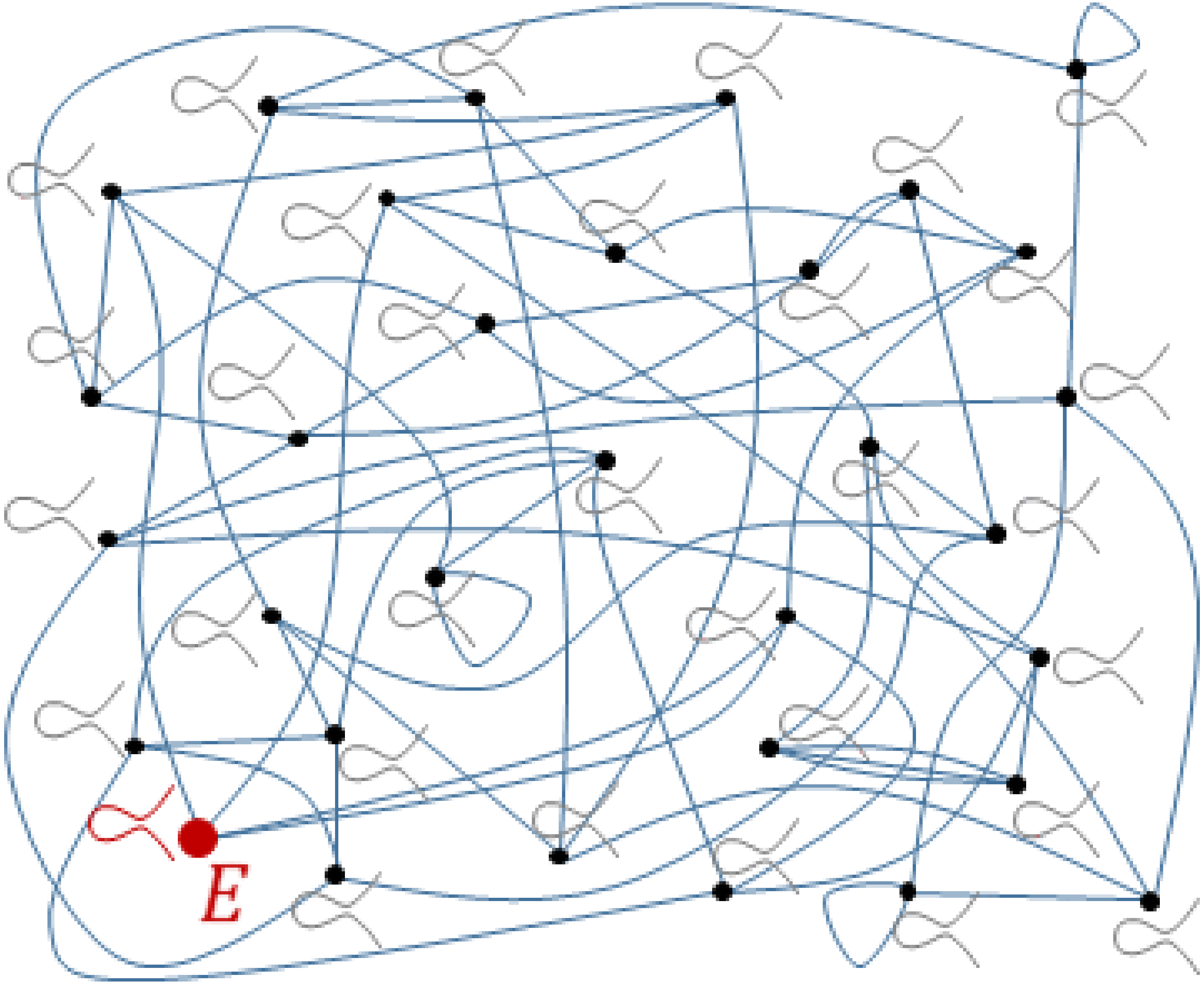
An introduction to supersingular isogeny-based cryptography

Craig Costello

November 10
ECC 2017
Nijmegen, The Netherlands

Microsoft®
Research



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

Part 1: Motivation

Part 2: Preliminaries

Part 3: SIDH

Diffie-Hellman key exchange (circa 1976)

$$q = 160693804425899027554196209234116260252220299378279283530 1301$$

$$g = 123456789$$

$g^a \bmod q = 784673745294226535797545963198527025754996929800857779485 93$

$560048104293218128667441021342483133802626271394299410128798 = g^b \bmod q$

$a =$
685408003627063
761059275919665
781694368639459
527871881531452

$b =$
362059131912941
987637880257325
269696682836735
524942246807440

$g^{ab} \bmod q = 437452857085801785219961443000845969831329749878767465041215$

Diffie-Hellman key exchange (circa 2016)

$q =$

580960599536995806285950253330457437068697517636289523666148615228720373099711022573733604453311840725132615775498051744399052959454004712166288567218703240103211116397
06440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580
16186020024749256844815024251530444957718760413642873858099017255157393414625583036640591500086964373205321856683254529110790372283163413859958640669032595972518744716
90595408050123102096390117507487600170953607342349457574162729948560133086169585299583046776370191815940885283450612858638982717634572948835466388795543116154464463301
99254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710
716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$g = 123456789$

$g^a \pmod q =$

197496648183227193286262018614250555971909799762533760654008147994875775445667054218578105133138217497206890599554928429450667899476
854668595594034093493637562451078938296960313488696178848142491351687253054602202966247046105770771577248321682117174246128321195678
537631520278649403464797353691996736993577092687178385602298873558954121056430522899619761453727082217823475746223803790014235051396
799049446508224661850168149957401474638456716624401906701394472447015052569417746372185093302535739383791980070572381421729029651639
304234361268764971707763484300668923972868709121665568669830978657804740157916611563508569886847487772676671207386096152947607114559
706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532
6052422101474898256696660124195726100495725510022002932814218768060112310763455404567248761396399633344901857872119208518550803791724

411604662069593306683228525653441872410777999220572079993574397237156368762038378332742471939666544968793817819321495269833613169937
986164811320795616949957400518206385310292475529284550626247132930124027703140131220968771142788394846592816111078275196955258045178
70525401646977350936925361994895894163065551105161929613139219782198757542984826465893457768888915561514505048091856159412977576049
073563225572809880970058396501719665853110101308432647427786565525121328772587167842037624190143909787938665842005691911997396726455
110758448552553744288464337906540312125397571803103278271979007681841394534114315726120595749993896347981789310754194864577435905673
172970033596584445206671223874399576560291954856168126236657381519414592942037018351232440467191228145585909045861278091800166330876
4073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$= g^b \pmod q$

$a =$

7147687166405; 9571879053605547396582
692405186145916522354912615715297097
100679170037904924330116019497881089
087696131592831386326210951294944584
4004974889298038584931918128447572321
023987160439062006177648318875457556
2337708539125052923646318332191217321
464134655845254917228378772756695589
845219962202945089226966507426526912
7802446416400\9025927104004338958261
1419862375878988193612187945591802864
062679\864839578139273043684955597764
13009721221824915810964579376354556\6
554629883777859568089157882151127357
4220422646379170599917677567\30420698
422392494816906777896174923072071297
603455802621072109220\54662739697748
553543758990879608882627763290293452
560094576029847\3913613887675543866
22479265299978059886472414530462194
52761811989\9746477252908878060493
17954195146382922889045577804592943
73052654\10485180264002079415193983
85114342508427311982036827478946058
7100\304977477069244278989689910572
12096357725203480402449913844583448

$g^{ab} =$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739
419999231378970715307039317876258453876701124543849520979430233302777503265010724513551209279573183234934359636696506
968325769489511028943698821518689496597758218540767517885836464160289471651364552490713961456608536013301649753975875
610659655755567474438180357958360226708742348175045563437075840969230826767034061119437657466993989389348289599600338
950372251336932673571743428823026014699232071116171392219599691096846714133643382745709376112500514300983651201961186
613464267685926563624589817259637248558104903657371981684417053993082671827345252841433337325420088380059232089174946
086536664984836041334031650438692639106287627157575758383128971053401037407031731509582807639509448704617983930135028
7596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468

$b =$

655456209464694; 93360682685816031704
969423104727624468251177438749706128
879957701\93698826859762790479113062
308975863428283798589097017957365590
672\83571386389571224667609499300898
554802446403039544300748002507962036
386619315229886063541005322448463915
89798641210273772558373965\486539312
854838650709031919742048649235894391
90352993032676961005\088404319792729
916038927477470940948581926791161465
02863521484987\086232861934222391717
121545686125300672760188085915004248
49476686\706784051068715397706852664
532638332403983747338379697022624261
377163163204493828299206039808703403
575100467337085017748387148822224875
309641791879395483731754620034884930
540399950519191679471224\05558557093
219350747155777569598163700850920394
705281936392411084\43600686183528465
724969562186437214972625833222544865
996160464558\54629937016589470425264
445624157899586972652935647856967092
689604\42796501209877036845001246792
761563917639959736383038665362727158

ECDH key exchange (1999 – nowish)

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

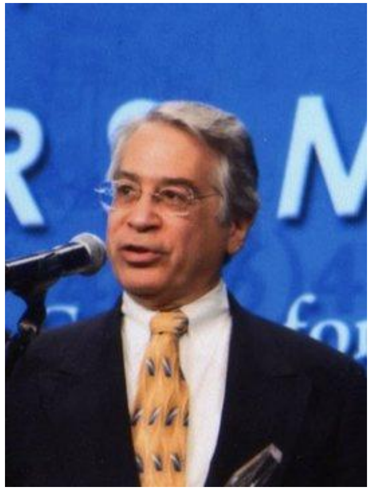
$$E/\mathbf{F}_p \colon y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,$
$36134250956749795798585127919587881956611106672985015071877198253568414405109)$

[a]$P = (84116208261315898167593067868200525612344221886333785331584793435449501658416,$
$102885655542185598026739250172885300109680266058548048621945393128043427650740)$

[b]$P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,$
$77887418190304022994116595034556257760807185615679689372138134363978498341594)$



$a =$
$89130644591246033577639770641462855023145028492835255603183721922317324614395$

[ab]$P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,$
$77887418190304022994116595034556257760807185615679689372138134363978498341594)$

$b =$
$10095557463932786418806938316190708032771910919058405391679781082193405190826$

Quantum computers ↔ Cryptopocalypse

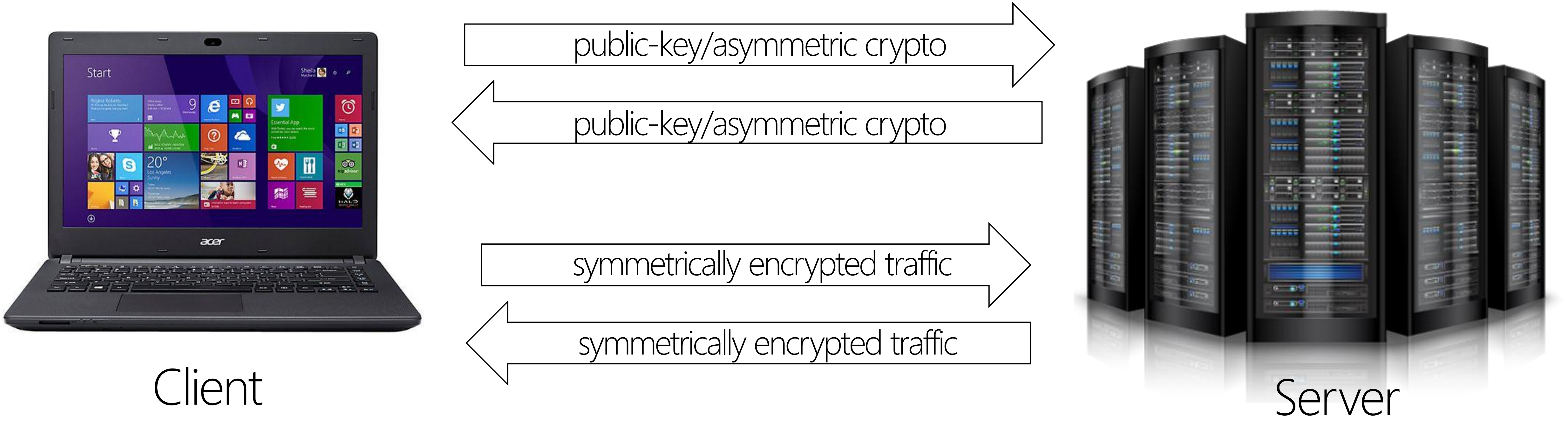
- Quantum computers break elliptic curves, finite fields, factoring, everything currently used for PKC
- Aug 2015: NSA announces plans to transition to quantum-resistant algorithms
- Feb 2016: NIST calls for quantum-secure submissions. Deadline Nov 30, 2017

Post-quantum key exchange

Which hard problem(s) to use now???

This talk: supersingular isogenies

Real-world (e.g., Internet/TLS) cryptography in one slide (oversimplified)



- Public-key cryptography used to

  ECC (1) establish a shared secret key (e.g., Diffie-Hellman key exchange)
  (2) authenticate one another (e.g., digital signatures)

- Symmetric key cryptography uses shared secret to encrypt/authenticate the subsequent traffic (e.g., block ciphers, AES/DES, stream ciphers, MACs)
- Hash functions used throughout (e.g., SHA's, Keccak)

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

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

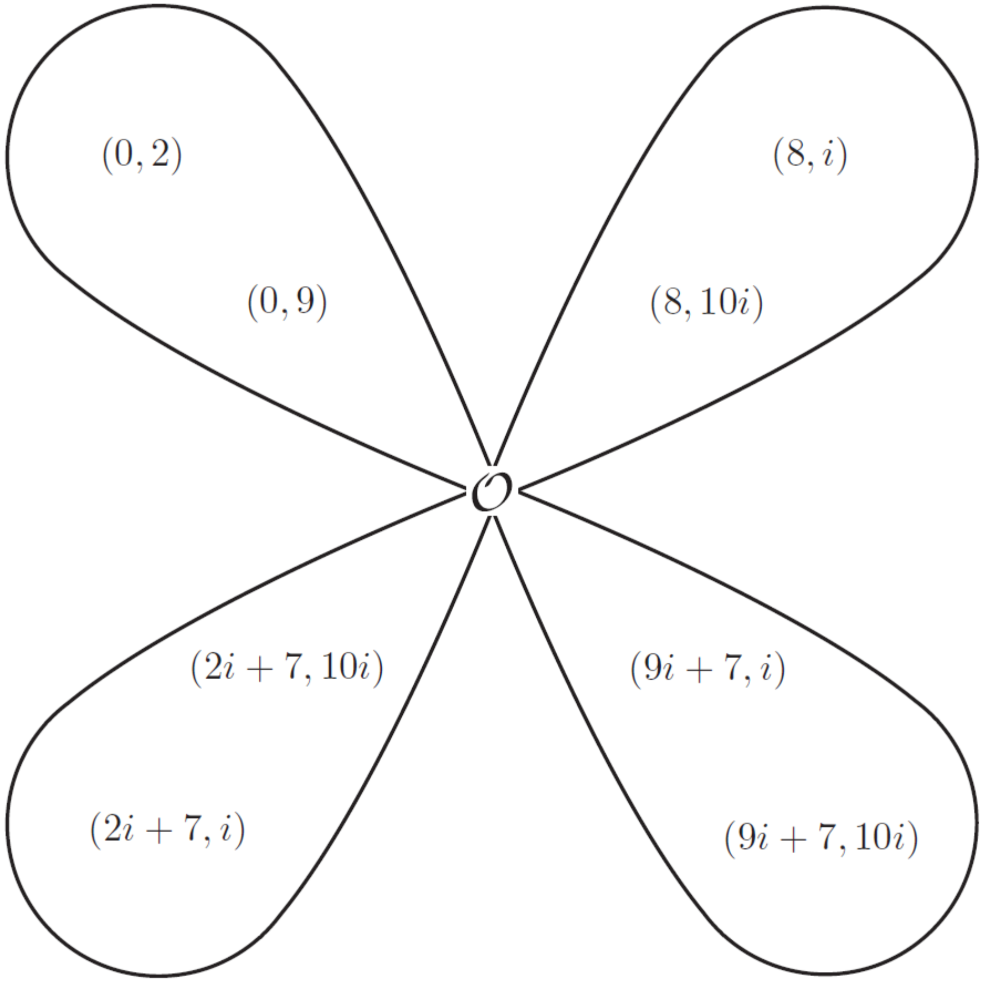
- Found as the roots of the n^{th} division polynomial ψ_n

- 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 $\boldsymbol{\phi} : \boldsymbol{E_1} \to \boldsymbol{E_2}$ (up to isomorphism) having kernel $\boldsymbol{G}$. Write $\boldsymbol{E_2} = \boldsymbol{\phi}(\boldsymbol{E_1}) = \boldsymbol{E_1}/\langle \boldsymbol{G} \rangle$.

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

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

- 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

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

And where ϕ maps (x, y) to

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

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

$$\boldsymbol{\phi} : \quad E \to E',$$

$$(x, y) \mapsto \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)} \right)$$

Example, cont.

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

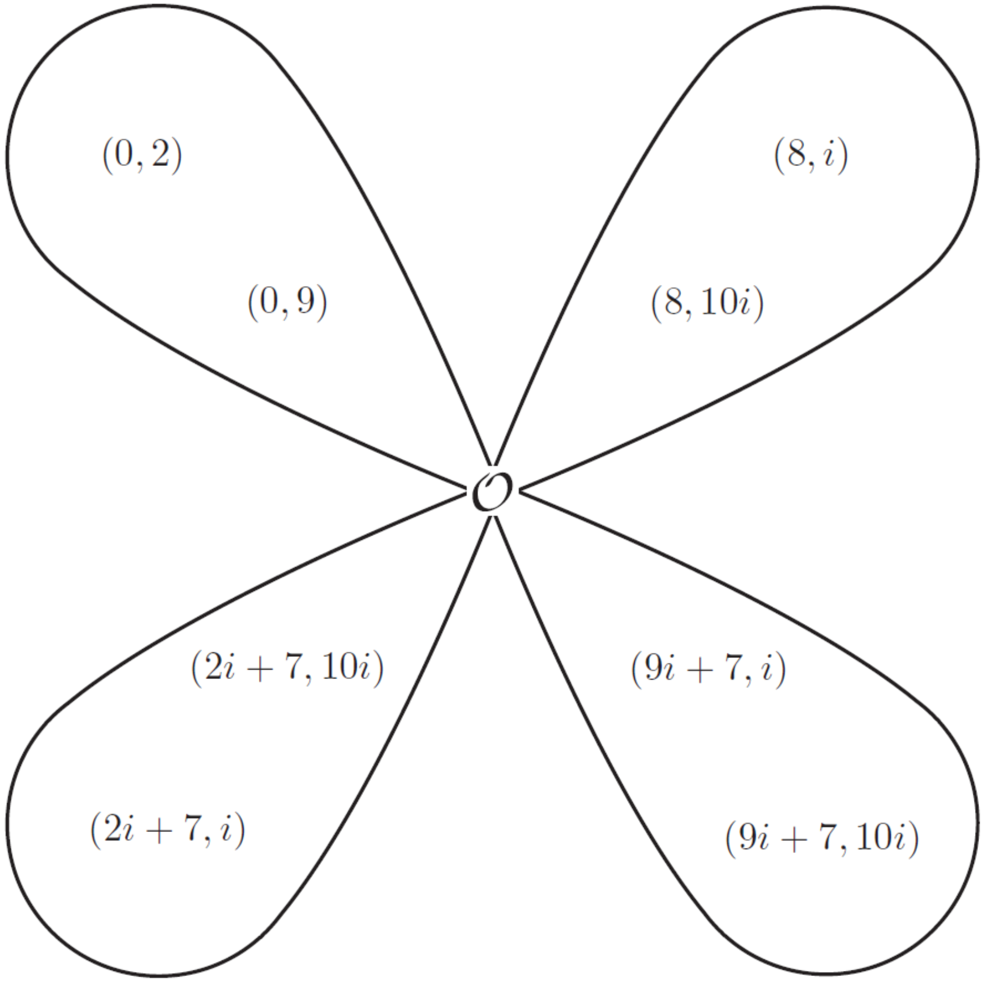
- Consider $[3] : E \to E$, the multiplication-by-3 endomorphism

- $G = \mathbf{ker}([3])$, 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?

$G = E[3]$



```
p:=11;
Fp:=GF(p);
Fp2<i>:=ExtensionField<Fp,x|x^2+1>;
_<x>:=PolynomialRing(Fp2);

//E:=EllipticCurve([Fp2|0,4]);
E:=EllipticCurve(x^3+4);
IsSupersingular(E);
true

ker1:=(x-0)*(x-0);
ker2:=(x-8)*(x-8);
ker3:=(x-(2*i+7))*(x-(2*i+7));
ker4:=(x-(9*i+7))*(x-(9*i+7));

E1,phi1:=IsogenyFromKernel(E,ker1);
E2,phi2:=IsogenyFromKernel(E,ker2);
E3,phi3:=IsogenyFromKernel(E,ker3);
E4,phi4:=IsogenyFromKernel(E,ker4);
```

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

```
E2;
Elliptic Curve defined by y^2 = x^3 + 5*x over GF(11^2)
```

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

```
phi2;
Elliptic curve isogeny from: CrvEll: E to CrvEll: E2
taking (x : y : 1) to ((x^3 + 6*x^2 + 8*x + 4) / (x^2 + 6*x + 9) :
(x^3*y + 9*x^2*y + 6*x*y + 5*y) / (x^3 + 9*x^2 + 5*x + 5) : 1)
```

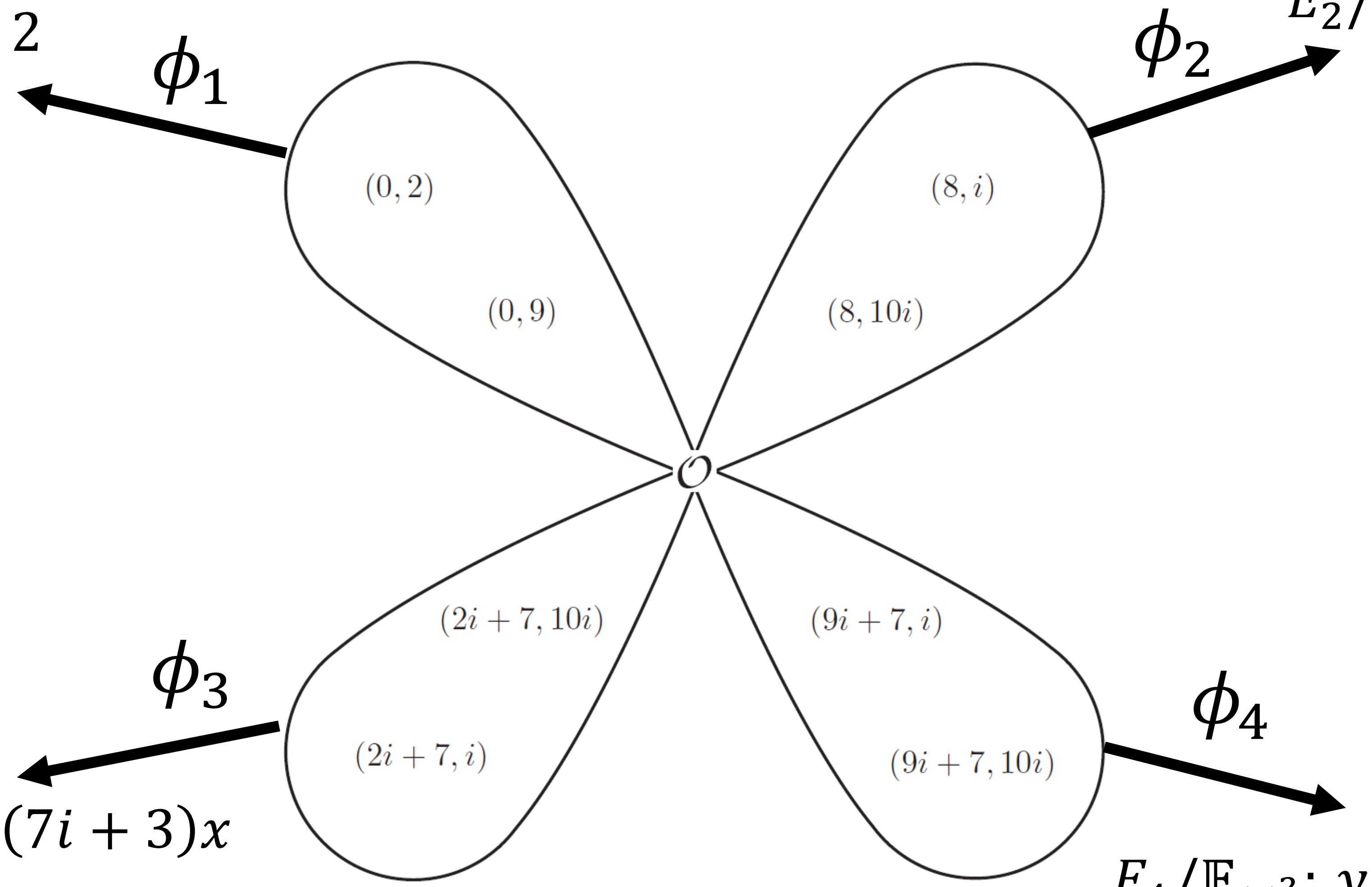
$$\phi_2 : E \to E_2,$$

$$(x, y) \mapsto \left(\frac{x^3 + 6x^2 + 8x + 4}{x^2 + 6x + 9}, y \cdot \frac{x^3 + 9x^2 + 6x + 5}{x^3 + 9x^2 + 5x + 5} \right)$$

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

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

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



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

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

E_1, E_2, E_3, E_4 all 3-isogenous to E, but what's the relation to each other?

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: $q + 1 - 2\sqrt{q} \leq \#E\left(\mathbb{F}_q\right) \leq q + 1 + 2\sqrt{q}$ (Hasse)

Upshot for fixed q

$O\left(\sqrt{q}\right)$ 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 $(\boldsymbol{\ell} + 1)$ directed regular graph $X(S_{p^2}, \ell)$

E.g. a supersingular isogeny graph

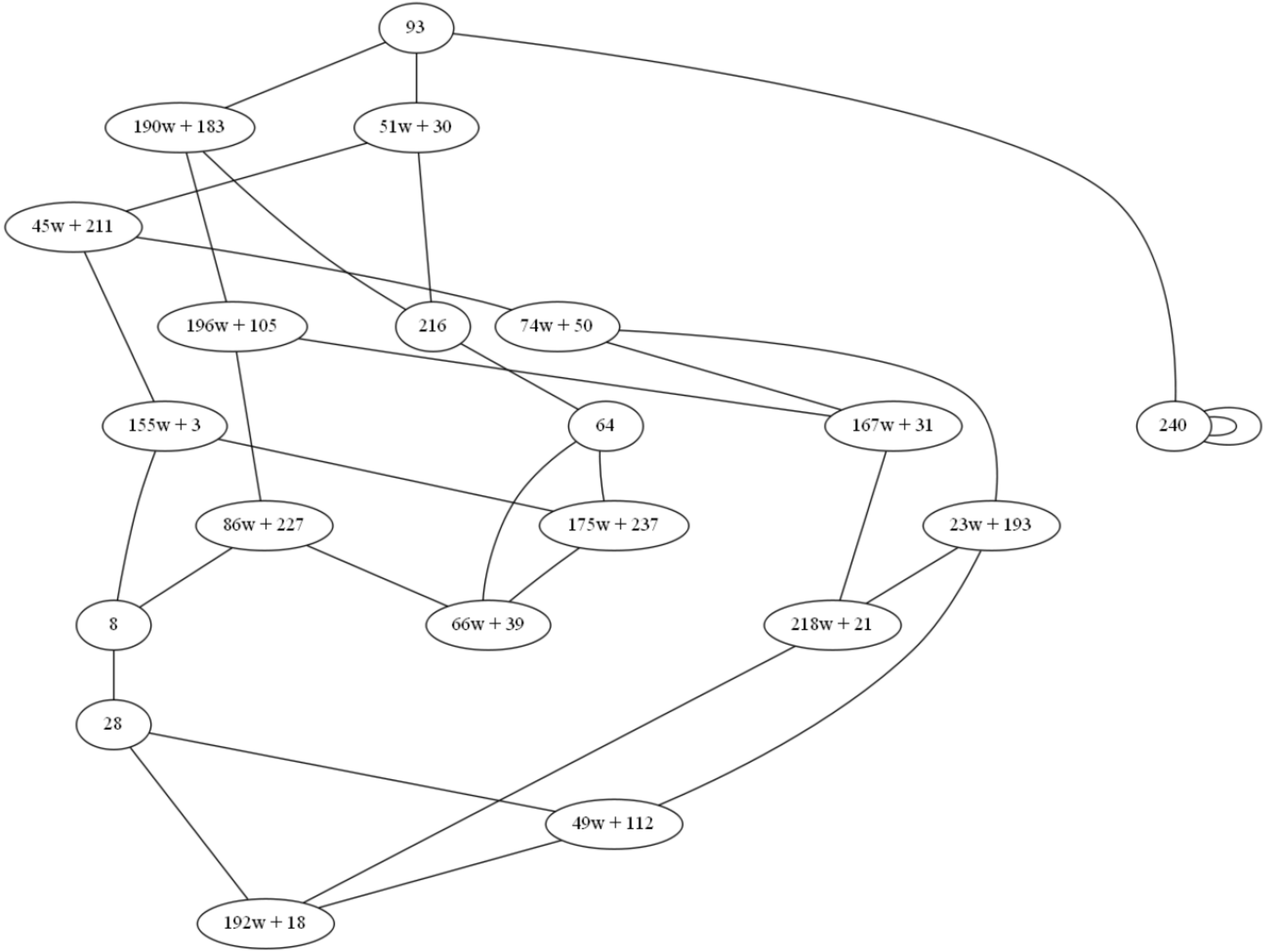
- Let $p = 241$, $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 - 3x + 7)$

- $\#S_{p^2} = 20$

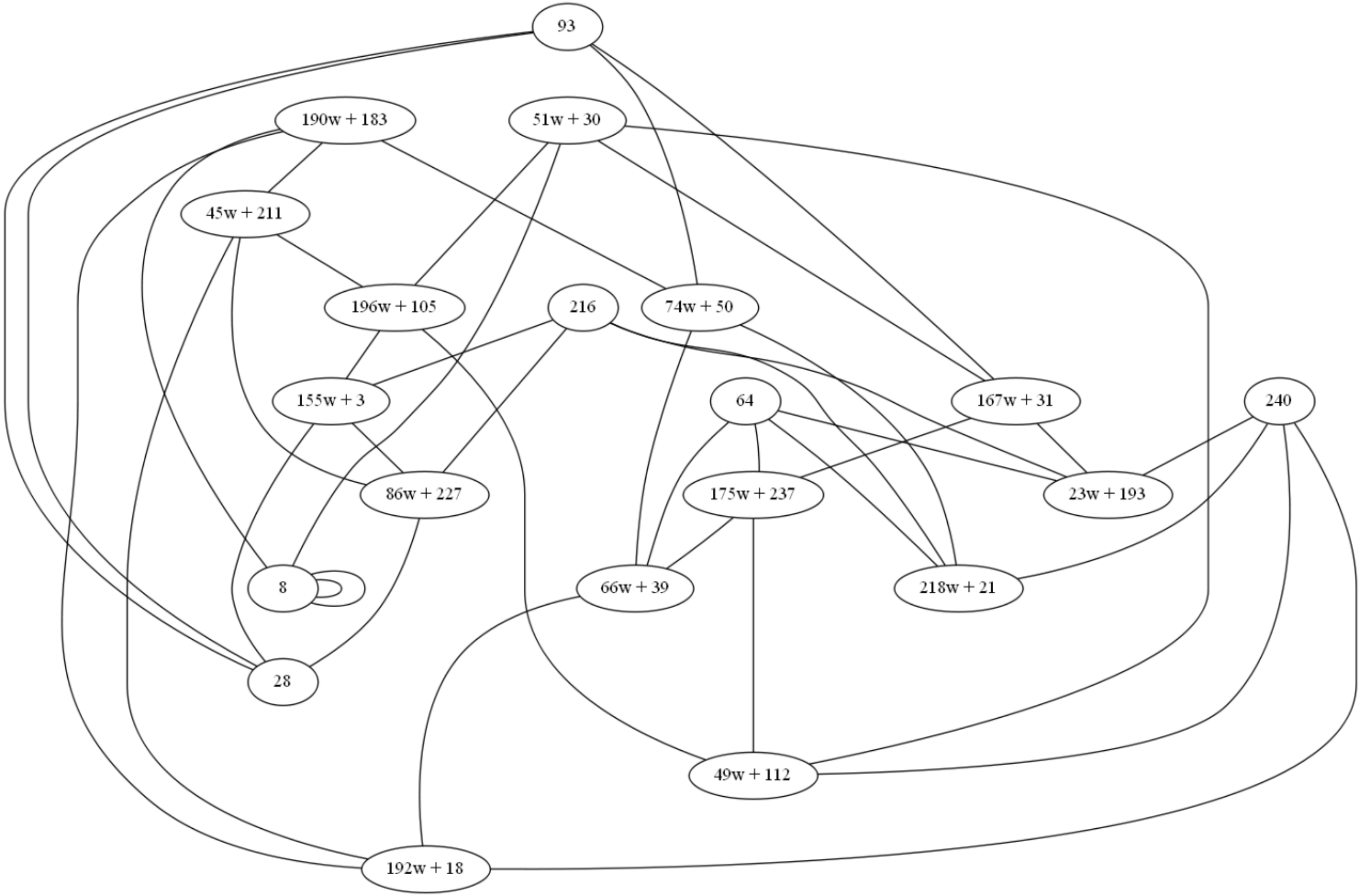
- $S_{p^2} = \{93,\ 51w + 30,\ 190w + 183,\ 240,\ 216,\ 45w + 211,\ 196w + 105,\ 64,\ 155w + 3,\ 74w + 50,\ 86w + 227,\ 167w + 31,\ 175w + 237,\ 66w + 39,\ 8,\ 23w + 193,\ 218w + 21,\ 28,\ 49w + 112,\ 192w + 18\}$

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 S be any subset of the vertices of the graph G, and x be any vertex in G. A "long enough" random walk will land in S with probability at least $\frac{|S|}{2|G|}$.

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

Part 1: Motivation

Part 2: Preliminaries

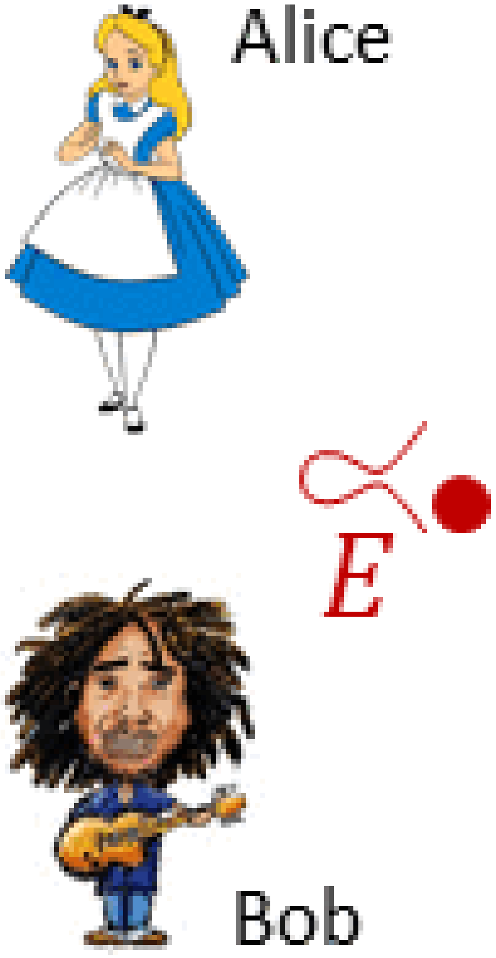
Part 3: SIDH

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 fix by choosing supersingular curves

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

$$
\begin{tikzcd}
 & E_0 \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A = E_0/\langle A \rangle \arrow[d, "\phi'_B"] \\
E_0/\langle B \rangle = E_B \arrow[r, phantom] & {} & {} \\
\end{tikzcd}
$$

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A = E_0/\langle A \rangle \arrow[d, "\phi'_B"] \\
E_0/\langle B \rangle = E_B \arrow[r, "{\phi_A}'"] & E_{AB} = E_0/\langle A, B \rangle
\end{tikzcd}
$$

SIDH: in a nutshell

params public private

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

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A = E_0/\langle P_A + [s_A]Q_A \rangle \arrow[d, "\phi_B'"'] \\
E_0/\langle P_B + [s_B]Q_B \rangle = E_B \arrow[r, "\phi_A{}'"] & E_{AB} = E_0/\langle A, B \rangle
\end{tikzcd}
$$

$$(R_A, S_A) = (\phi_A(P_B), \phi_A(Q_B))$$

$$(\phi_B(P_A), \phi_B(Q_A)) = (R_B, S_B)$$

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

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

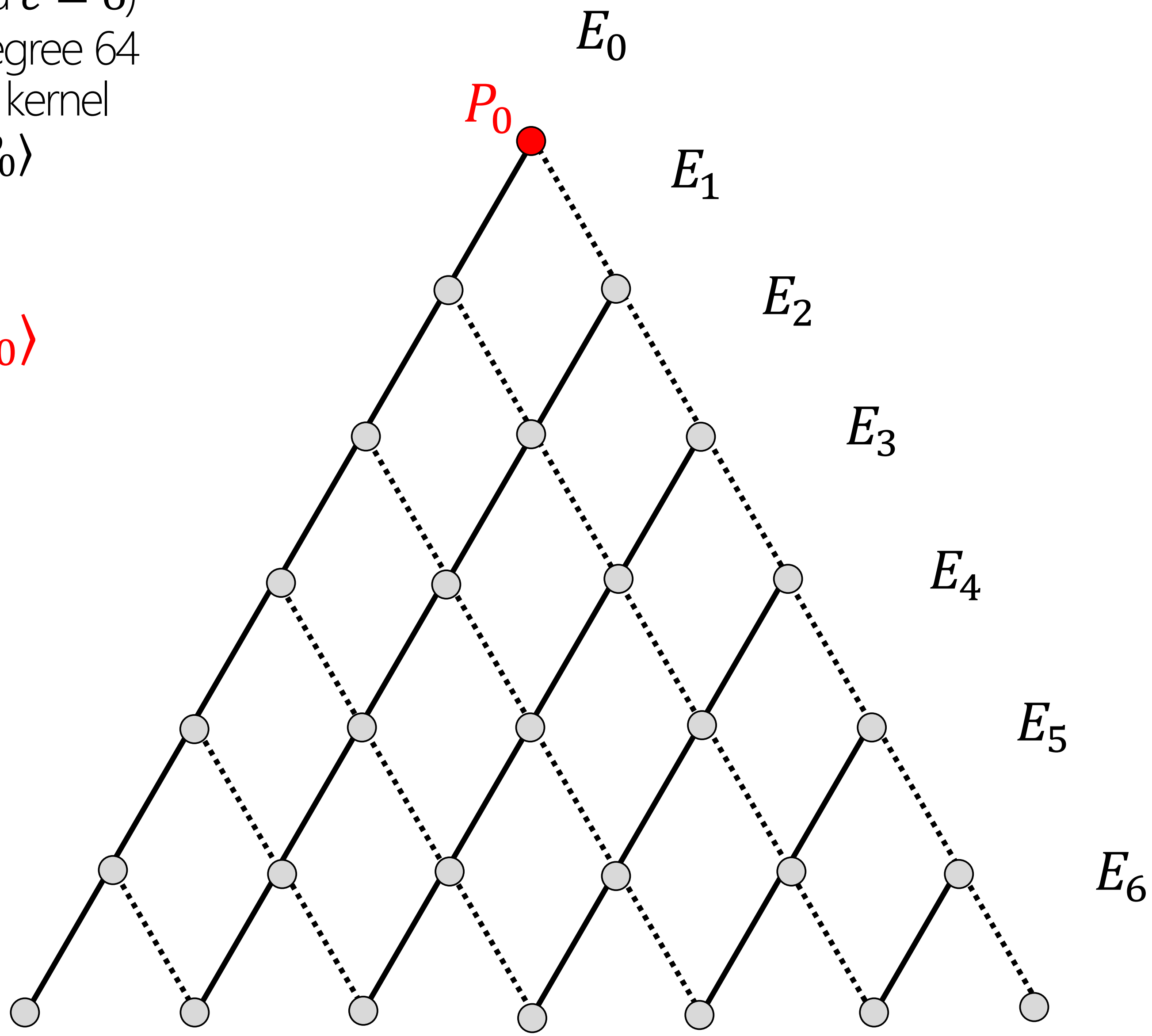
Exploiting smooth degree isogenies

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

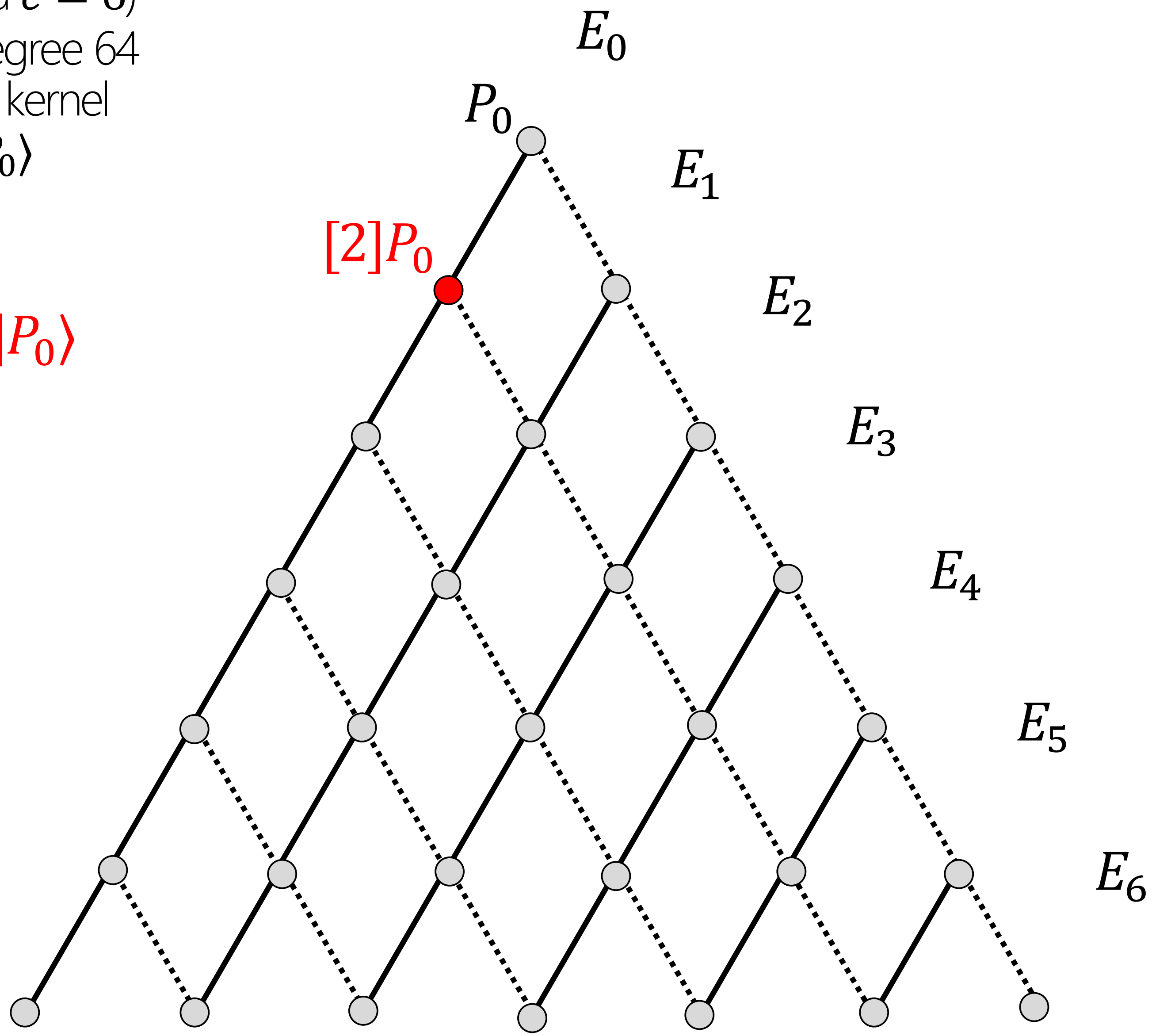
$E_6 = E_0/\langle P_0 \rangle$



Computing ℓ^e degree isogenies

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

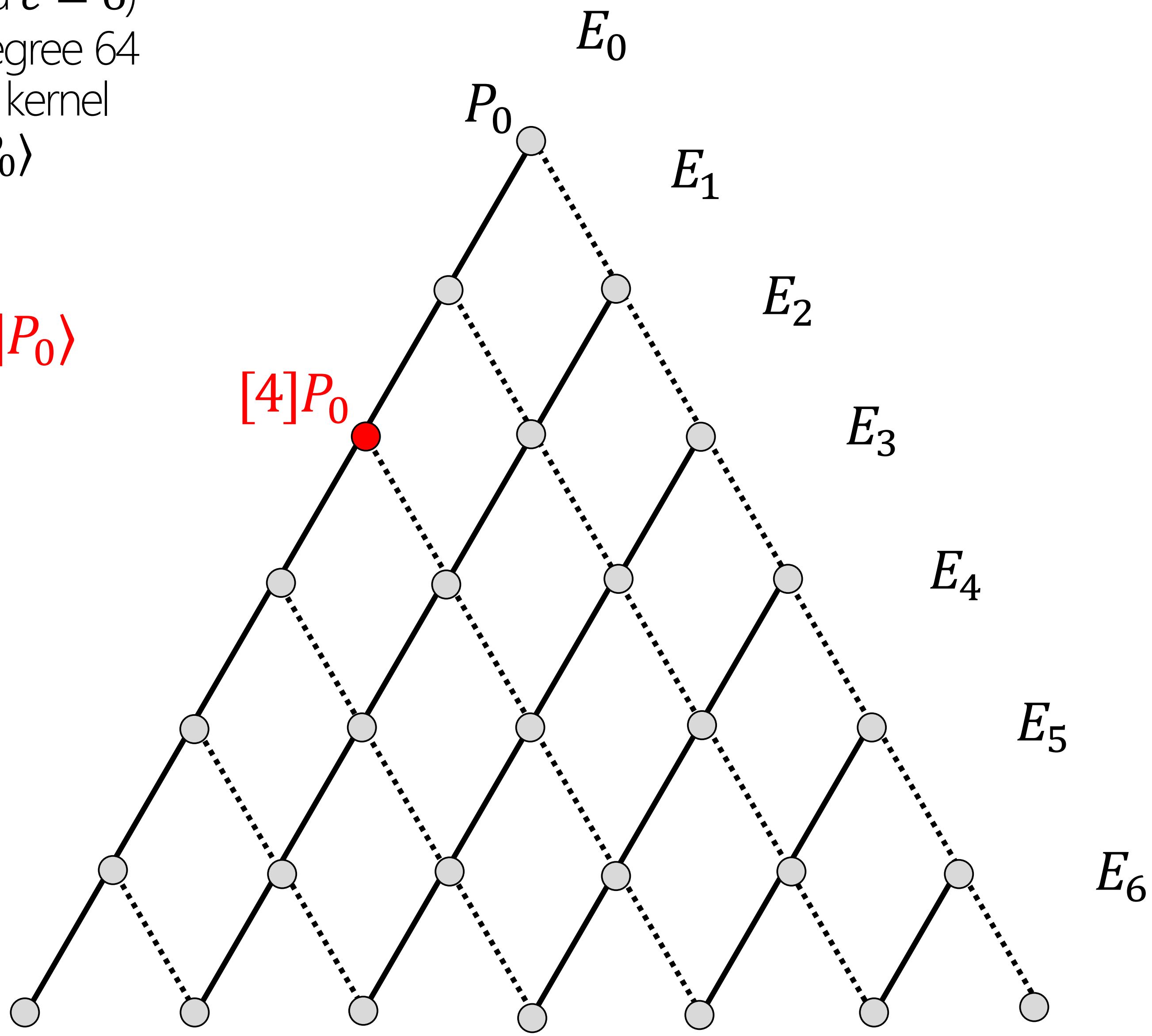
$E_5 = E_0 / \langle [2]P_0 \rangle$



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

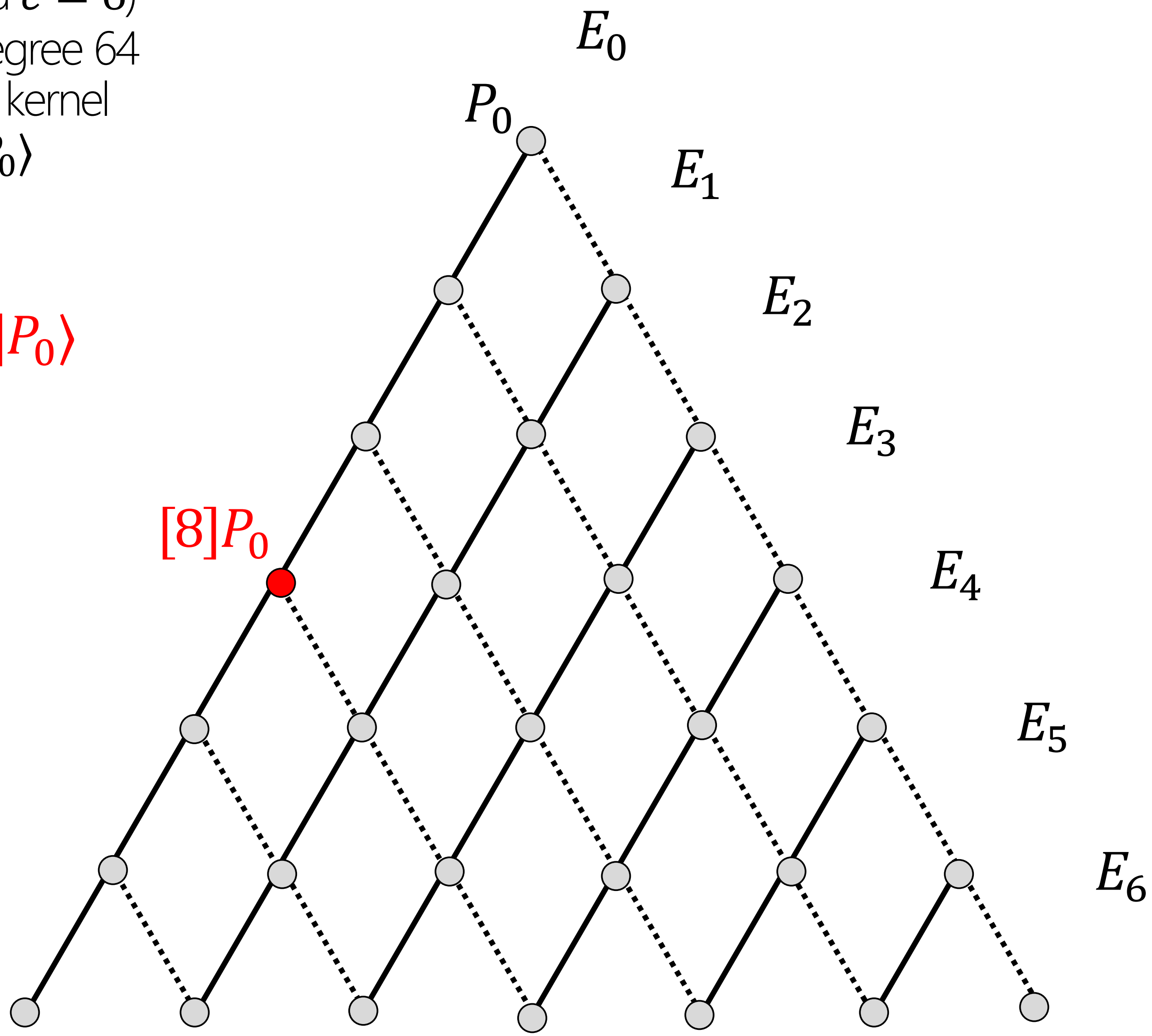
$E_4 = E_0/\langle [4]P_0 \rangle$



Computing ℓ^e degree isogenies

(suppose $\ell = 2$ and $e = 6$)
$\phi : E_0 \to E_6$ 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

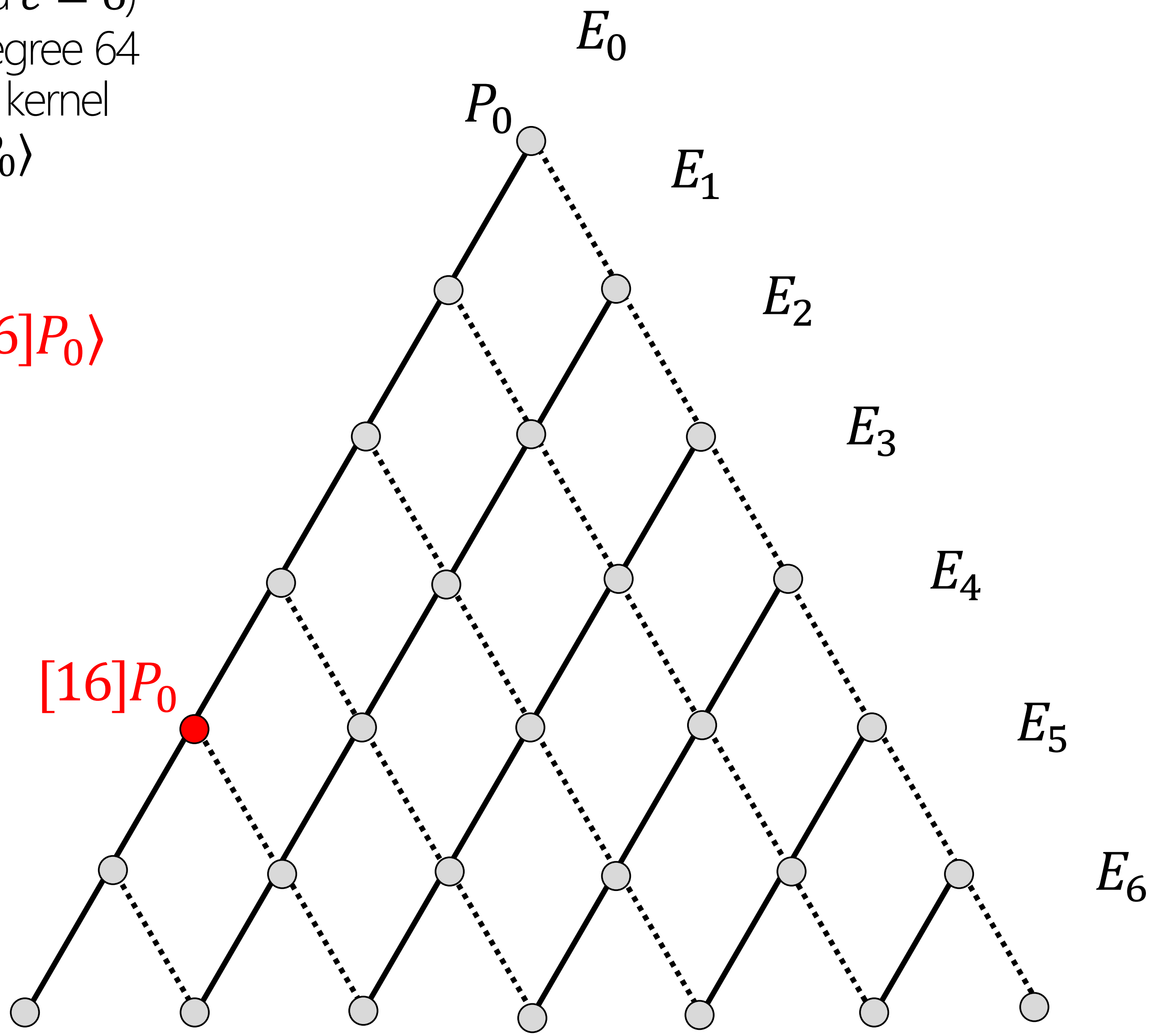
(suppose $\ell = 2$ and $e = 6$)

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

64 elements in its kernel

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

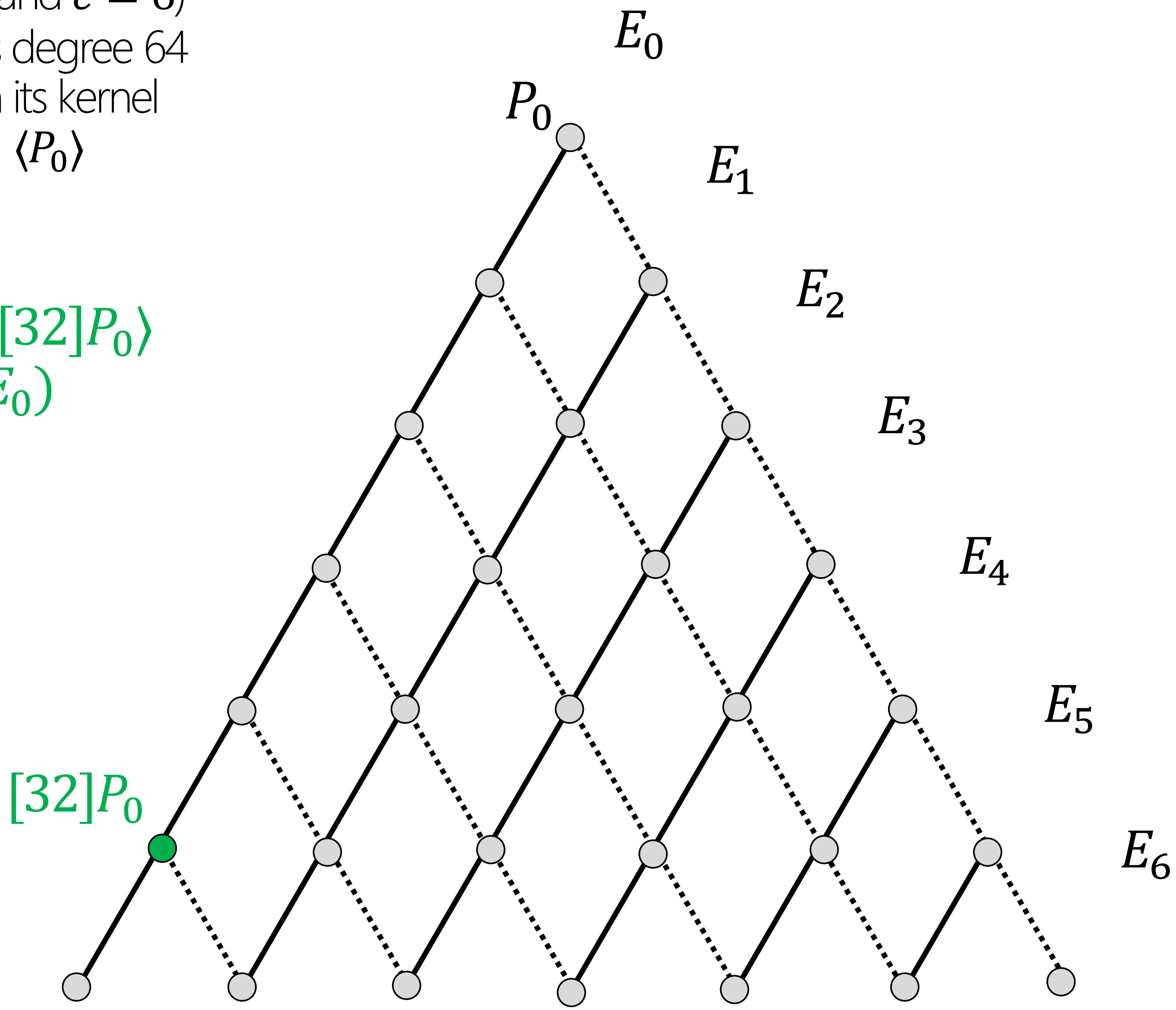
$E_2 = E_0 / \langle [16]P_0 \rangle$



Computing ℓ^e degree isogenies

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

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

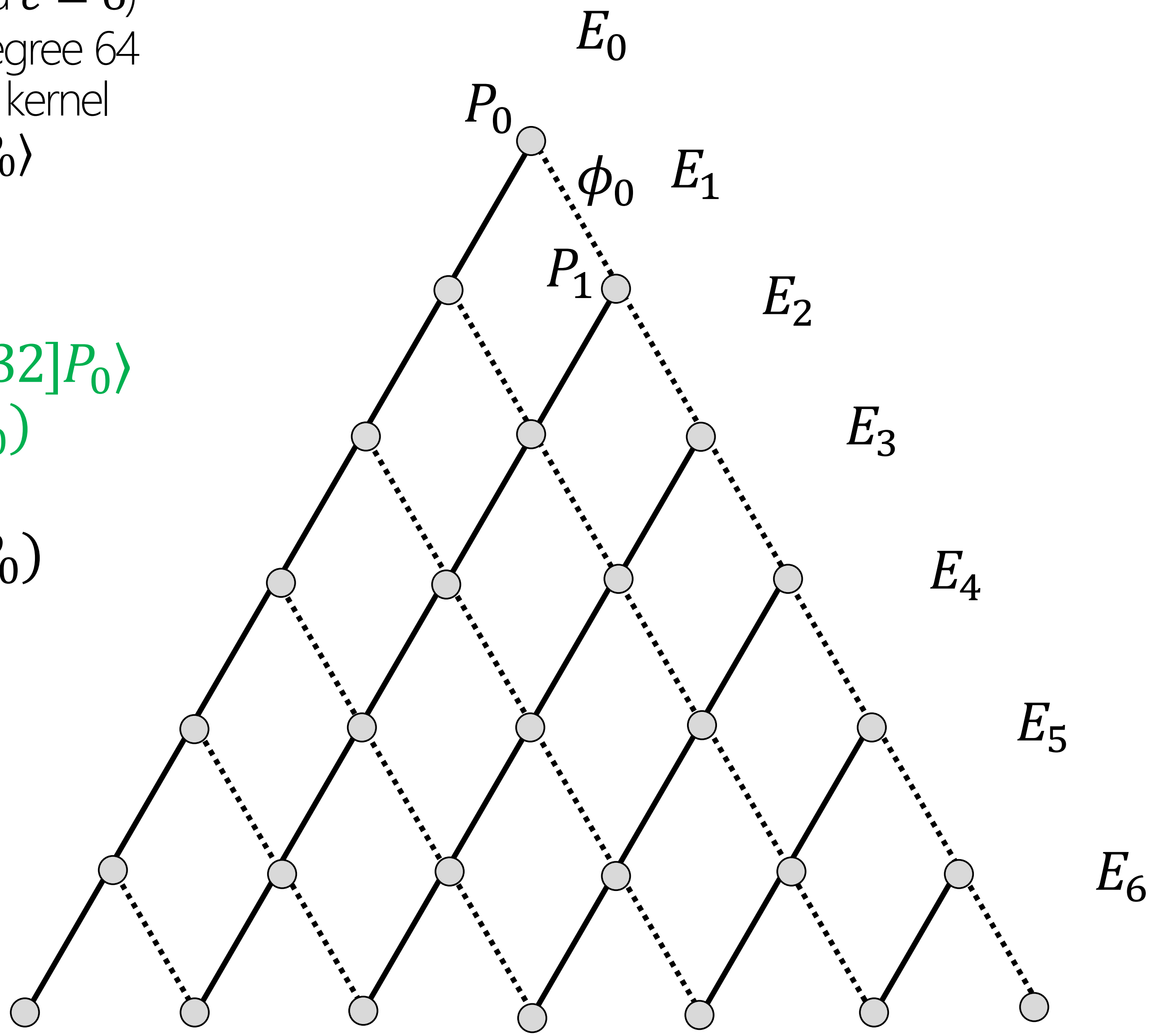


Computing ℓ^e degree isogenies

(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

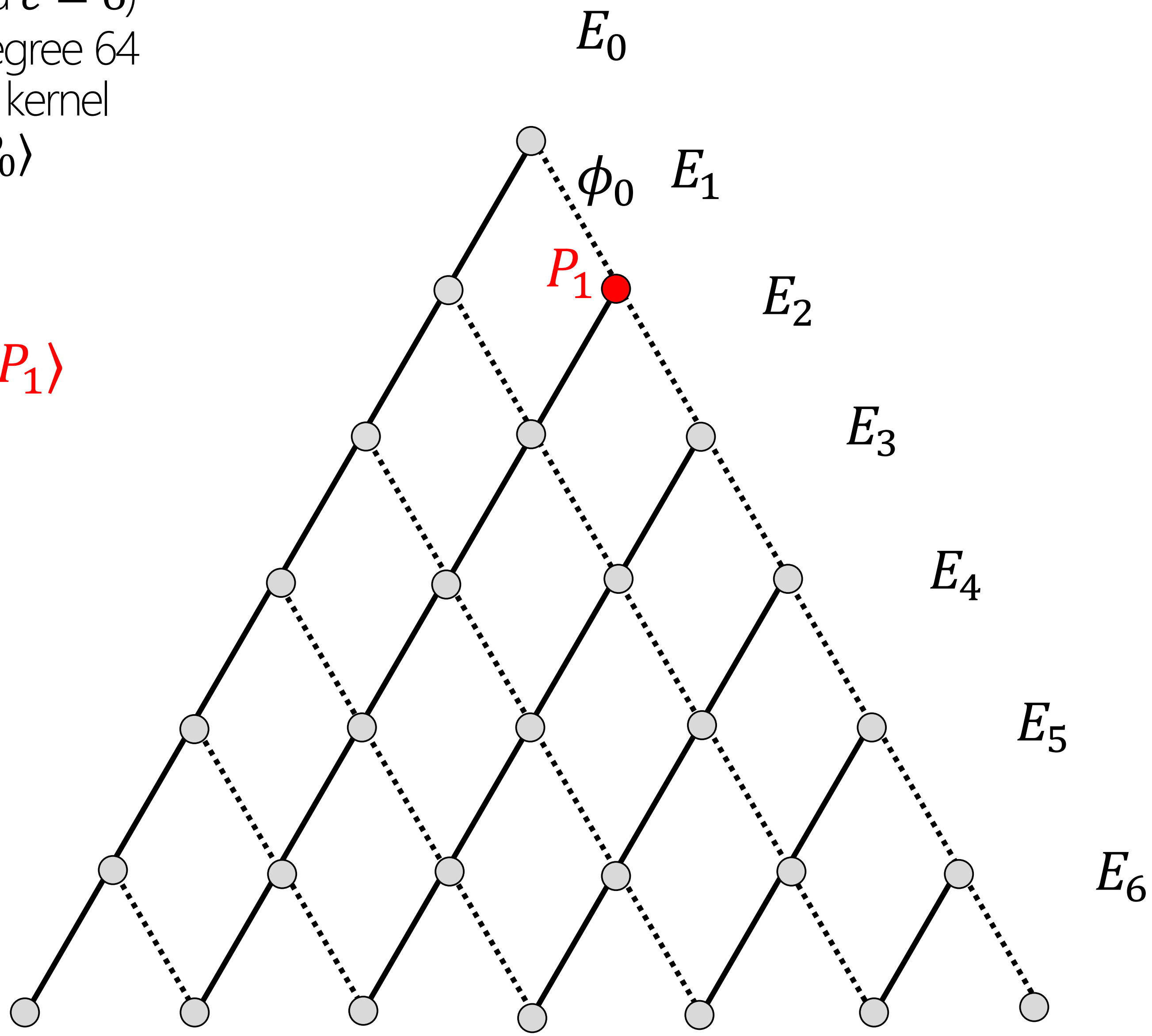
(suppose $\ell = 2$ and $e = 6$)

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

64 elements in its kernel

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

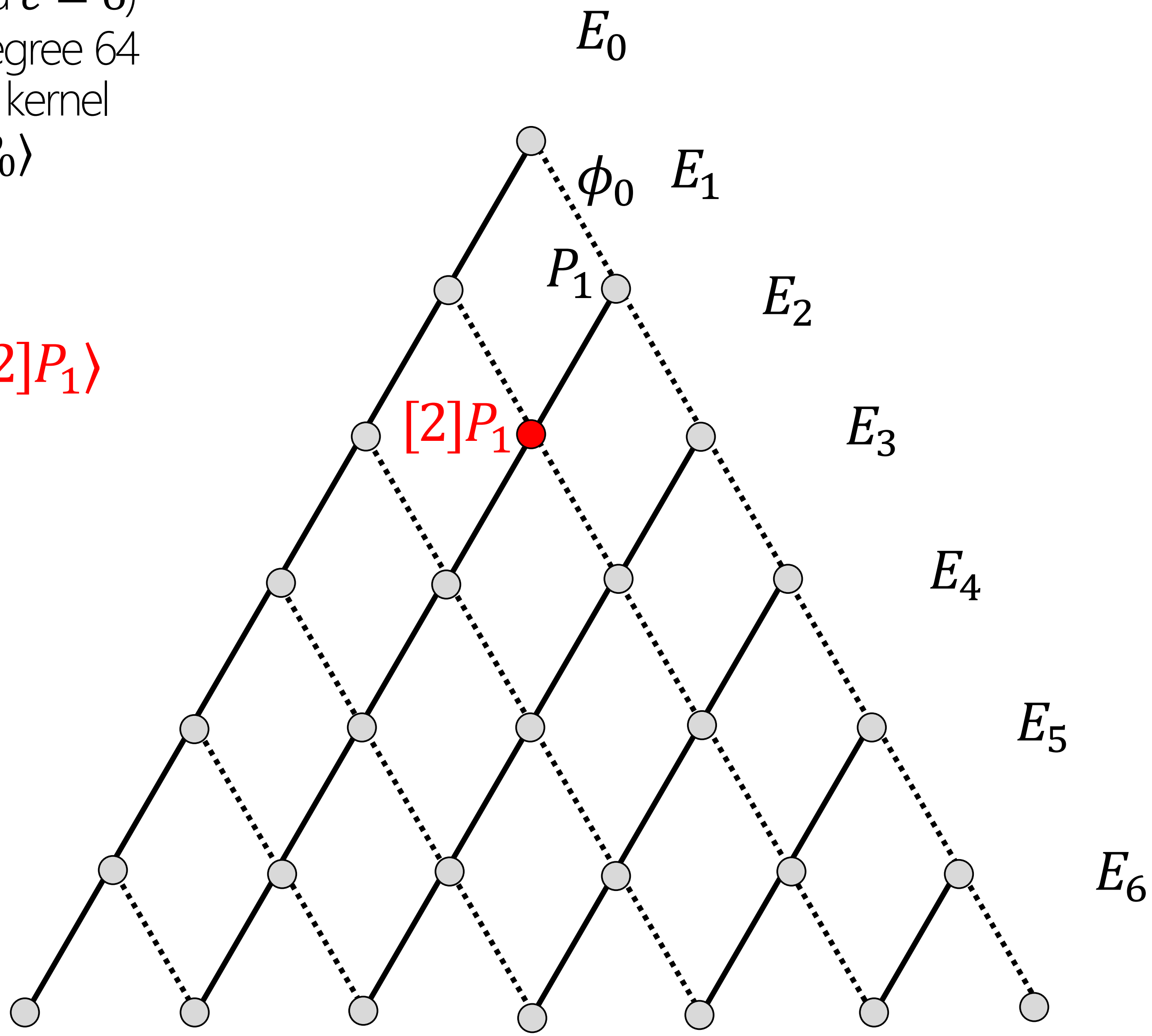
$E_6 = E_1 / \langle P_1 \rangle$



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

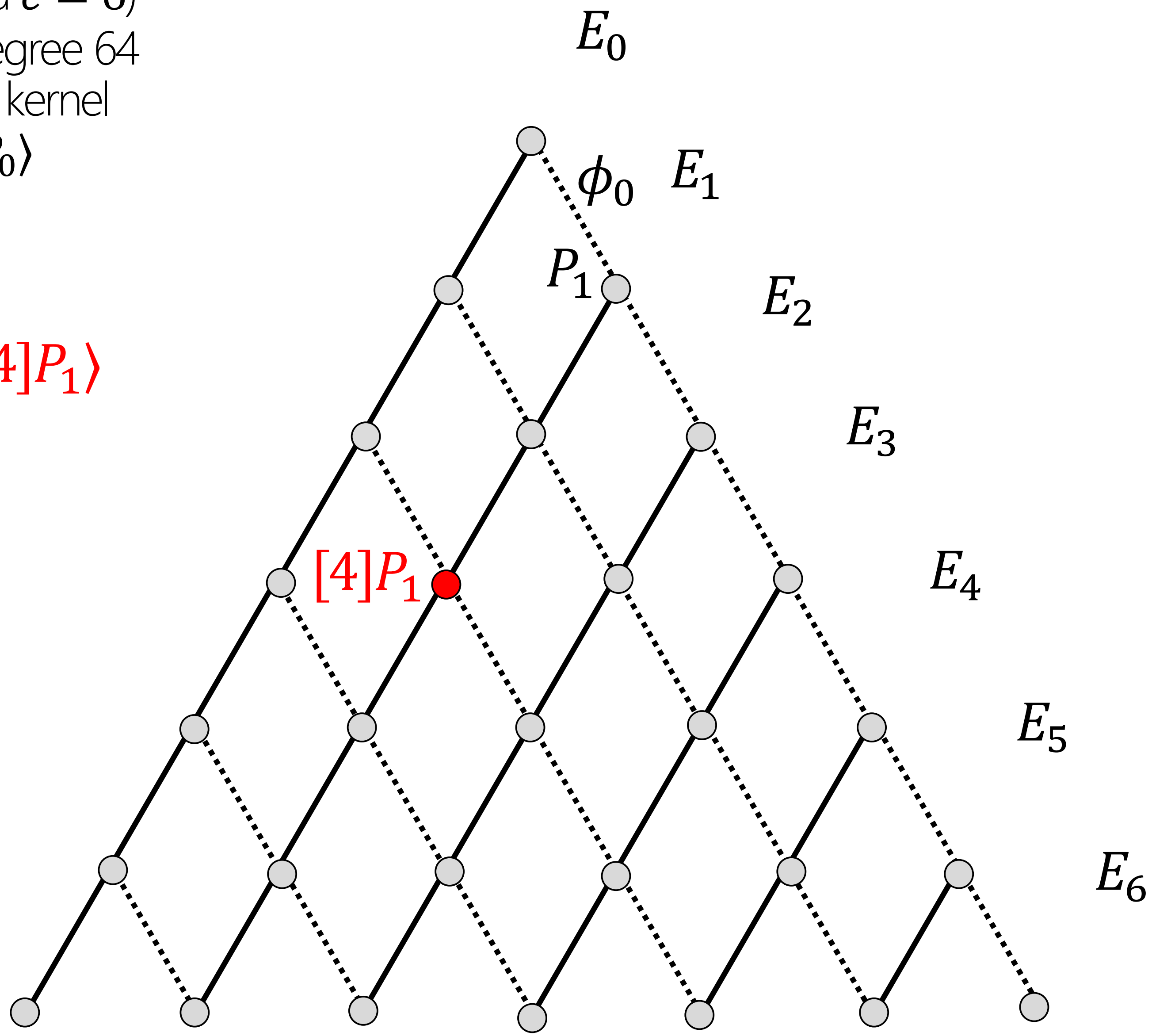
$E_5 = E_1 / \langle [2]P_1 \rangle$



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

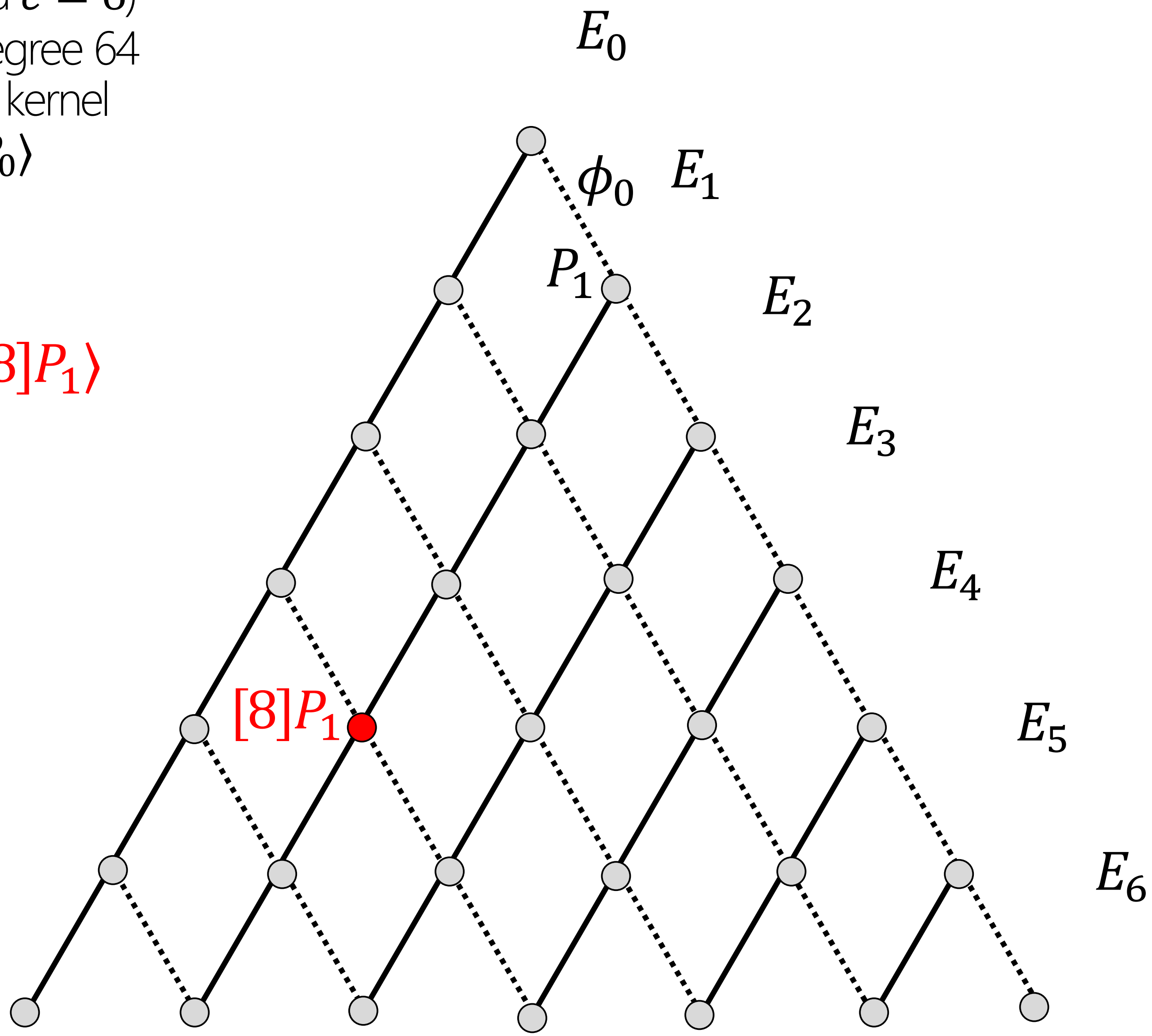
$E_4 = E_1 / \langle [4]P_1 \rangle$



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

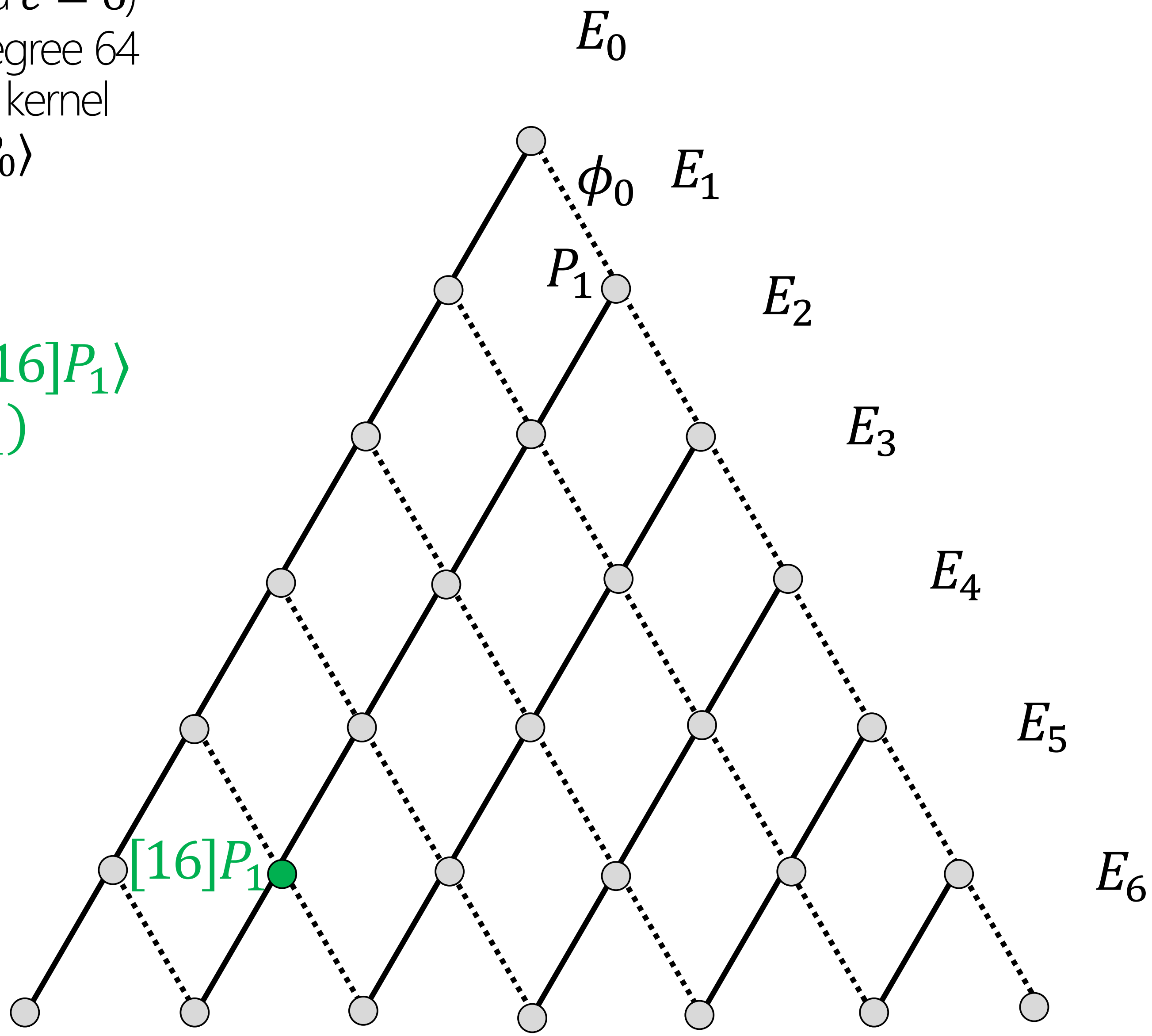
$E_3 = E_1 / \langle [8]P_1 \rangle$



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

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

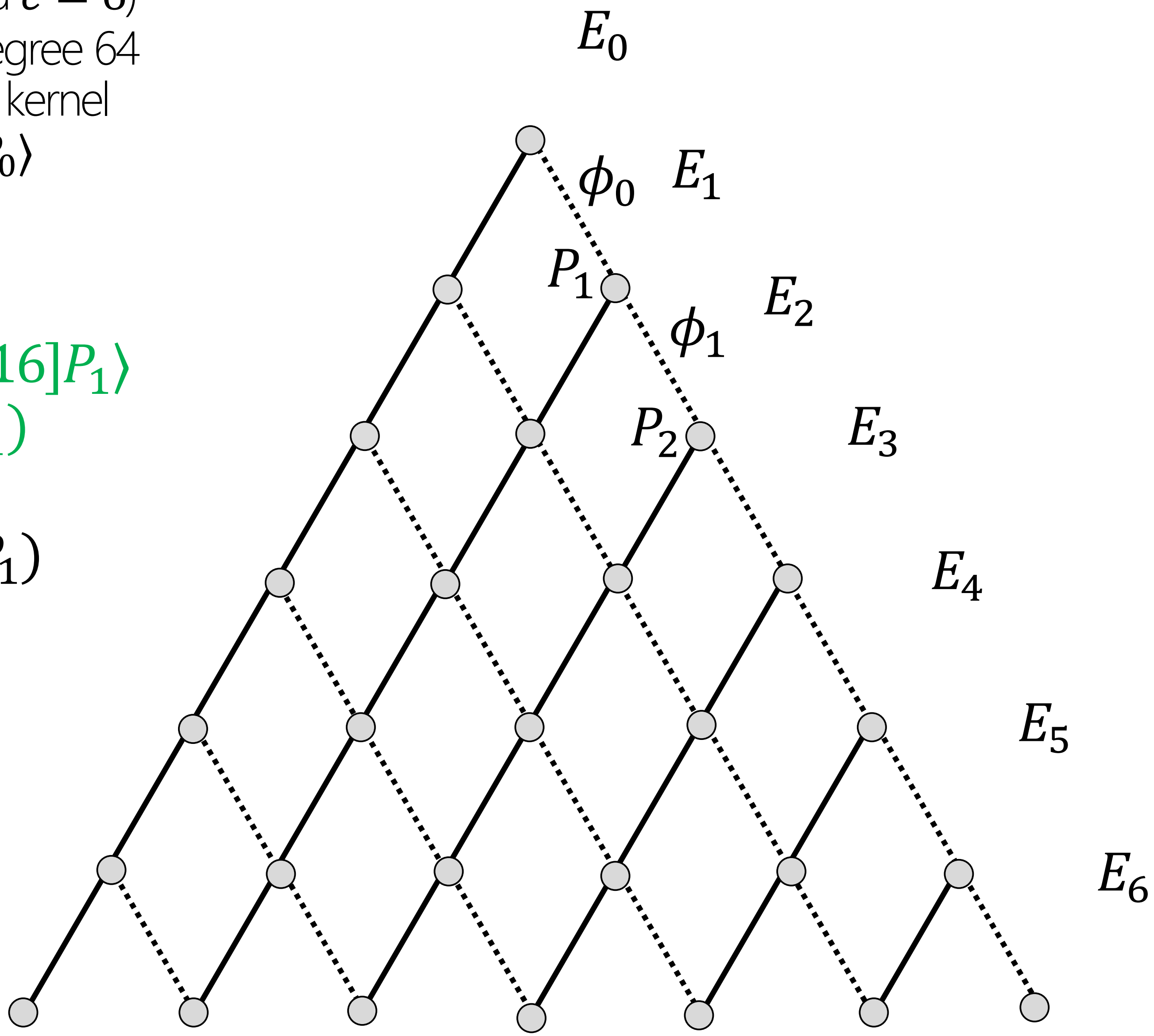


Computing ℓ^e degree isogenies

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

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

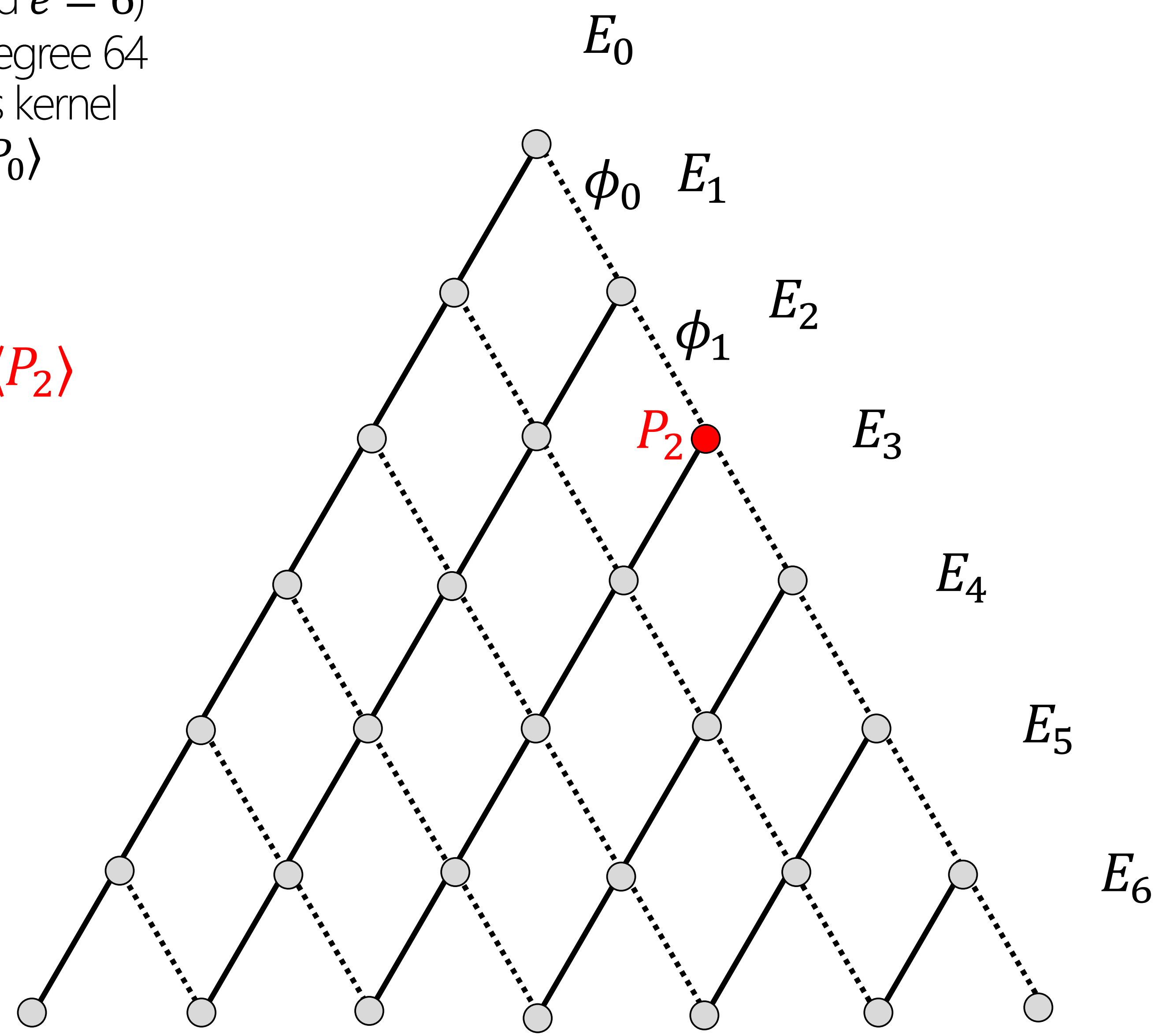
$$P_2 = \phi_1(P_1)$$



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

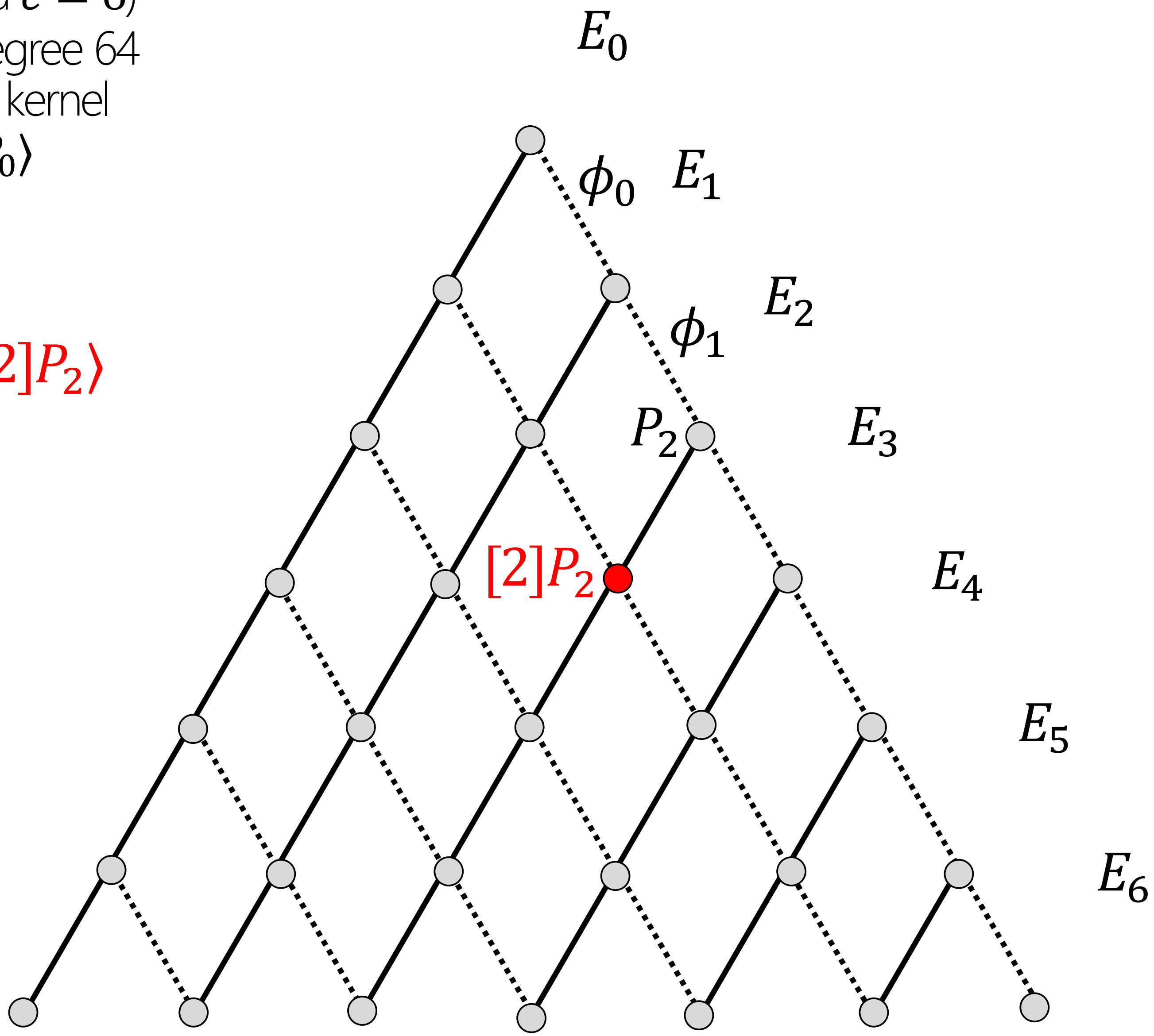
$E_6 = E_2 / \langle P_2 \rangle$



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

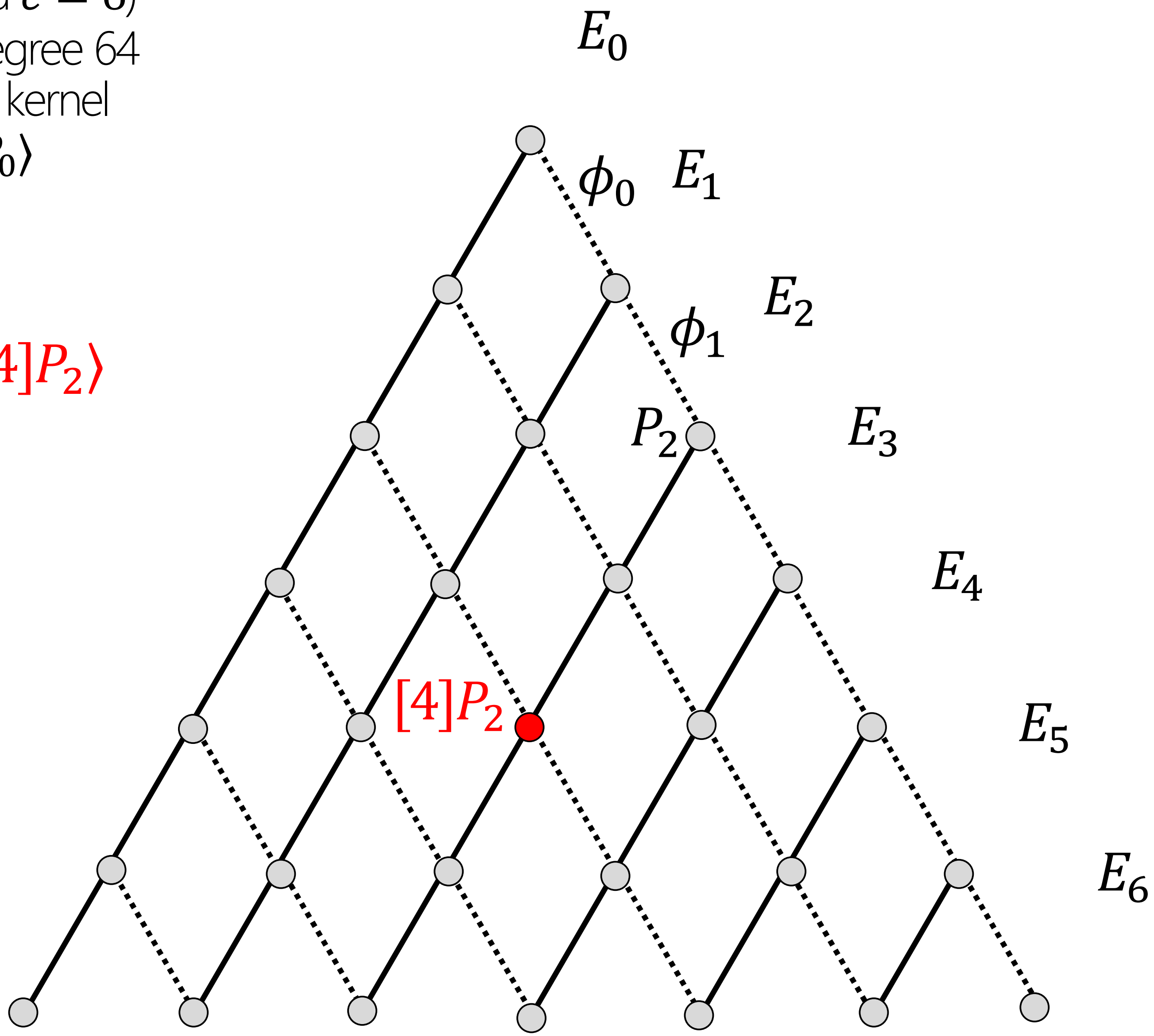
$E_5 = E_2 / \langle [2] P_2 \rangle$



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

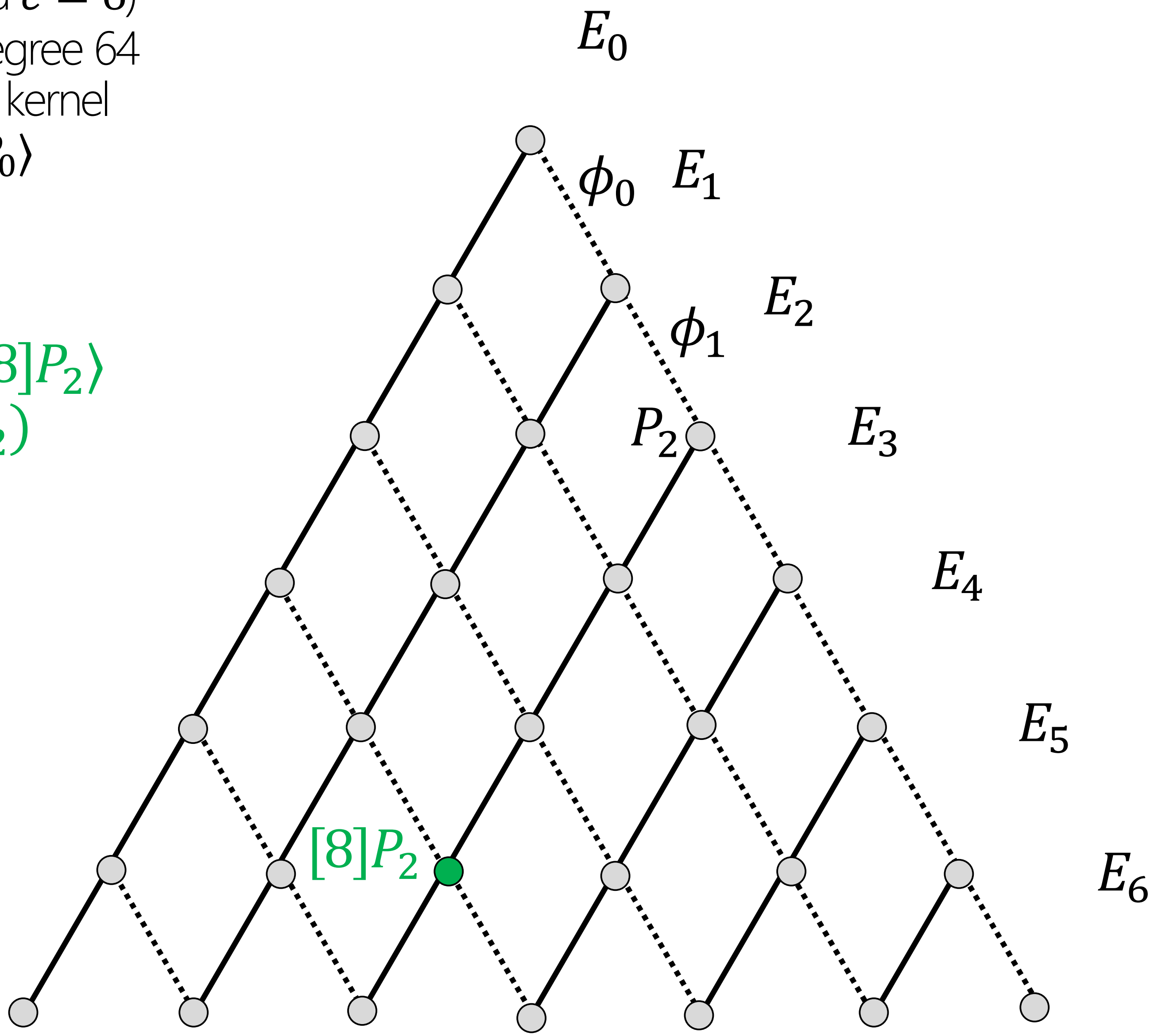
$E_4 = E_2/\langle [4]P_2 \rangle$



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 $e = 6$)

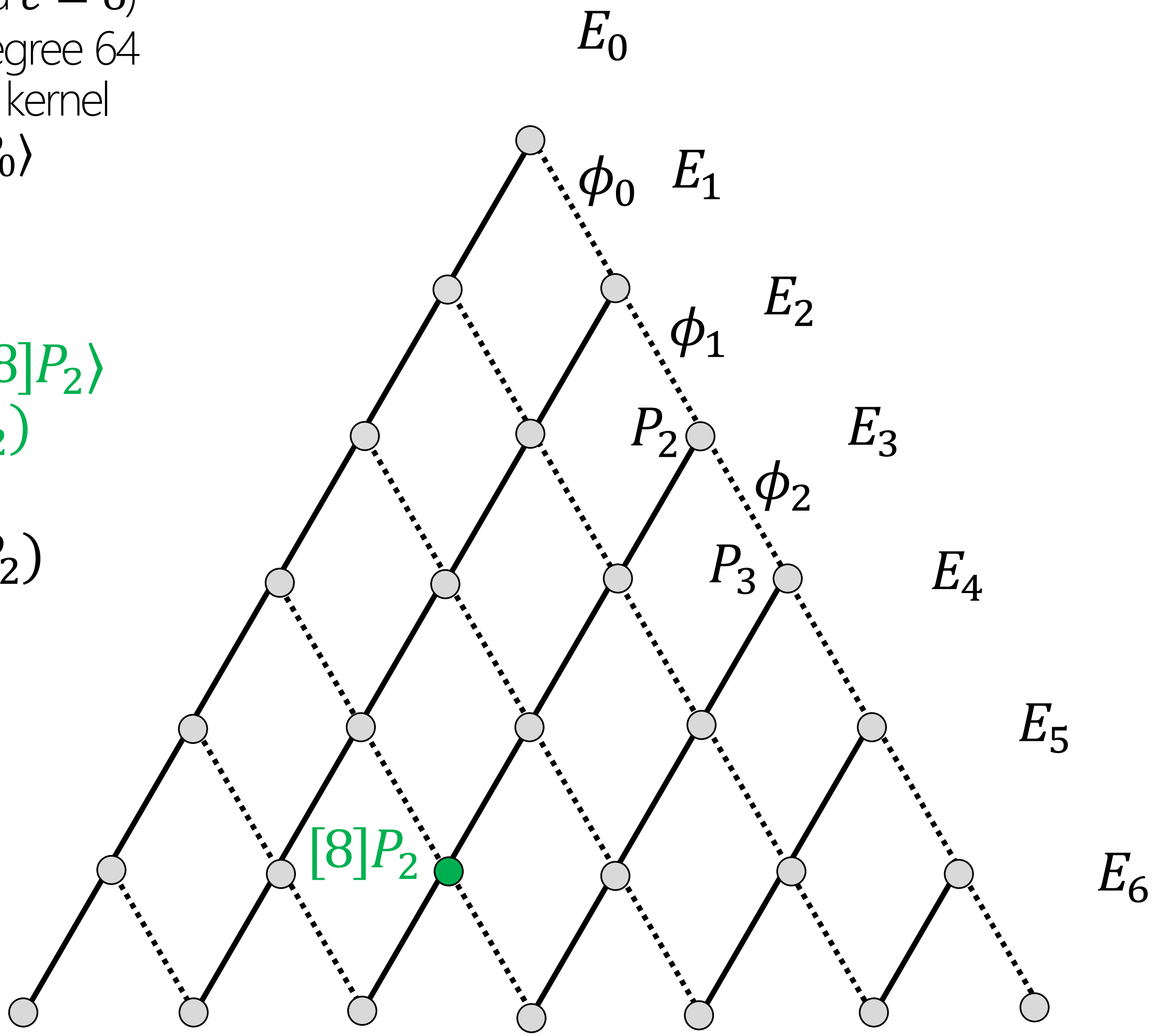
$\phi: \ E_0 \to E_6$ is degree 64

64 elements in its kernel

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

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

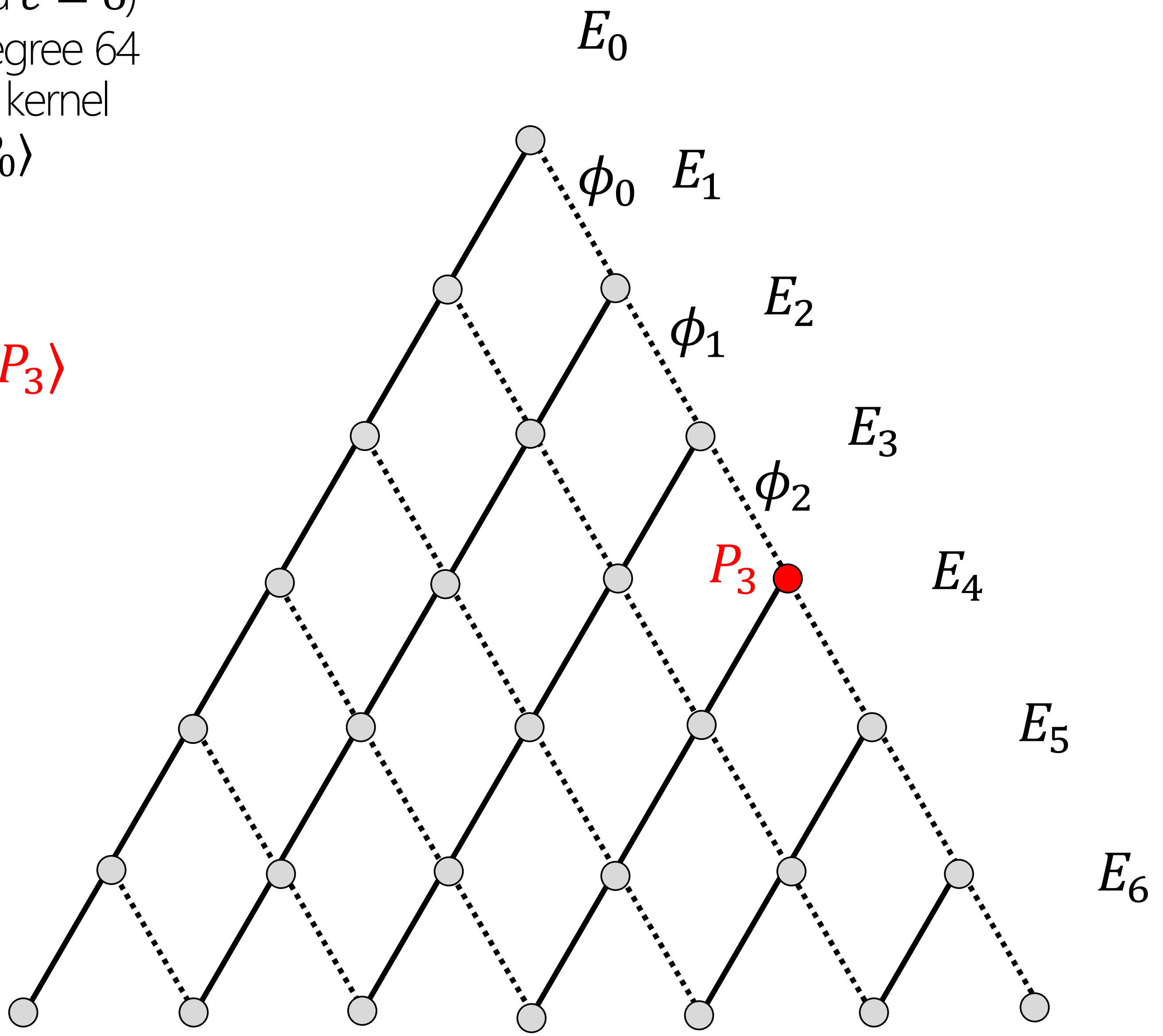
$$P_3 = \phi_2(P_2)$$



Computing ℓ^e degree isogenies

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

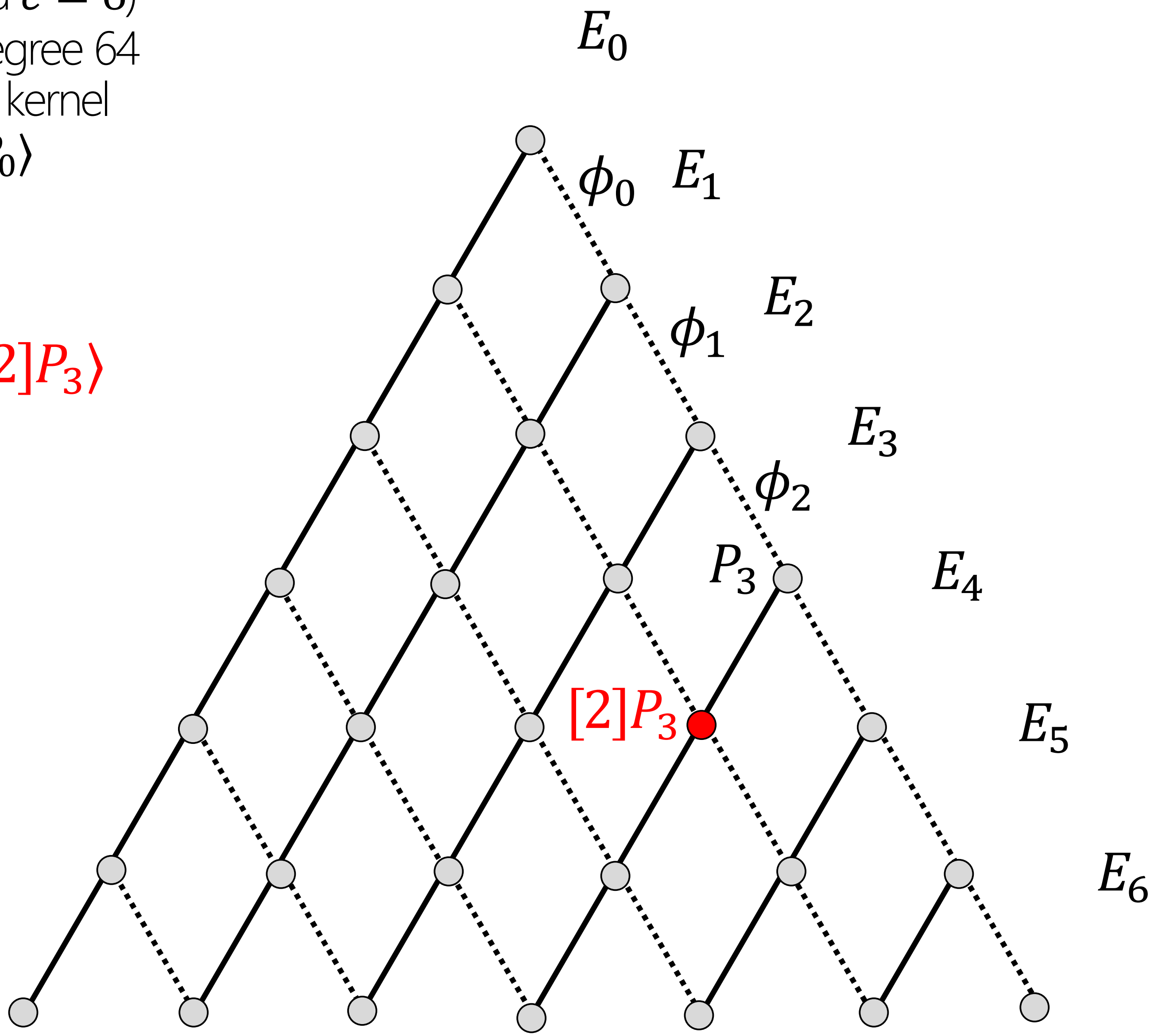
$E_6 = E_3 / \langle P_3 \rangle$



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

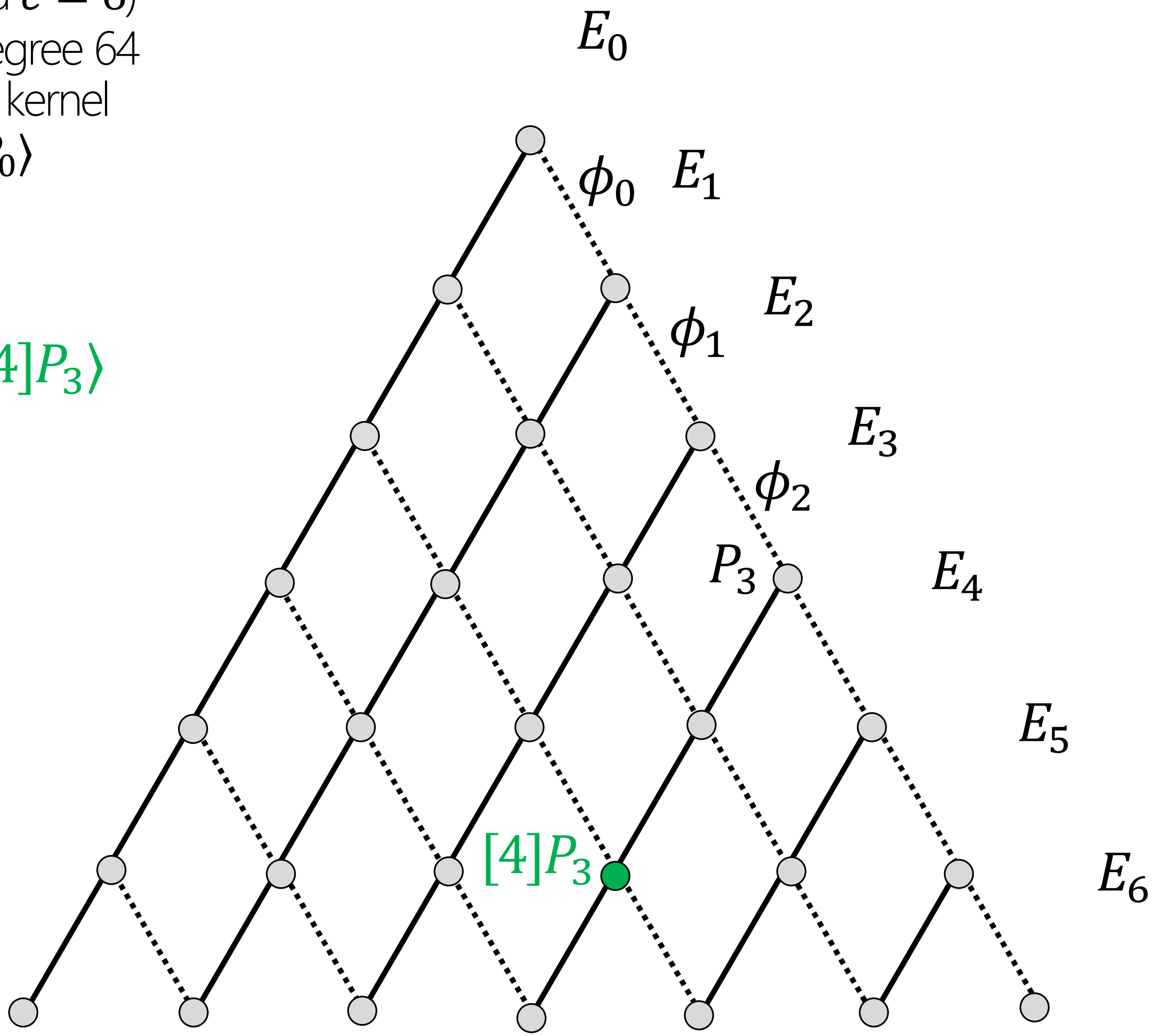
$E_5 = E_3/\langle [2]P_3 \rangle$



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

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

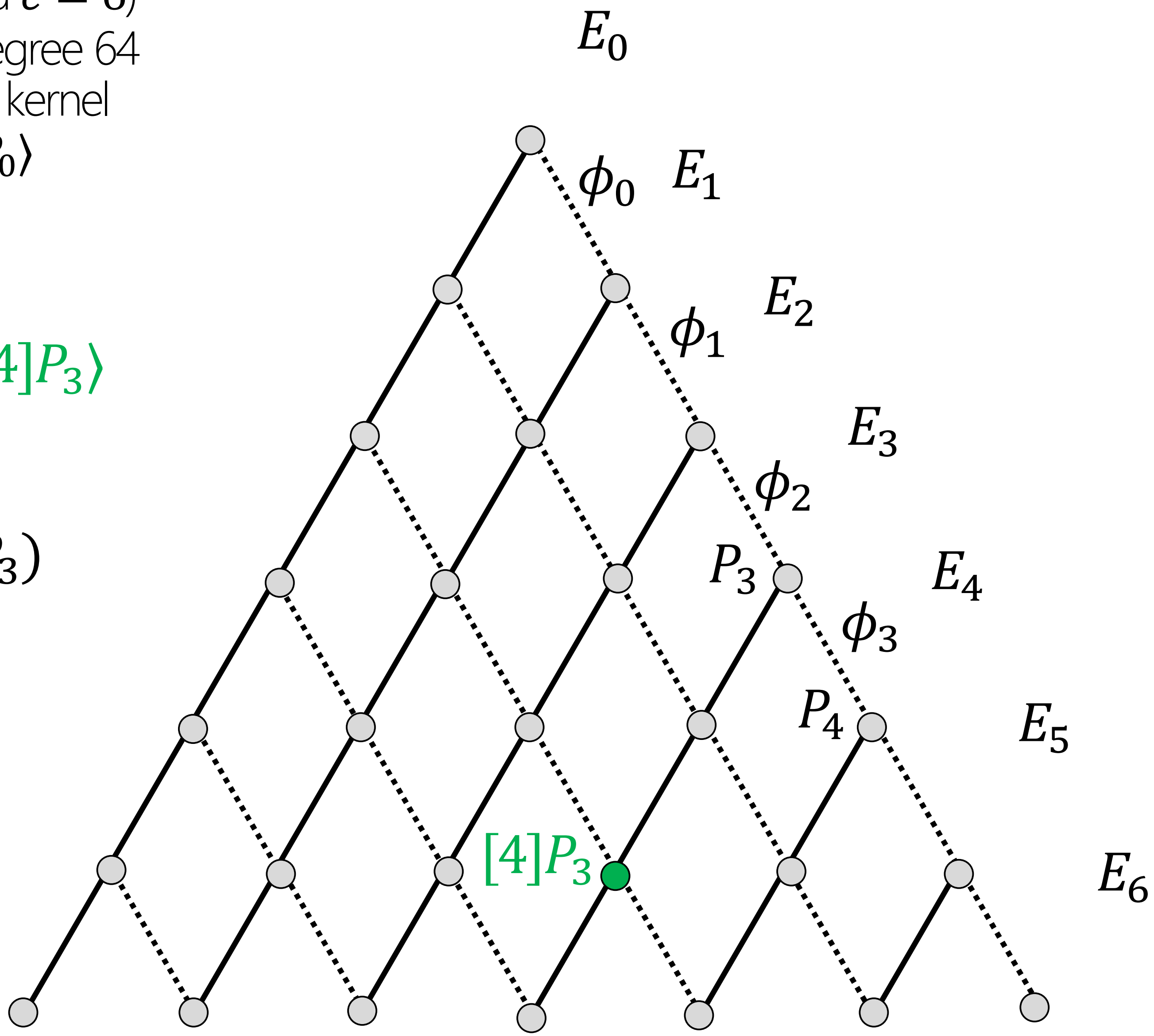


Computing ℓ^e degree isogenies

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

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

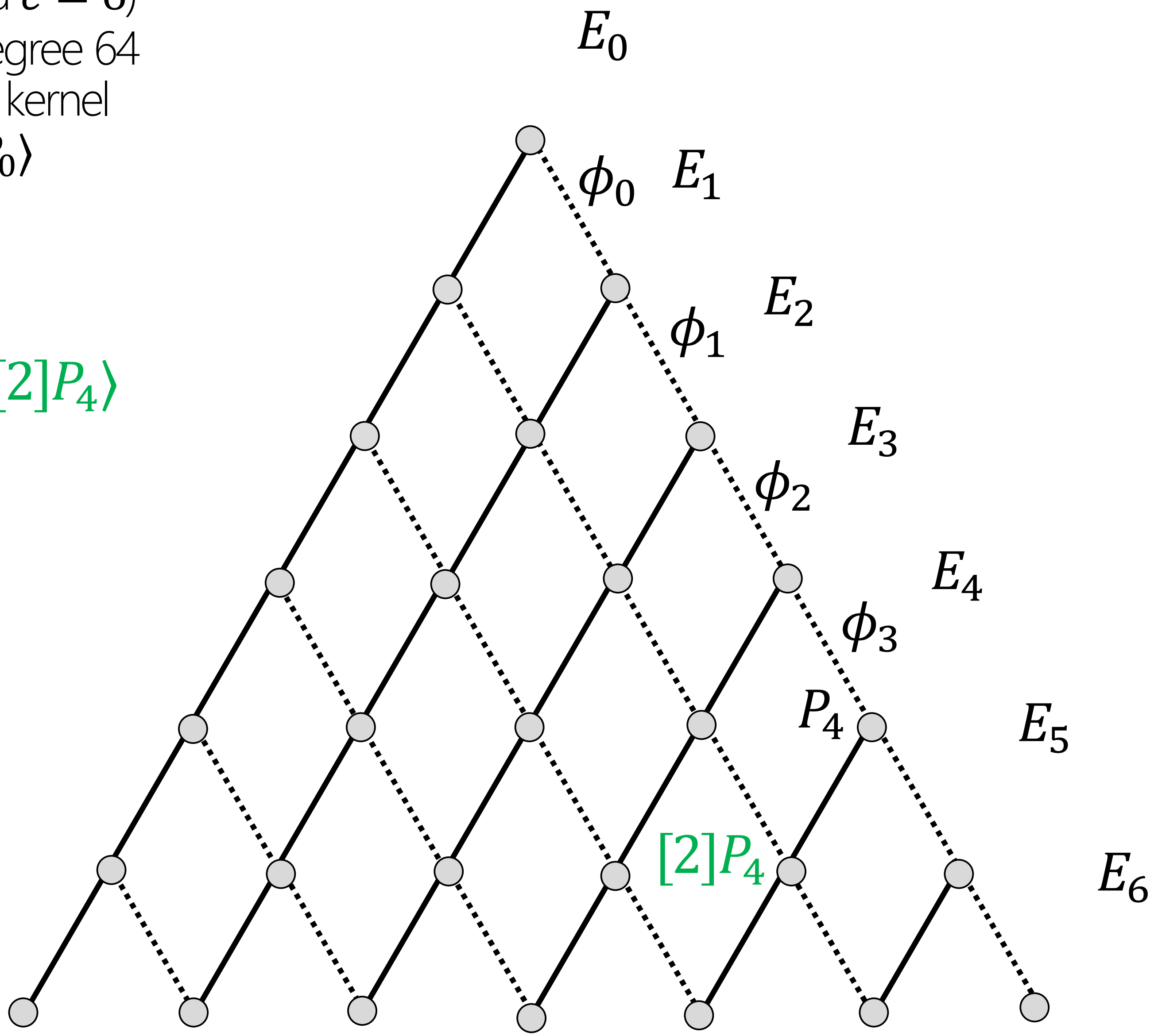
$P_4 = \phi_3(P_3)$



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

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

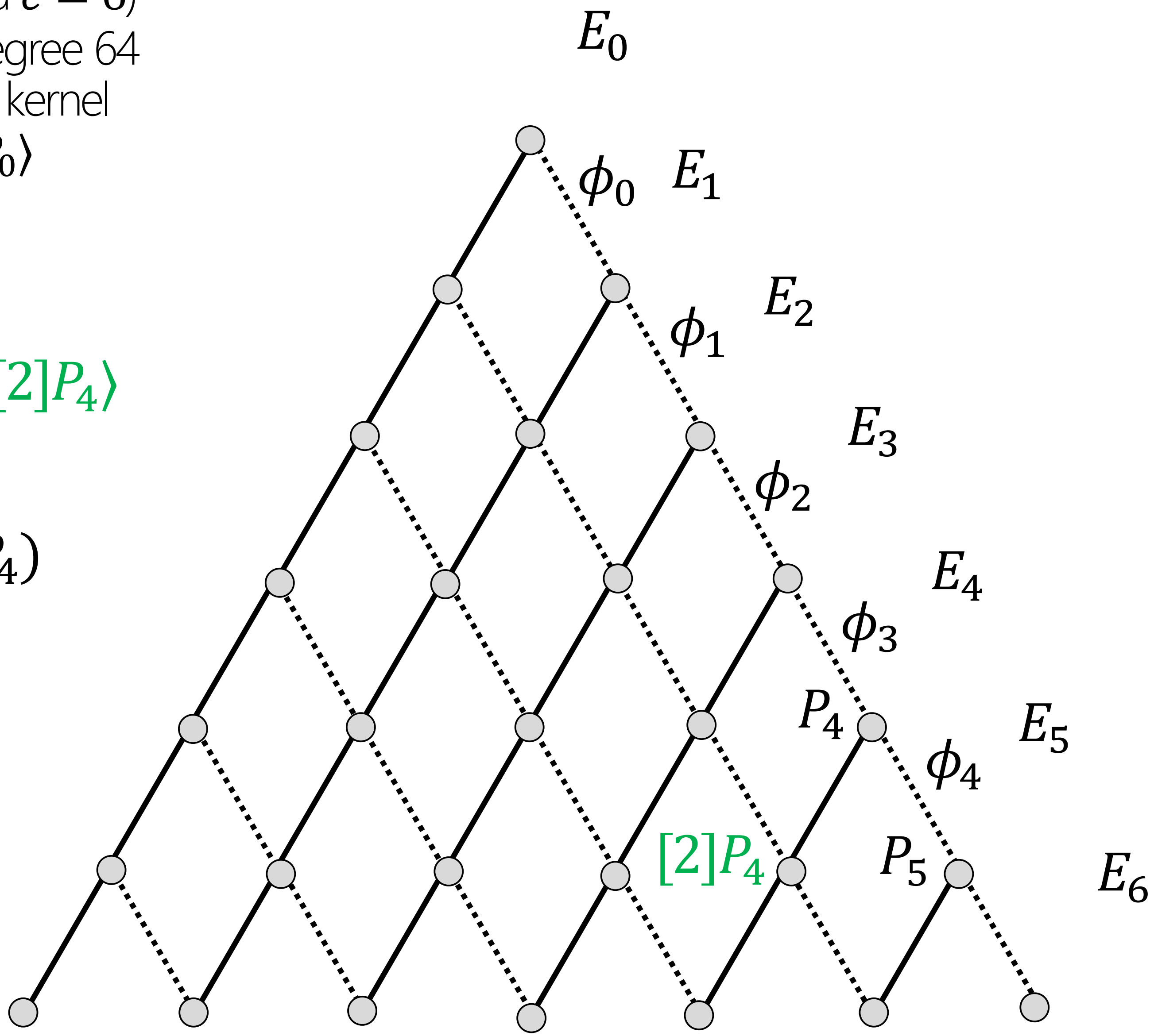


Computing ℓ^e degree isogenies

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

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

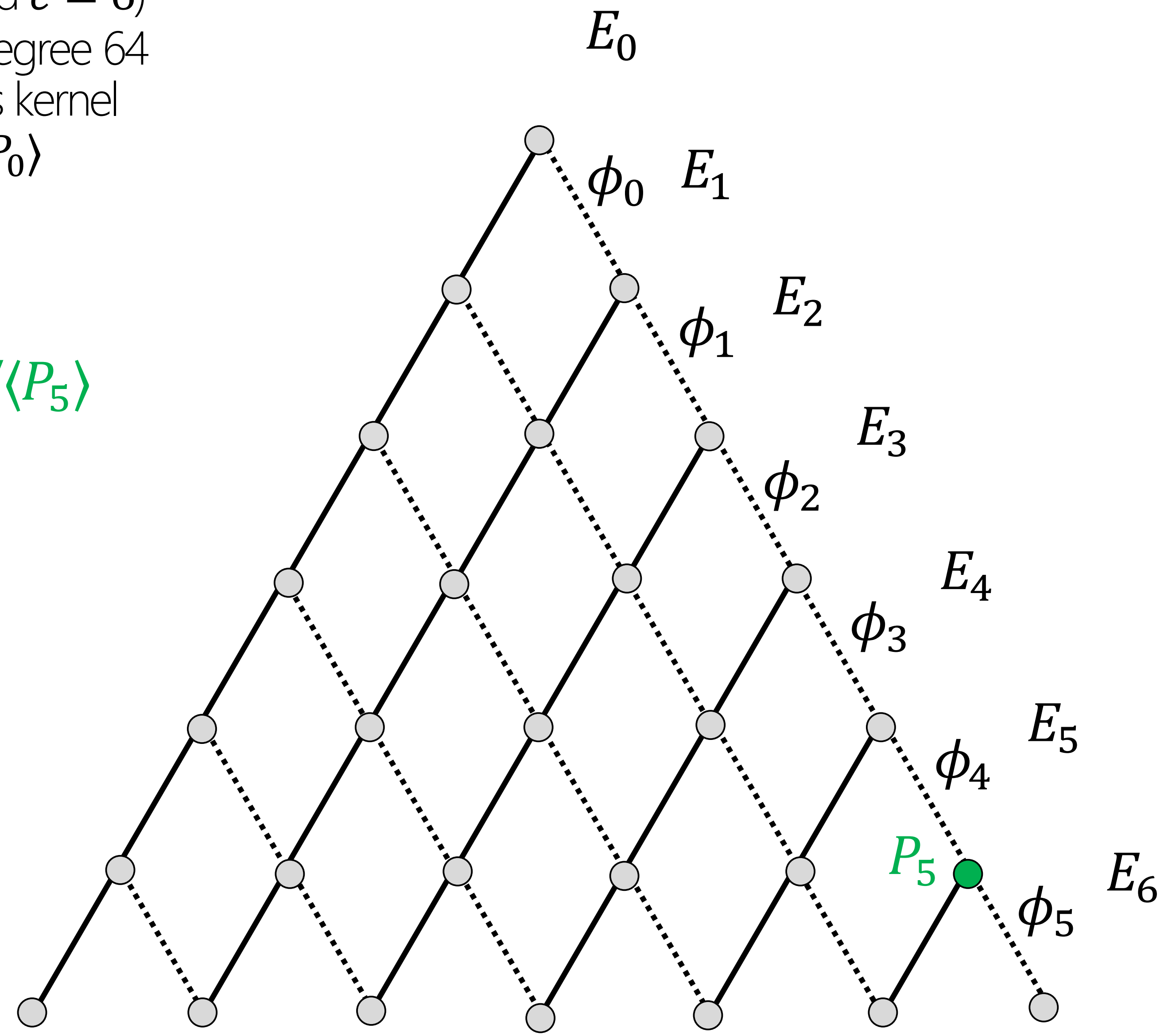
$P_5 = \phi_4(P_4)$



Computing ℓ^e degree isogenies

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

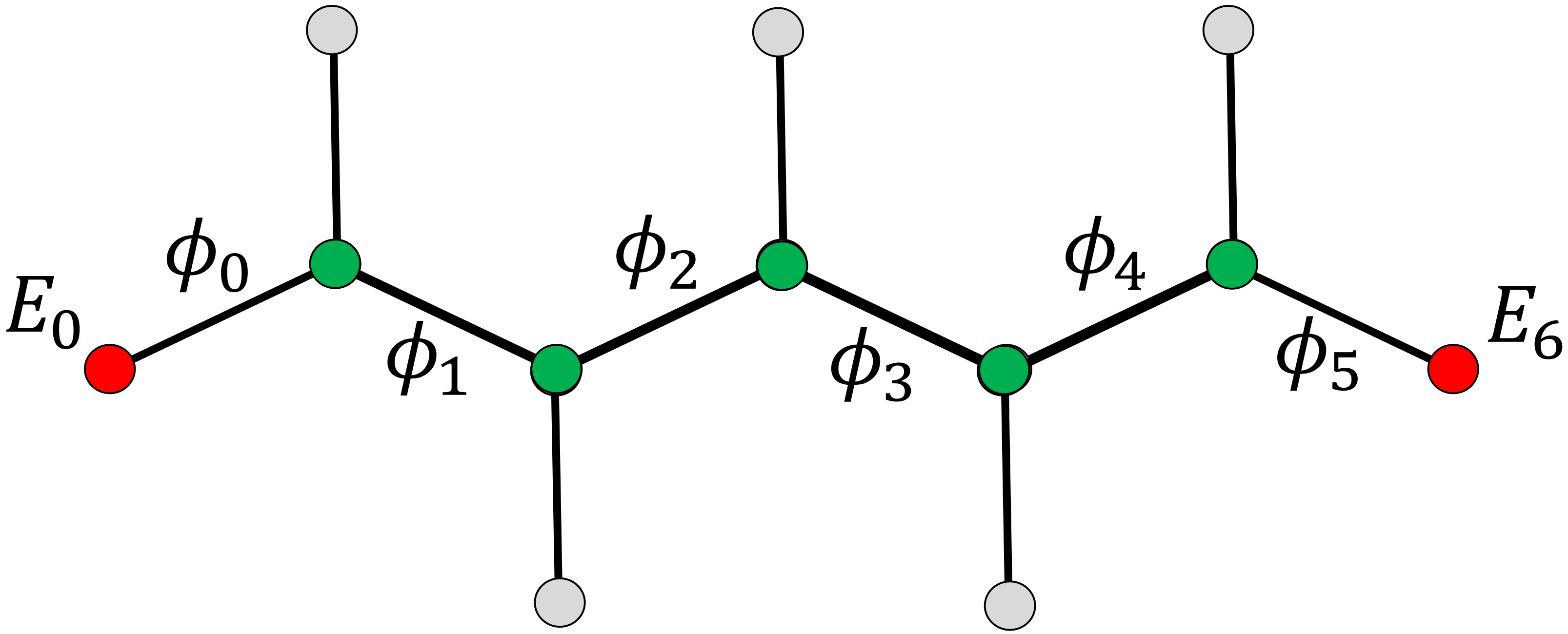
$E_6 = E_5 / \langle P_5 \rangle$



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'

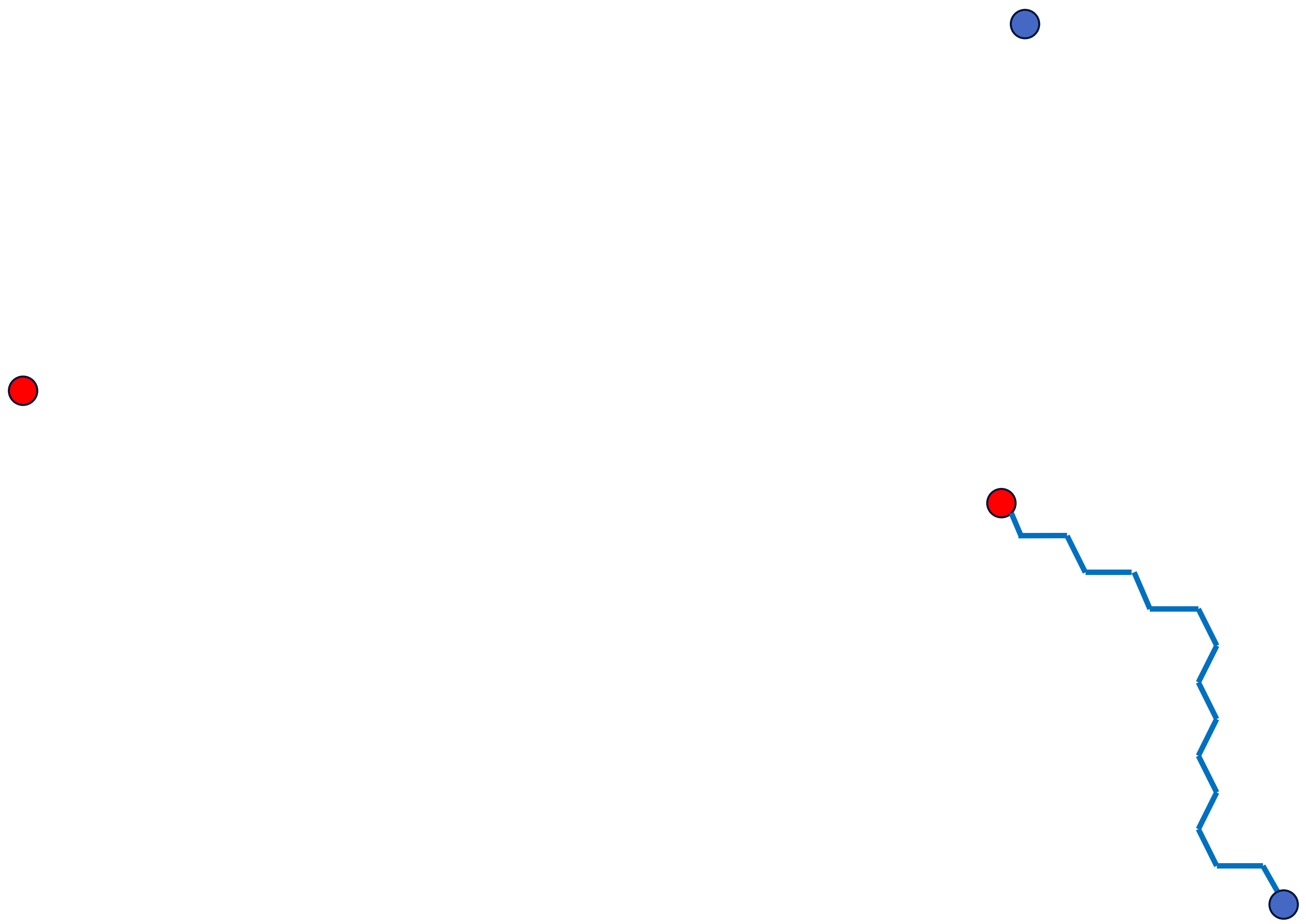
Claw algorithm

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

Claw algorithm

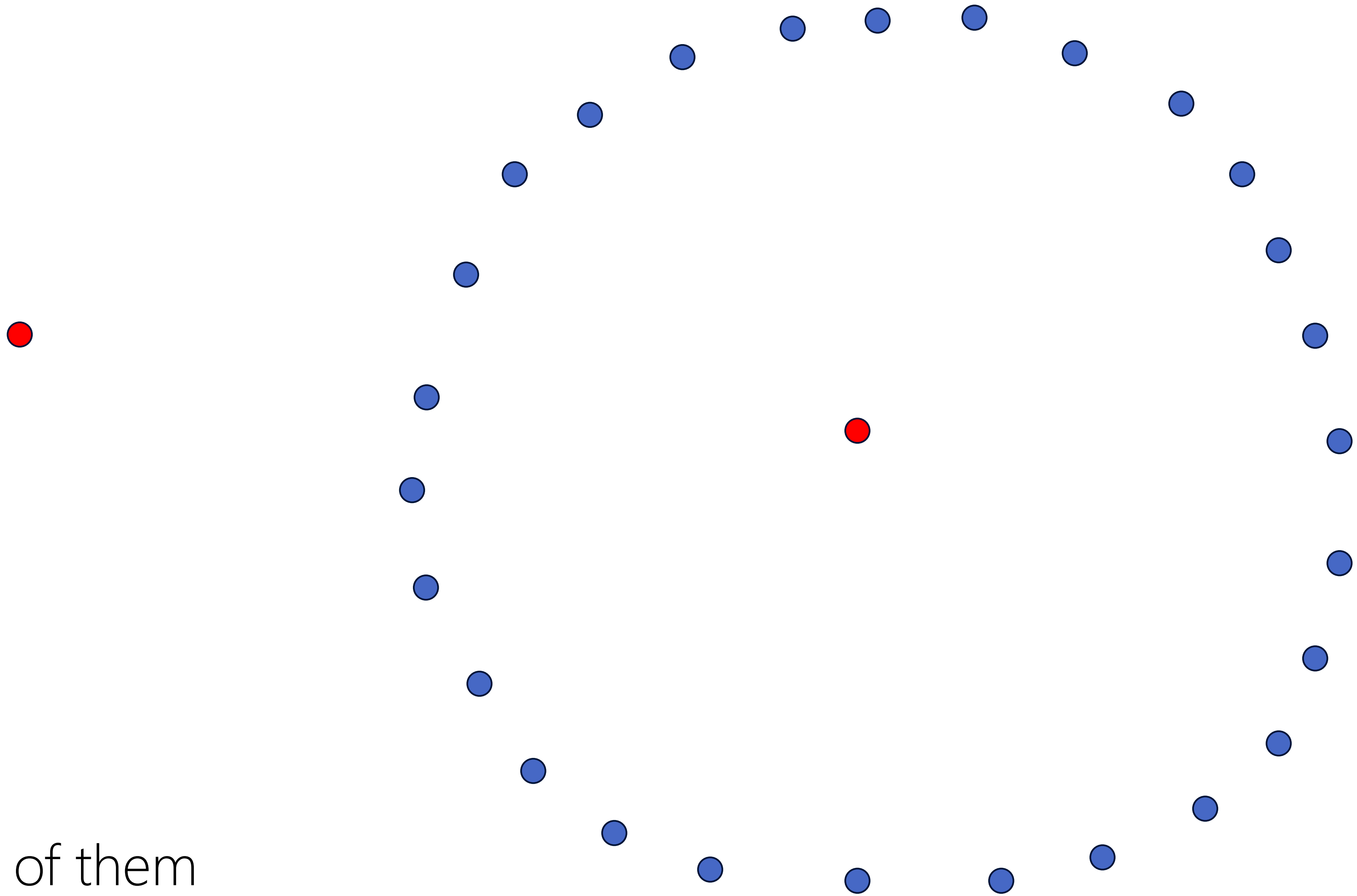
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



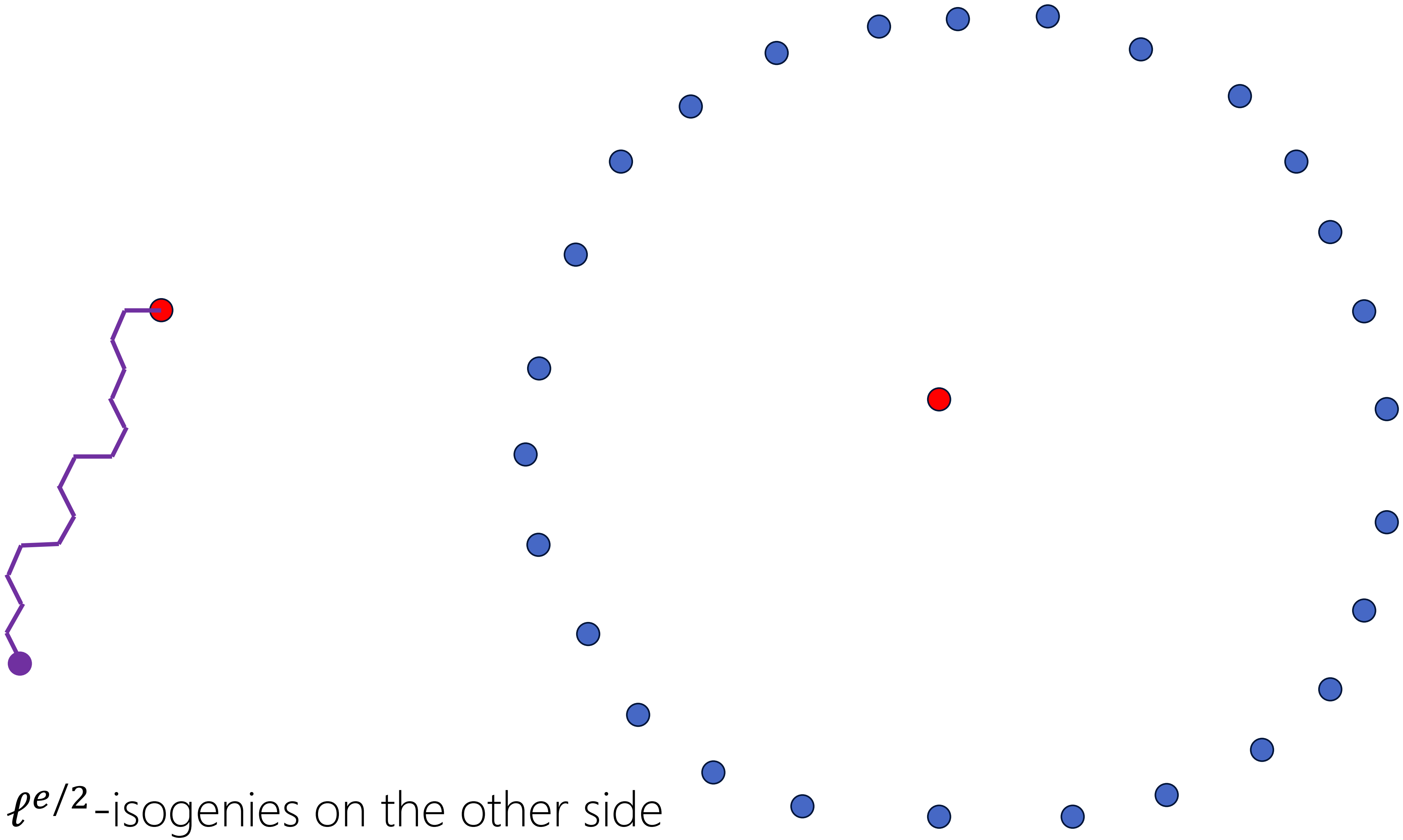
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



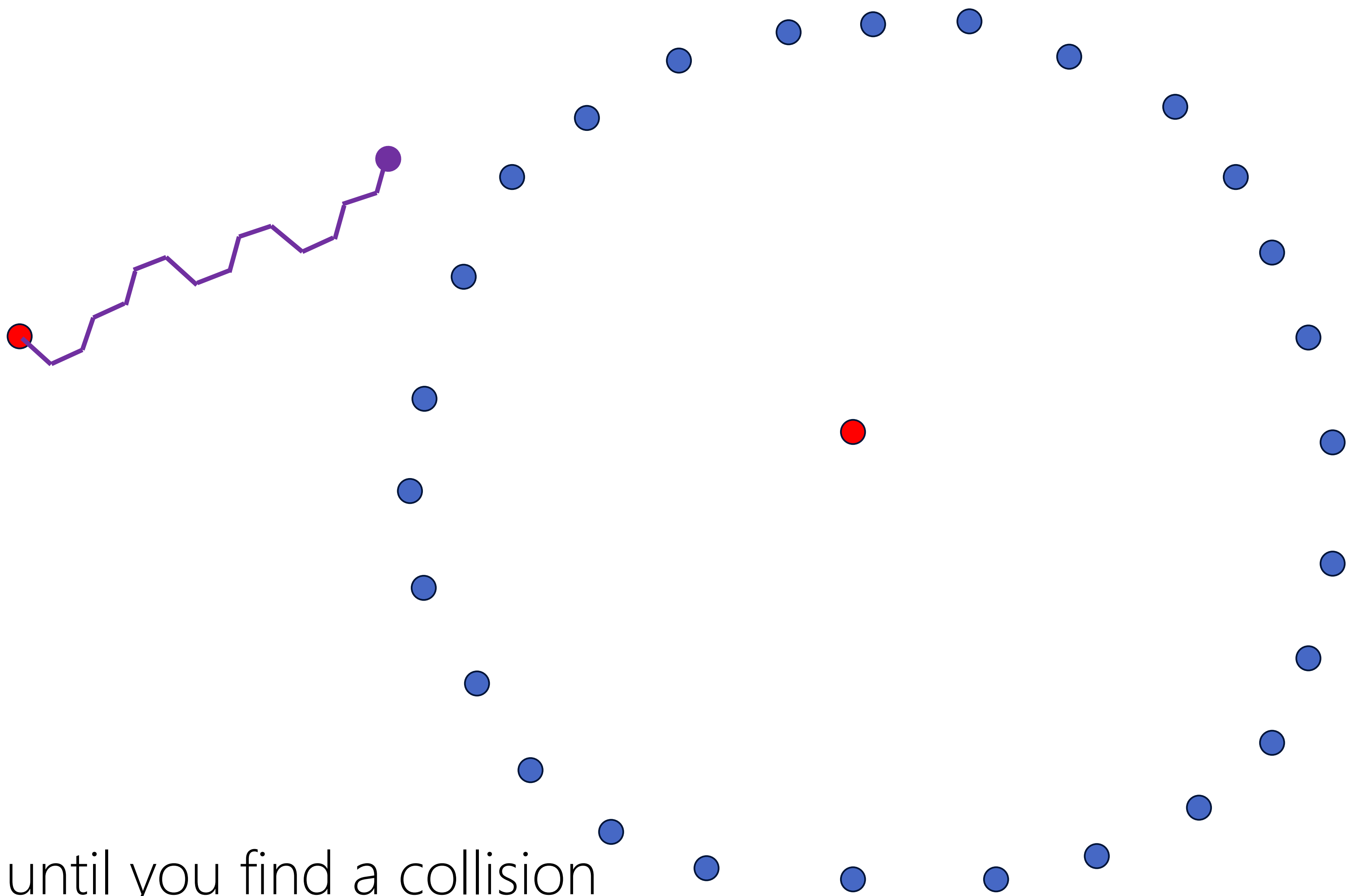
… until you have all of them

Claw algorithm



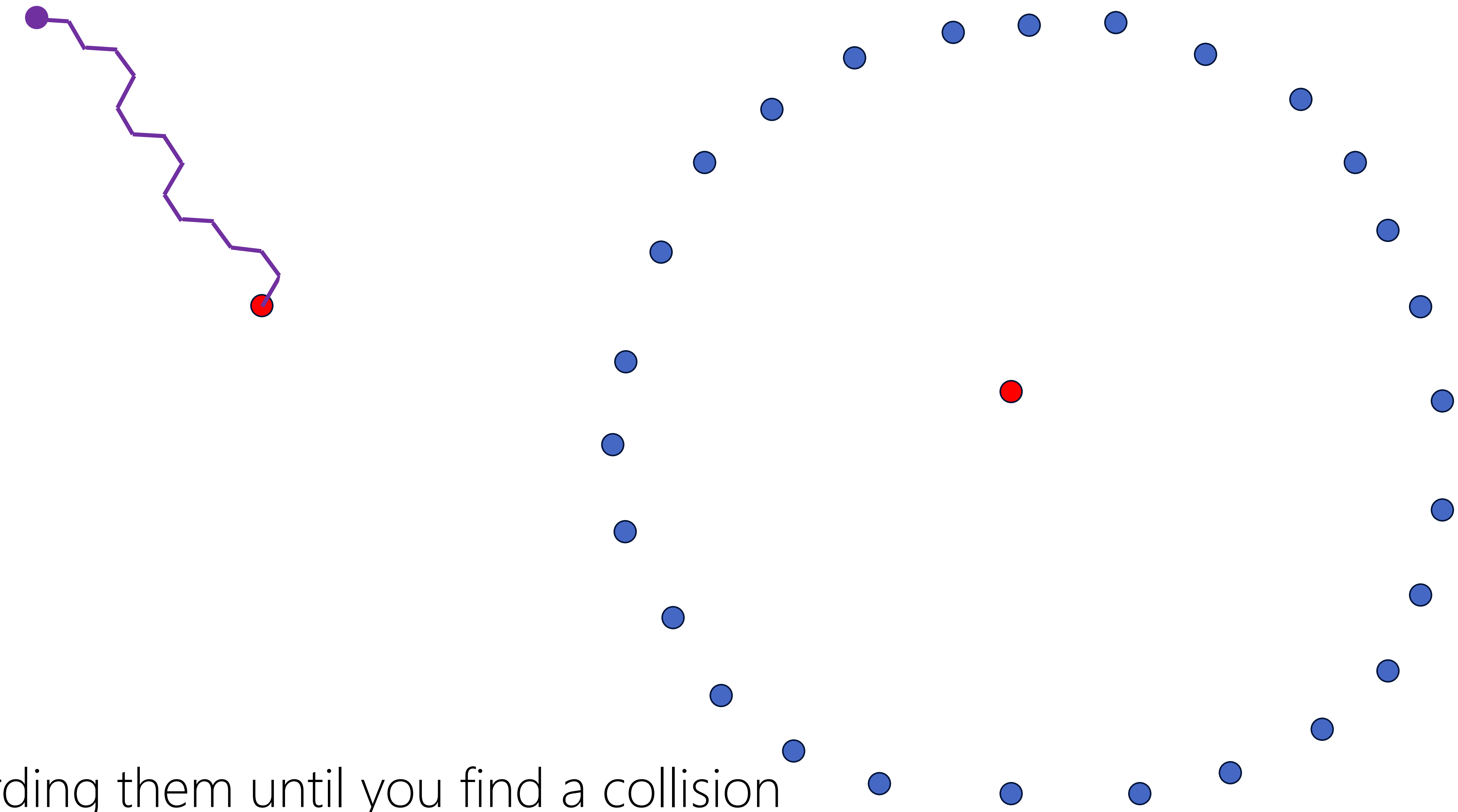
Now compute $\ell^{e/2}$-isogenies on the other side

Claw algorithm



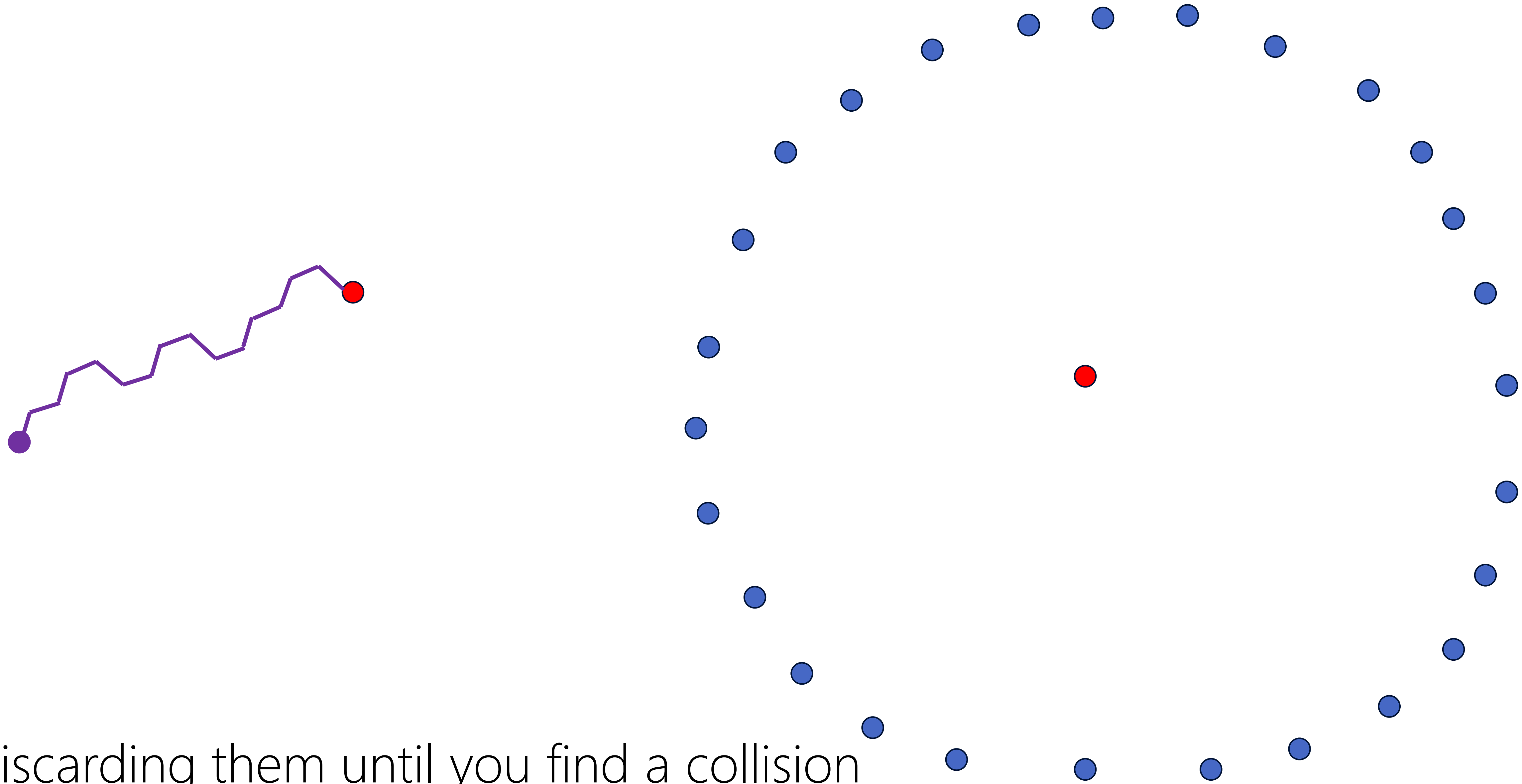
… discarding them until you find a collision

Claw algorithm



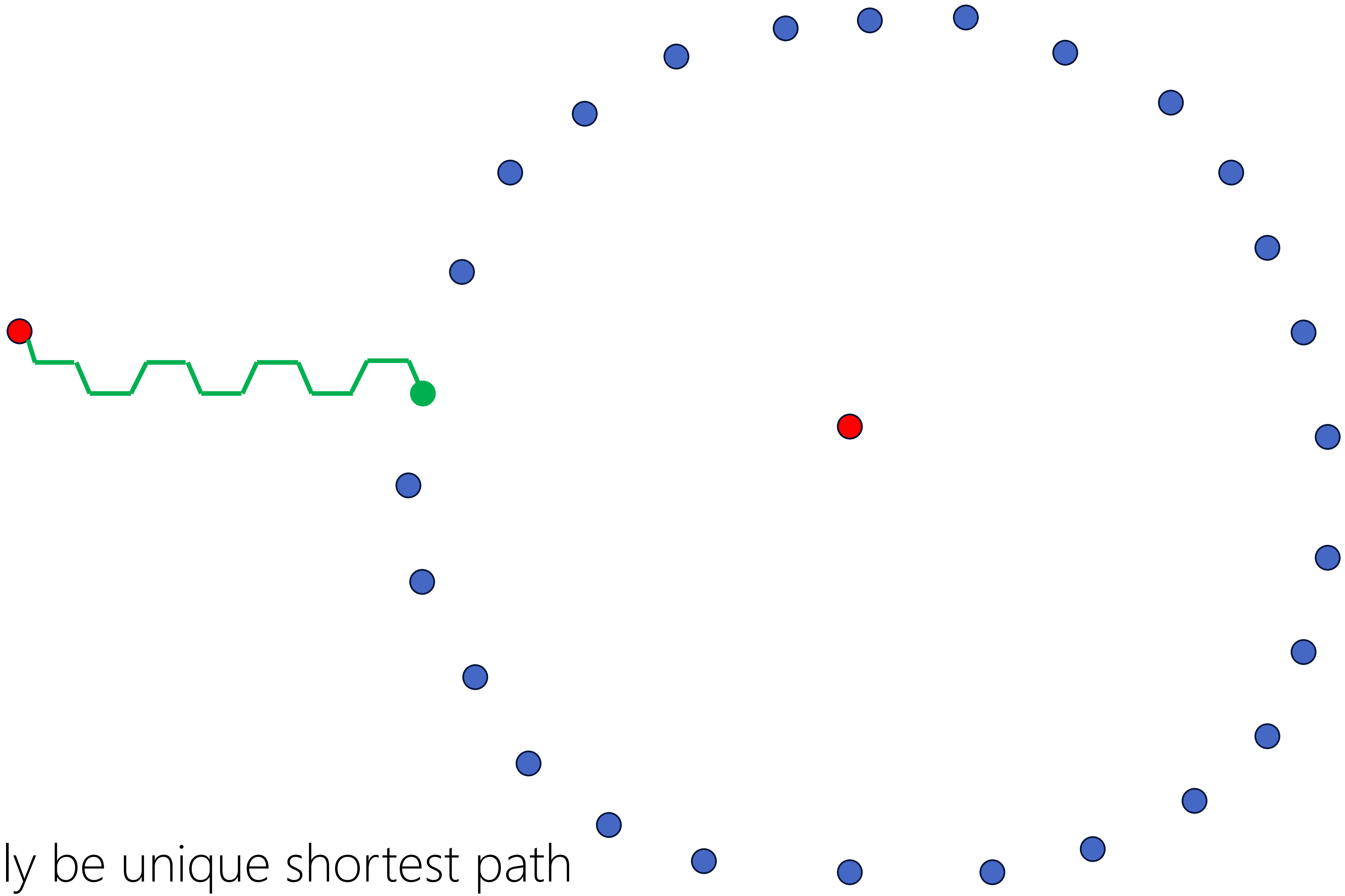
… discarding them until you find a collision

Claw algorithm



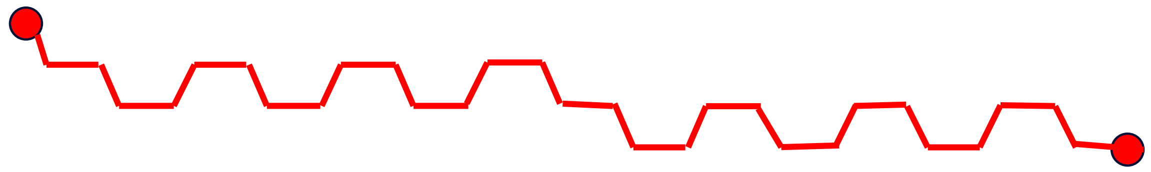
... discarding them until you find a collision

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 $O(p^{1/6})$

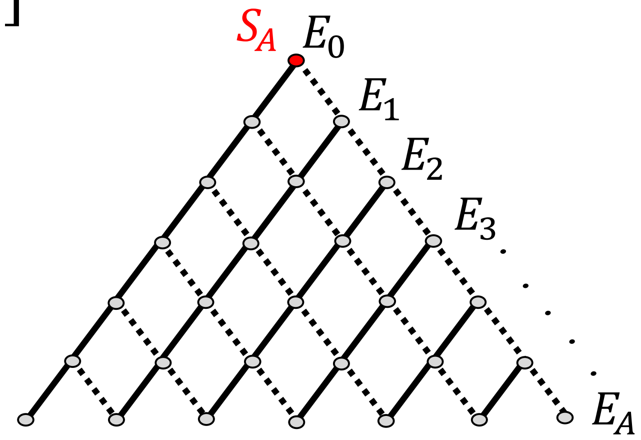
- **Confidence:** above complexities are optimal for (above generic) claw attack

SIDH: summary

$$\begin{tikzcd} E_0 \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E_A = E_0/\langle S_A \rangle \arrow[d, "\phi_B'"] \\ E_0/\langle S_B \rangle = E_B \arrow[r, "\phi_A'"] & {} \end{tikzcd}$$

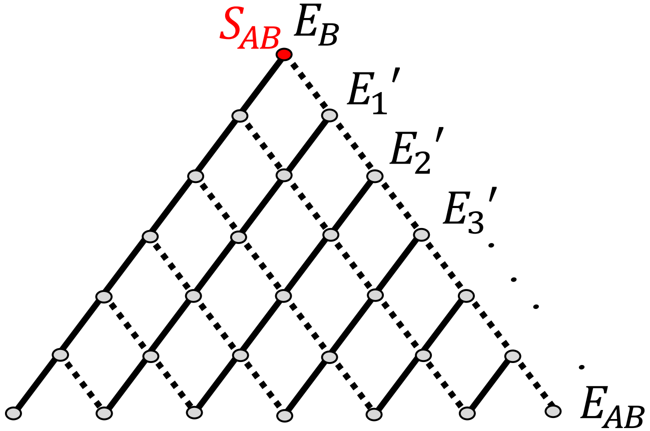
- **Setting:** supersingular elliptic curves $E/\mathbb{F}_{p^2}$ where $p = 2^i 3^j - 1$
- **Parameters:**

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



- **Public key generation (Alice):**

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



- **Shared key generation (Alice):**

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

Questions?