A gentle introduction to isogeny-based cryptography

Craig Costello

Tutorial at SPACE 2016
December 15, 2016
CRRao AIMSCS, Hyderabad, India

Microsoft®
Research

Part 1: Motivation

Part 2: Preliminaries

Part 3: Brief SIDH sketch

Diffie-Hellman key exchange (circa 1976)

$$q = 1606938044258990275541962092341162602522202993782792835301301$$
$$g = 123456789$$

$$g^a \bmod q = 78467374529422653579754596319852702575499692980085777948593$$

$$56004810429321812866744102134248313380262627139429941012879 8 = g^b \bmod q$$

$a =$
685408003627063
761059275919665
781694368639459
527871881531452

$b =$
362059131912941
987637880257325
269696682836735
524942246807440

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

Diffie-Hellman key exchange (circa 2016)

$q =$

58096059953699580628595025333045743706869751763628952366614861522872037309971102257373360445331184072513261577549805174439905295945400471216628856721870324010321116397
06440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580
16186020024749256844815024251530444957718760413642873858099017255157393414625583036640591500086964373205321856683254529110790372283163413859958640669032595972518744716
90595408050123102096390117507487600170953607342349457574162729948560133086169585299583046776370191815940885283450612858638982717634572948835466388795543116154464463301
99254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710
716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$g = 123456789$

$g^a \pmod{q} =$

197496648183227193286262018614250555971909799762533760654008147994875775445667054218578105133138217497206890599554928429450667899476
854668595594034093493637562451078938296960313488696178848142491351687253054602202966247046105770771577248321682117174246128321195678
537631520278649403464797353691996736993577092687178385602298873558954121056430522899619761453727082217823475746223803790014235051396
799049446508224661850168149957401474638456716624401906701394472447015052569417746372185093302535739383791980070572381421729029651639
304234361268764971707763484300668923972868709121665568669830978657804740157916611563508569886847487772676671207386096152947607114559
706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532
605242210147489825669666012419572610049572551002200293281421876806011231076345540456724876139639963334490185787211920851855080379172 4

411604662069593306683228525653441872410777999220572079993574397237156368762038378332742471939666544968793817819321495269833613169937
986164811320795616949957400518206385310292475529284550626247132930124027703140131220968771142788394846592816111078275196955258045178
705254016469773509936925361994895894163065551105161929613139219782198757542984826465893457768888915561514505048091856159412977576049
073563225572809880970058396501719665853110101308432647427786565525121328772587167842037624190143909787938665842005691911997396726455
110758448552553744288464337906540312125397571803103278271979007681841394534114315726120595749993896347981789310754194864577435905673
172970033596584445206671223874399576560291954856168126236657381519414592942037018351232440467191228145585909045861278091800166330876
407323844719948807012687304886027922176162928196104625521958432771481724862624396241361307595677001801738572499949511777914941688218 8

$= g^b \pmod{q}$

$a =$

7147687166405; 9571879053605547396582
6924051861459165223549126157152970 97
10067917003790492433011601949788108 9
08769613159283138632621095129494458 4
40049748892980385849319181284475723 21
02398716043906200617764831887545755 6
23377085391250529236463183321912173 21
46413465584525491722837877275669558 9
84521996220294508922696650742652691 2
7802446416400\902592710400433895826 1
14198623758789881936121879455918028 64
062679\864839578139273043684955597764
1300972122182491581096457937635455 6\6
5546298837778595680891578821511273 57
422042264637917059991767756 7\30420698
4223924948169067778961749230720712 97
60345580262107210922 0\54662739697748
55354375899087960888262776329029345 2
560094576029847\391361388767554386 6
22479265299978059886472414530462194
52761811989\97464772529088780604 93
17954195146382922889045577804592943
73052654\10485180264002079415193983
85114342508427311982036827478946058
7100\30497747706924427898968991057 2
12096357725203480402449913844583448

$b =$

655456209464694; 93360682685816031704
96942310472762446825117743874970612 8
879957701\9369882685976279047911306 2
30897586342828379858909701795736559 0
672\8357138638957122466760949930089 8
55480244640303954430074800250796203 6
38661931522988606354100532244846391 5
8979864121027377255837396 5\486539312
85483865070903191974204864923589439 1
903529930326769610 05\088404319792729
91603892747747094094858192679116146 5
028635214849 87\086232861934222391717
12154568612530067276018808591500424 8
49476686\706784051068715397706852664
53263833240398374733837969702262426 1
37716316320449382829920603980870340 3
57510046733708501774838714882222487 5
30964179187939548373175462003488493 0
5403999505191916794712 24\05558557093
21935074715557775695981637008509203 94
705281936392411084\436006861835284 65
72496956218643721497262583322254486 5
996160464558\546299370165894704252 64
44562415789958697265293564785696709 2
689604\427965012098770368450012467 92
76156391763995973638303866536272715 8

$g^{ab} =$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739
419999231378970715307039317876258453876701124543849520979430233302777503265010724513551209279573183234934359636696506
968325769489511028943698821518689496597758218540767517885836464160289471651364552490713961456608536013301649753975875
610659655755567474438180357958360226708742348175045563437075840969230826767034061119437657466993989389348289599600338
950372251336932673571743428823026014699232071116171392219599691096846714133643382745709376112500514300983651201961186
613464267685926563624589817259637248558104903657371981684417053993082671827345252841433337325420088380059232089174946
086536664984836041334031650438692639106287627157575758383128971053401037407031731509582807639509448704617983930135028
7596589383292751993079161318883904312132911893000994819789990758698610895359142027942687477942356022103846 8

ECDH key exchange (1999 – nowish)

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

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

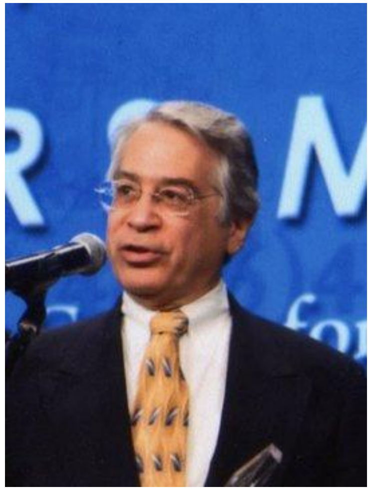
$$E/\mathbf{F}_p : y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,$
$36134250956749795798585127919587881956611106672985015071877198253568414405109)$

[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

Post-quantum key exchange

What hard problem(s) do we use now???

This talk + Sunday's: isogenies

Diffie-Hellman instantiations

	DH	ECDH	R-LWE [BCNS'15, newhope, NTRU]	LWE [Frodo]	SIDH [DJP14, CLN16]
elements	integers g modulo prime	points P in curve group	elements a in ring $R = \mathbb{Z}_q[x]/\langle\Phi_n(x)\rangle$	matrices A in $\mathbb{Z}_q^{n\times n}$	curves E in isogeny class
secrets	exponents x	scalars k	small errors $s, e \in R$	small $s, e \in \mathbb{Z}_q^n$	isogenies ϕ
computations	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$a, s, e \mapsto as + e$	$A, s, e \mapsto As + e$	$\phi, E \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $a, as + e$ find s	given $A, As + e$ find s	given $E, \phi(E)$ find ϕ

Part 1: Motivation

Part 2: Preliminaries

Part 3: Brief SIDH sketch

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-$\boldsymbol{n}$ map:
$$n : E \to E, \qquad P \mapsto [n]P$$

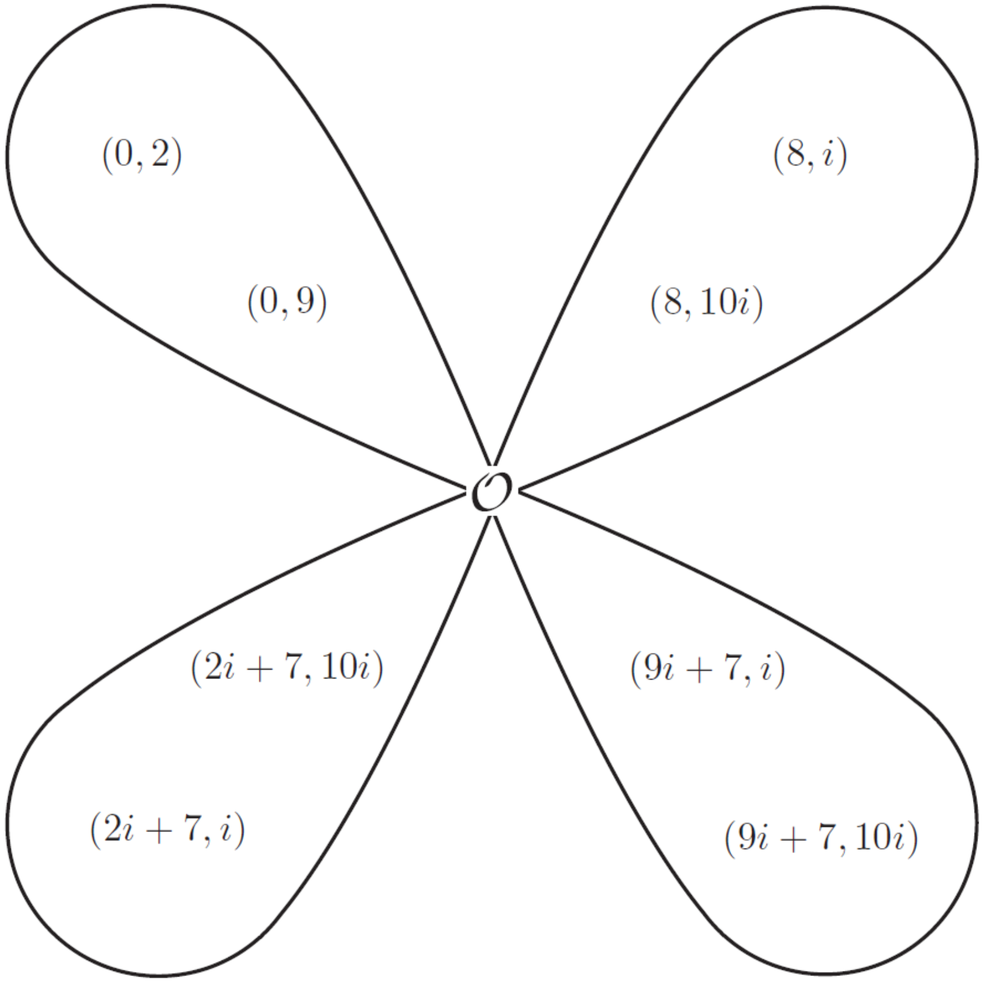
- The $\boldsymbol{n}$-torsion subgroup is the kernel of $[n]$
$$E[n] = \{P \in E(\bar{K}) : \; [n]P = \infty\}$$

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

- If $\mathbf{char}(K)$ doesn't divide $\boldsymbol{n}$, then
$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n$$

Example

- 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 $\psi_3(x) = x(x+3)(x^2+8x+9)$
- 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

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

Isogenies

- 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

$$E' : \mathrm{y}^2 = \mathrm{x}^3 + \big(-(4\mathrm{a} + 2\mathrm{b}_1)\big)\mathrm{x}^2 + (\mathrm{b}_1^2 - 4\mathrm{b}_0)\mathrm{x}$$

And where ϕ maps (x, y) to

$$\left(\frac{x^3-(a-b_1)x^2-(b_1a-b_0)x-b_0a}{x-a}, \frac{\big(\mathrm{x}^2-(2\mathrm{a})\mathrm{x}-(\mathrm{b}_1\mathrm{a}+\mathrm{b}_0)\big)\mathrm{y}}{(\mathrm{x}-\mathrm{a})^2}\right)$$

Velu's formulas

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

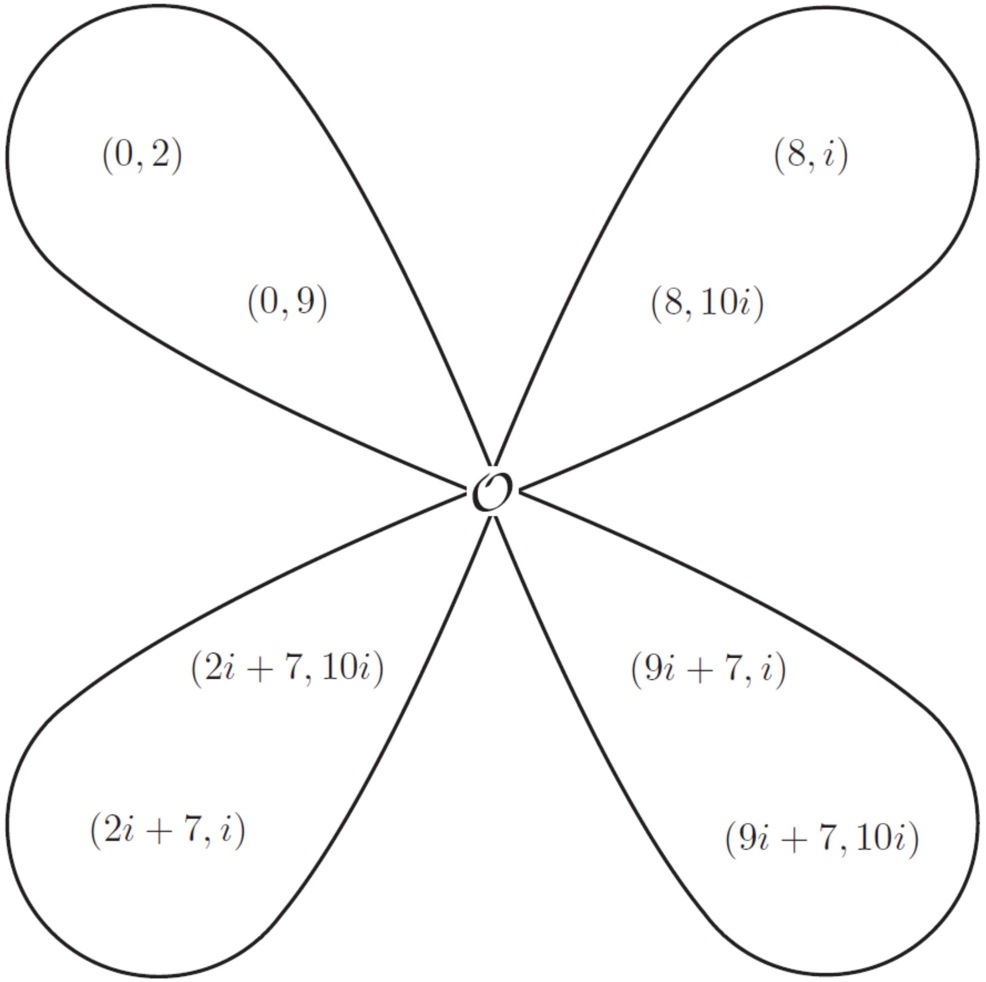
$$\phi : \; E \to E',$$

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

Example, cont.

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

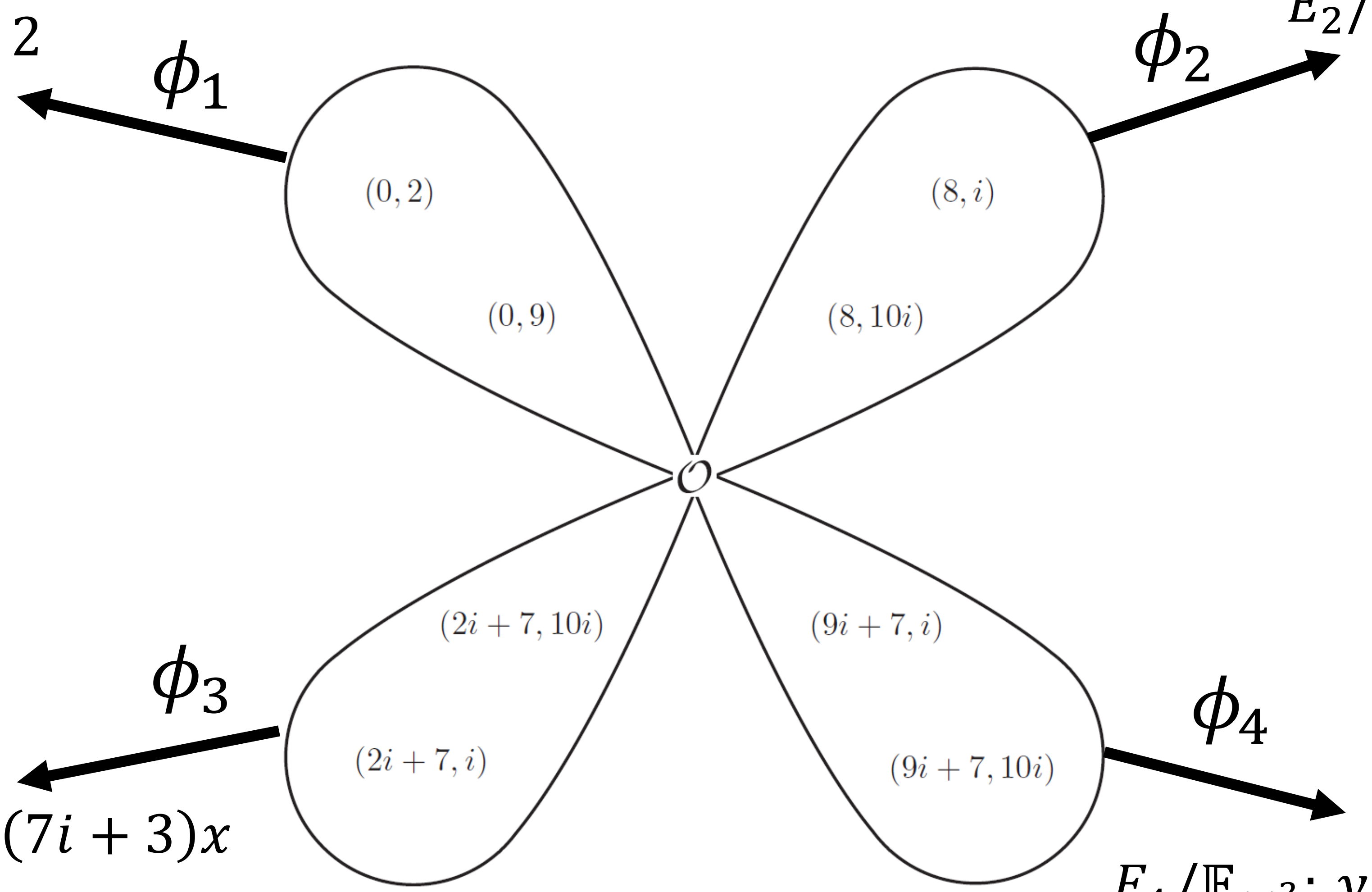
$G = E[3]$



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?

The dual isogeny

For every isogeny $\psi: E_1 \to E_2$ of degree n, there exists (unique, up to isomorphism) dual isogeny $\hat{\psi} : E_2 \to E_1$ of degree n, such that

$$\hat{\psi} \circ \psi = [n]_{E_1}$$

and

$$\psi \circ \hat{\psi} = [n]_{E_2}$$

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 (Tate): E_1 and E_2 isogenous if and only if $\#E_1 = \#E_2$
- Thm (Mestre): all supersingular curves over $\mathbb{F}_{p^2}$ in same isogeny class
- Fact (see previous slides): for every prime ℓ not dividing p, there exists $\ell + 1$ isogenies of degree ℓ originating from any supersingular curve

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

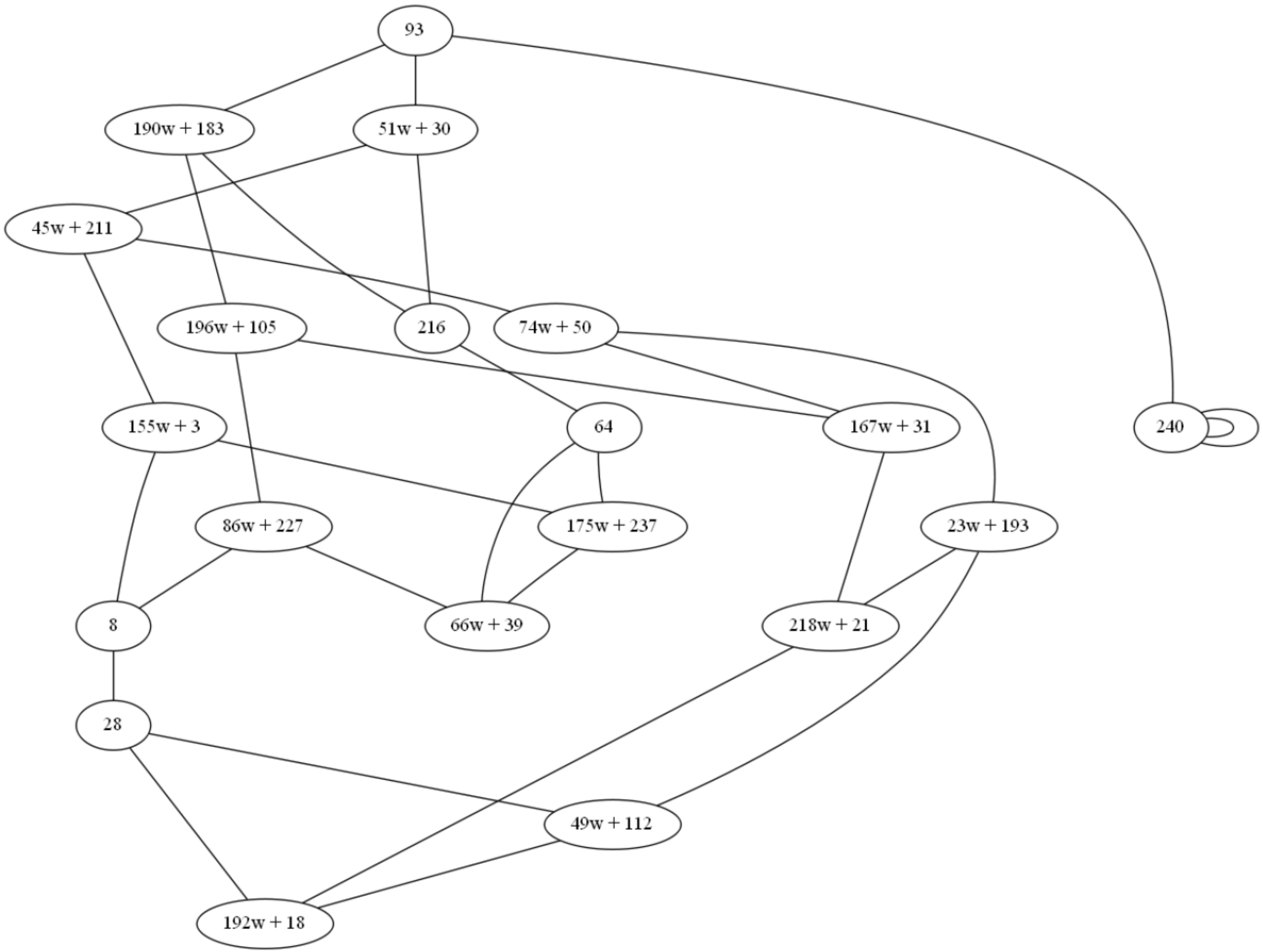
- Previous example actually had $E_2 \cong E_3 \cong E_4$, so let's increase the size a little to get a picture of how this all pans out…

E.g. a supersingular isogeny graph

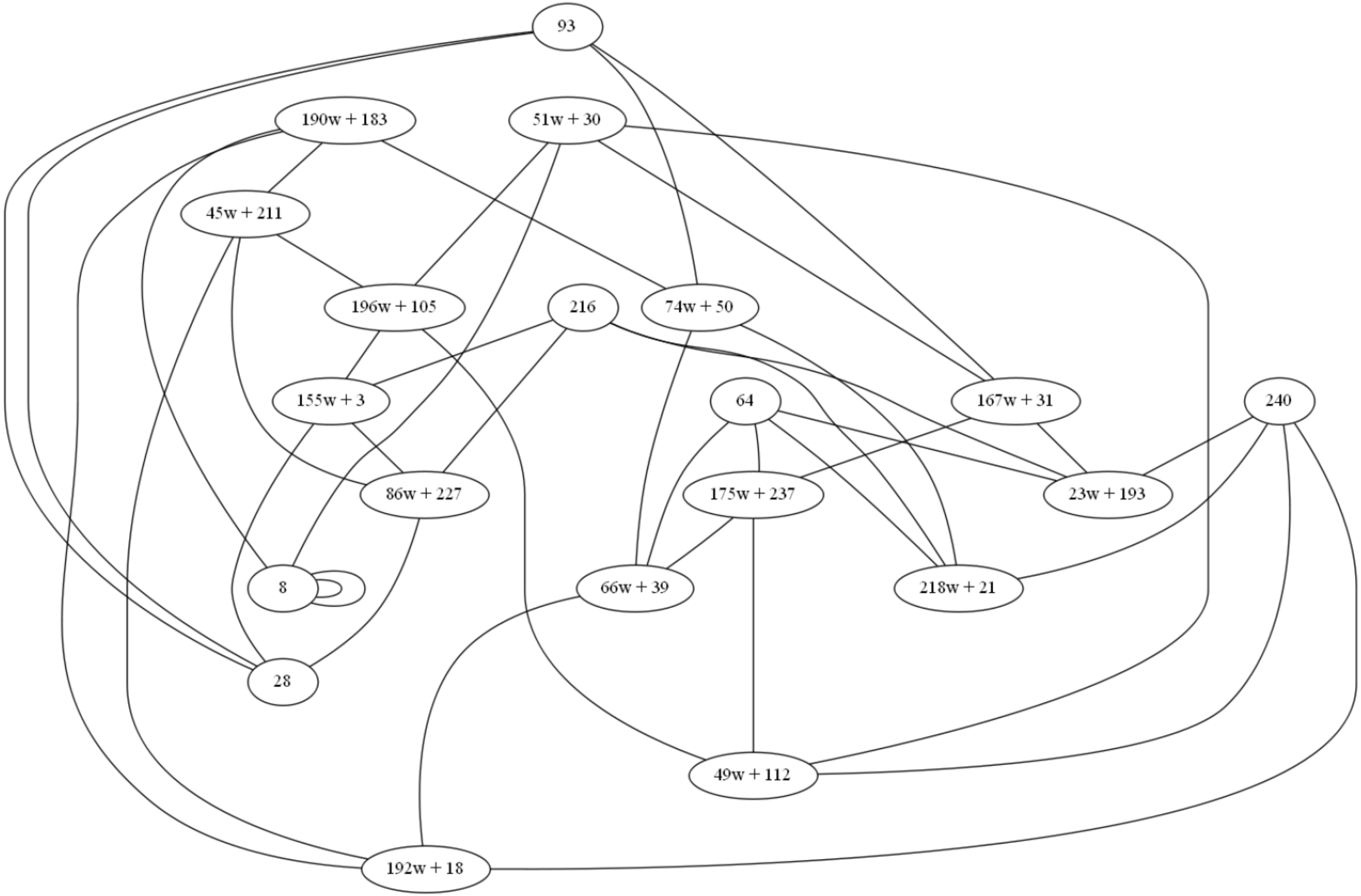
- Let $p = 241$, $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 - 3x + 7)$
- $\#S_{p^2} = 20$
- $S_{p^2} = \{93,\ 51w + 30,\ 190w + 183,\ \ 240,\ 216,\ 45w + 211,\ 196w + 105,\ 64,\ 155w + 3,\ 74w + 50,\ \ 86w + 227,\ 167w + 31,\ 175w + 237,\ 66w + 39,\ 8,\ 23w + 193,\ 218w + 21,\ 28,\ 49w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

Credit to Fre Vercauteren for example and picture…

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

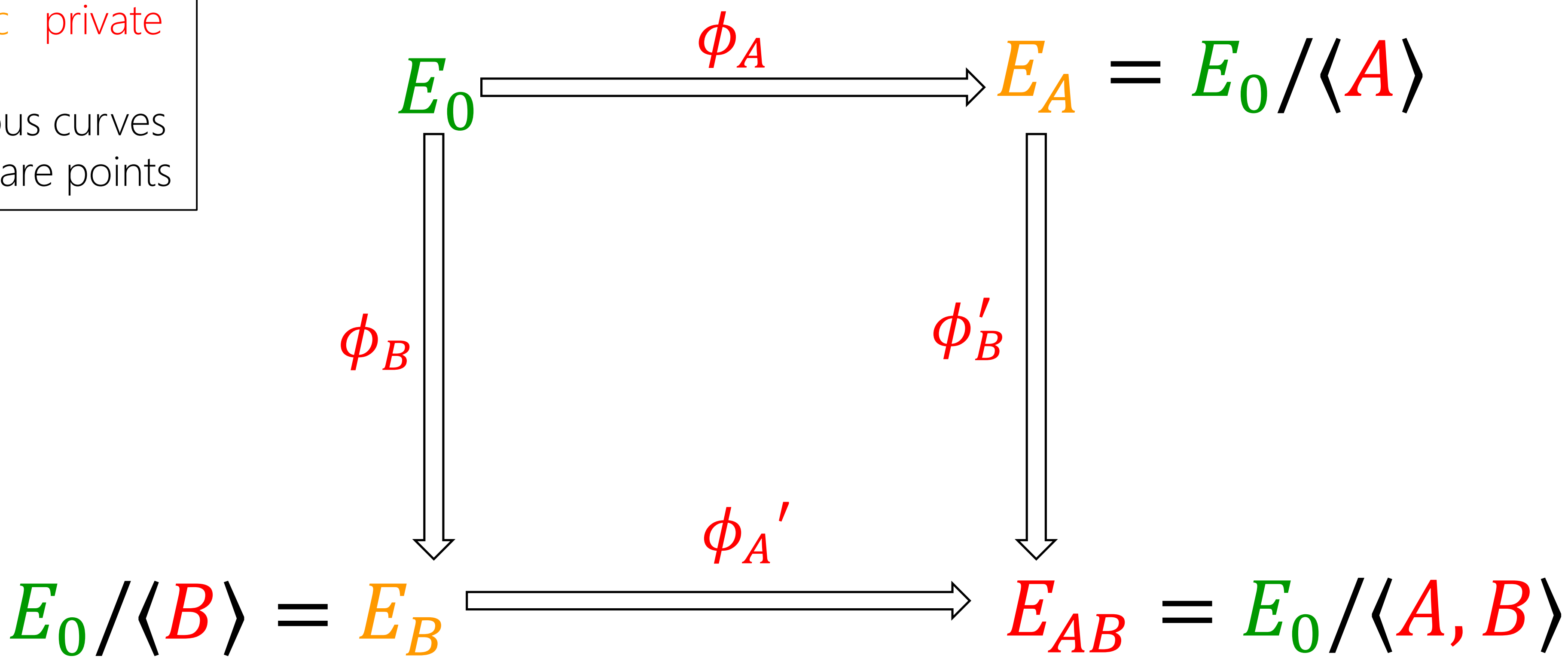
Part 2: Preliminaries

Part 3: Brief SIDH sketch

SIDH: in a nutshell

params public private

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



- Non-commutative, so $\phi_B \phi_A \neq \phi_A \phi_B$ (can't even multiply), hence ϕ_A' and ϕ_B'
- Alice can't just take $E_B/\langle A \rangle$, A doesn't lie on E_B

SIDH: in a nutshell

params public private

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

$$E_0 \xrightarrow{\phi_A} E_A = E_0/\langle P_A + [s_A]Q_A \rangle$$

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

$$E_0 \xrightarrow{\phi_B} E_B, \quad E_A \xrightarrow{\phi_B'} E_{AB}$$

$$E_0/\langle P_B + [s_B]Q_B \rangle = E_B \xrightarrow{\phi_A{}'} E_{AB} = E_0/\langle A, B \rangle$$

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

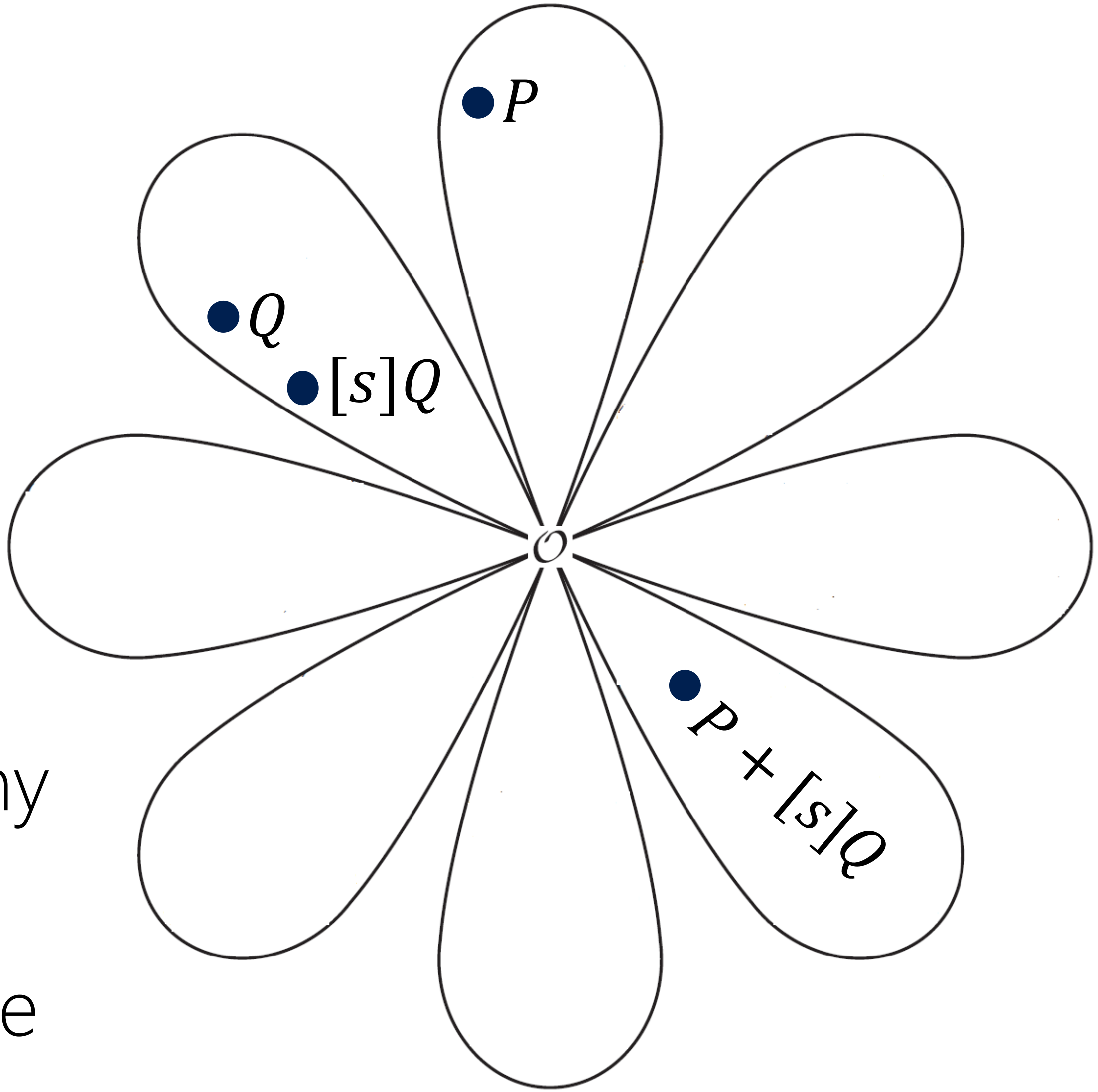
Key: Alice sends her isogeny evaluated at Bob's generators, and vice versa

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

- Why $E' = E/\langle P + [s]Q \rangle$, etc?
- Why not just $E' = E/\langle [s]Q \rangle$?... because here E' is ≈ independent of s
- Need two-dimensional basis to span two-dimensional torsion
- Every different s now gives a different order n subgroup, i.e., kernel, i.e. isogeny
- Composite same thing, just uglier picture

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

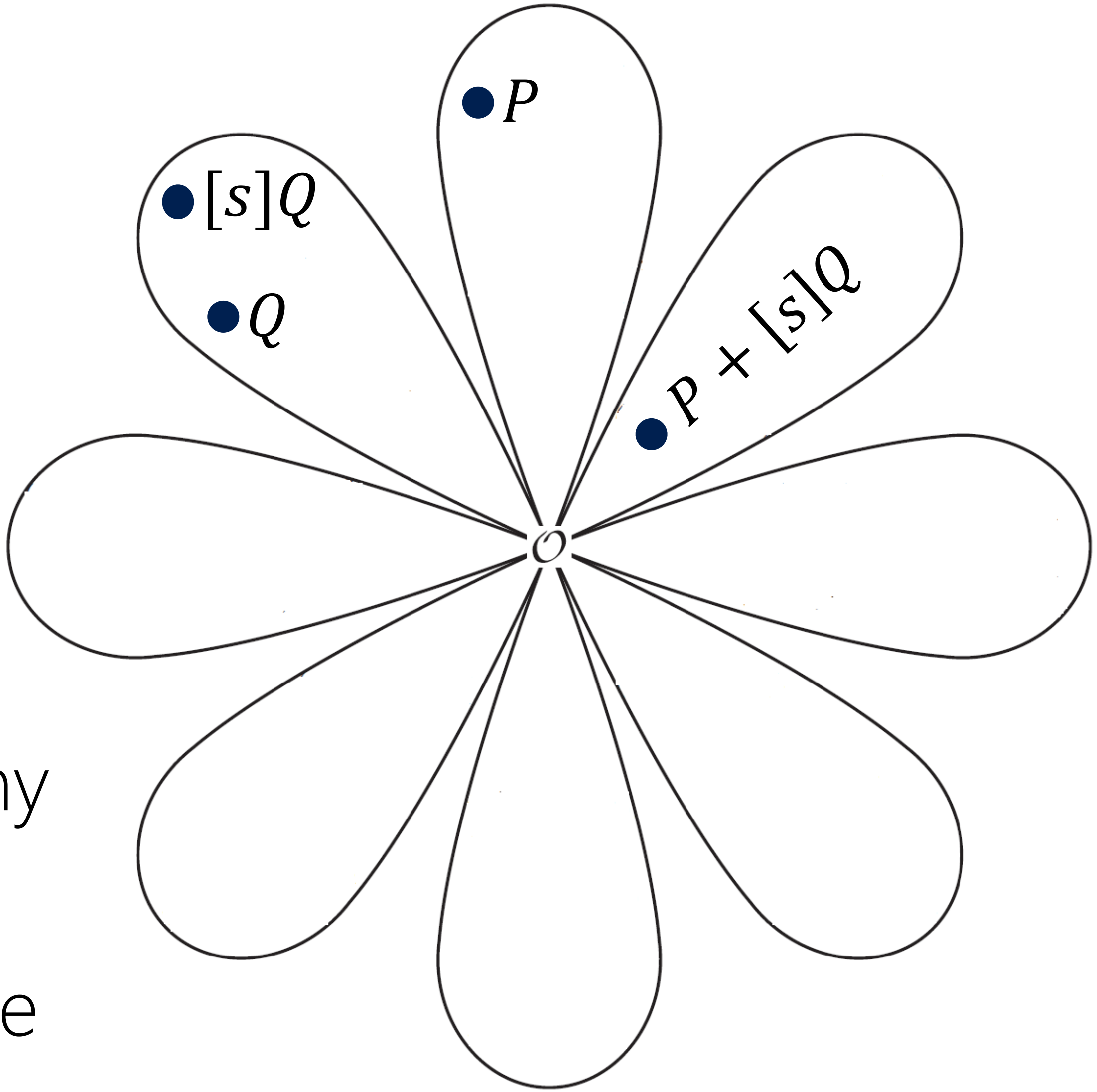
(n prime depicted below)
$n+1$ cyclic subgroups order n



- Why $E' = E/\langle P + [s]Q \rangle$, etc?
- Why not just $E' = E/\langle [s]Q \rangle$?...
  because here E' is $\approx$ independent of s
- Need two-dimensional basis to span two-dimensional torsion
- Every different s now gives a different order n subgroup, i.e., kernel, i.e. isogeny
- Composite same thing, just uglier picture

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

(n prime depicted below)
$n + 1$ cyclic subgroups order n



- Why $E' = E/\langle P + [s]Q \rangle$, etc?

- Why not just $E' = E/\langle [s]Q \rangle$?...
  because here E' is $\approx$ independent of s

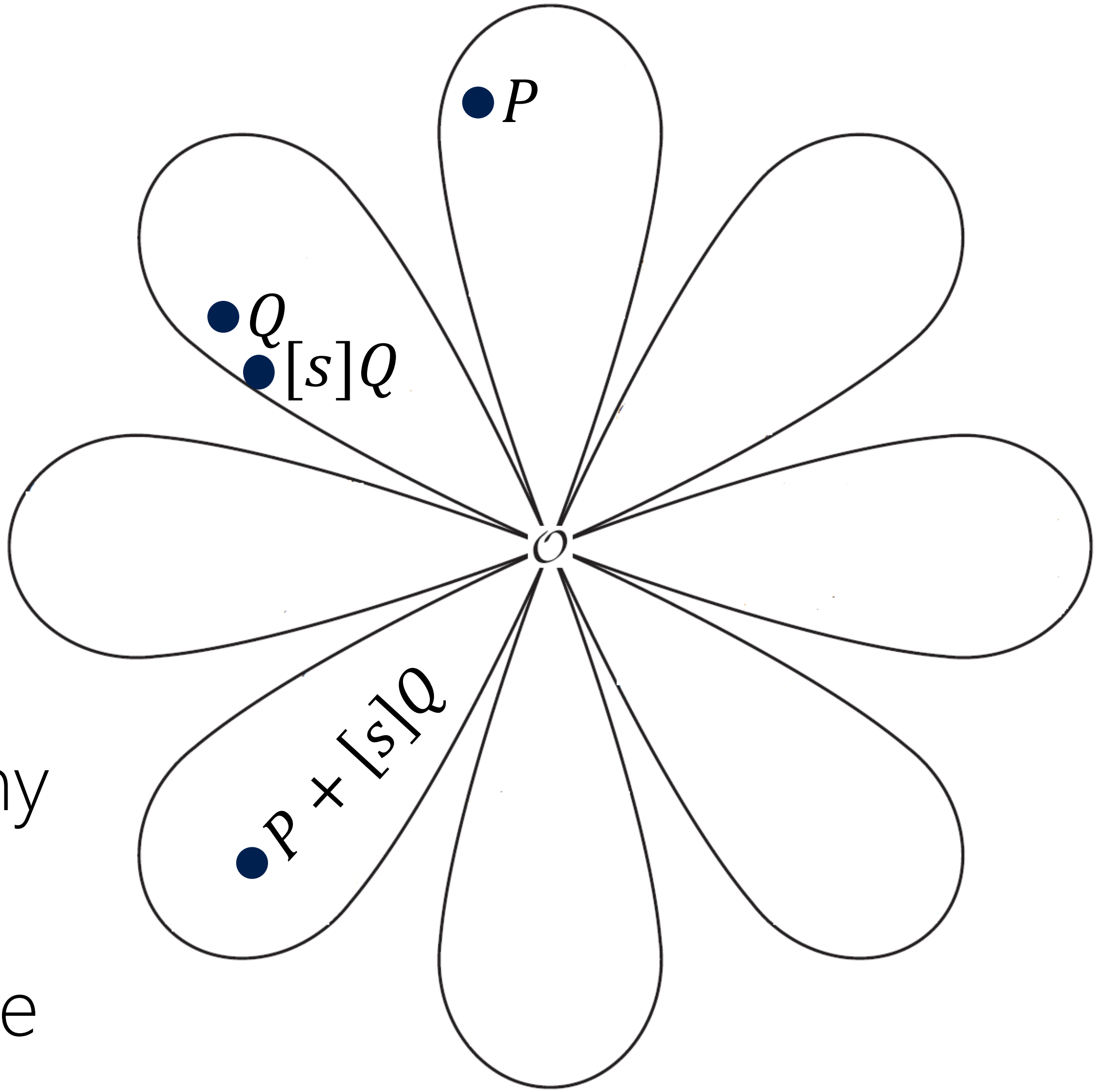
- Need two-dimensional basis to span two-dimensional torsion

- Every different s now gives a different order n subgroup, i.e., kernel, i.e. isogeny

- Composite same thing, just uglier picture

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

(n prime depicted below)
$n + 1$ cyclic subgroups order n



- Why $E' = E/\langle P + [s]Q \rangle$, etc?

- Why not just $E' = E/\langle [s]Q \rangle$?...
  because here E' is $\approx$ independent of s

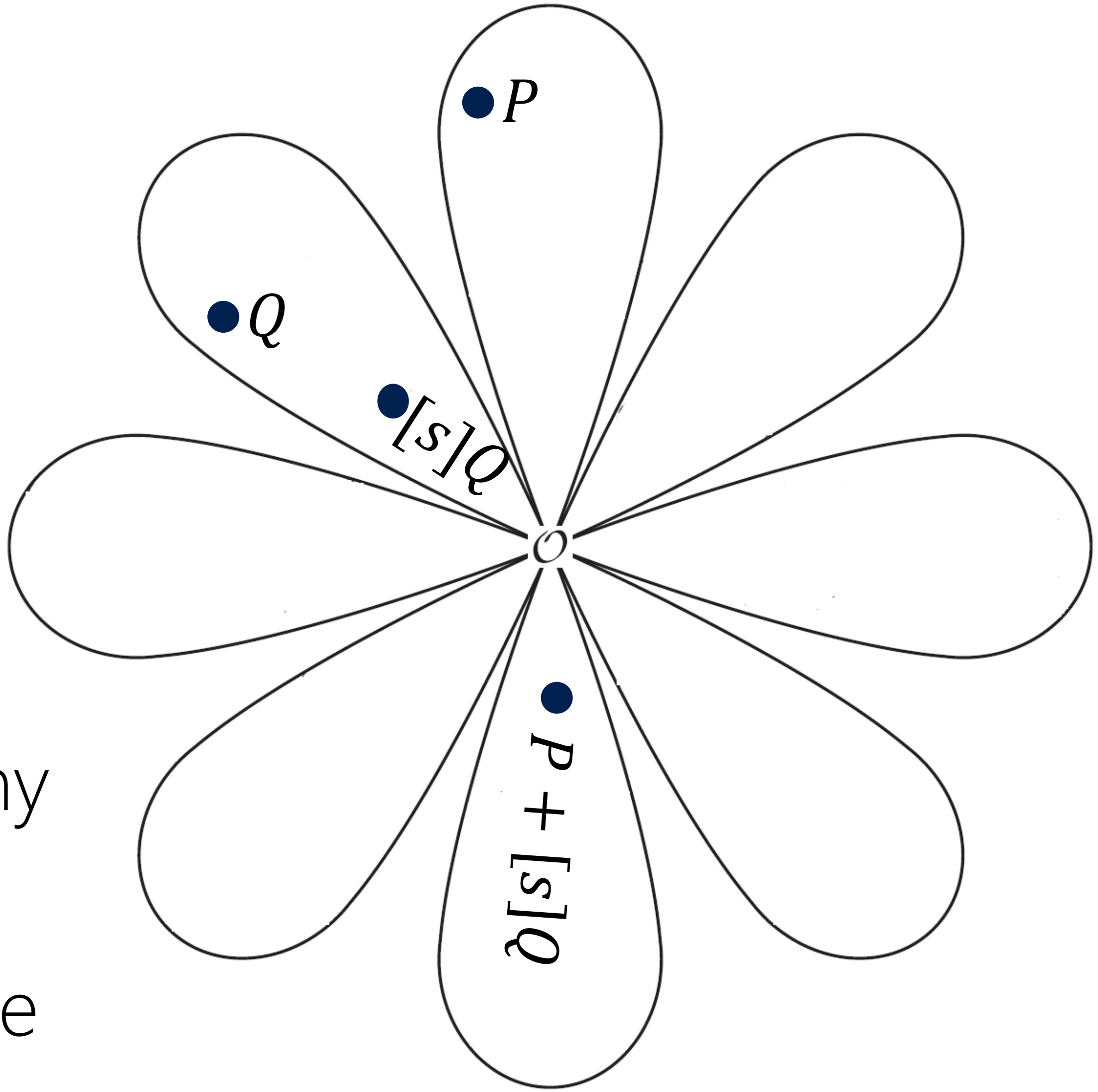
- Need two-dimensional basis to span two-dimensional torsion

- Every different s now gives a different order n subgroup, i.e., kernel, i.e. isogeny

- Composite same thing, just uglier picture

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

(n prime depicted below)
$n + 1$ cyclic subgroups order n



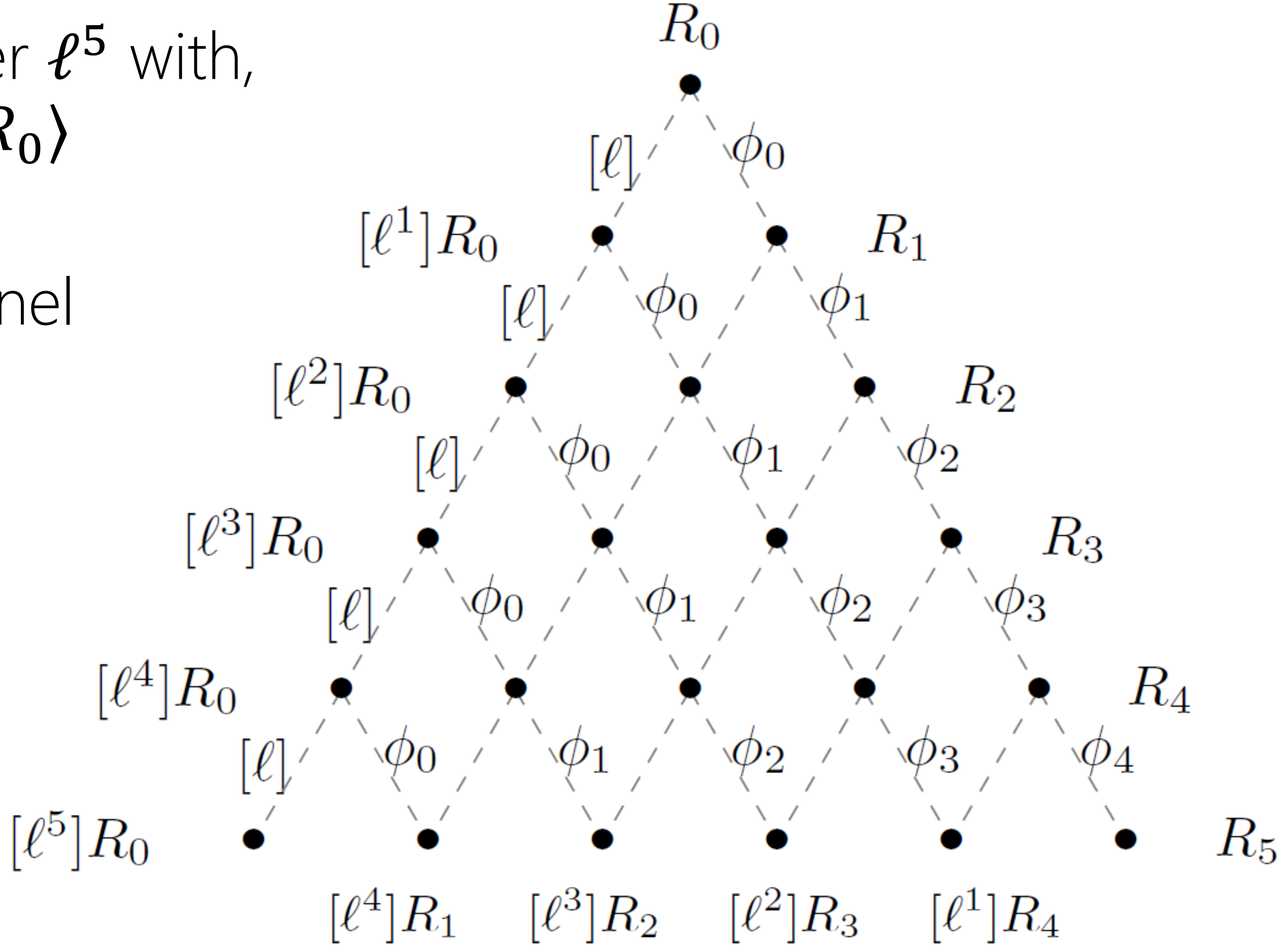
Exploiting smooth degree isogenies

- Computing isogenies of prime degree ℓ at least $O(\ell)$, 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 ℓ^e for $\ell \in \{2,3\}$

Exploiting smooth degree isogenies

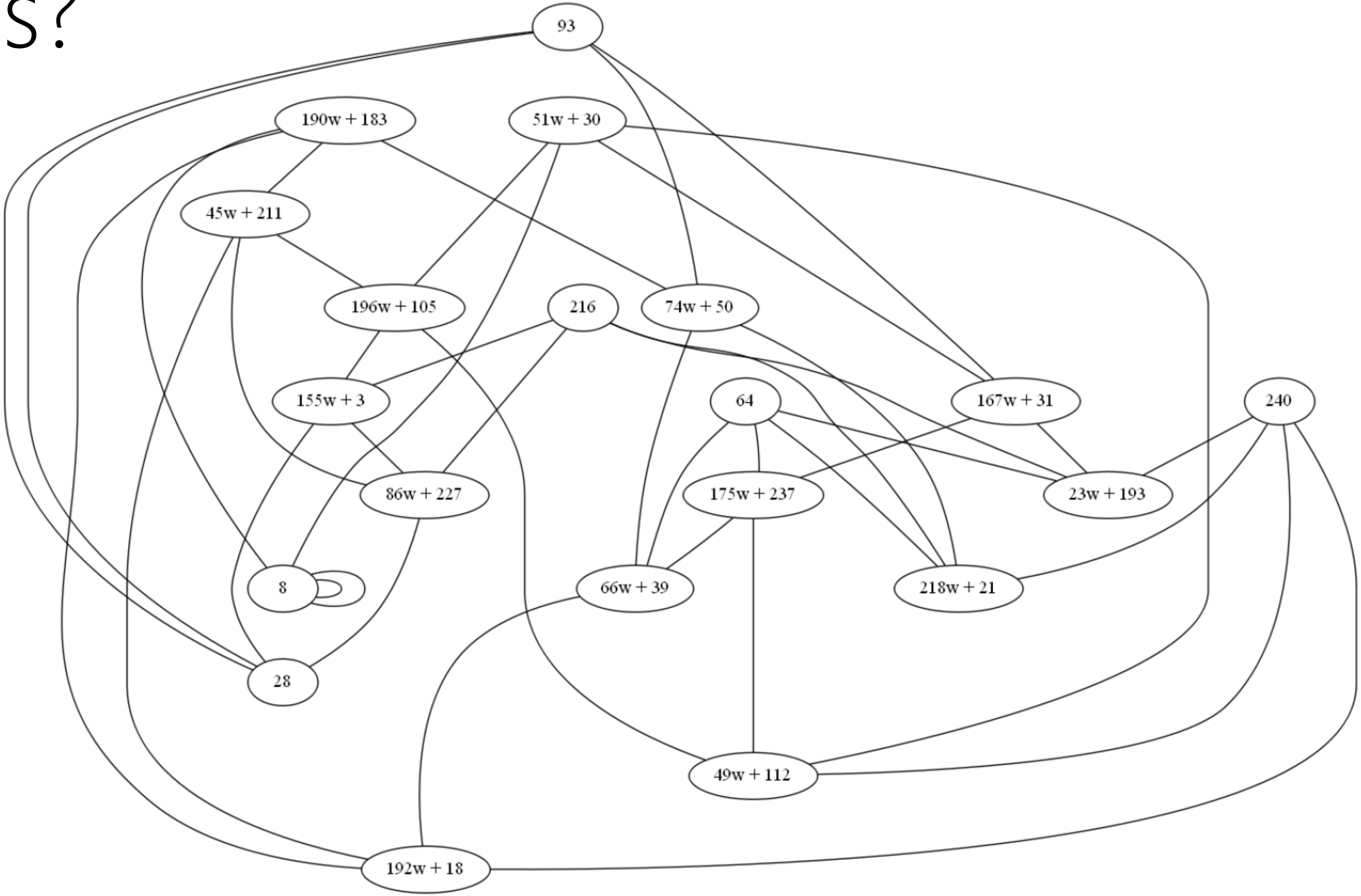
- Suppose our secret point R_0 has order ℓ^5 with, e.g., $\ell \in \{2,3\}$, we need $\phi : E \to E/\langle R_0 \rangle$
- Could compute all ℓ^5 elements in kernel (but only because exp is 5)
- Better to factor $\phi = \phi_4\phi_3\phi_2\phi_1\phi_0$, where all ϕ_i have degree ℓ, and

$$\phi_0 = E_0 \to E_0/\langle [\ell^4]R_0 \rangle,\ R_1 = \phi_0(R_0);$$
$$\phi_1 = E_1 \to E_1/\langle [\ell^3]R_1 \rangle,\ R_2 = \phi_1(R_1);$$
$$\phi_2 = E_2 \to E_2/\langle [\ell^2]R_2 \rangle,\ R_3 = \phi_2(R_2);$$
$$\phi_3 = E_3 \to E_3/\langle [\ell^1]R_3 \rangle,\ R_4 = \phi_3(R_3);$$
$$\phi_4 = E_4 \to E_4/\langle R_4 \rangle.$$



(credit DJP'14 for picture, and for a much better way to traverse the tree)

Questions?



93
190w + 183
51w + 30
45w + 211
196w + 105
216
74w + 50
155w + 3
64
167w + 31
240
86w + 227
175w + 237
23w + 193
8
66w + 39
218w + 21
28
49w + 112
192w + 18