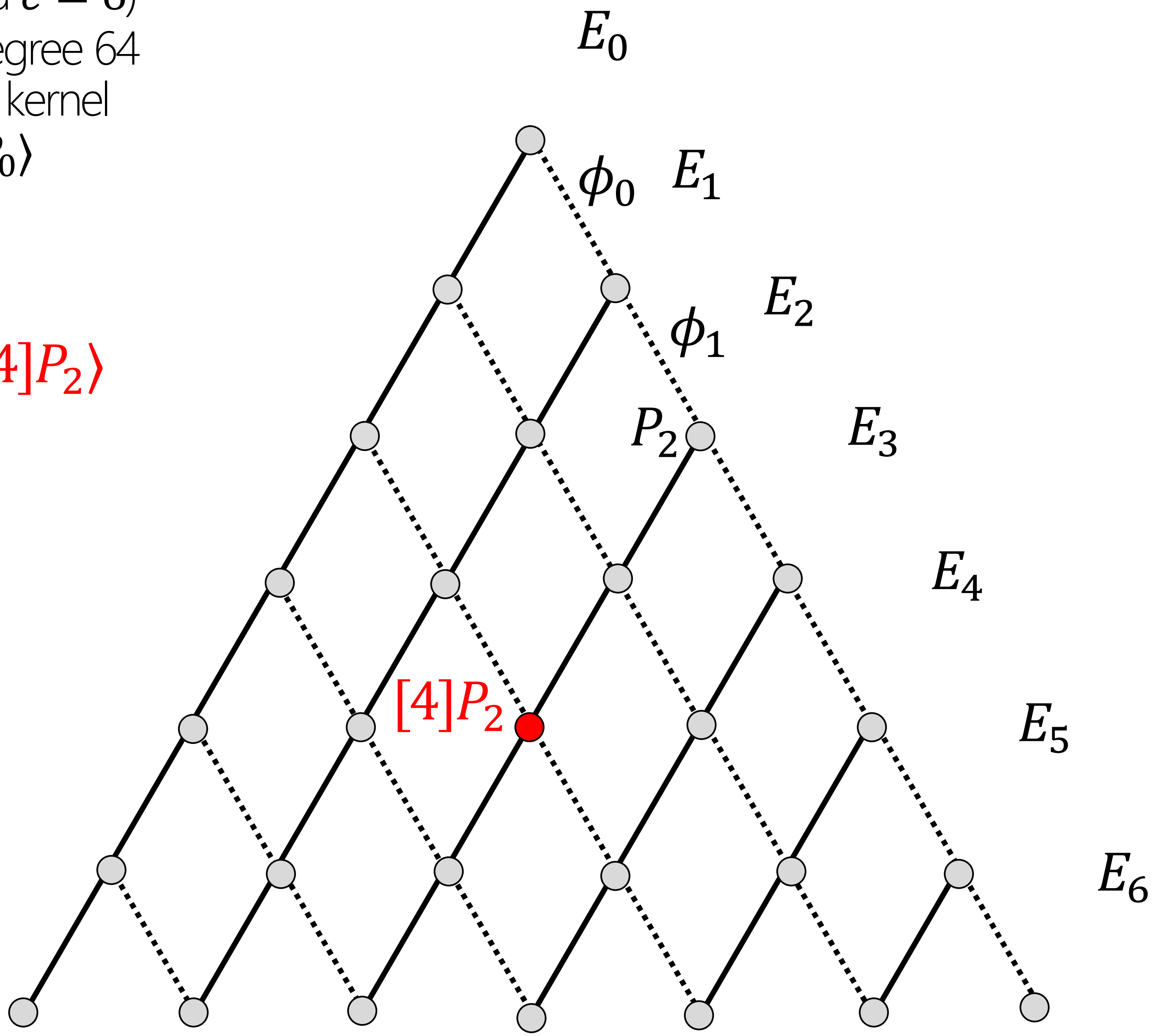
$E_5 = E_2/\langle [2]P_2 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

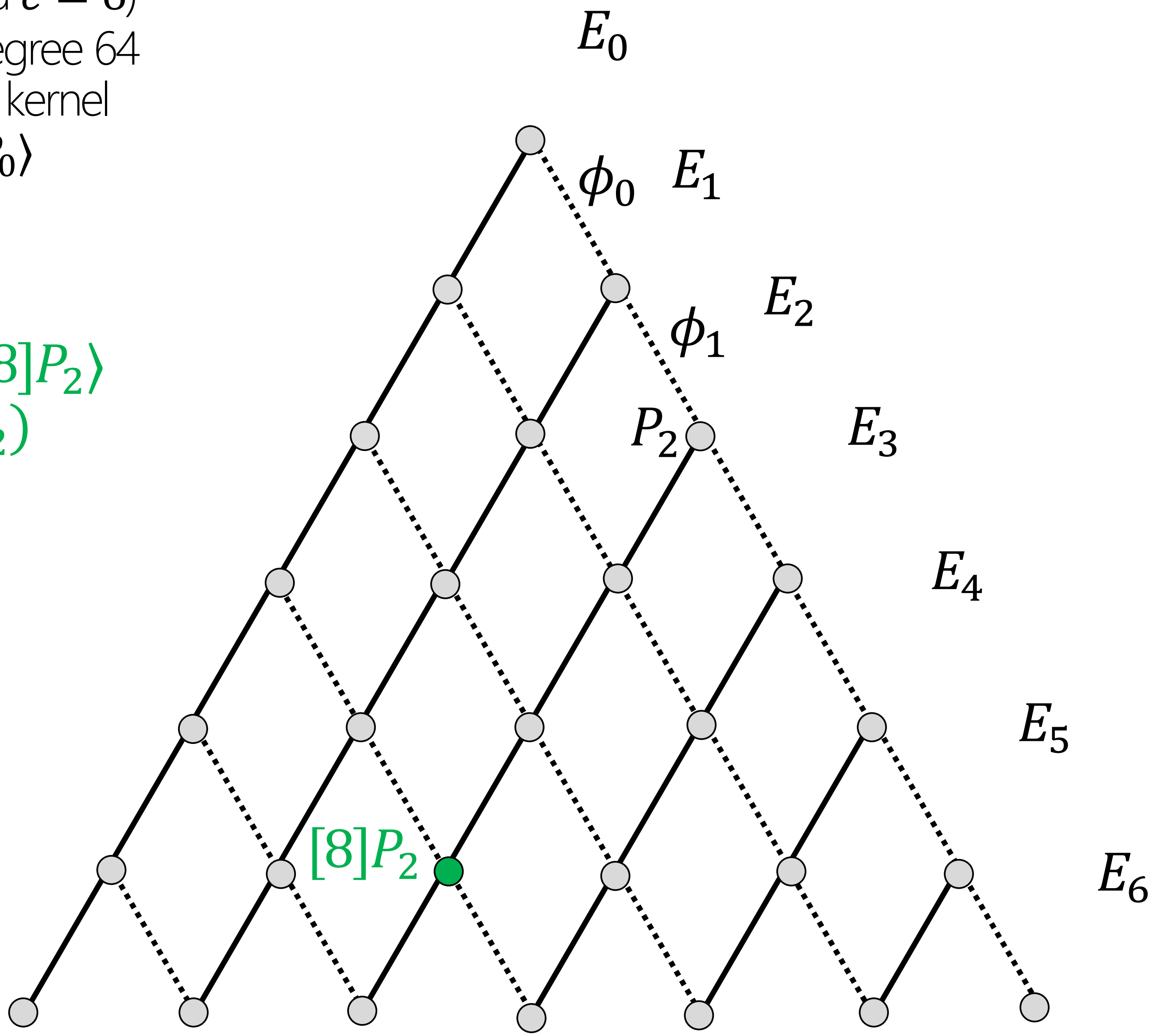
$E_4 = E_2 / \langle [4]P_2 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: \ E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_3 = E_2 / \langle [8]P_2 \rangle$
$= \phi_2(E_2)$

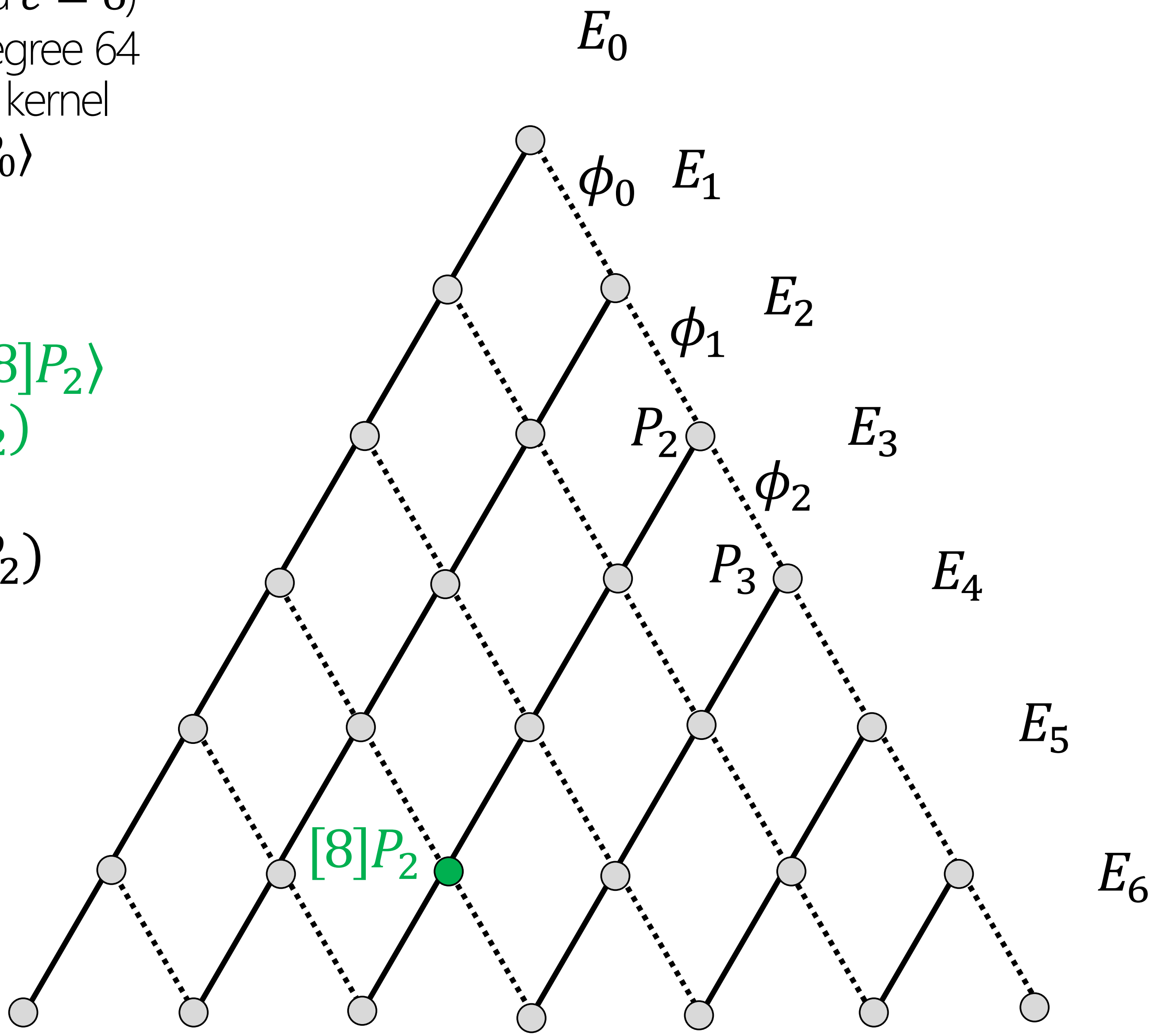


Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_3 = E_2/\langle [8]P_2 \rangle$
$= \phi_2(E_2)$

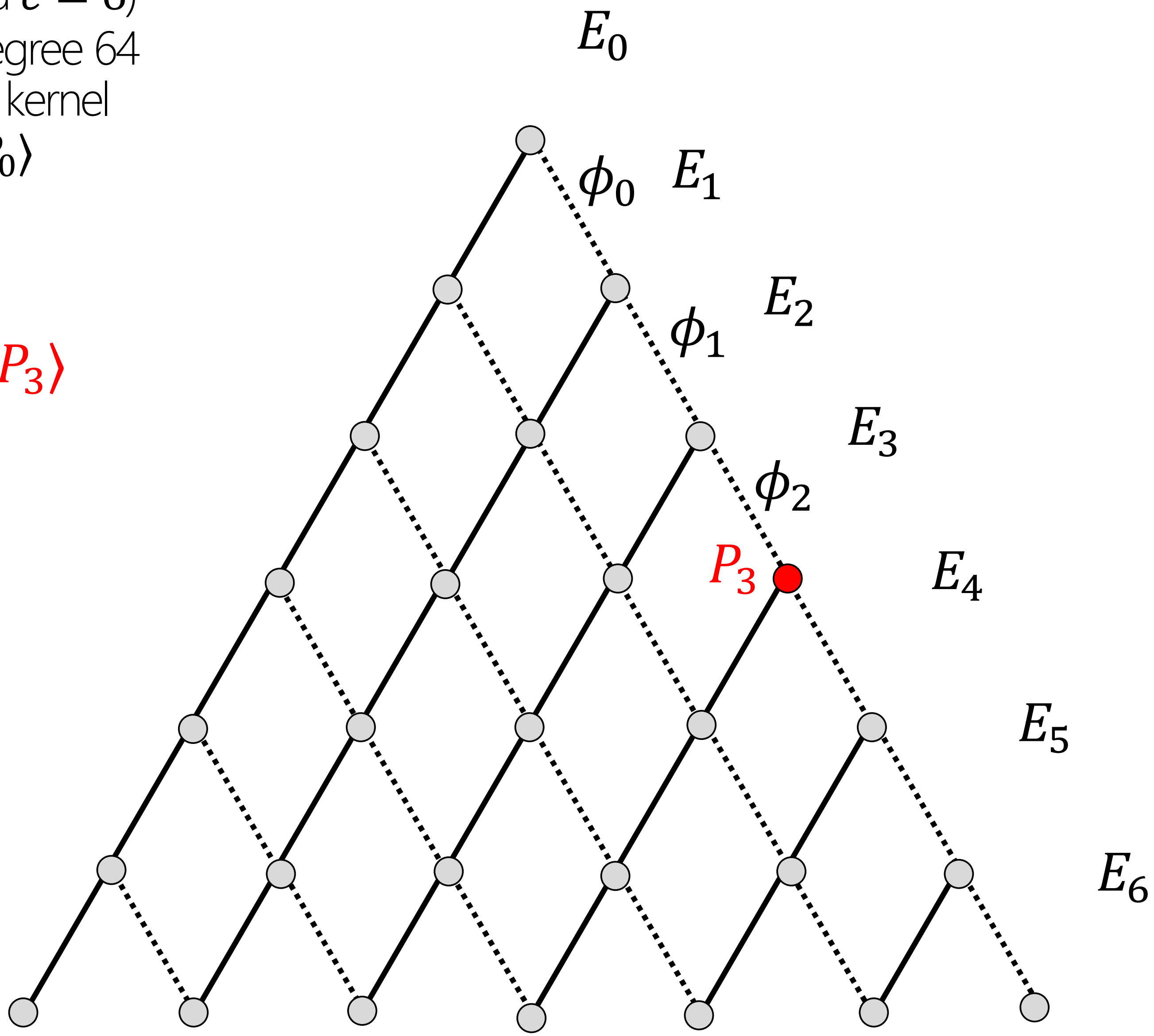
$P_3 = \phi_2(P_2)$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: \ E_0 \rightarrow E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

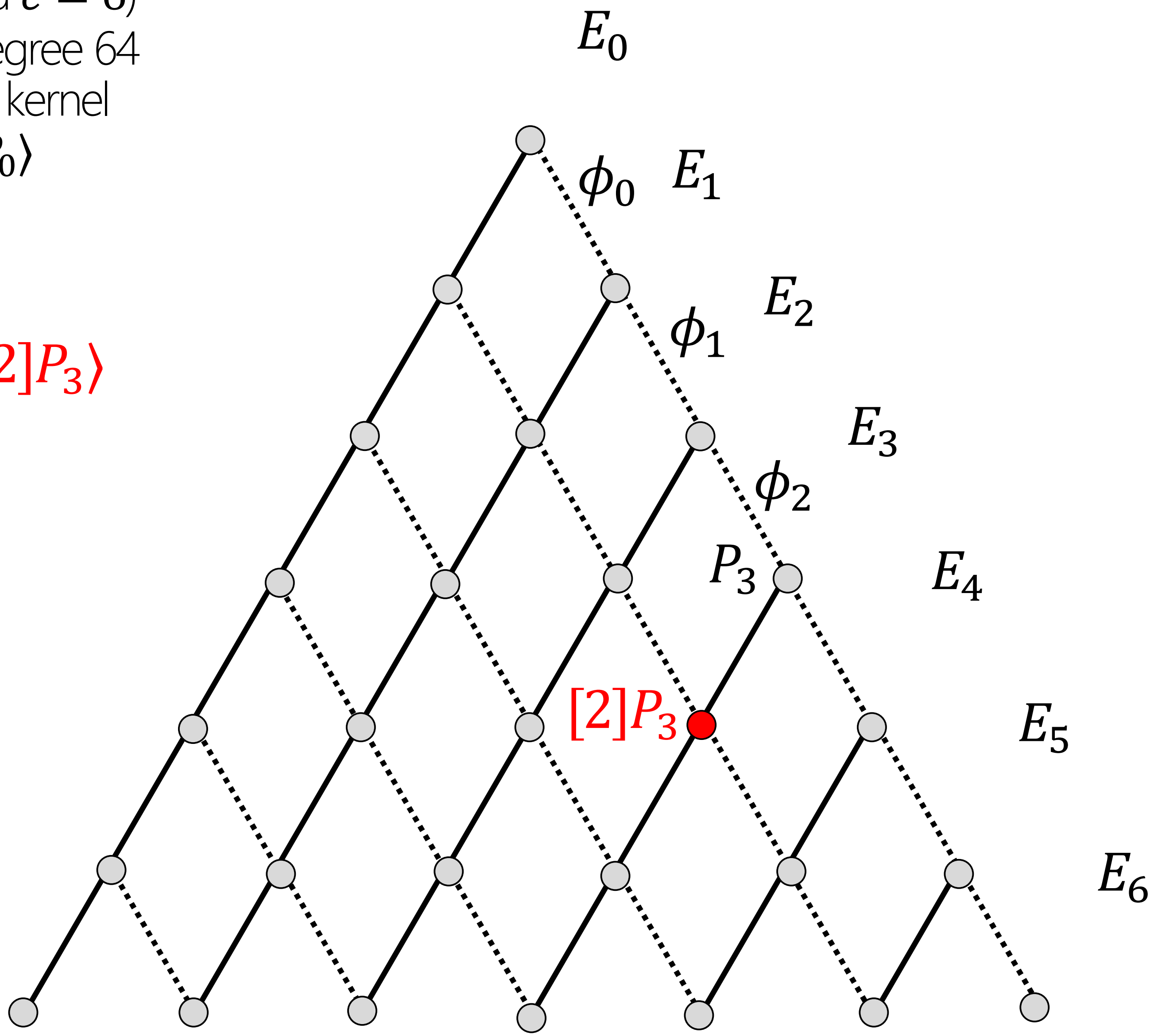
$E_6 = E_3/\langle P_3 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

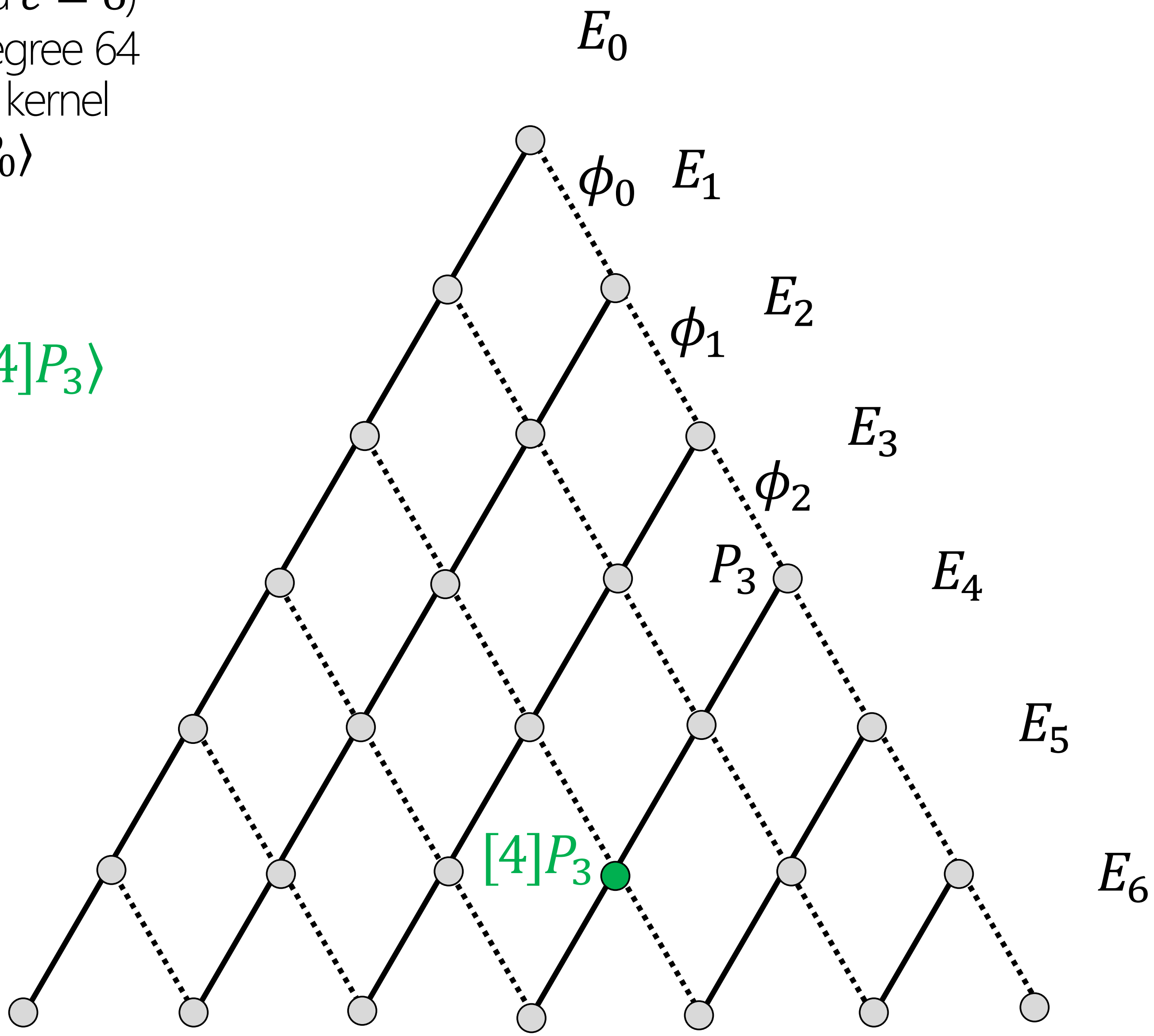
$E_5 = E_3/\langle [2]P_3 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi: E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_4 = E_3 / \langle [4]P_3 \rangle$

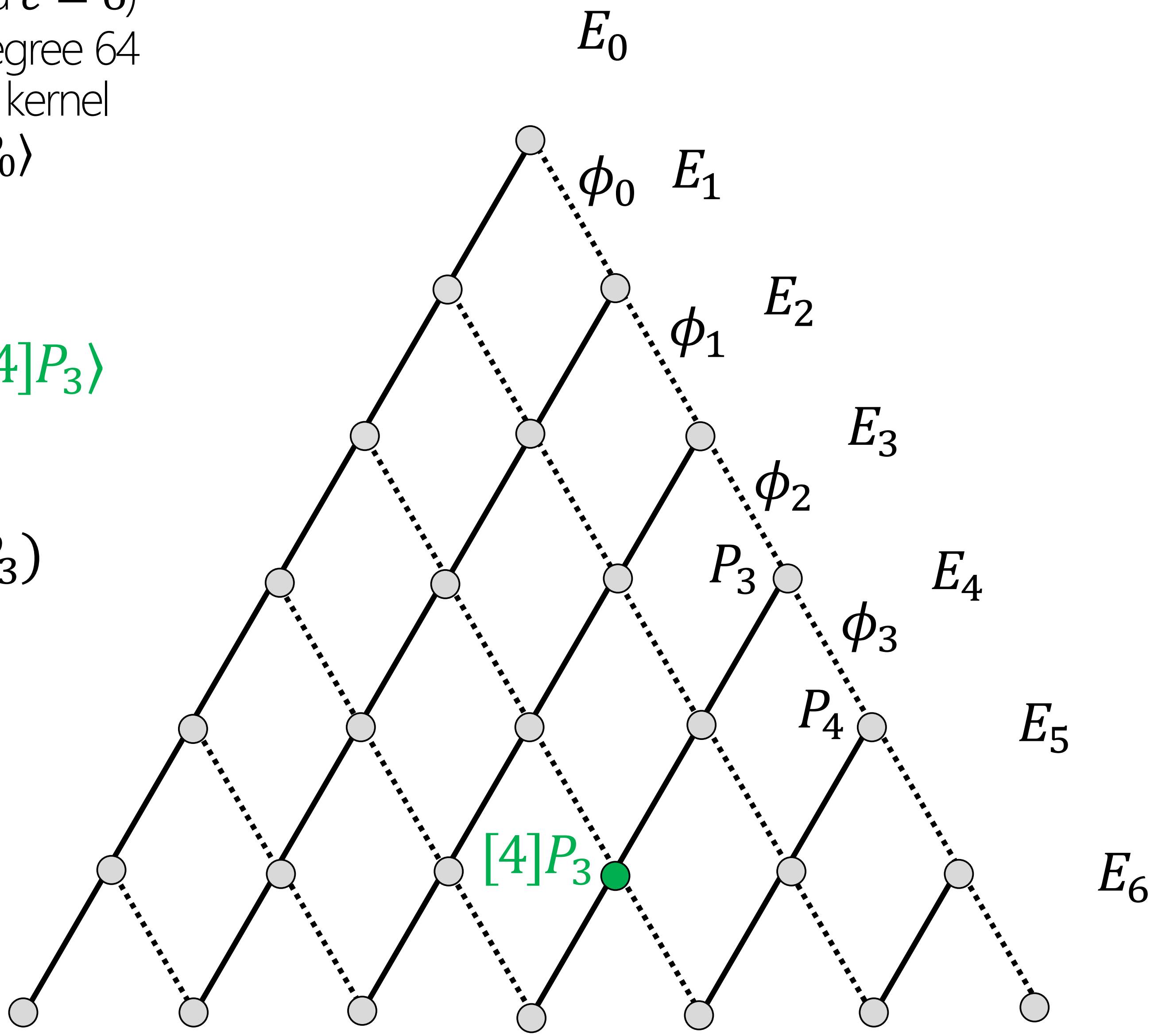


Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_4 = E_3/\langle [4]P_3 \rangle$

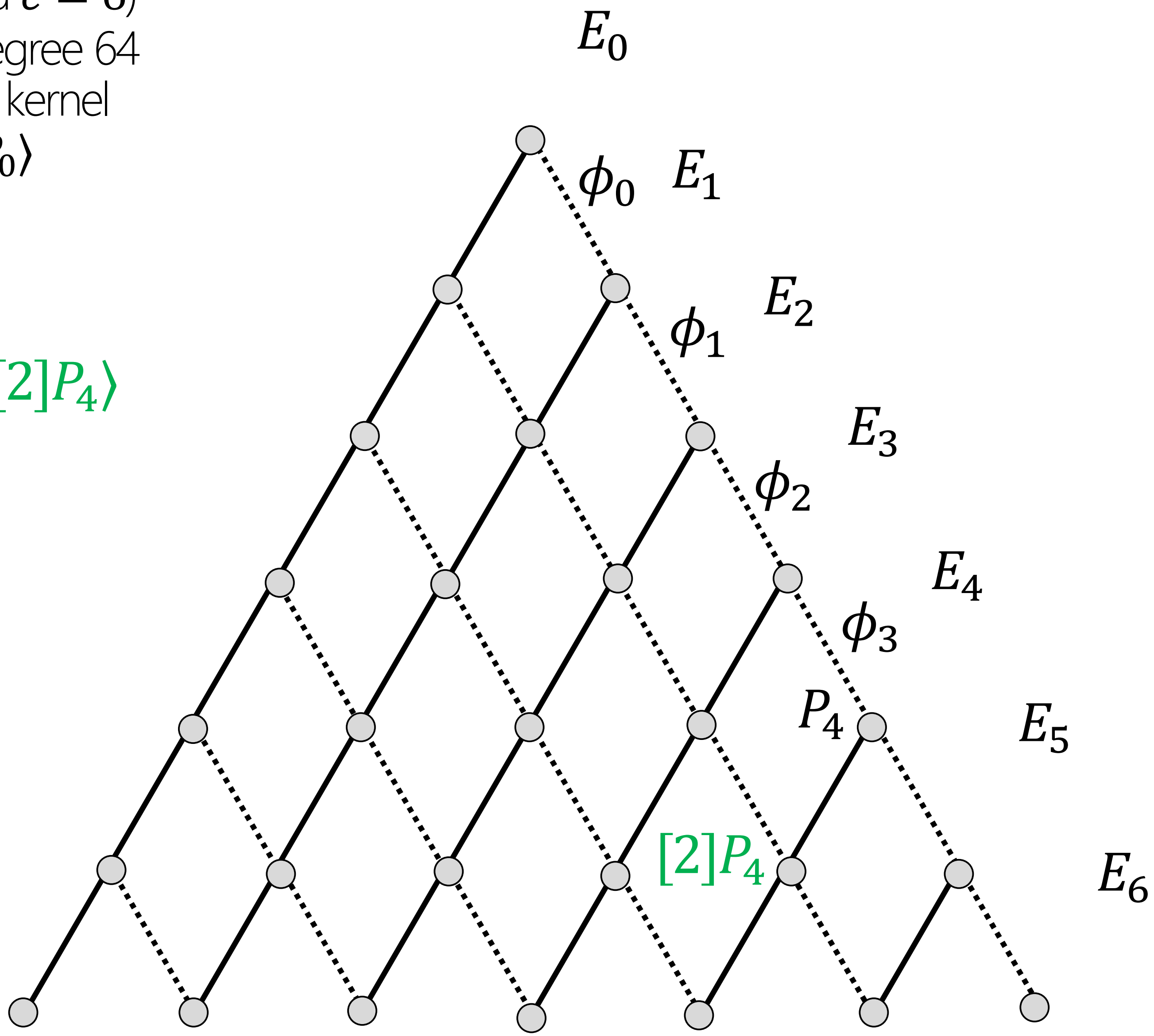
$P_4 = \phi_3(P_3)$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_5 = E_4 / \langle [2]P_4 \rangle$

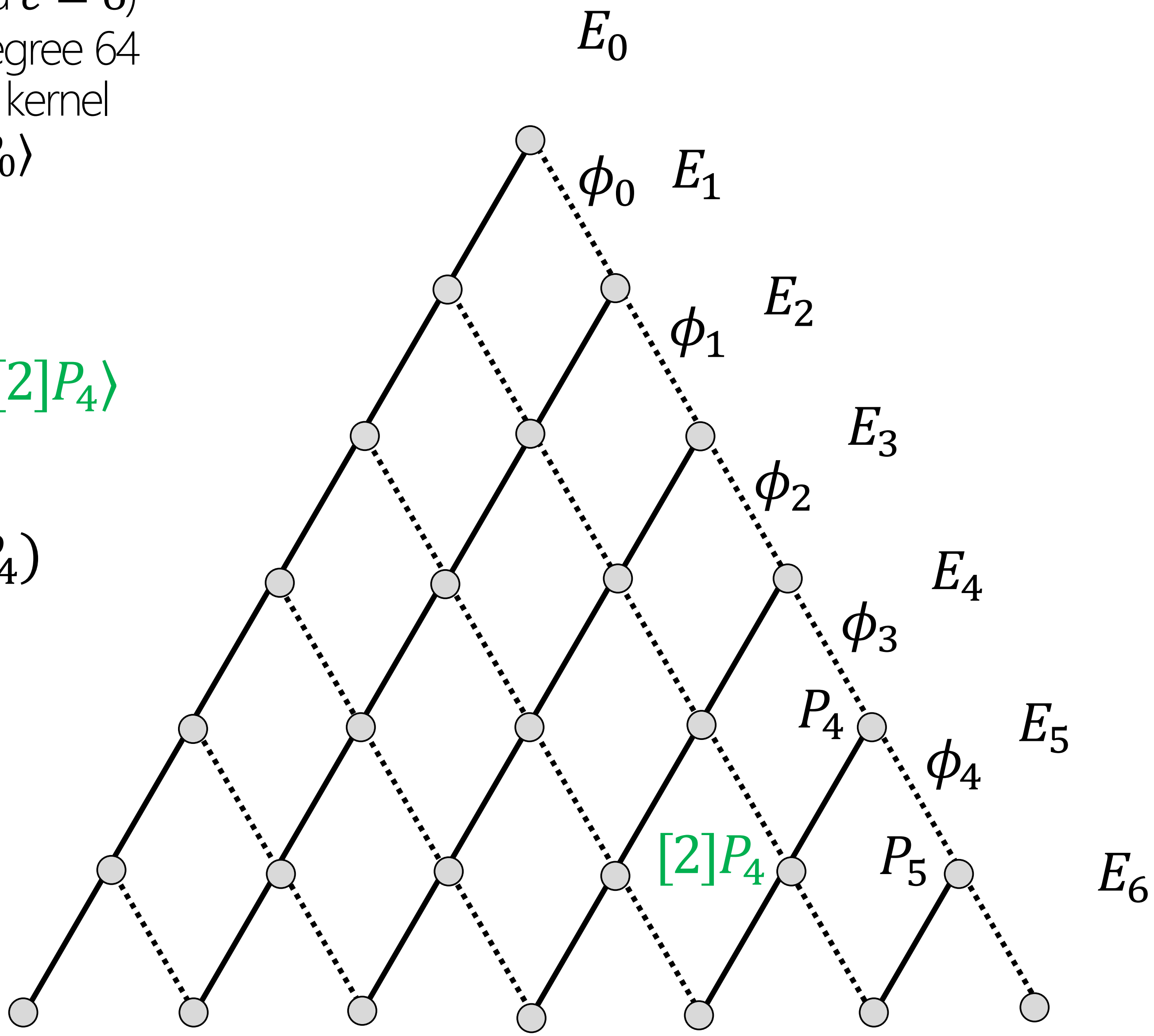


Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

$E_5 = E_4 / \langle [2]P_4 \rangle$

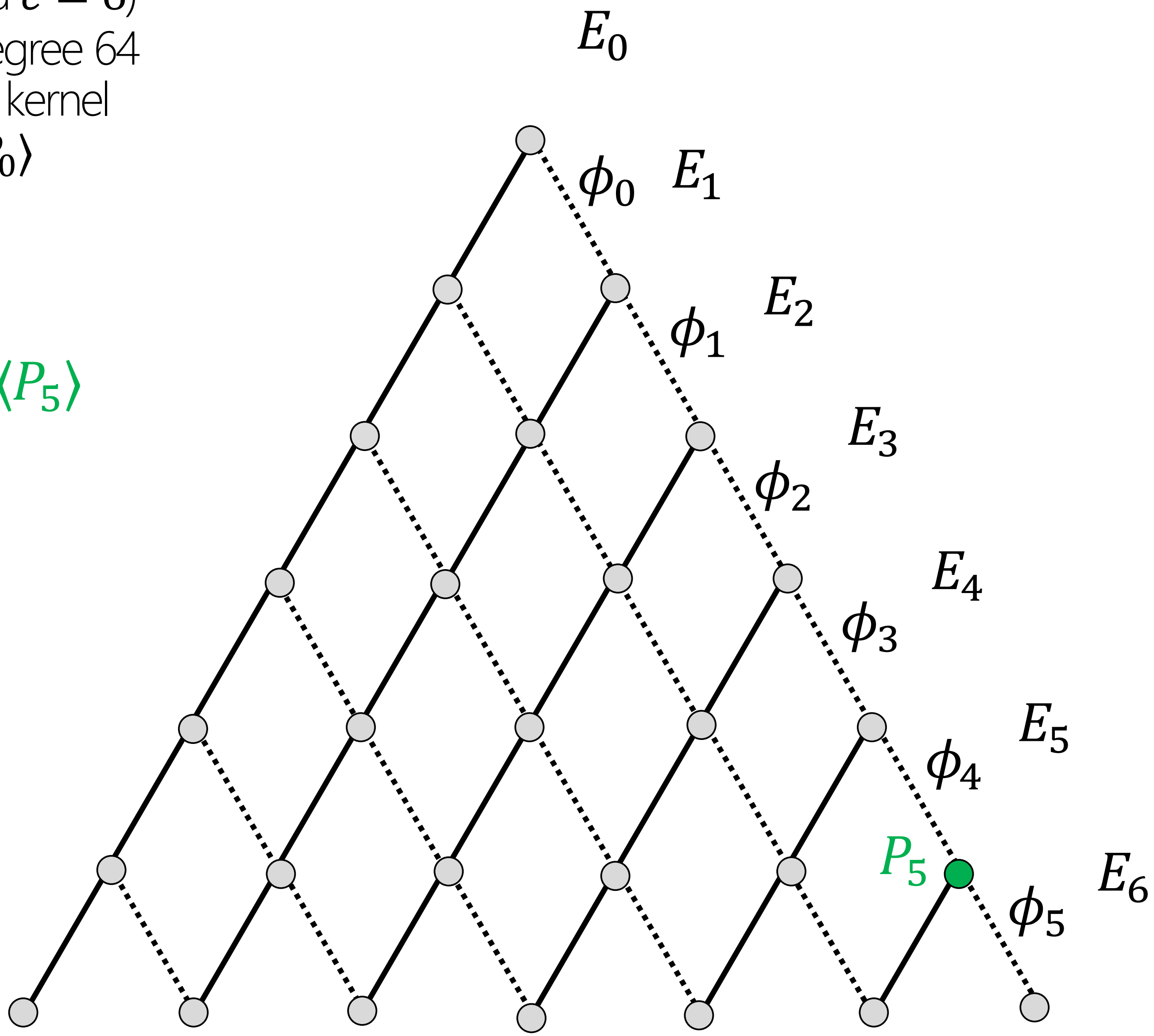
$P_5 = \phi_4(P_4)$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \rightarrow E_6$ is degree 64
64 elements in its kernel
$\ker(\phi) = \langle P_0 \rangle$

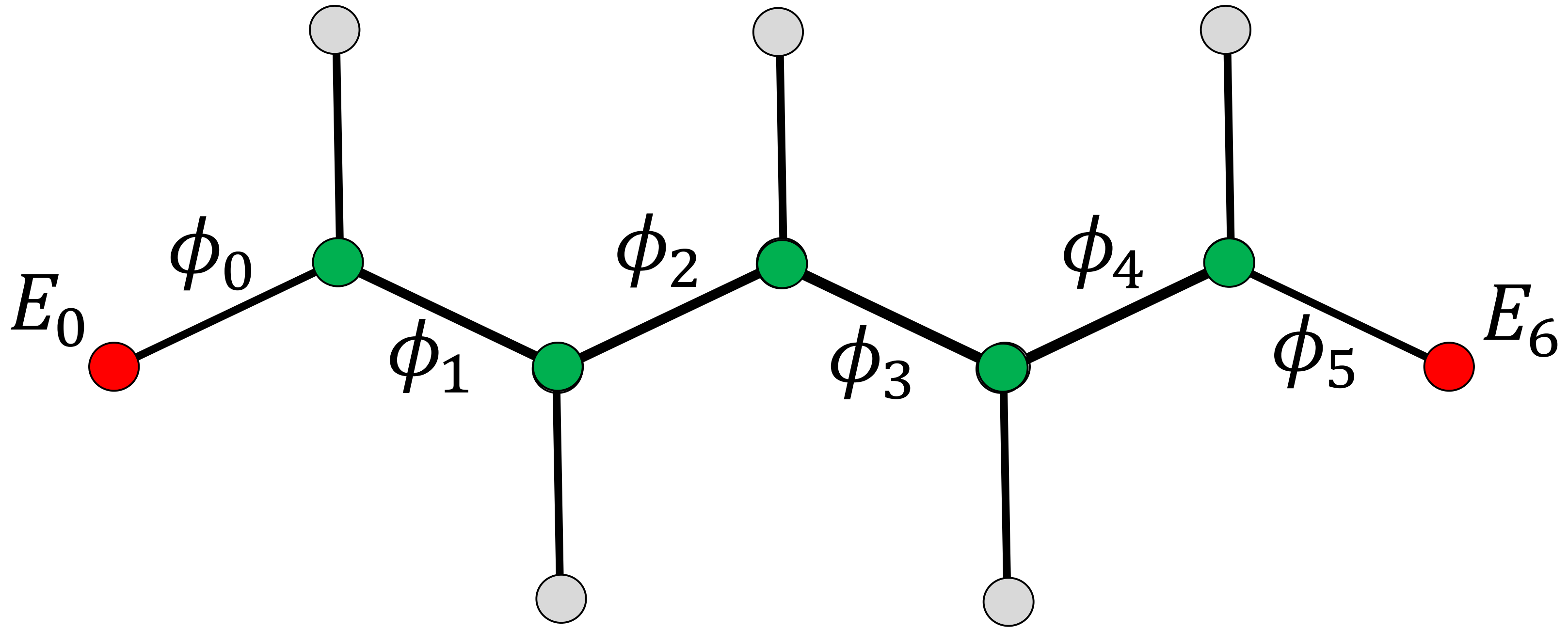
$E_6 = E_5/\langle P_5 \rangle$



Computing ℓ^e degree isogenies

$$\phi : E_0 \to E_6$$

$$\phi = \phi_5 \circ \phi_4 \circ \phi_3 \circ \phi_2 \circ \phi_1 \circ \phi_0$$




E
?
E′

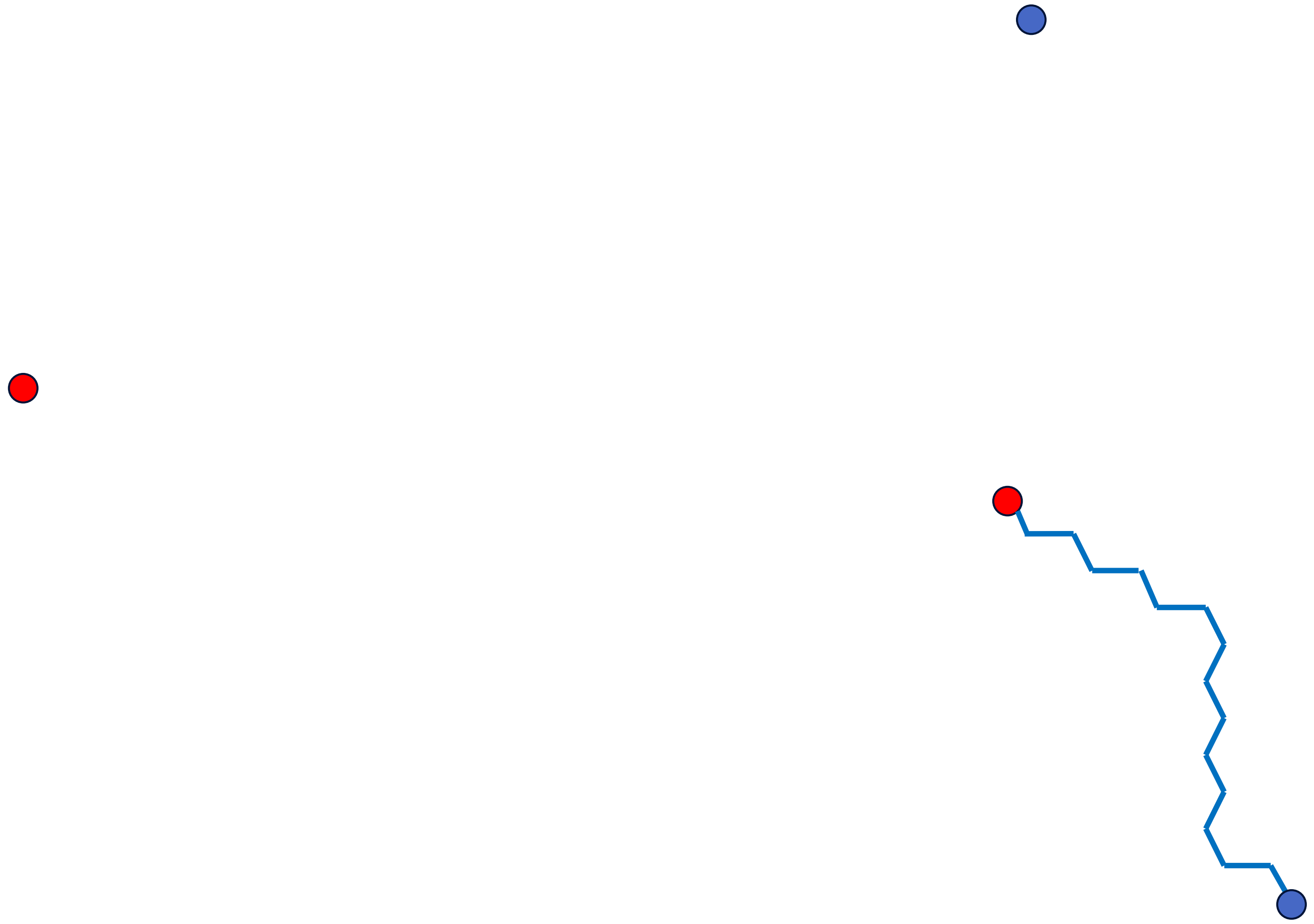
Claw algorithm

Given E and $E' = \phi(E)$, with ϕ degree ℓ^e, find ϕ

Claw algorithm

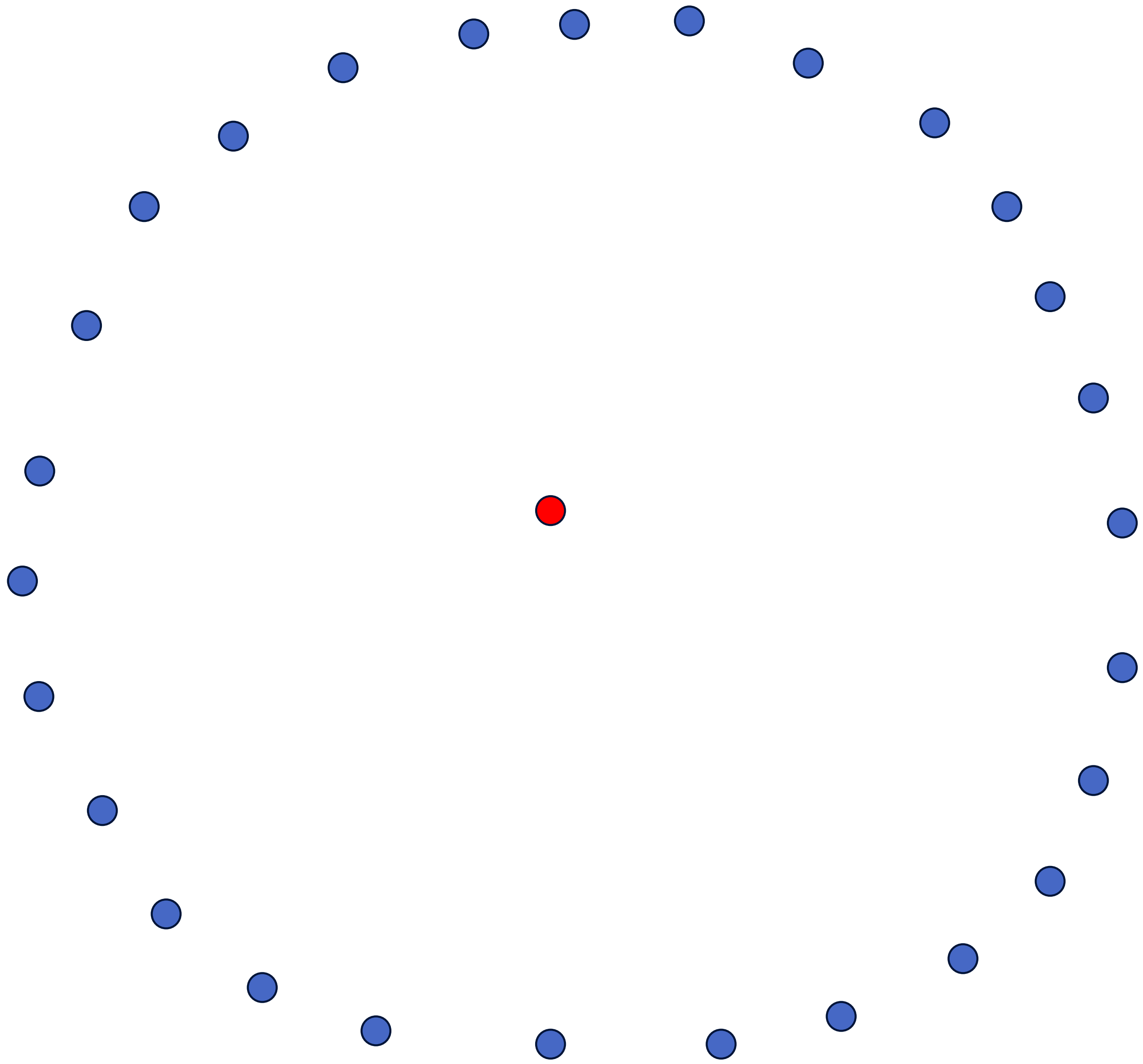
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



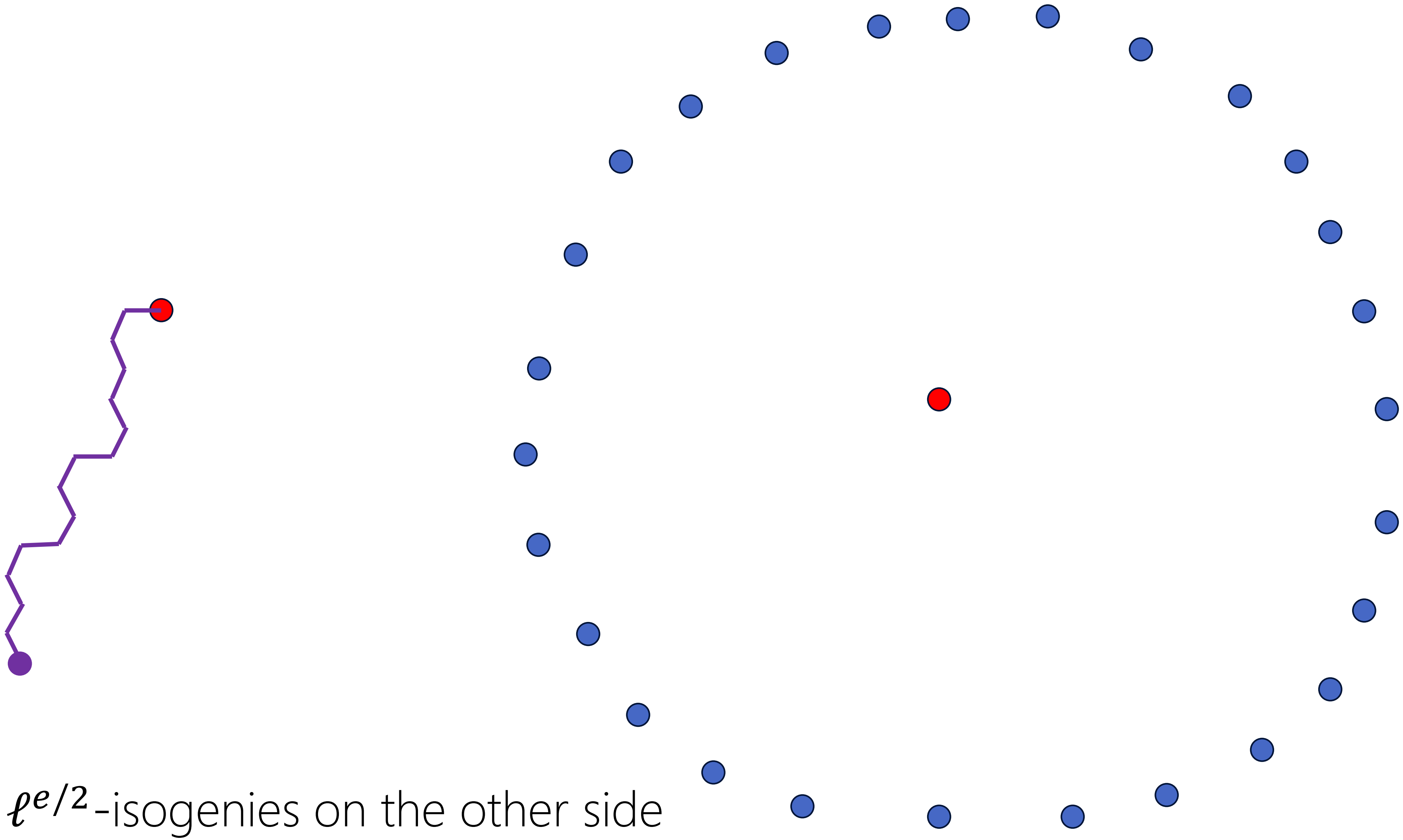
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



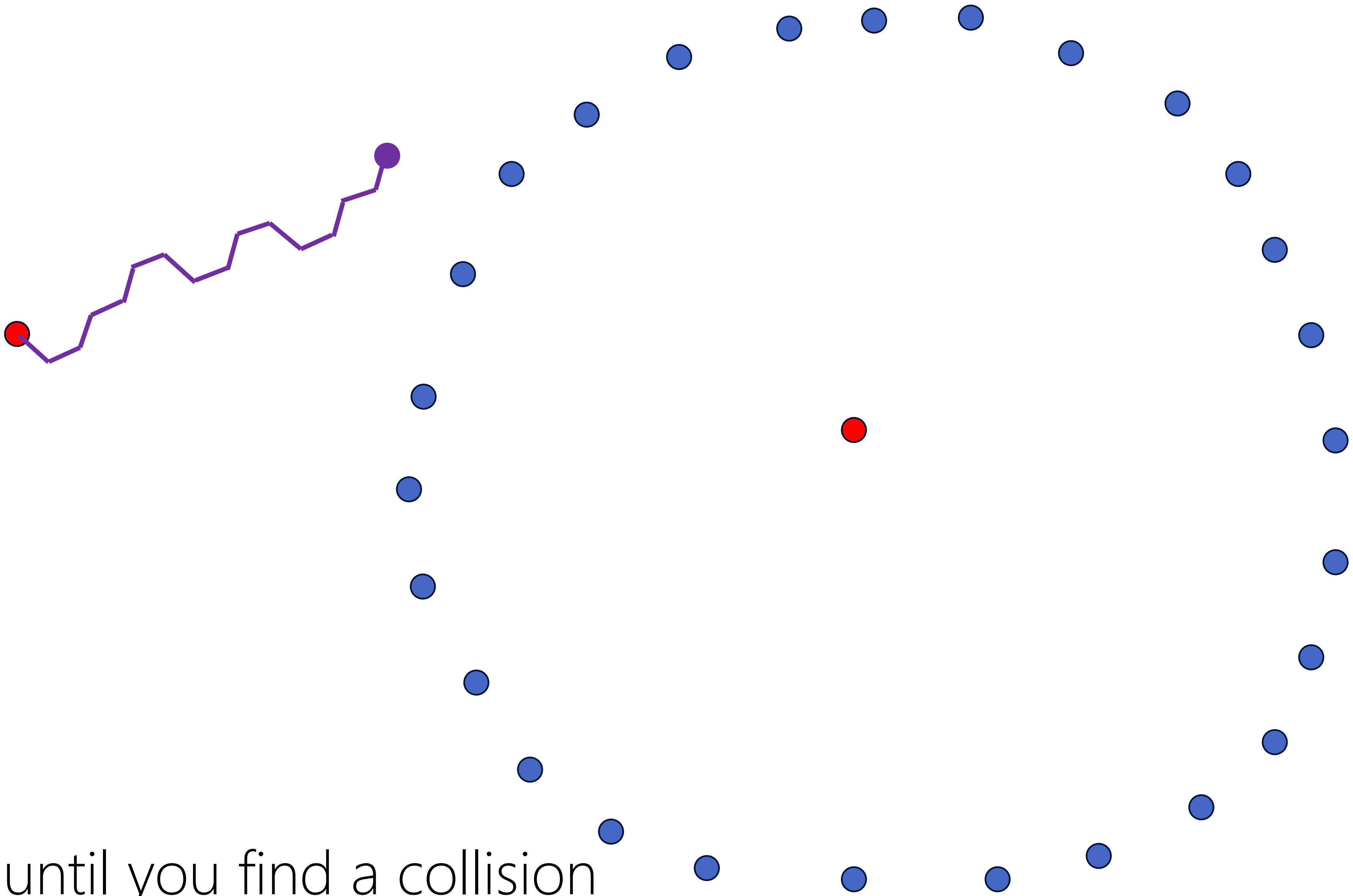
... until you have all of them

Claw algorithm



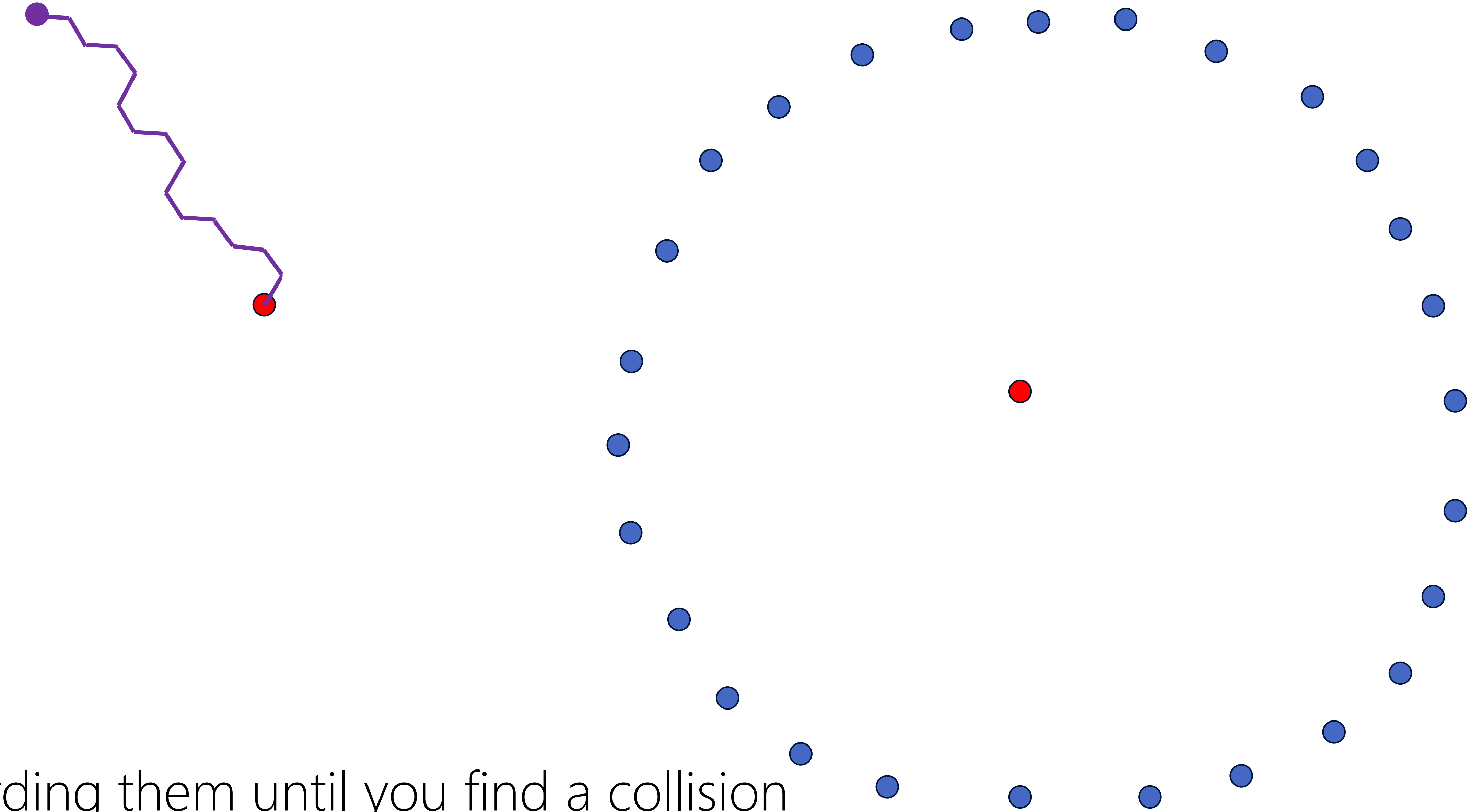
Now compute $\ell^{e/2}$-isogenies on the other side

Claw algorithm



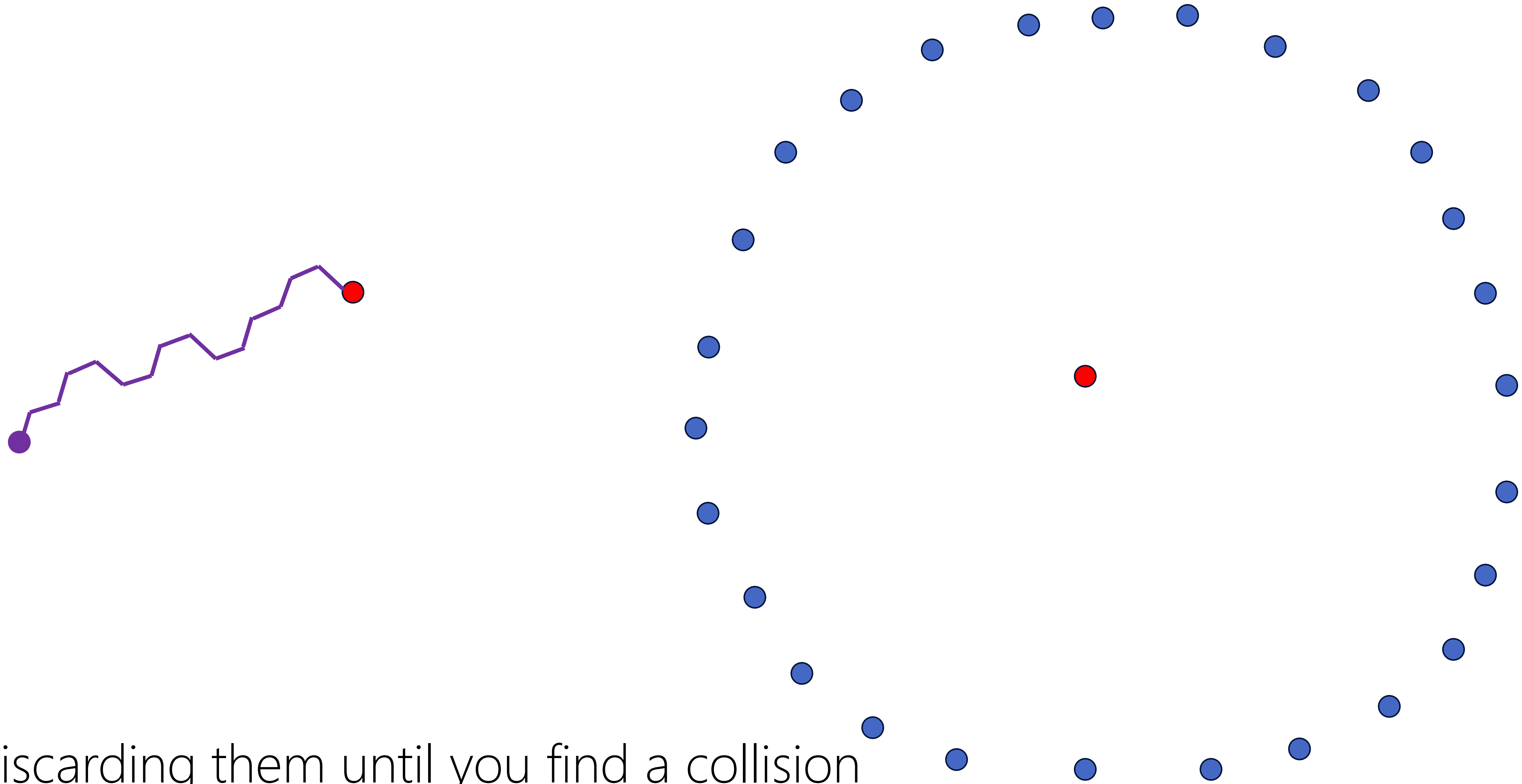
… discarding them until you find a collision

Claw algorithm



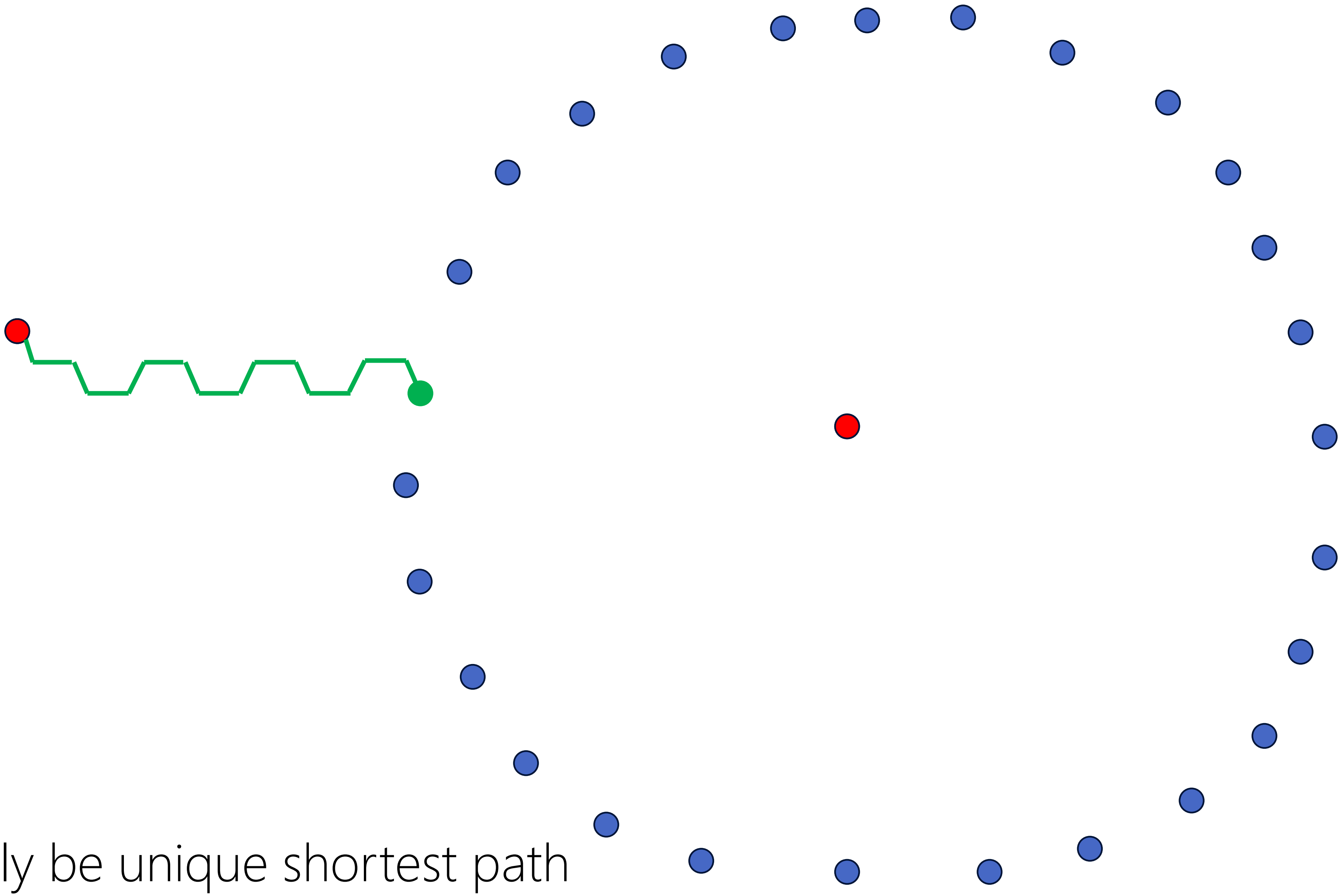
… discarding them until you find a collision

Claw algorithm



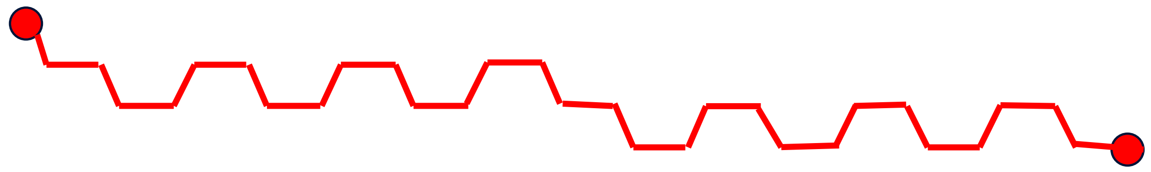
… discarding them until you find a collision

Claw algorithm



Collision will most likely be unique shortest path

Claw algorithm



This path describes secret isogeny $\phi : E \to E'$

Claw algorithm: classical analysis

- There are $O(\ell^{e/2})$ curves $\ell^{e/2}$-isogenous to E' (the blue nodes)

thus $O(\ell^{e/2}) = O(p^{1/4})$ classical memory

- There are $O(\ell^{e/2})$ curves $\ell^{e/2}$-isogenous to E' (the blue nodes), and there are $O(\ell^{e/2})$ curves $\ell^{e/2}$-isogenous to E (the purple nodes)

thus $O(\ell^{e/2}) = O(p^{1/4})$ classical time

- **Best (known) attacks:** classical $O(p^{1/4})$ and quantum $O(p^{1/6})$
- **Confidence:** both complexities are optimal for a black-box claw attack

SIDH: security summary

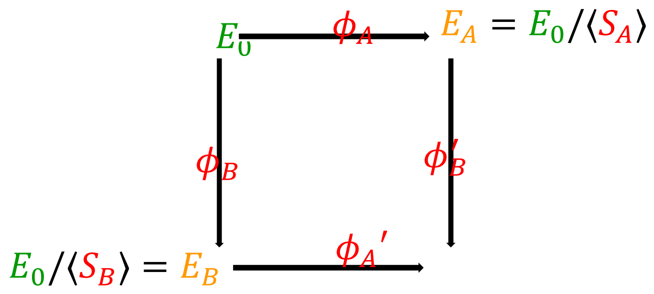
- **Setting:** supersingular elliptic curves $E/\mathbb{F}_{p^2}$ where p is a large prime

- **Hard problem**: Given $P, Q \in E$ and $\phi(P), \phi(Q) \in \phi(E)$, compute ϕ
  (where ϕ has fixed, smooth, public degree)

- **Best (known) attacks:** classical $O(p^{1/4})$ and quantum $O(p^{1/6})$

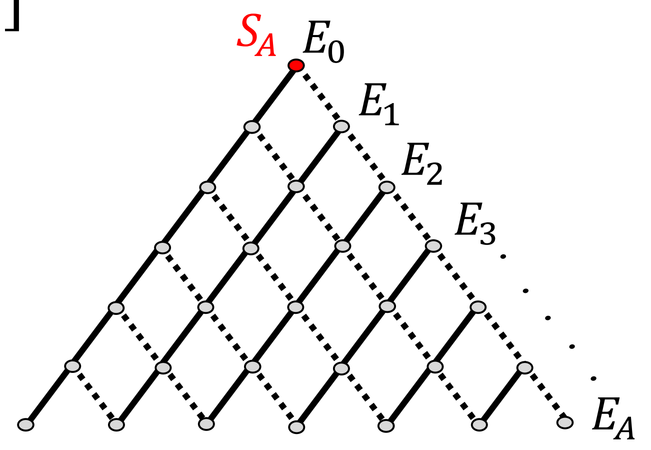
- **Confidence:** above complexities are optimal for (above generic) claw attack

SIDH: summary



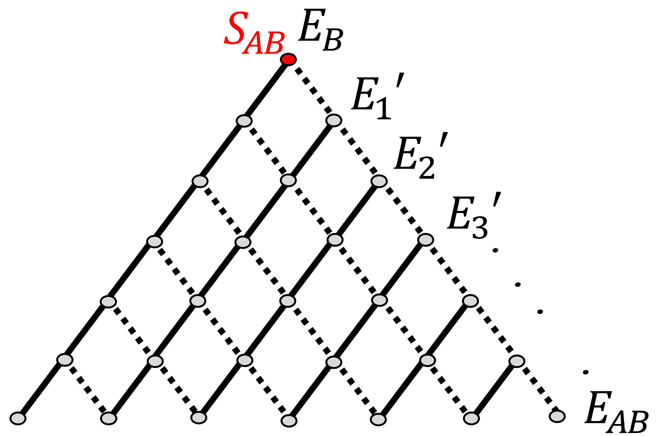
- **Setting:** supersingular elliptic curves $E/\mathbb{F}_{p^2}$ where $p = 2^i 3^j - 1$
- **Parameters:**

$$E_0/\mathbb{F}_{p^2} : y^3 = x^3 + x \quad \text{with} \quad \#E_0 = \left(2^i 3^j\right)^2$$
$$P_A, Q_A \in E_0\left[2^i\right] \text{ and } P_B, Q_B \in E_0[3^j]$$



- Public key generation (Alice):

$$s \in [0, 2^i)$$
$$S_A = P_A + [s]Q_A$$
$$\phi_A : \ E_0 \to E_A := E_0/\langle S_A \rangle$$
$$\text{send } E_A, \phi_A(P_B), \phi_A(Q_B) \text{ to Bob}$$



- Shared key generation (Alice):

$$S_{AB} = \phi_B(P_A) + [s]\phi_B(Q_A) \in E_B$$
$$\phi_{A'} : \ E_B \to E_{AB} := E_B/\langle S_{AB} \rangle$$
$$j_{AB} = j(E_{AB})$$

SIKE: Supersingular Isogeny Key Encapsulation

(static key SIDH falls prey to active attacks)

amazon

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

TEXAS INSTRUMENTS

Microsoft Research

Radboud University

IN·DEI·NOMINE·FELICITER

FAU FLORIDA ATLANTIC UNIVERSITY

UNIVERSITY OF WATERLOO

INFOSEC GLOBAL

Actively secure key encapsulation (IND-CCA KEM)

Alice

$$PK_A = [\ \phi_A(E_0), \phi_A(P_B), \phi_A(Q_B)\ ]$$

$$s \in_R \{0,1\}^\ell$$

Bob

$$m \in_R \{0,1\}^\ell$$

$$r = H_2(PK_A, m)$$

$$PK_B(r) = [\ \phi_B(E_0), \phi_B(P_A), \phi_B(Q_A)\ ]$$

$$j = j(E_{BA}) = j\left(\phi_B\big(\phi_A(E_0)\big)\right)$$

$$K = H_3(c, m)$$

$$c = [PK_B(r)\ , H_1(j) \oplus m]$$

$$j = j(E_{AB}) = j\left(\phi_A\big(\phi_B(E_0)\big)\right)$$

$$m' = c[2] \oplus H_1(j)$$

$$r' = H_2(PK_A, m')$$

if $PK_B(r') = c[1]$ then $K = H_3(c, m')$ else $K = H_3(c, s)$

$$H_1(j) = \text{cSHAKE256}(j, k, \text{" "}, 2)$$

$$H_2(PK_A, m) = \text{cSHAKE256}(m || PK_A, e_2, \text{" "}, 0)$$

$$H_3(c, m) = \text{cSHAKE256}(m || c, k, \text{" "}, 1)$$

The curves and their security estimates

$$p = 2^{e_A} 3^{e_B} - 1$$

Name (SIKEp+ $\lceil \log_2 p \rceil$)	$(\boldsymbol{e_A}, \boldsymbol{e_B})$	$\boldsymbol{k}$	$\mathbf{2^{k-1}}$	**min** $(\sqrt{\mathbf{2}^{e_A}}, \sqrt{\mathbf{3}^{e_3}})$	$\sqrt{\mathbf{2}^{k}}$	**min** $(\sqrt[3]{\mathbf{2}^{e_2}}, \sqrt[3]{\mathbf{3}^{e_3}})$
SIKEp503	(250,159)	128	2^{127}	2^{125}	2^{64}	2^{83}
SIKEp761	(372,239)	192	2^{191}	2^{186}	2^{96}	2^{124}
SIKEp964	(486,301)	256	2^{255}	2^{238}	2^{128}	2^{159}

classical

quantum

SIKE vs. IND-CCA lattice KEMs

Name	**Primitive**	**Encaps+ Decaps (ms)**	**Size of Encaps. (KB)**
NTRU-KEM	NTRU	0.03	1.3
Kyber	M-LWE	0.07	1.2
FrodoKEM	LWE	1.2 – 2.3	9.5 – 15.4
SIKE	Supersingular Isogeny	10 – 30	0.4 – 0.6

Results obtained on 3.4GHz Intel Haswell (Kyber and NTRU-KEM) or Skylake (FrodoKEM and SIKE)

Other recent isogeny-based crypto

- **Compression**: Azarderakhsh et al (eprint 2016/229) and C- et al (2016/963) and Zanon et al (2017/1143)
  Halve the keys for (now less than) twice the cost

- **Signatures**: Yoo et al (2017/186) and Galbraith-Petit-Silva (2016/1154)
  Fiat-Shamir bit-by-bit: big and slow

- **OIDH**: De Feo-Kieffer-Smith (2018/485)
  Optimising the ordinary/commutative case: cool, but slow and painful

- **CSIDH**: Castryck et al (2018/383)
  As in 2018/485 but supersingular over $\mathbb{F}_p$: non-interactive!, interesting…

Questions?