An introduction to supersingular isogeny-based cryptography

Craig Costello

Summer School on Real-World Crypto and Privacy
June 8, 2017
Šibenik, Croatia

Microsoft®
Research

Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

LUCA DE FEO, DAVID JAO, JÉRÔME PLÛT

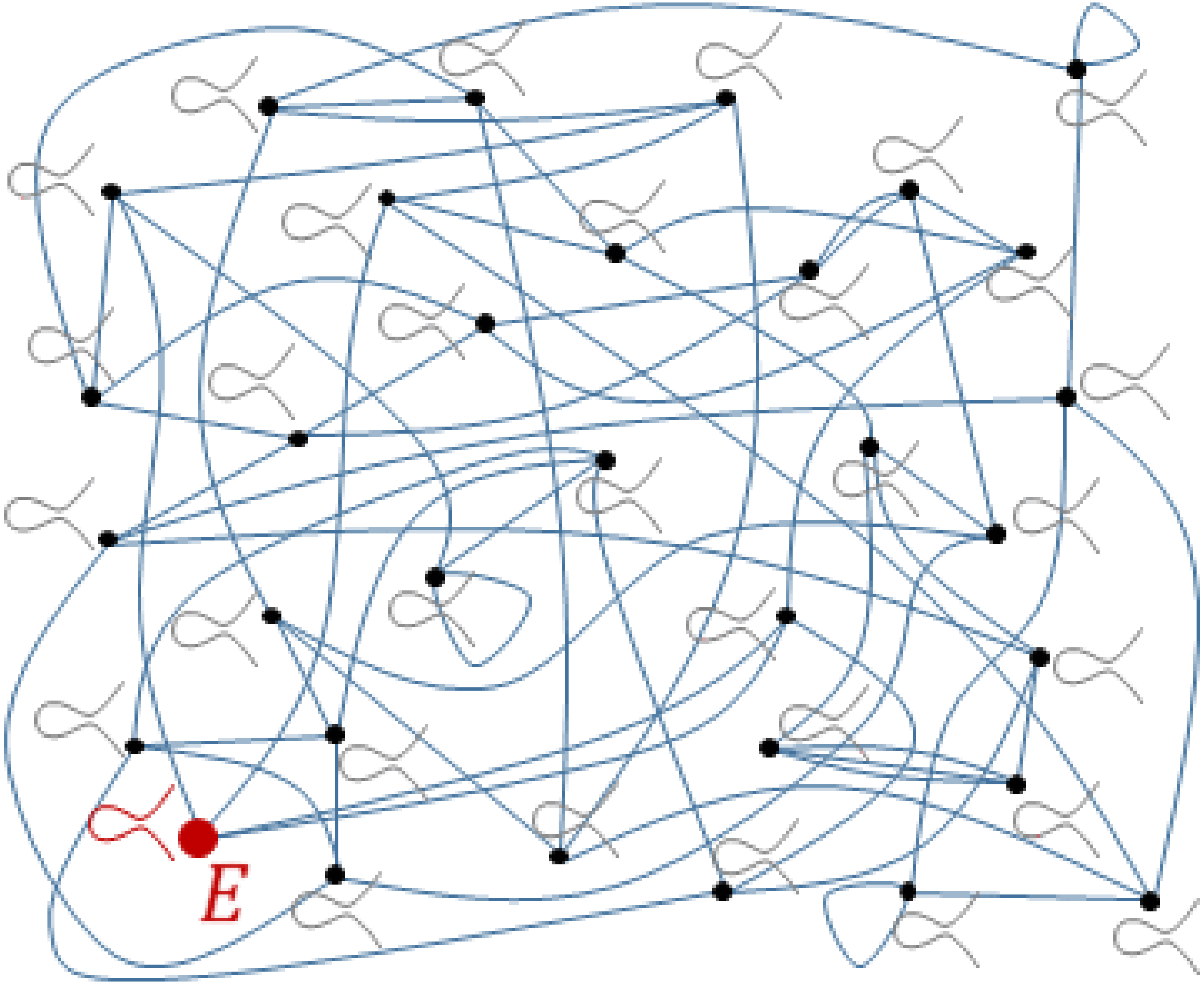
http://eprint.iacr.org/2011/506

Full version of Crypto'16 paper
(joint with P. Longa and M. Naehrig)
http://eprint.iacr.org/2016/413

Full version of Eurocrypt'17 paper
(joint with D. Jao, P. Longa, M. Naehrig, D. Urbanik, J. Renes)
http://eprint.iacr.org/2016/963

Preprint of recent work on flexible SIDH
(joint with H. Hisil)
http://eprint.iacr.org/2017/504

SIDH library v2.0
https://www.microsoft.com/en-us/research/project/sidh-library/



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

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

Diffie-Hellman(ish) 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: 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., $E' \colon y^2 = x^3 + au^2x + bu^3$ 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:
$$n : E \to E, \qquad P \mapsto [n]P$$

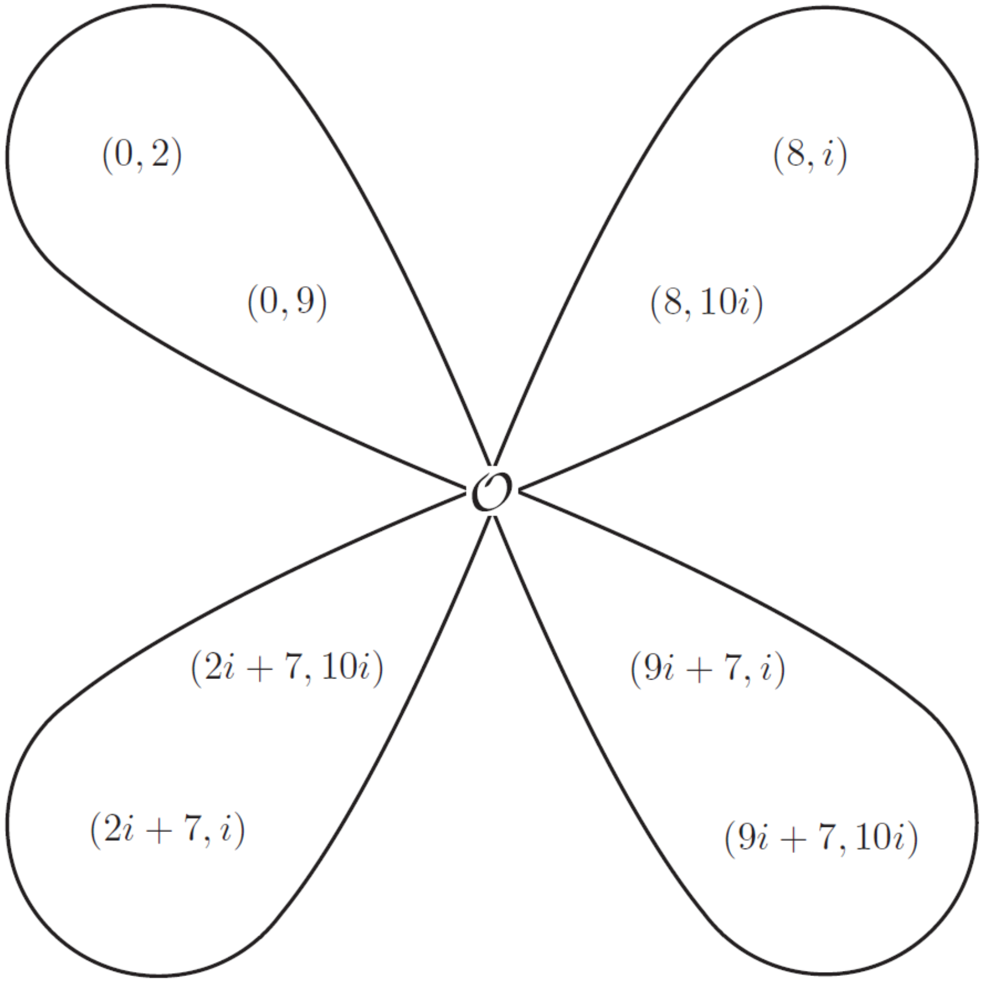
- The n-torsion subgroup is the kernel of $[n]$
$$E[n] = \{P \in E(\overline{K}) : \ [n]P = \infty\}$$

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

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

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

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

And where ϕ maps (x, y) to

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

Velu's formulas

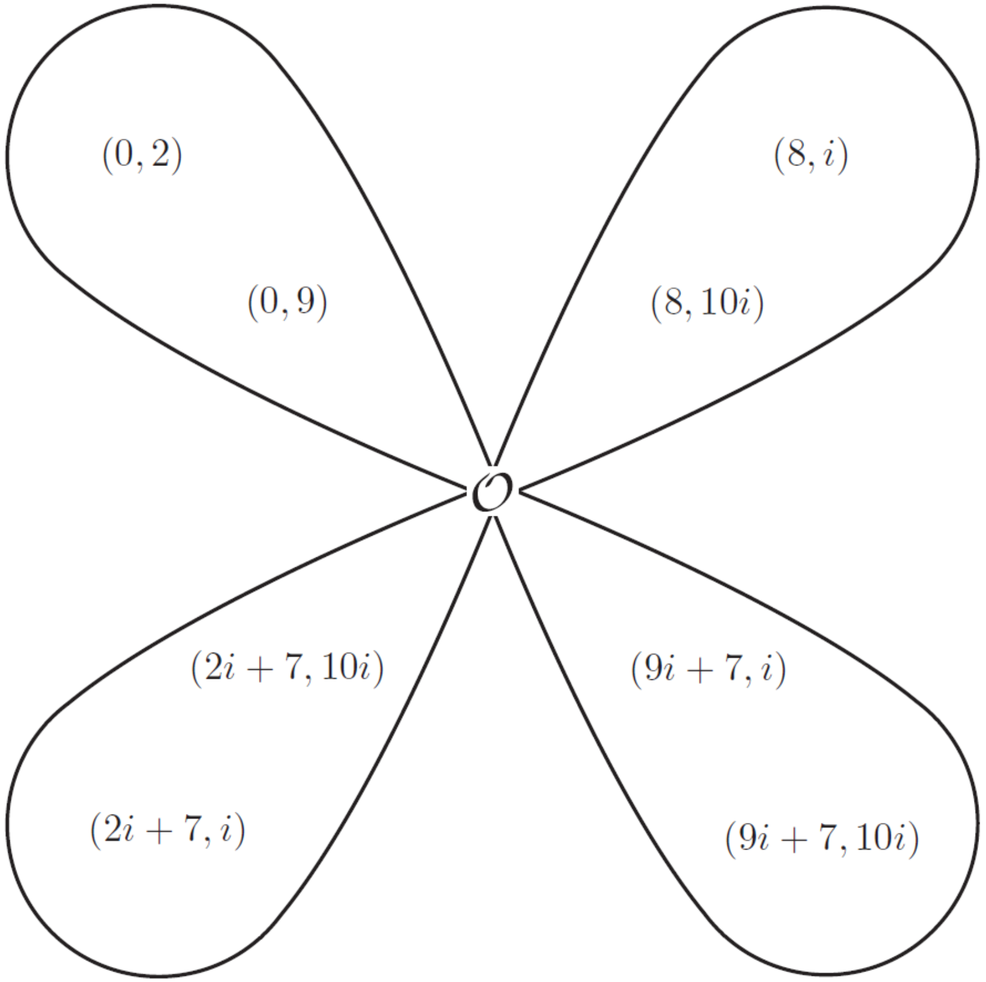
Given curve coefficients a, b for E, and **all** of the x-coordinates x_i of the subgroup $G \in E$, Velu's formulas output a', b' for E', and the map

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

Example, cont.

$$G = E[3]$$

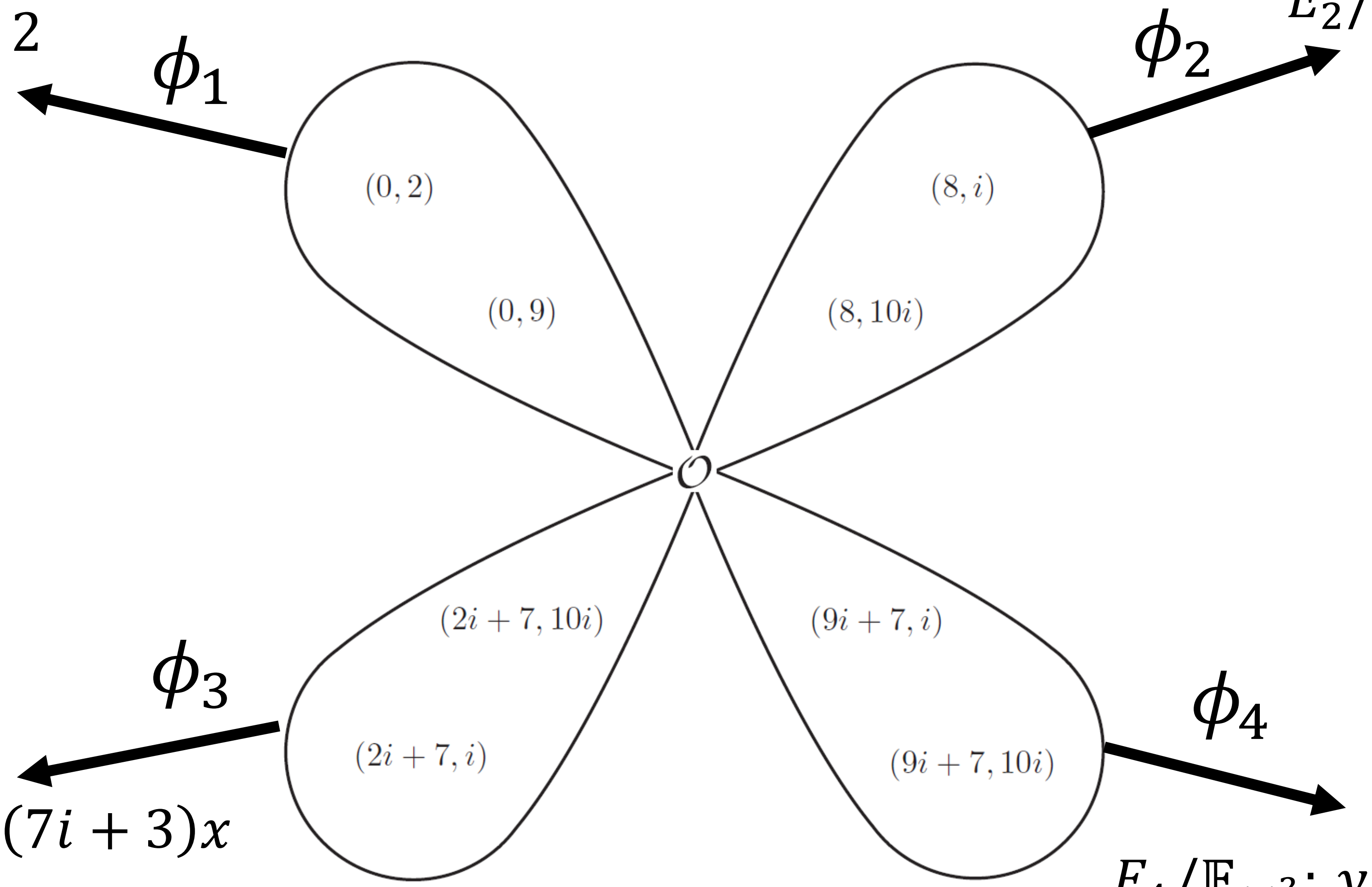
- Recall $E/\mathbb{F}_{11}: y^2 = x^3 + 4$ with $\#E(\mathbb{F}_{11}) = 12$
- Consider $[3] : E \to E$, the multiplication-by-3 endomorphism
- $G = \ker([3])$, which is not cyclic
- Conversely, given the subgroup G, the unique isogeny ϕ with $\ker(\phi) = G$ turns out to be the endormorphism $\phi =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



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

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

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



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

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

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: $q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$ (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 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 $X(S_{p^2}, \ell)$

E.g. a supersingular isogeny graph

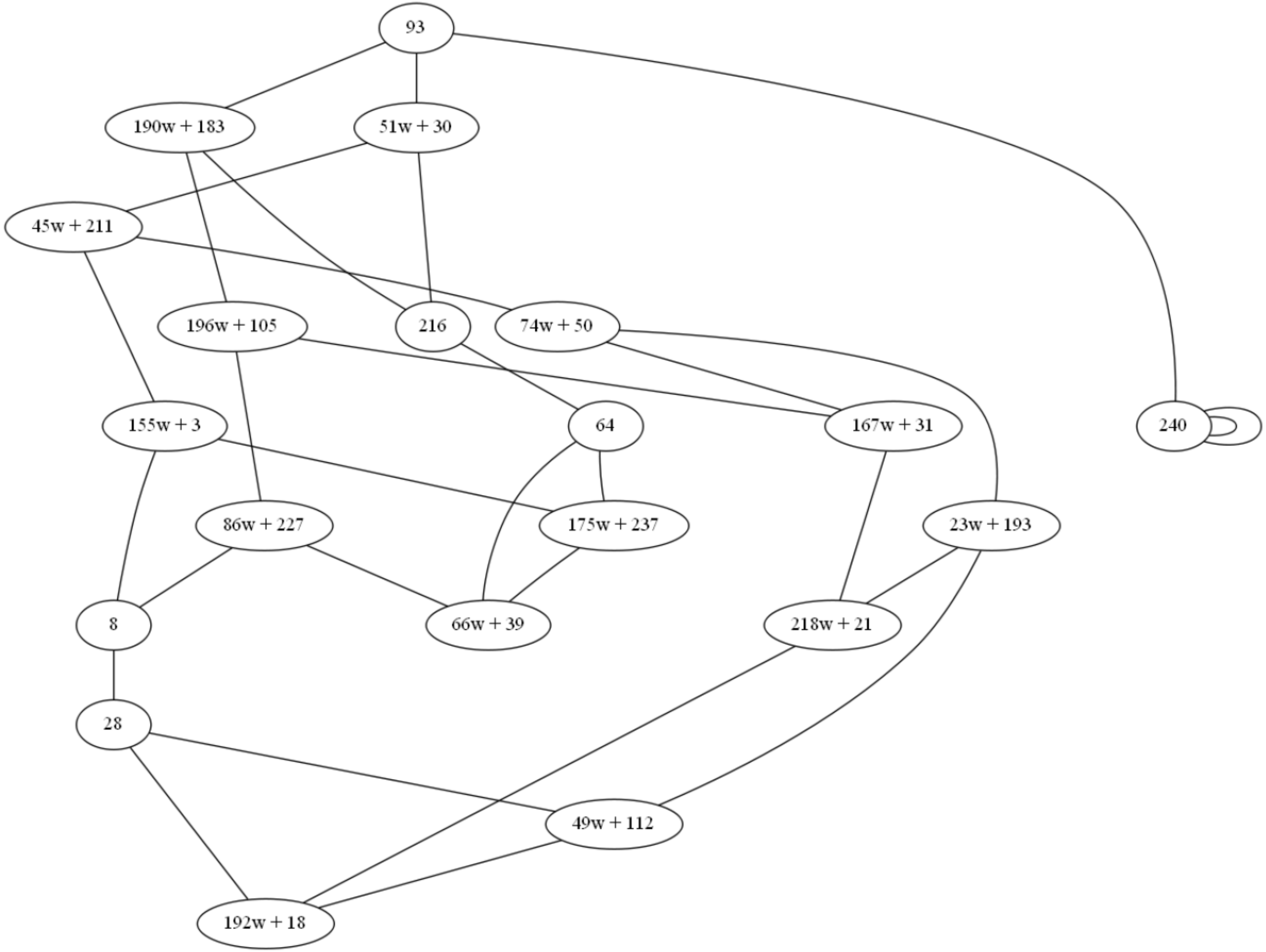
- Let $p = 241$, $\mathbb{F}_{p^2} = \mathbb{F}_p[w] = \mathbb{F}_p[x]/(x^2 - 3x + 7)$

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

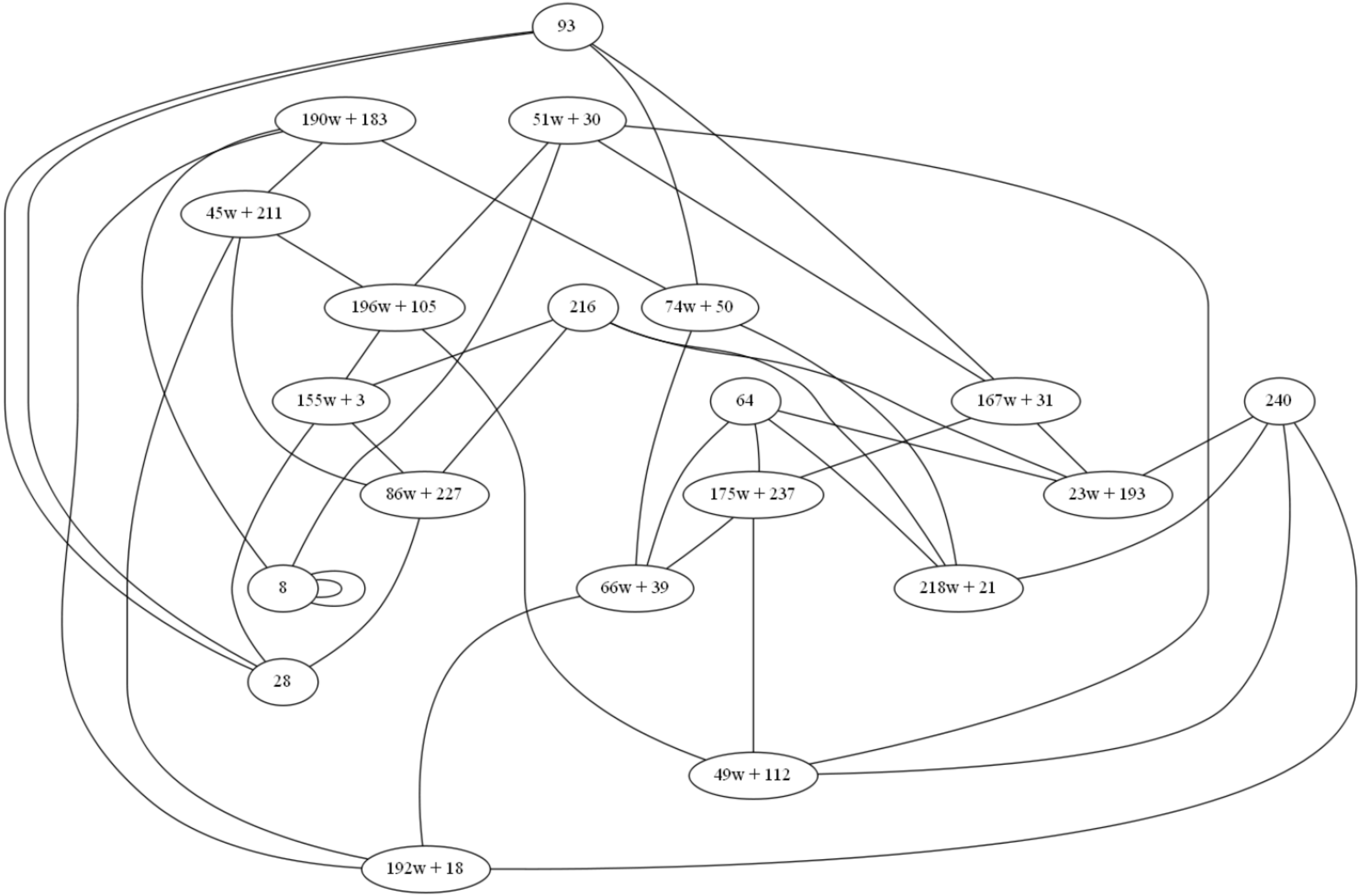
- $S_{p^2} = \{93,\ 51w + 30,\ 190w + 183,\ \ 240,\ 216,\ 45w + 211,\ 196w + 105,\ 64,\ 155w + 3,\ 74w + 50,\ \ 86w + 227,\ 167w + 31,\ 175w + 237,\ 66w + 39,\ 8,\ 23w + 193,\ 218w + 21,\ 28,\ 49w + 112,\ 192w + 18\}$

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

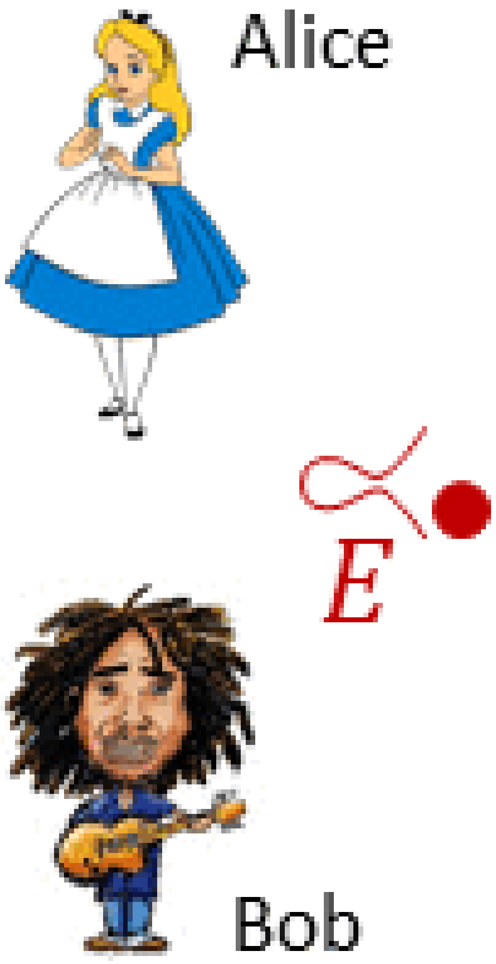
SIDH: history

- **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

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

SIDH: in a nutshell

params public private

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

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

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

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

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

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

- 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

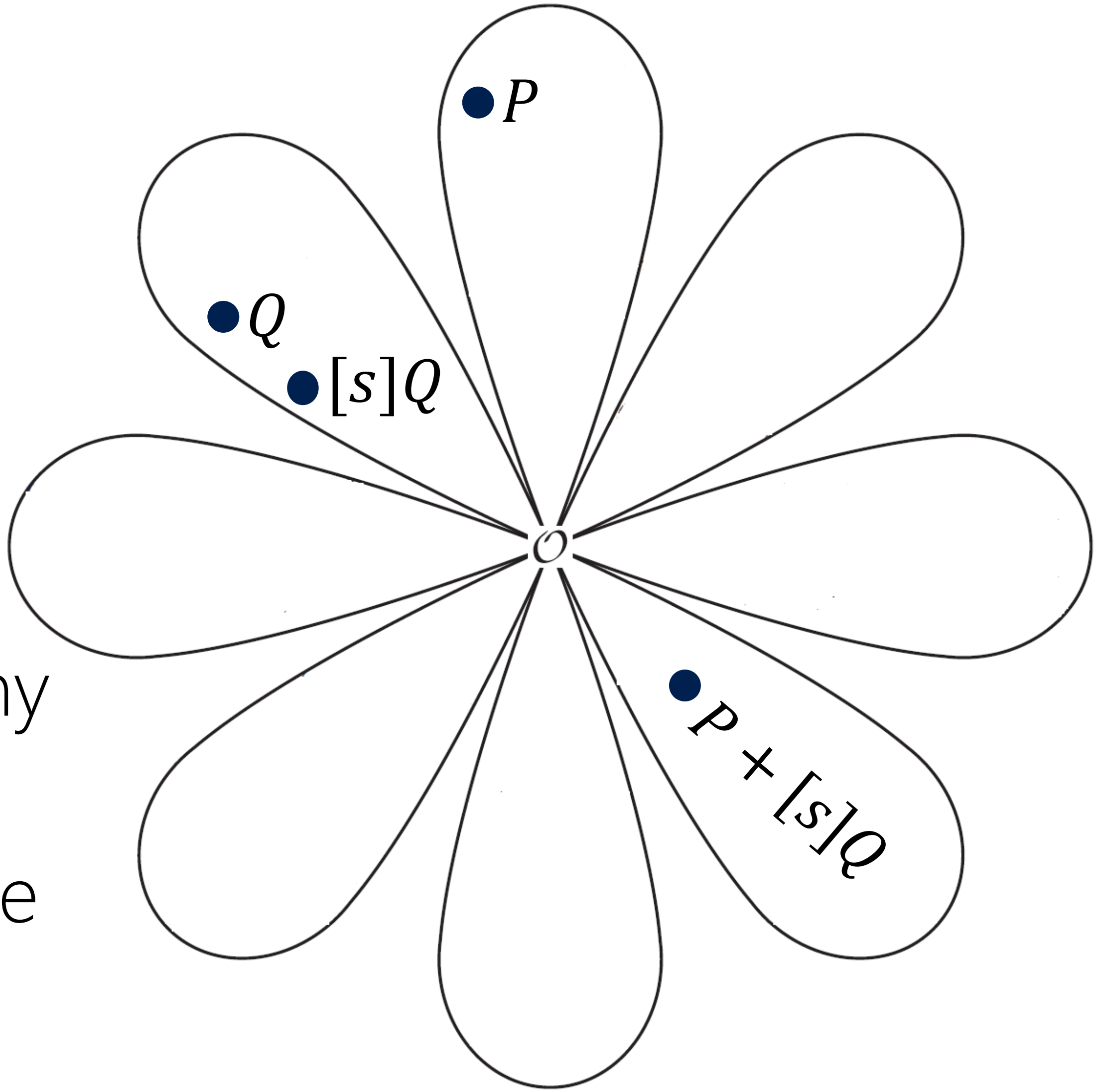
- Need two-dimensional basis to span two-dimensional torsion

- 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

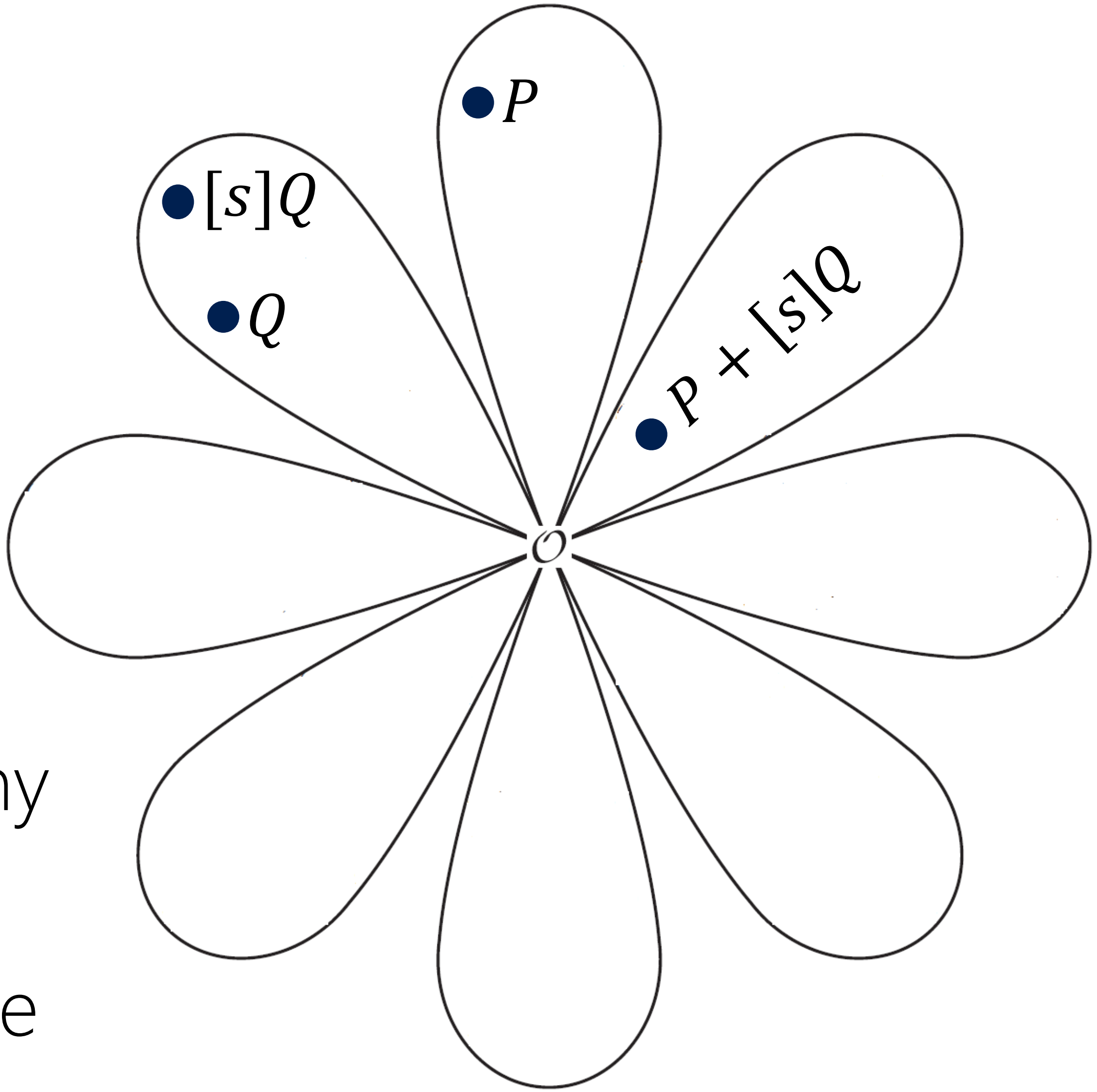
- Need two-dimensional basis to span two-dimensional torsion

- 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

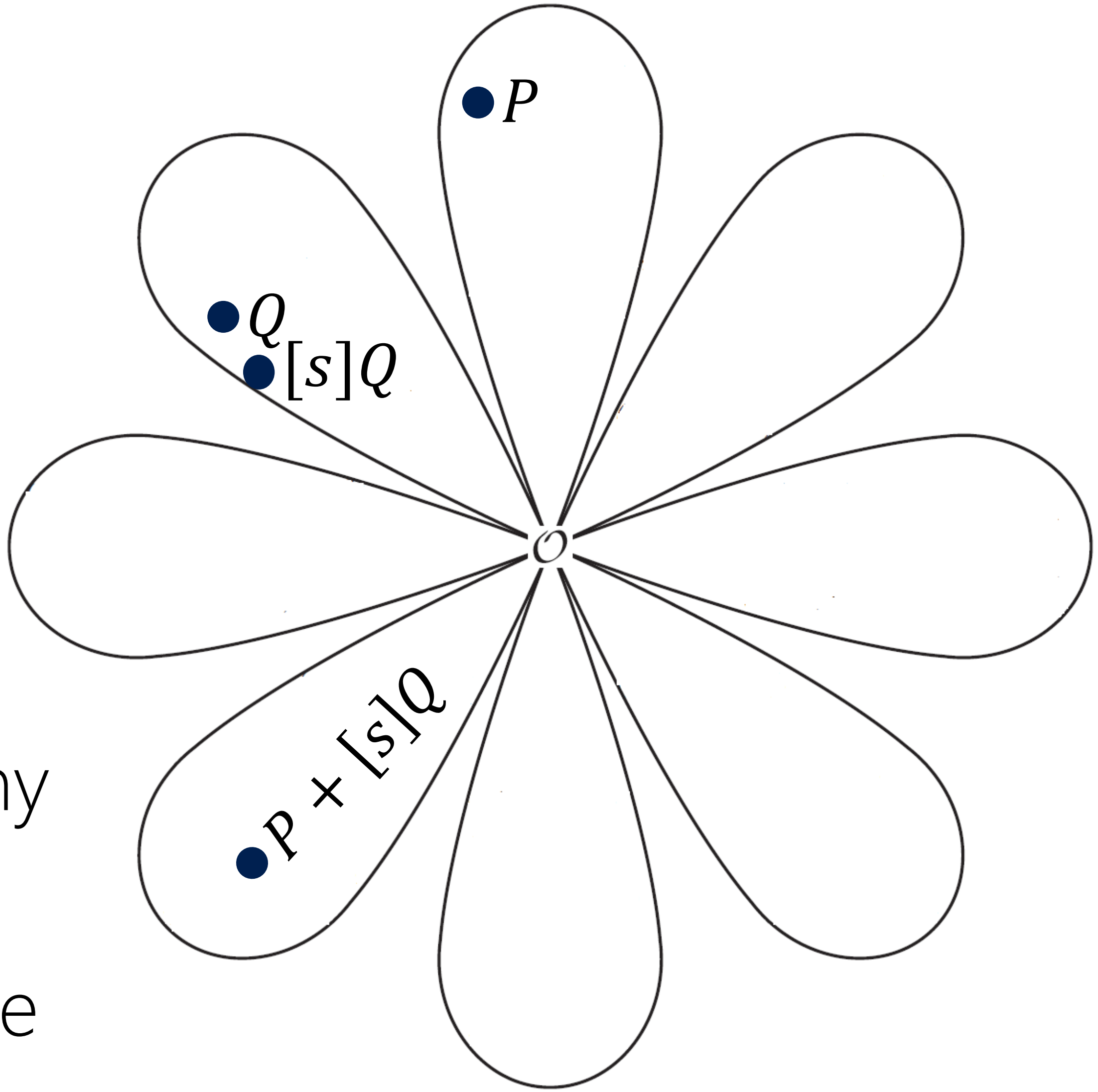
- Need two-dimensional basis to span two-dimensional torsion

- 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



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

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

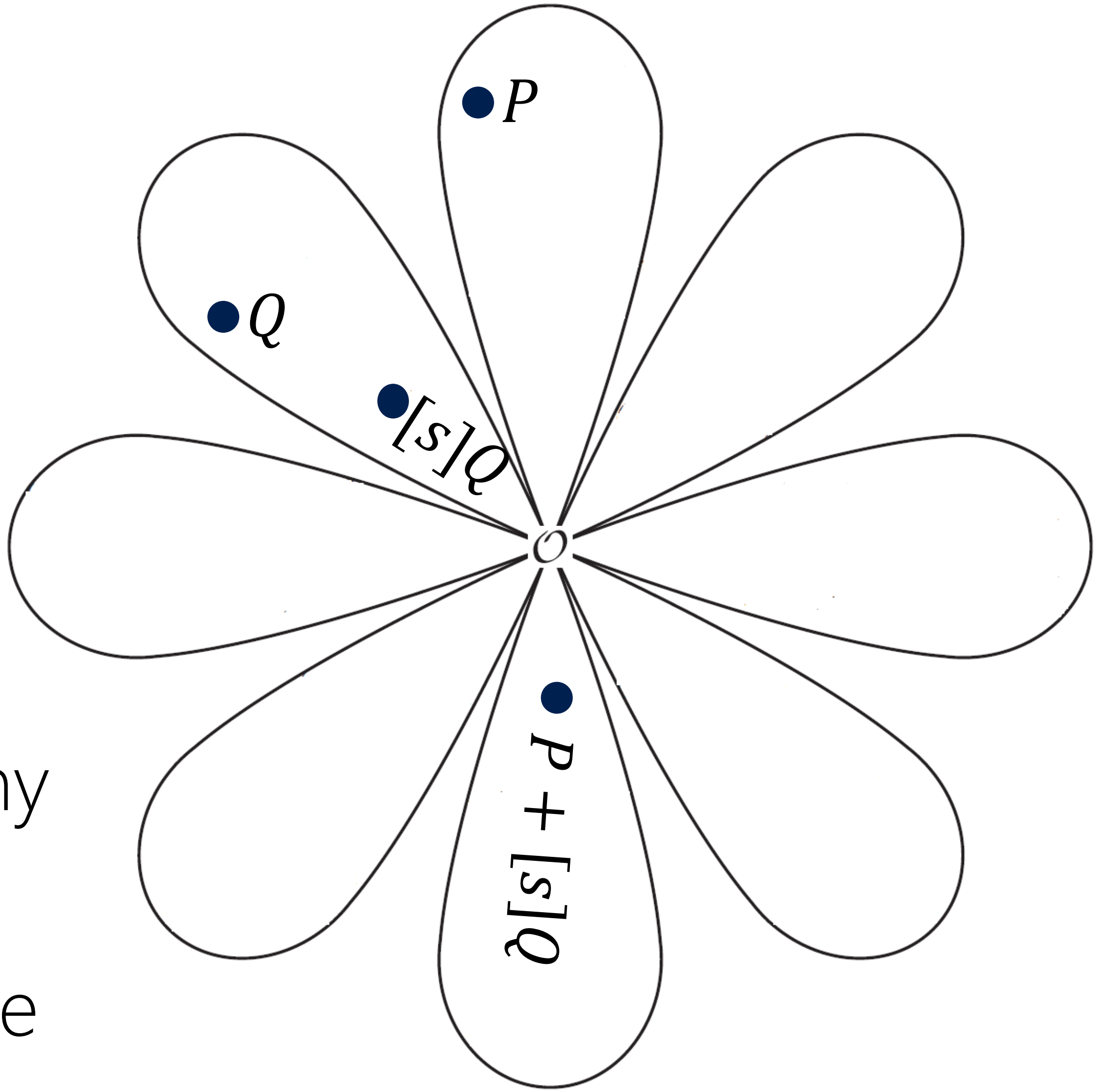
- Why $E' = E/\langle P + [s]Q \rangle$, etc?

- 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



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 $\ell \in \{2,3\}$

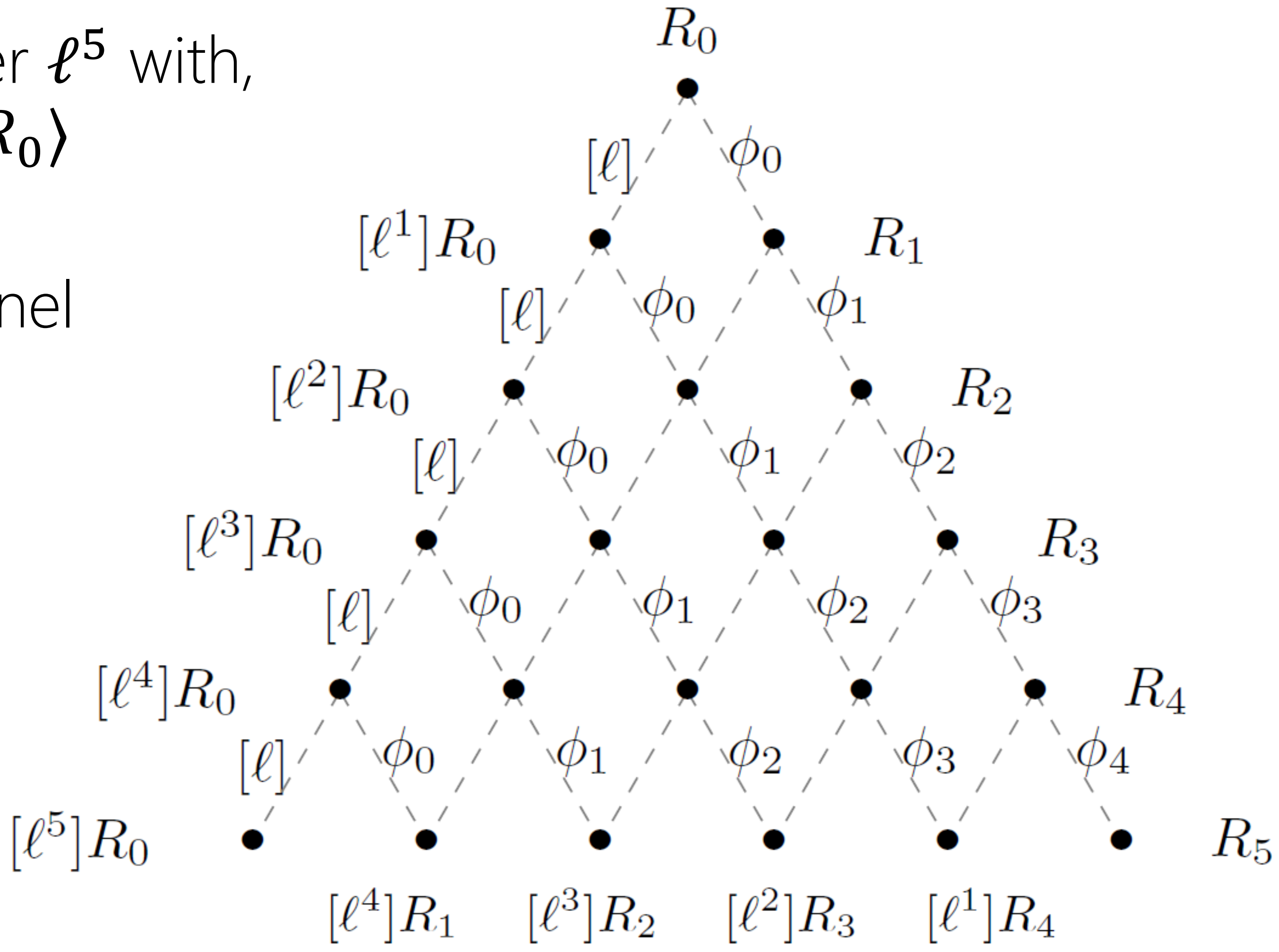
Exploiting smooth degree isogenies

- 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)

SIDH: security

- **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

(Our) parameters

params public private

$$p = 2^{372}3^{239} - 1$$

$p \approx 2^{768}$ gives $\approx$ 192 bits classical and 128 bits quantum security against best known attacks

$$E_0 / \mathbb{F}_{p^2} : y^2 = x^3 + x$$

$$\#E_0 = (p+1)^2 = (2^{372}3^{239})^2$$

Easy ECDLP

$$P_A, P_B \in E_0(\mathbb{F}_p),\ Q_A = \tau(P_A),\ Q_B = \tau(P_B)$$

376 bytes

48 bytes

$$s_A, s_B \in \mathbb{Z}$$

$$\mathrm{PK} = [x(P), x(Q), x(Q-P)] \in \left(\mathbb{F}_{p^2}\right)^3$$

564 bytes

188 bytes

$$j(E_{AB}) \in \mathbb{F}_{p^2}$$

Point *and* isogeny arithmetic in $\mathbb{P}^1$

ECDH: move around different points on a fixed curve.

SIDH: move around different points and different curves

$$E_{\mathrm{a,b}}: \quad by^2 = x^3 + ax^2 + x$$

$(x, y) \leftrightarrow (X : Y : Z)$ $\qquad$ $(a, b) \leftrightarrow (A : B : C)$

$$E_{(\mathrm{A:B:C})}: \quad BY^2Z = CX^3 + AX^2Z + CXZ^2$$

The Montgomery B coefficient only fixes the quadratic twist. Can ignore it in SIDH since $j(E) = j(E')$

$\mathbb{P}^1$ point arithmetic (Montgomery): $(X : Z) \mapsto (X' : Z')$

$\mathbb{P}^1$ isogeny arithmetic (this work): $(A : C) \mapsto (A' : C')$

Performance

comparison		our work	prior work
public key size (bytes)	uncompressed	564	768
	compressed	330	385
uncompressed speed (cc x 10^6)	Alice total	90	267
	Bob total	102	274
compressed speed (cc x 10^6)	Alice total	239	6887
	Bob total	263	8514

(see papers for references and benchmarking details)

SIDH vs. lattice "DH" primitives

Name	Primitive	Full DH (ms)	PK size (bytes)
Frodo	LWE	2.600	11,300
NewHope	R-LWE	0.310	1,792
NTRU	NTRU	2.429	1,024
SIDH	Supersingular Isogeny	900	564

Table: ms for full DH round (Alice + Bob) on 2.6GHz Intel Xeon i5 (Sandy Bridge)
See "Frodo" for benchmarking details.

All numbers above are for plain C implementations (e.g., SIDH w. assembly optimizations is 56ms)

Compressed SIDH vs. lattice "DH" primitives

Name	Primitive	Full DH (ms)	PK size (bytes)
Frodo	LWE	2.600	11,300
NewHope	R-LWE	0.310	1,792
NTRU	NTRU	2.429	1,024
SIDH	Supersingular Isogeny	≈ **2390**	330

Compressed SIDH roughly 2-3 slower than uncompressed SIDH.

Further topics and recent work…

Validating public keys

- Issues regarding public key validation: Asiacrypt2016 paper by Galbraith-Petit-Shani-Ti
- NSA countermeasure: “Failure is not an option: standardization issues for PQ key agreement”
- Thus, library currently supports ephemeral DH only
- But all PQ key establishment (codes, lattice) suffer from this

BigMont: a strong SIDH+ECDH hybrid

- No clear frontrunner for PQ key exchange
- Hybrid particularly good idea for (relatively young) SIDH
- Hybrid particularly easy for SIDH

There are exponentially many $\boldsymbol{A}$ such that $E_A\,/\mathbb{F}_{p^2}\colon y^2 = x^3 + Ax^2 + x$ is in the supersingular isogeny class. These are all unsuitable for ECDH.

There are also exponentially many $\boldsymbol{A}$ such that $E_A\,/\mathbb{F}_{p^2}\colon y^2 = x^3 + Ax^2 + x$ is suitable for ECDH, e.g. $\boldsymbol{A = 624450}$.

SIDH vs. SIDH+ECDH hybrid

comparison		SIDH	SIDH+ECDH
bit security (hard problem)	classical	192 (SSDDH)	384 (ECDHP)
	quantum	128 (SSDDH)	128 (SSDDH)
public key size (bytes)		564	658
Speed (cc x 10^6)	Alice key gen.	46	52
	Bob key gen.	52	58
	Alice shared sec.	44	50
	Bob shared sec.	50	57

Colossal amount of classical security almost-for-free (≈ no more code)

Simple, compact, (relatively) efficient isogenies of arbitrary degree

C-Hisil: For odd order $\ell = 2d + 1$ point P on Montgomery curve E, map

$$\phi : E \to E', \quad (x, y) \mapsto (\phi_x(x), y \cdot \phi_x'(x))$$

with

$$\phi_x(x) = x \cdot \prod_{1 \leq i \leq d} \left(\frac{x \cdot x_{[i]P} - 1}{x - x_{[i]P}} \right)^2$$

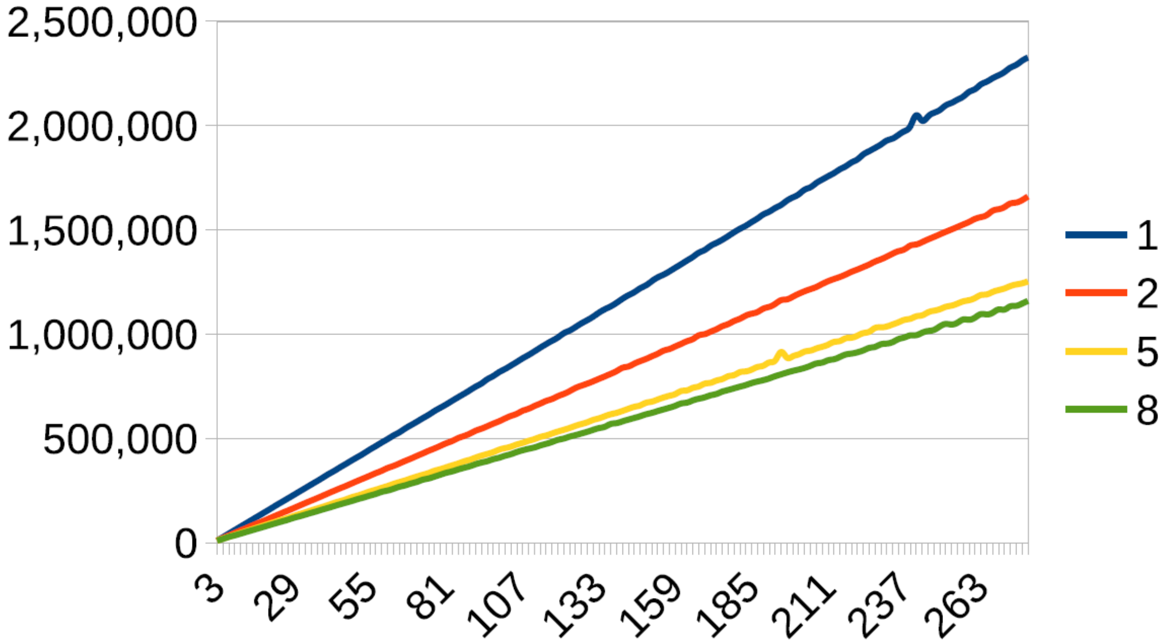
is ℓ-isogeny with $\mathbf{ker}(\phi) = \langle P \rangle$, and moreover, E' is Montgomery curve.

Arbitrary degree isogenies

Need not have $p = 2^i 3^j - 1$, can easily implement

$$p = \left(\prod q_i^{m_i}\right) \cdot \left(\prod r_j^{n_j}\right) - 1$$

with $\mathbf{gcd}\left(\prod q_i, \prod r_j\right) = 1$



Questions?