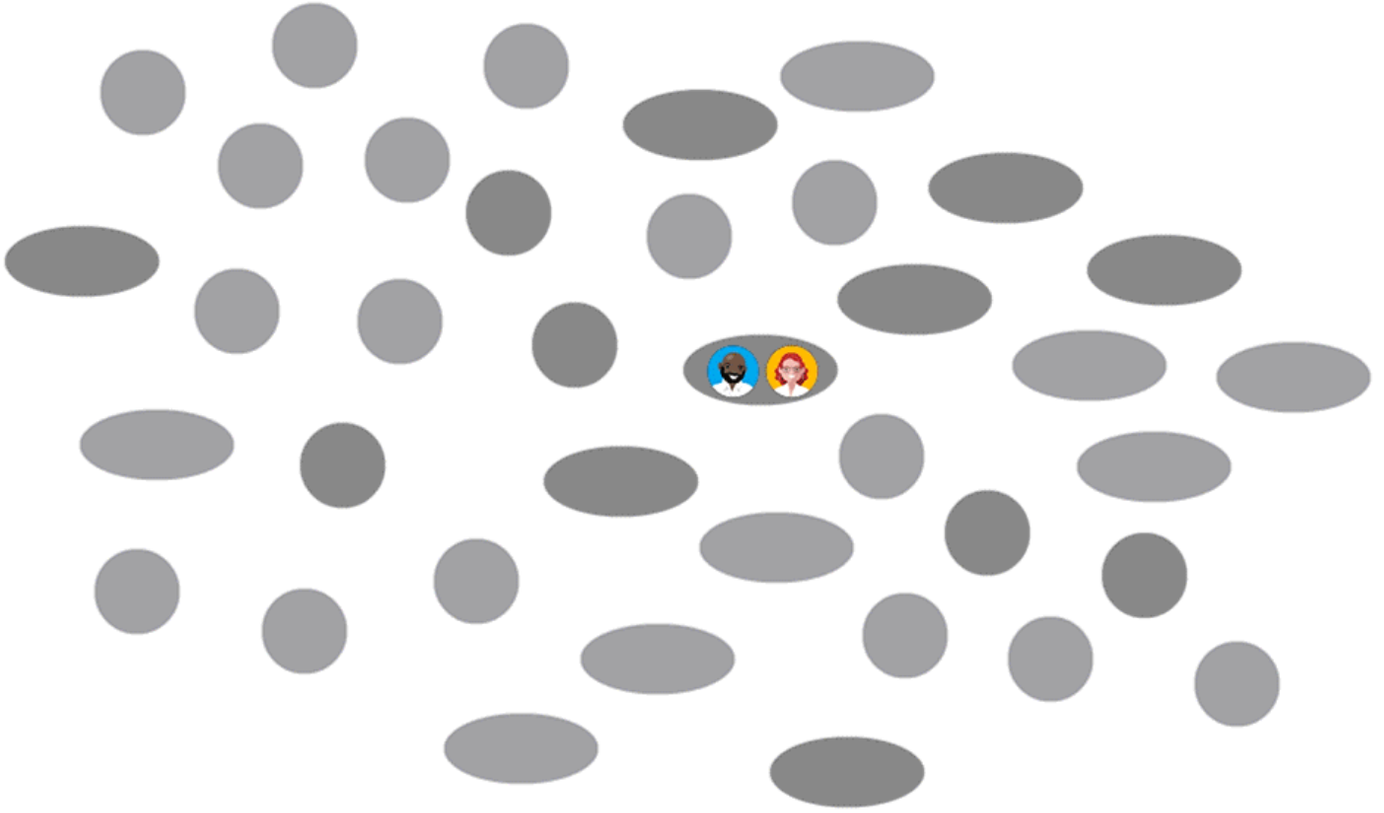
B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion



Microsoft Research

Craig Costello

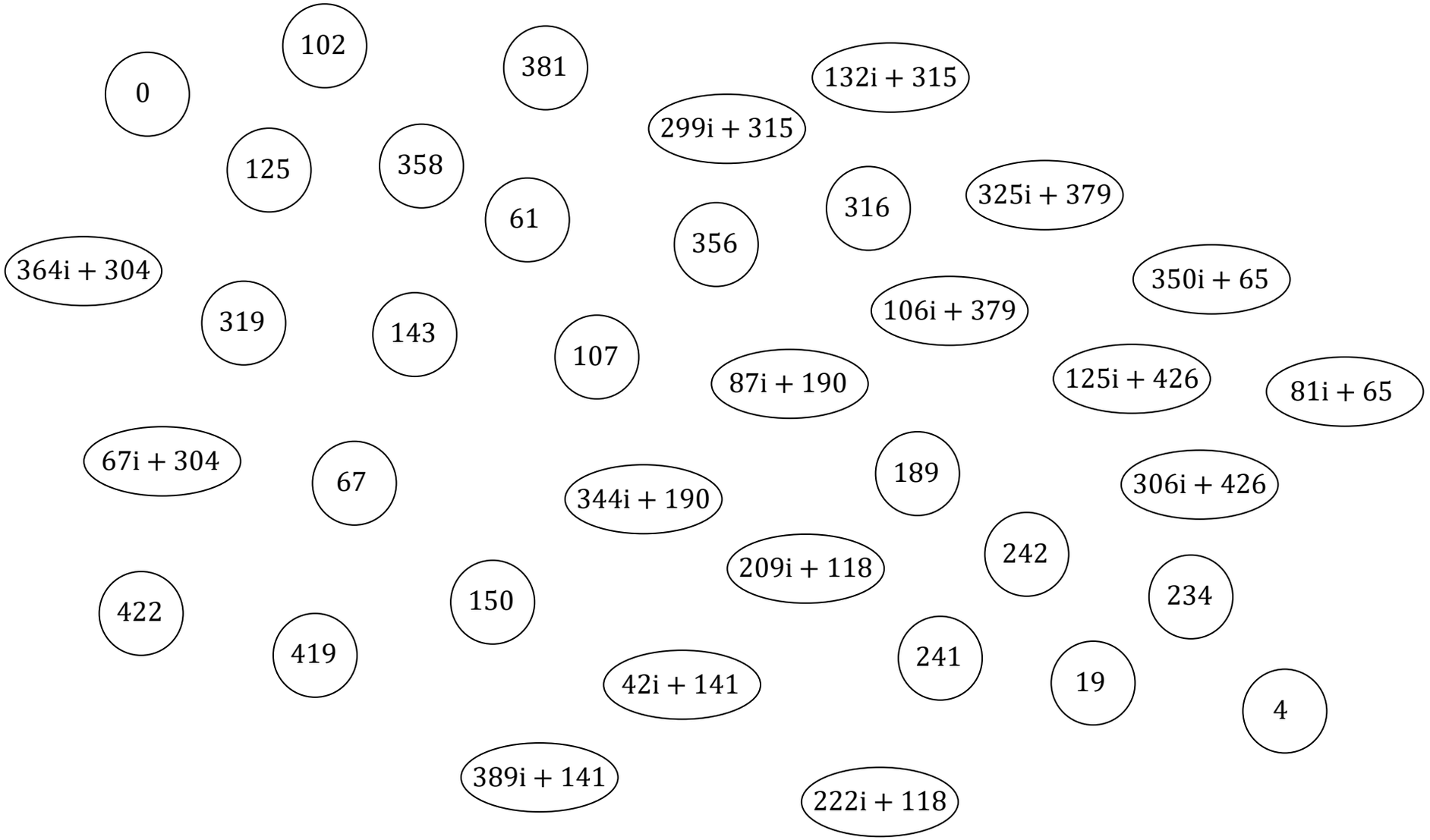
ASIACRYPT 2020

International Association for Cryptologic Research

$$p = 431 = 2^4 3^3 - 1$$

$\mathbb{F}_{p^2} = \mathbb{F}_p(i)$;

$i^2 + 1 = 0$

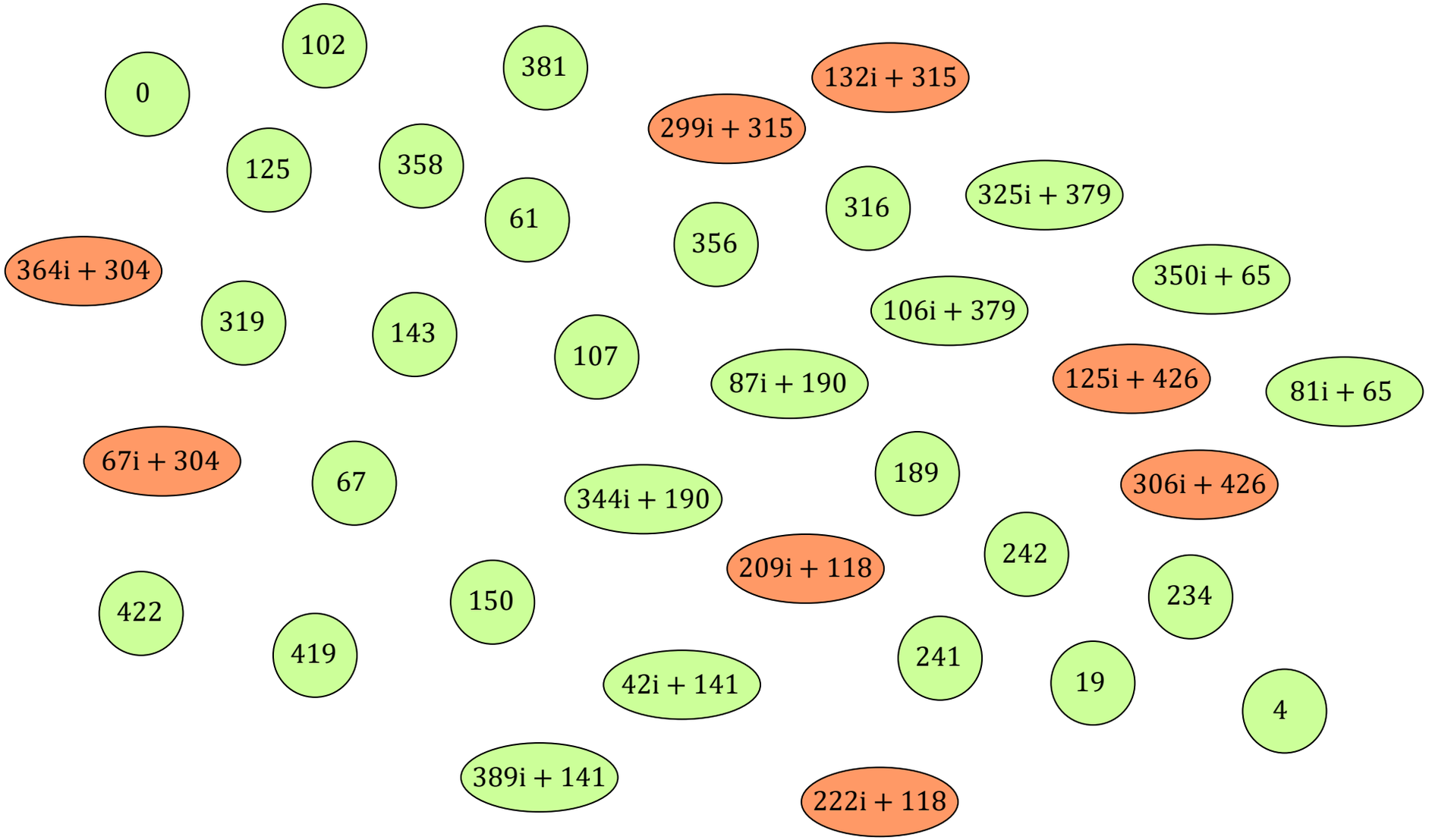


S:=SupersingularInvariants(431);

$$p = 431 = 2^4 3^3 - 1$$

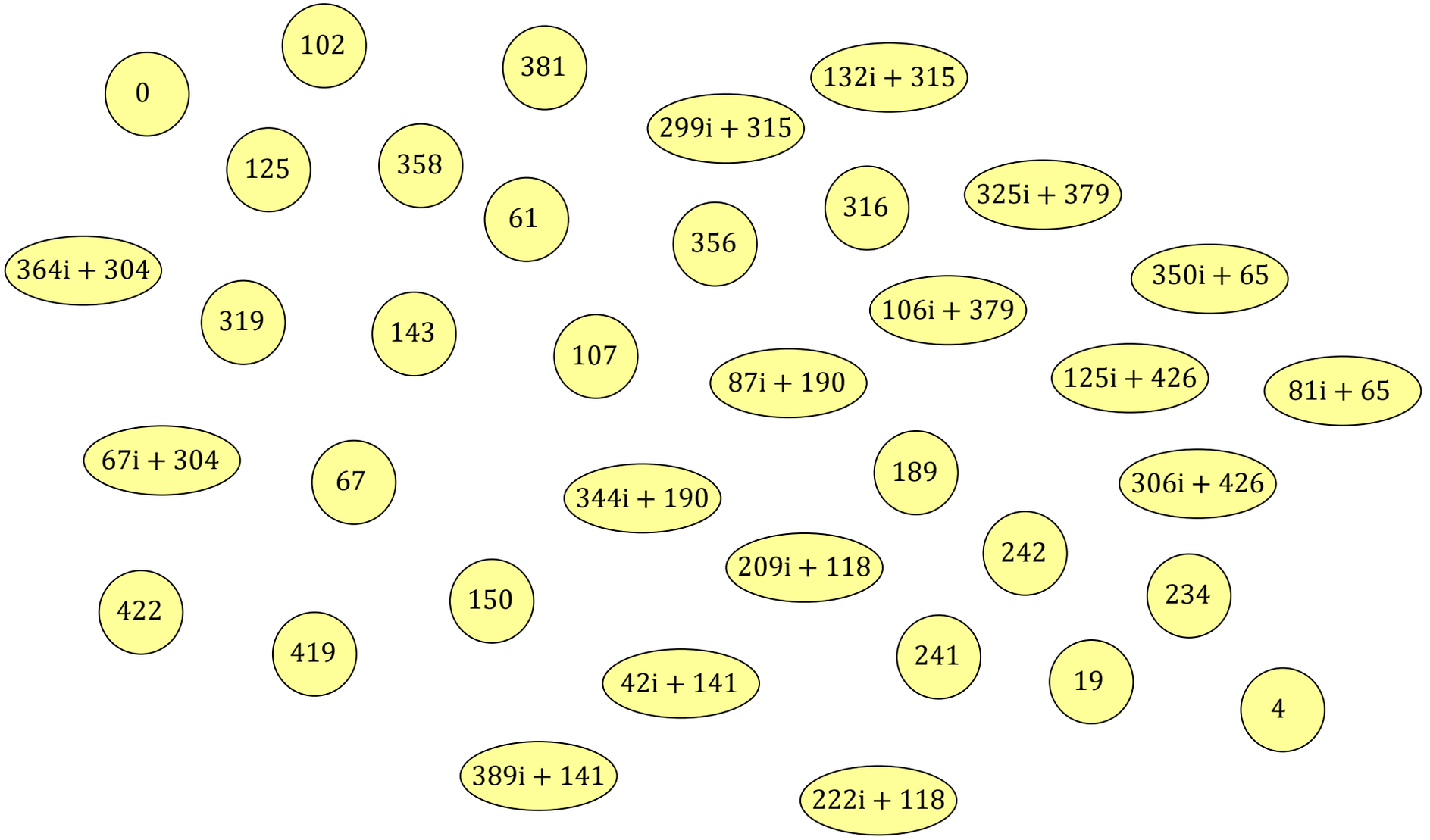
$$\#E = (p+1)^2$$

$$\#E = (p-1)^2$$



#EllipticCurveFromjInvariant(j), j in S

$$\#E = (p \pm 1)^2$$


0
102
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
234
422
150
419
241
19
42i + 141
4
389i + 141
222i + 118

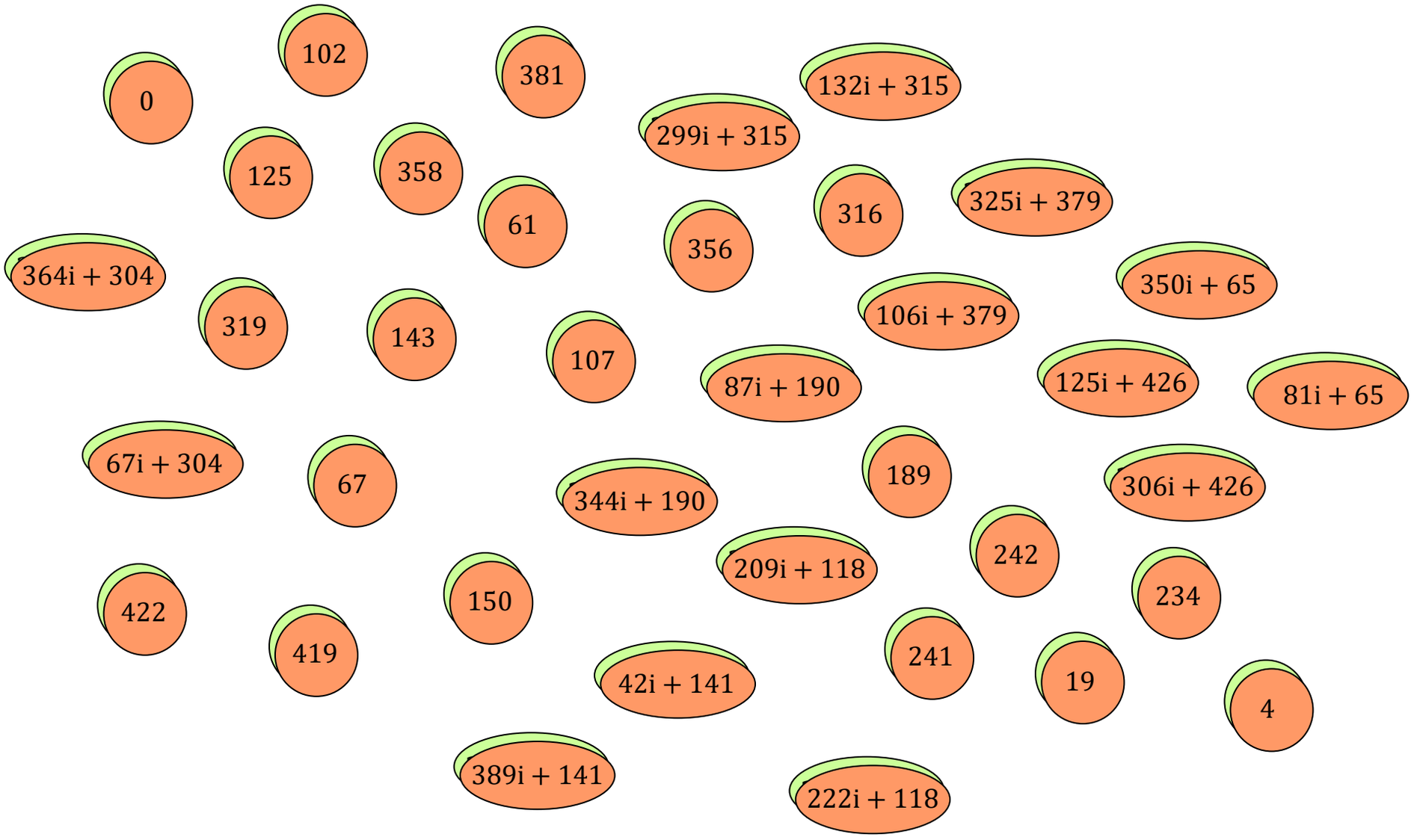
the A-side

$$\#E = (p+1)^2$$

0
102
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
234
422
150
419
241
42i + 141
19
4
389i + 141
222i + 118

the B-side

$$\#E = (p-1)^2$$

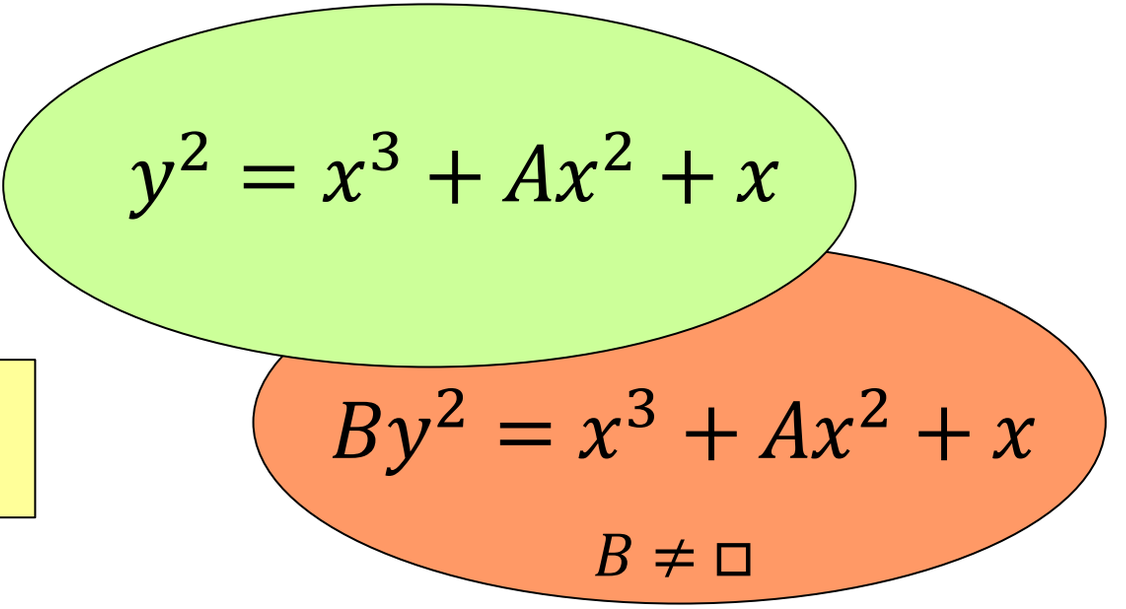


Twist-agnostic Montgomery arithmetic

$[n]\colon (x, -) \mapsto (x', -)$

$\phi : \big((x, -), (A, -)\big) \mapsto \big((x', -), (A', -)\big)$

$j = j(A)$



upshot: no changes to protocol/arithmetic

Smaller fields

- Security of SIDH/SIKE depends on degree of isogeny, not on p
- SIDH/SIKE takes $p = 2^a 3^b - 1$ to squeeze Alice and Bob *into* $p + 1$
- But we can squeeze Alice into $p + 1$ and Bob into $p - 1$
- Take $p + 1 = 2M$ and $p - 1 = 2N$, so $\mathbf{gcd}(M, N) = 1$
- Alice computes M-isogenies, Bob computes N-isogenies
- Can have $M = 2^a$ and $N = 3^b$, but largest such prime is $p = 17$

Twin smooths

- Goal: find p where $p \pm 1$ both smooth
- Equiv.: find $(m, m+1)$ smooth with $2m+1$ prime

- Largest 3-smooth twins $(8,9)$.
- Largest 5-smooth twins $(80,81)$.

⋮

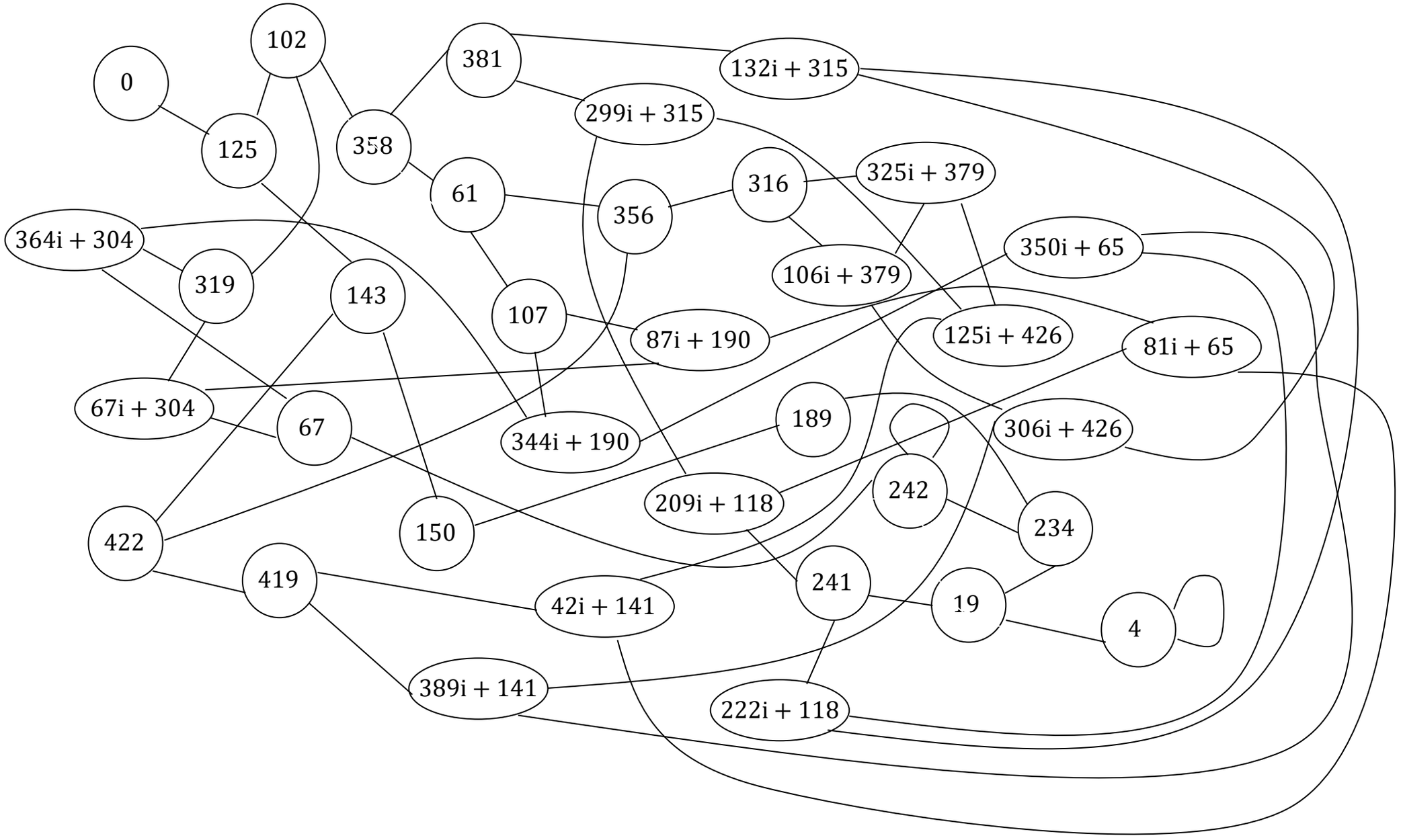
- Largest 113-smooth twins have $m = 193161583770739238340000 \approx 2^{74}$
- Largest 113-smooth twins with prime sum $m = 759541500560601866624 \approx 2^{66}$

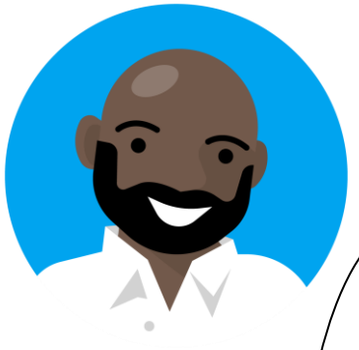
⋮

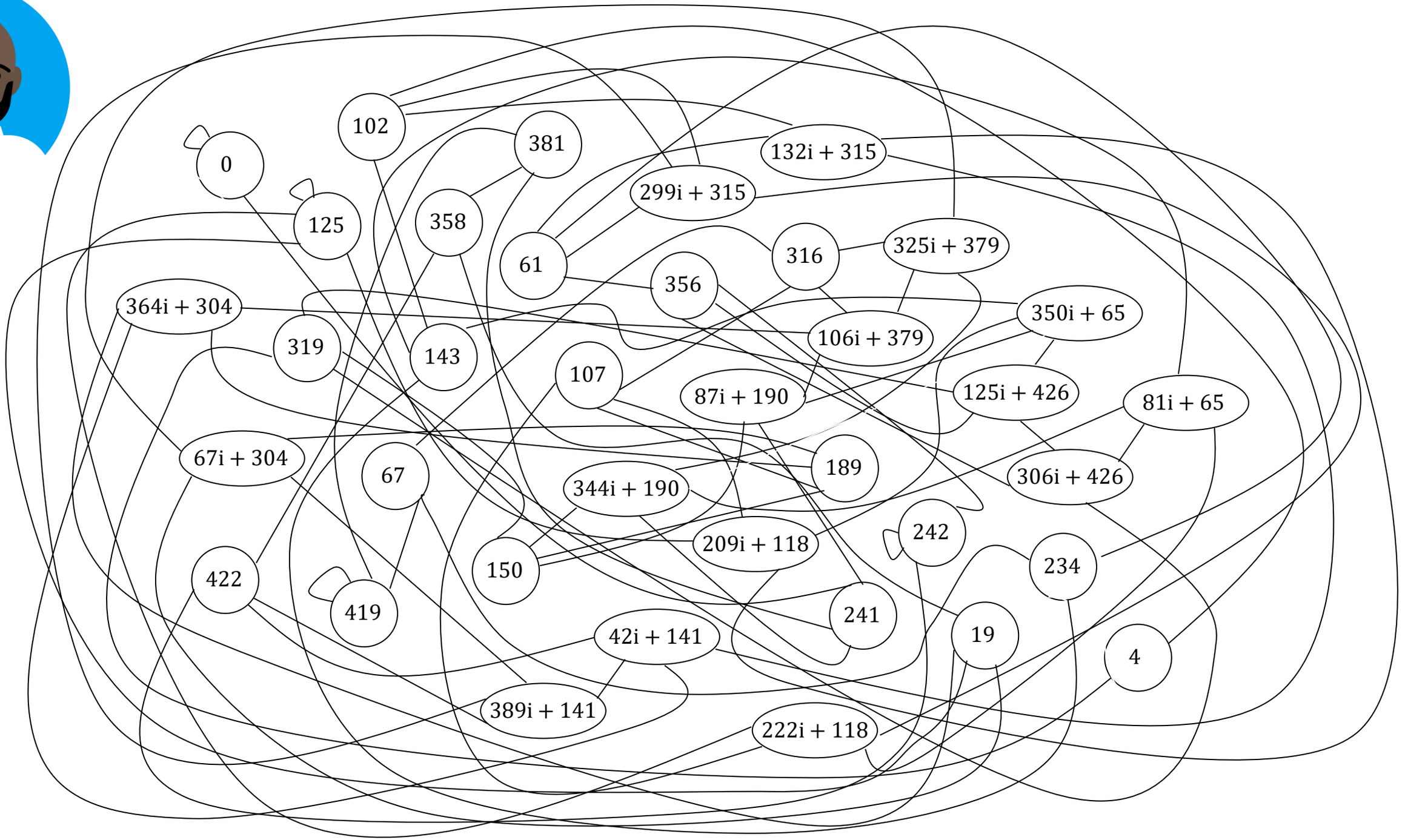
- Largest B-smooth twins requires solving $2^{\pi(B)}$ Pell equations (Störmer/Lehmer)

upshot 1: Alice and Bob can't **both** have prime-power isogenies

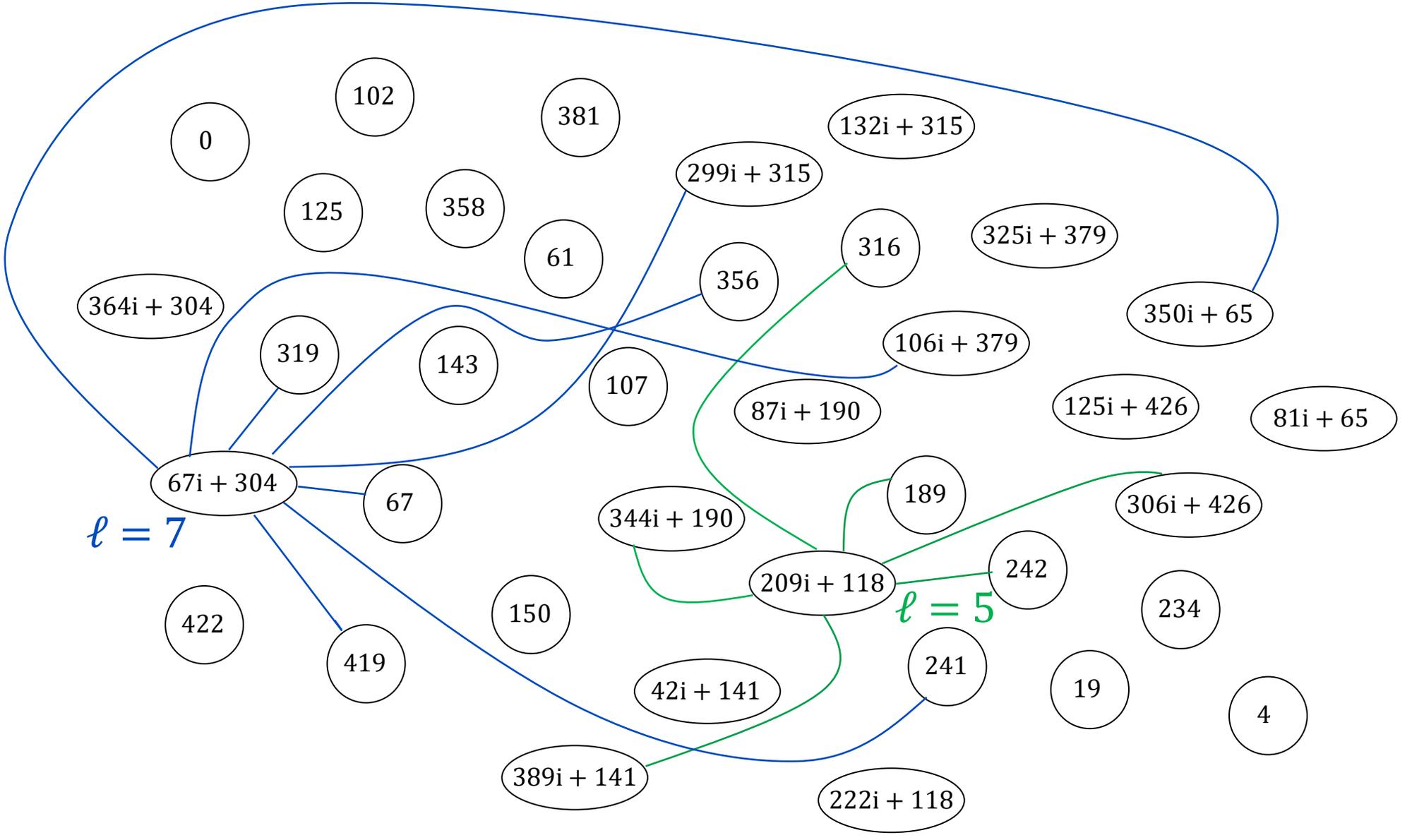
upshot 2: finding optimal (smoothest) parameters non-trivial


0
102
125
358
381
132i + 315
299i + 315
61
356
316
325i + 379
364i + 304
319
143
107
106i + 379
350i + 65
87i + 190
125i + 426
81i + 65
67i + 304
67
344i + 190
189
306i + 426
209i + 118
242
234
422
150
419
42i + 141
241
19
4
389i + 141
222i + 118




0
102
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
150
234
422
419
241
19
42i + 141
4
389i + 141
222i + 118

Non-prime-power isogenies



Conjecture$_{\approx}$: hardness of L-isogeny problem depends on size of L, not its factorisation

Searching for twin smooths

$m \approx 2^{256}$ $B = 2^{16}$

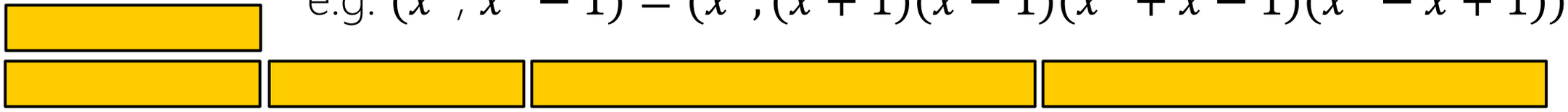
Method 1 (Naïve): search smooth $m \approx 2^{256}$, check $m \pm 1$

Pr(smooth) $\approx 2^{-70}$

Method 2 (XGCD): search smooth coprime $a, b \approx 2^{128}$ set $m = |as|$ and $m + 1 = |bt|$

Pr(smooth) $\approx 2^{-50}$

Method 3 (Power): search $(m, m-1) = (x^n, x^{n-1})$,
e.g. $(x^6, x^6 - 1) = (x^6, (x+1)(x-1)(x^2+x-1)(x^2-x+1))$



Pr(smooth) $\approx 2^{-36.2}$

Better twin smooth searching

[C-Meyer-Naehrig] https://eprint.iacr.org/2020/1283.pdf

search $(m, m-1) = (a(x), b(x))$, a, b completely split

e.g. $a(x) = (x-2)^2(x-21)^2(x-40)^2/2822400$

$b(x) = x(x-5)(x-16)(x-26)(x-37)(x-42)/2822400$

With $u = 36144284257450$

$p = a(u) + b(u) \approx 2^{250}$

$= 1579971331793459093924543296403864959833416422864200413149968739428198012481$

$p + 1 = 2 \cdot 19^6 \cdot 151^2 \cdot 601^2 \cdot 1009^2 \cdot 1103^2 \cdot 1427^2 \cdot 2011^2 \cdot 6599^2 \cdot 7321^2 \cdot 9091^2 \cdot 32191^2$

$p - 1 = 2^6 \cdot 3^3 \cdot 5 \cdot 13 \cdot 17 \cdot 23 \cdot 107 \cdot 149 \cdot 401 \cdot 503 \cdot 599 \cdot 727 \cdot 941 \cdot 977 \cdot 2351 \cdot 3469 \cdot 3779 \cdot 4273 \cdot 5051 \cdot 6211 \cdot 9001 \cdot 11447 \cdot 12589 \cdot 14159 \cdot 14779 \cdot 24919.$

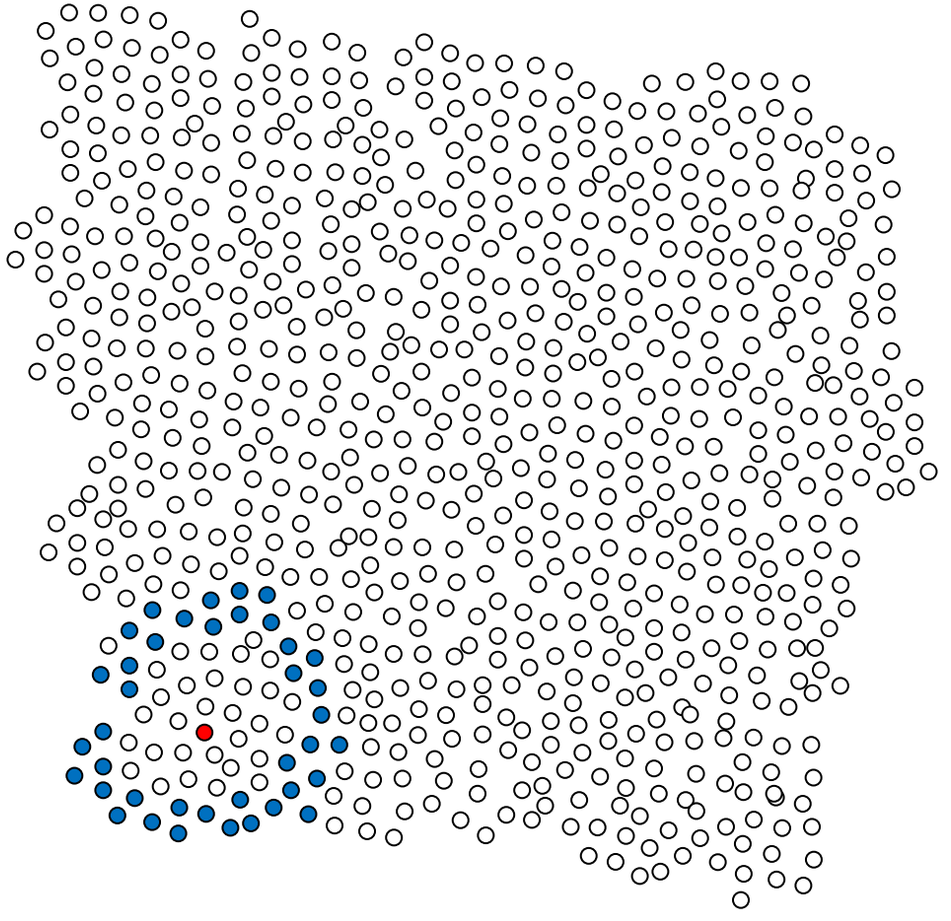
Security of SIDH

Classical*: claw finding $O(p^{1/4})$

Classical: vOW $\approx \frac{1}{\sqrt{m}} \cdot p^{3/8}$

Quantum*: $O(p^{1/6})$

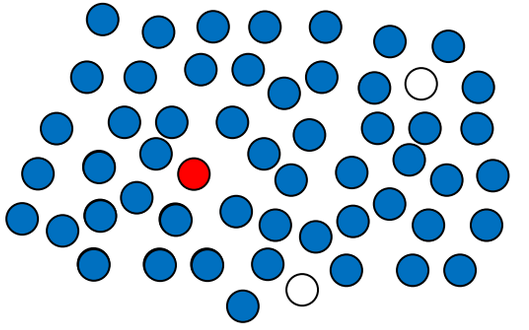
* = big memory



Security of B-SIDH

Classical: Delfs-Galbraith $O(p^{1/2})$

Quantum: Biasse-Jao-Sankar $O(p^{1/4})$



- DG and BJS both memory-free, perfectly parallelizable
- O just hides cost of isogeny oracle
- Nice match to NIST (i.e. AES) classical/quantum security
- e.g. $2^{240} < p < 2^{256}$ for level 1
- Assumes (to be safe) that any path suffices

Comparisons to SIDH/SIKE

- Pros

  - Smaller public keys
  - No compression (simplicity)
  - Clean, memory-free security analysis (classical/quantum complexities match AES)
  - Hybrid security matches perfectly

- Cons

  - *currently* Efficiency (see Adj, Chi-Dominguez, Rodriguez-Henriquez 1109.pdf (iacr.org))

- Unclear

  - Conjecture: factorization of L does not (meaningfully) affect difficulty of L-isogeny problem
  - Smaller p. Could be new attacks (irrelevant in SIDH/SIKE). But could turn out to be a feature?

Future work

1. Better parameters. How smooth can we get?

2. Faster ℓ-isogenies. Is $O(\sqrt{\ell})$ optimal?

3. Can B-SIDH/B-SIKE outperform SIDH/SIKE?