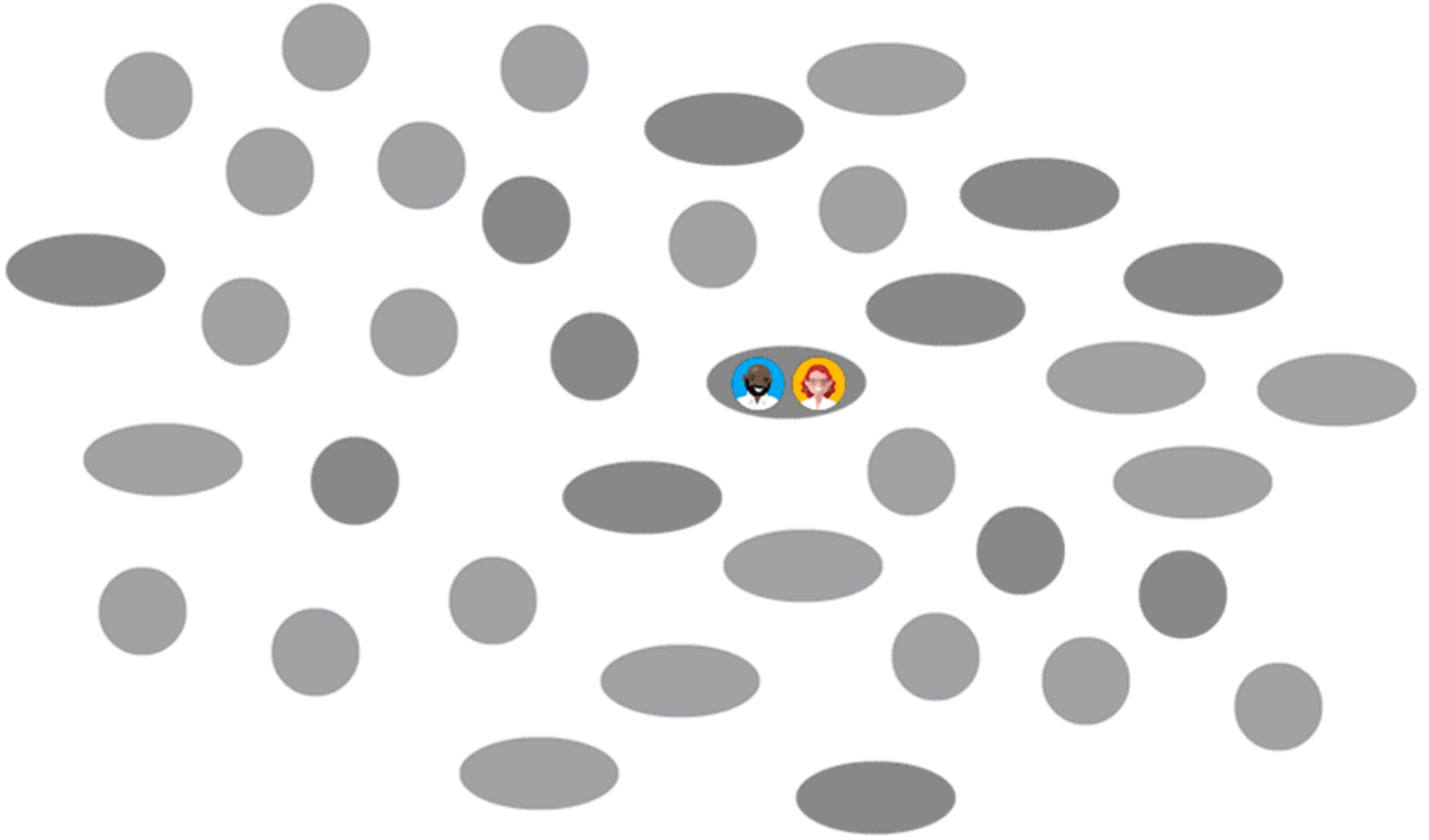
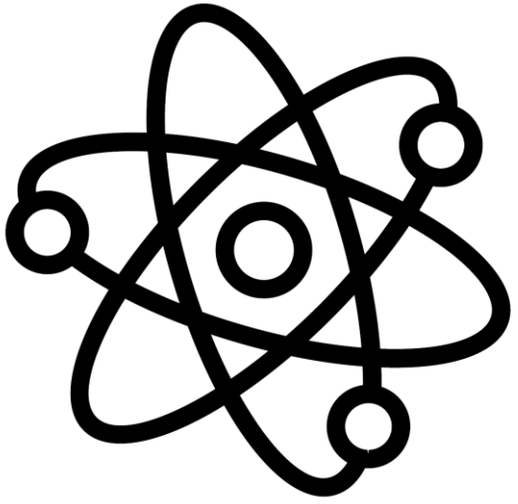
Post-quantum cryptography: supersingular isogenies for beginners



Craig Costello

Why?



Elliptic curves

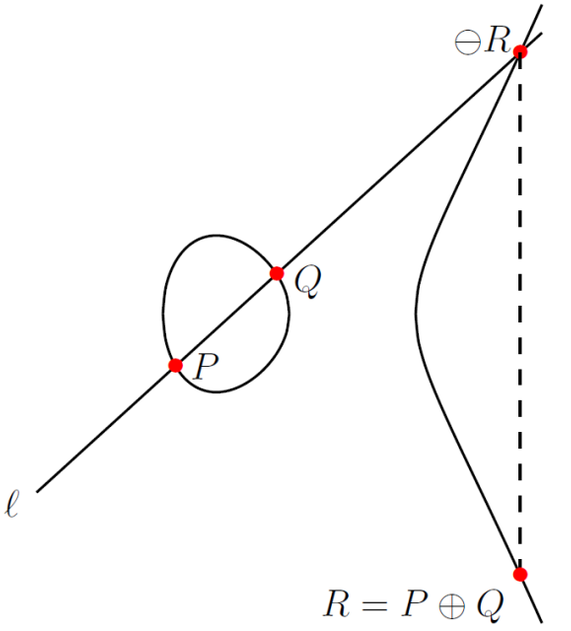
- Cubic curves $E/K : \quad y^2 = x^3 + \ldots$

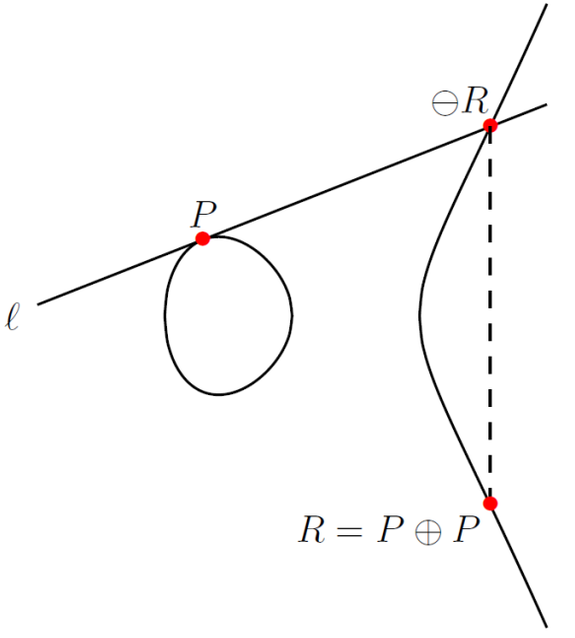
- Old school ECC
  - K is a finite field $\mathbb{F}_q$
  - Curve fixed once-and-for-all
  - Group elements are points e.g. $P = (x_P, y_P)$ and $\mathcal{O}_E$

- Fundamental operation is scalar multiplication
  - $P \mapsto [n]P$
  - $S = [n]P = (x_S, y_S) = (f(x_P), g(x_P, y_P))$

- ECDLP: given $P, S \in E$, find $n \in \mathbb{Z}$

- Elliptic curves are algebraic and geometric





Isomorphisms and j-invariants

- Two elliptic curves are isomorphic iff they have the same j-invariant

e.g.: $E_a : y^2 = x^3 + ax^2 + x$ has $j(E_a) = \frac{256(a^3-3)^3}{a^2-4}$

Let $K = \mathbb{F}_{431^2}$, where $\mathbb{F}_{431^2} = \mathbb{F}_{431}(i)$ and $i^2 + 1 = 0$.

The curves $E = E_{208i+161}$ and $E' = E_{172i+162}$ have $j(E) = 364i + 304 = j(E')$, so…

$$E \cong E'$$

$$\psi : E \to E', \quad (x, y) \mapsto \big((66i + 182)x + (300i + 109), (122i + 159)y\big)$$
$$\psi^{-1} : E' \to E, \quad (x, y) \mapsto \big((156i + 40)x + (304i + 202), (419i + 270)y\big)$$

$\psi(\mathcal{O}_E) = \mathcal{O}_{E'}$, and $\psi^{-1}(\mathcal{O}_{E'}) = \mathcal{O}_E$ (trivial kernel)

Isogenies

- Isogenies are more general maps between elliptic curves

e.g.:

$$E_a : y^2 = x^3 + (208i + 161)x^2 + x \quad \text{has} \quad j(E_a) = 364i + 304$$
$$E_{a'} : y^2 = x^3 + (102i + 423)x^2 + x \quad \text{has} \quad j(E_{a'}) = 344i + 190$$

$$\phi: \quad E_a \to E_{a'}$$

$$(x, y) \mapsto \left(\frac{x\big((350i + 68)x - 1\big)}{x - (350i + 68)}, \quad (155i + 260)y \cdot \frac{\big(x^2 - (269i + 126)x + 1\big)}{\big(x - (350i + 68)\big)^2} \right)$$

Now kernels are non-trivial $\ker(\phi) = \{\mathcal{O}_E, \big((350i + 68), 0\big)\}$ and $j(E_a) \neq j(E_{a'})$ in general!

- Seperable isogenies ↔ kernels
- Vélu's formulas: input E and any subgroup G, outputs E' and ϕ.
- $\deg(\phi) = |G|$ - Vélu's formulas are $O(|G|)$ for prime $|G|$
- $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_3$, $\deg(\phi_2 \circ \phi_1) = \deg(\phi_2) \cdot \deg(\phi_1)$
- Isogenies are (algebraic and geometric) morphisms: $\phi(P + Q) = \phi(P) + \phi(Q)$

Keeping it simple

- Whether it's $[n]: E \to E$, or $\phi_n: E \to E'$, we always have

$$(x, y) \mapsto \left(f(x), c\ y\ f'(x)\right)$$

  for some constant c.

- So it's easier to ignore y-coordinates and work with

$$(x, -) \mapsto (f(x), -)$$

- Happily, this is also what is fastest/simplest/done in state-of-the-art classical and post-quantum ECC!

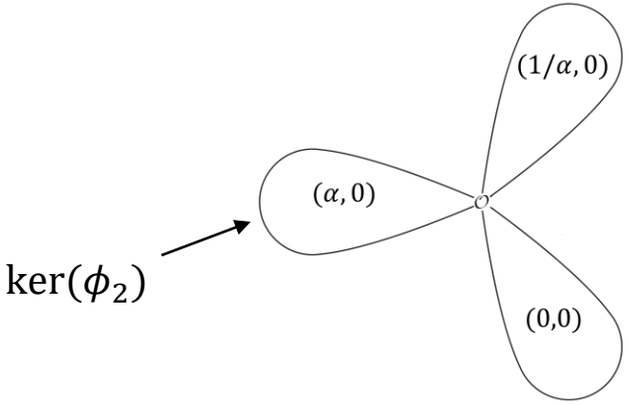
- Fortunately, we only need $n = 2$ and $n = 3$ to do SIDH!

Explicit formulas

$$[2] : E_a \to E_a\,, \qquad x \mapsto \frac{\left(x^2-1\right)^2}{4x(x-\alpha)(x-1/\alpha)}$$

$$\phi_2 : E_a \to E_{a'}\,, \qquad x \mapsto x \cdot \left(\frac{\alpha x - 1}{x-\alpha}\right)$$

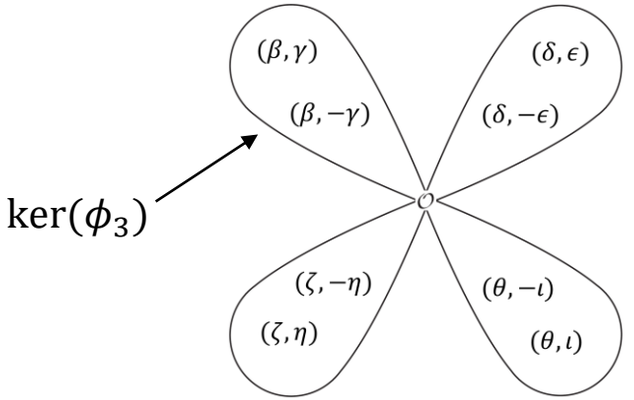
$$a' = 2\left(1-2\alpha^2\right)$$



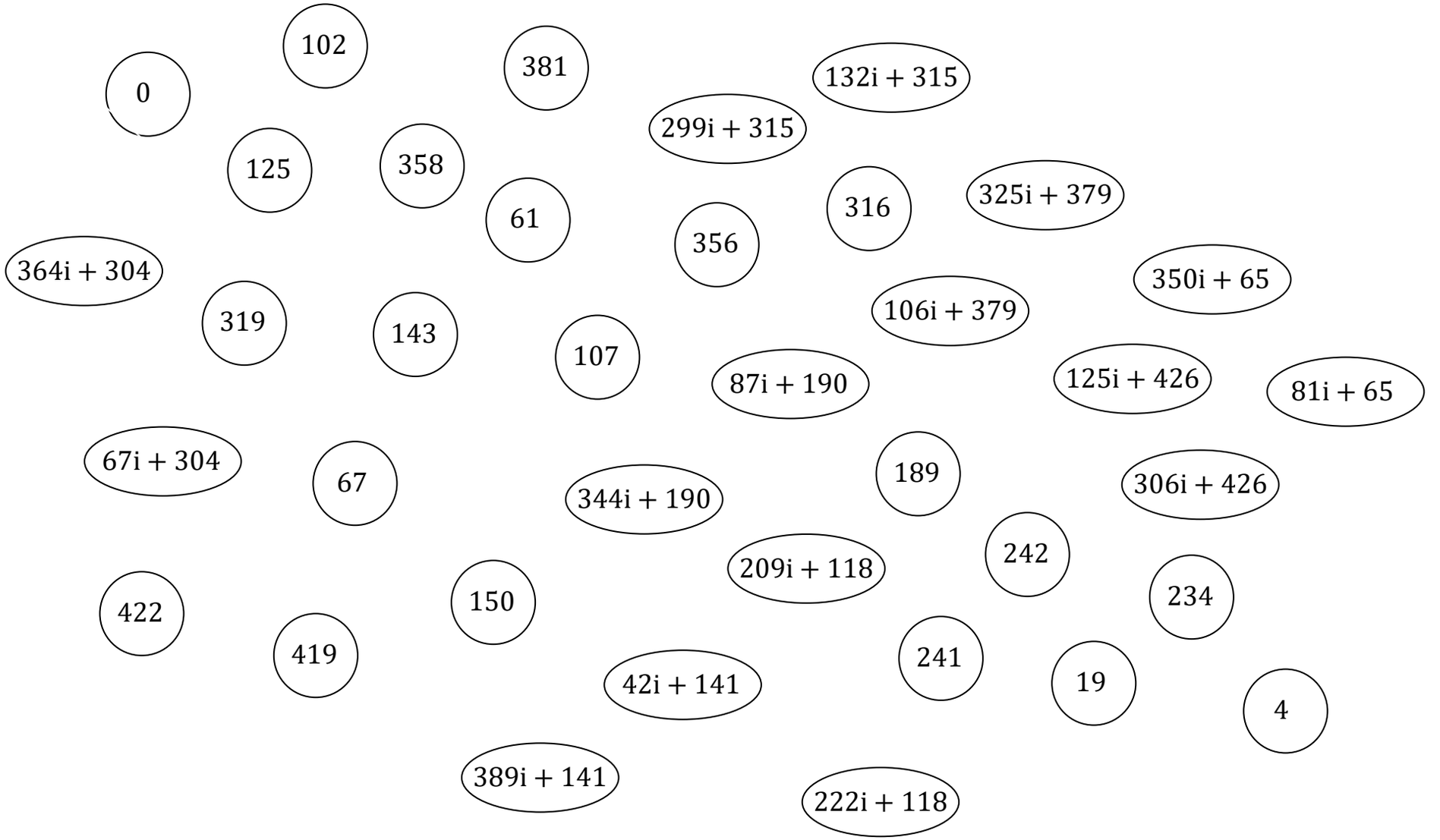
$$[3] : E_a \to E_a, \qquad x \mapsto \frac{\left(x^4-6x^2-4ax-3\right)^2 x}{(3x^4+4ax^3+6x^2-1)^2}$$

$$\phi_3 : E_a \to E_{a'}\,, \qquad x \mapsto x \cdot \left(\frac{\beta x - 1}{x-\beta}\right)^2$$

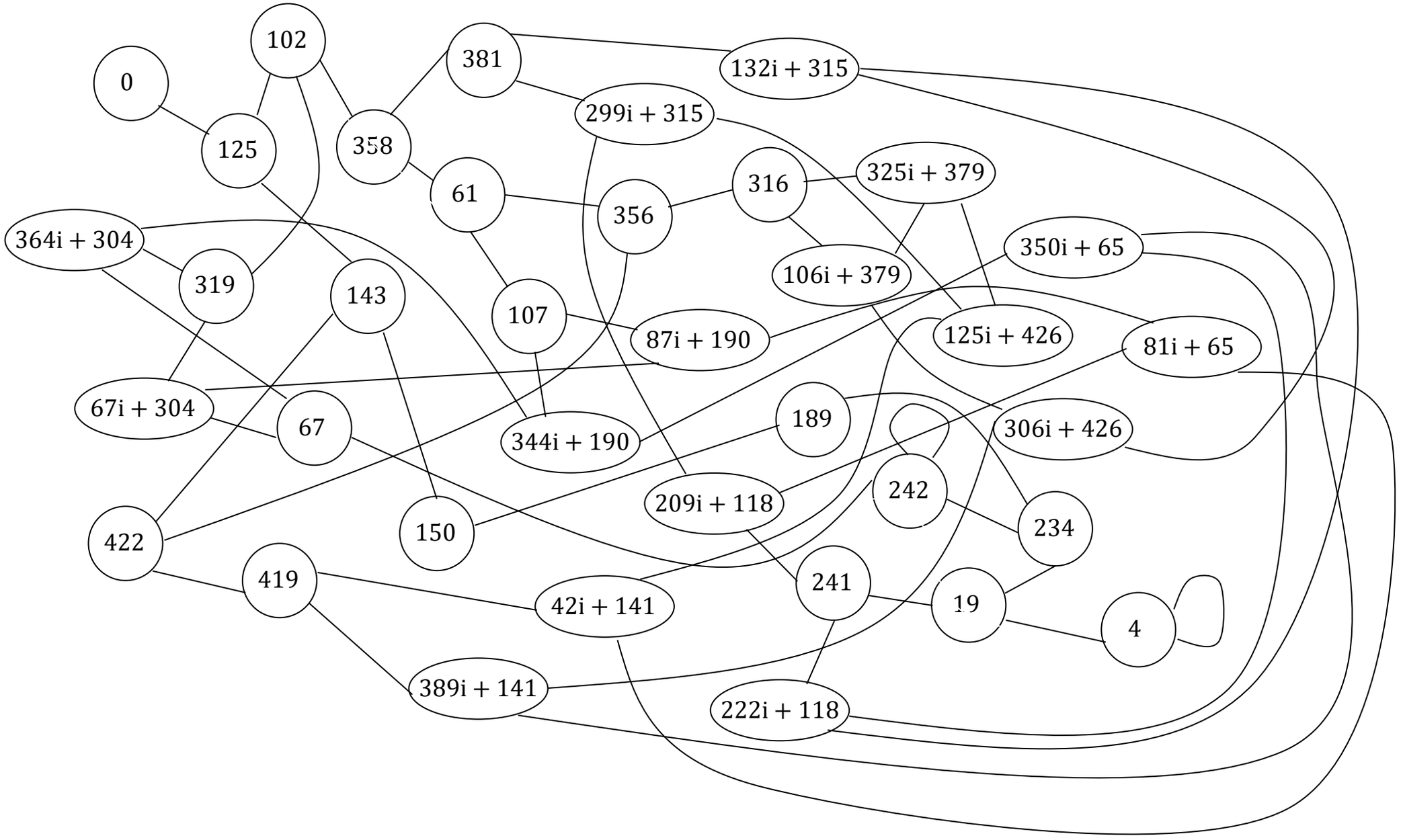
$$a' = \left(a\beta - 6\beta^2 + 6\right)\beta$$

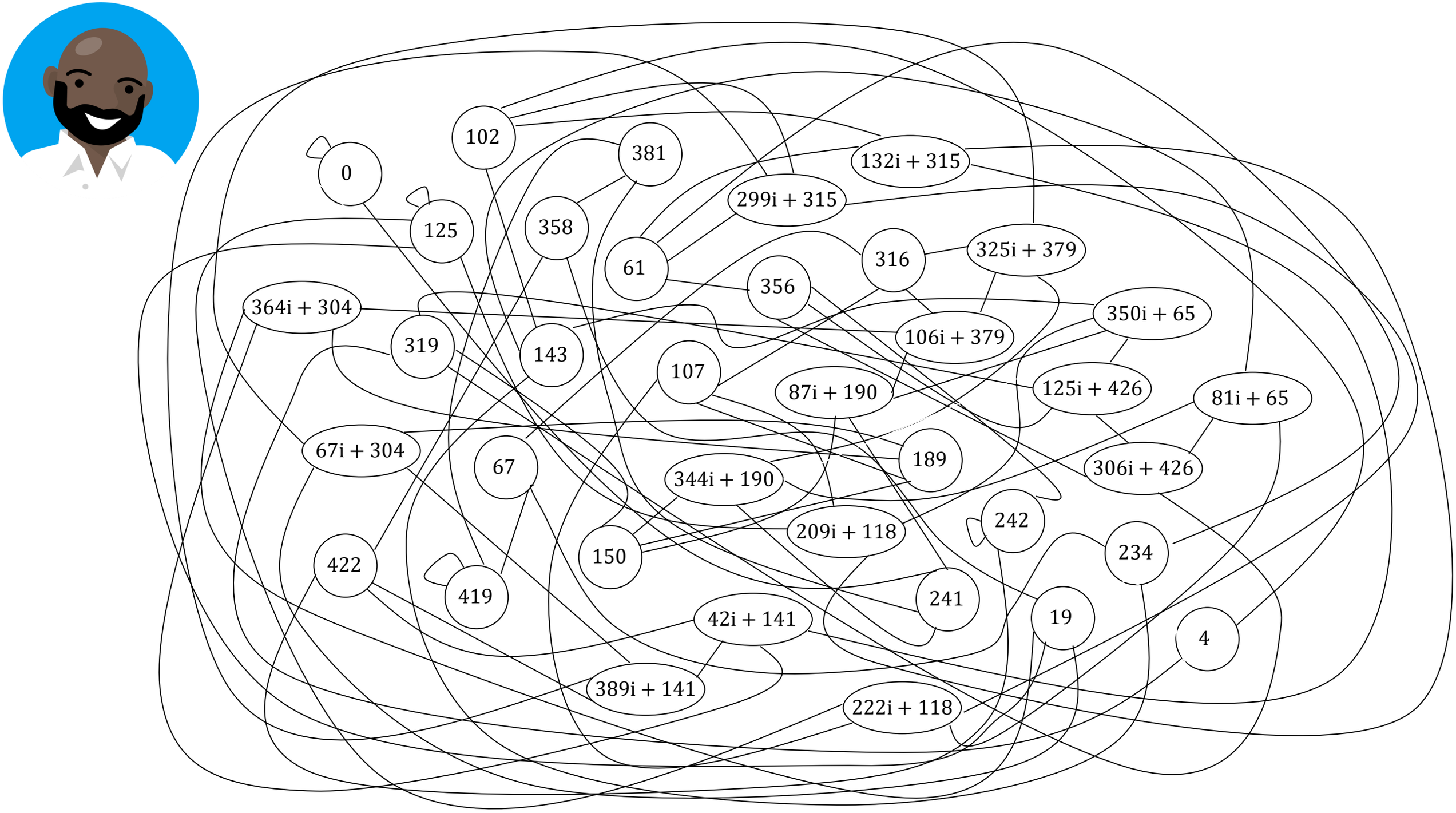


e.g. supersingular isogeny graph – the nodes



$p := 431$: there are 37 supersingular j's (all over $\mathbb{F}_{p^2} := \mathbb{F}_p(i)$, $i^2 + 1 = 0$)


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

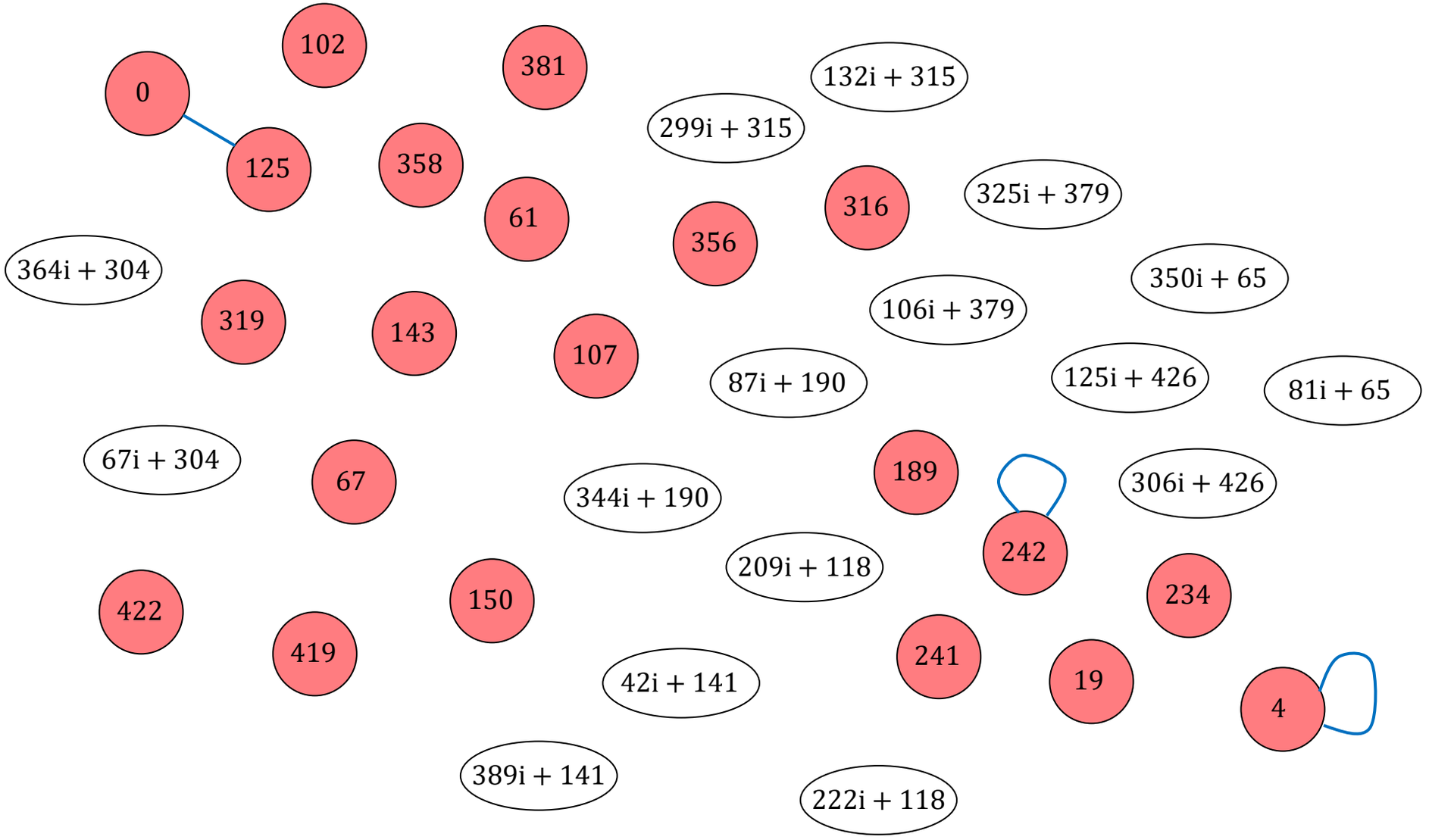

0
102
381
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
350i + 65
106i + 379
319
143
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
306i + 426
344i + 190
242
209i + 118
150
234
422
419
241
42i + 141
19
4
389i + 141
222i + 118

Curse of the small example

More than half the nodes here are in $\mathbb{F}_p$, but as $p \to \infty$, there are $O(p)$ nodes and only $O(\sqrt{p})$ lie in $\mathbb{F}_p$.

These (self edges, double/triple edges) look relatively common here, but as $p \to \infty$, they aren't

$p = 431$

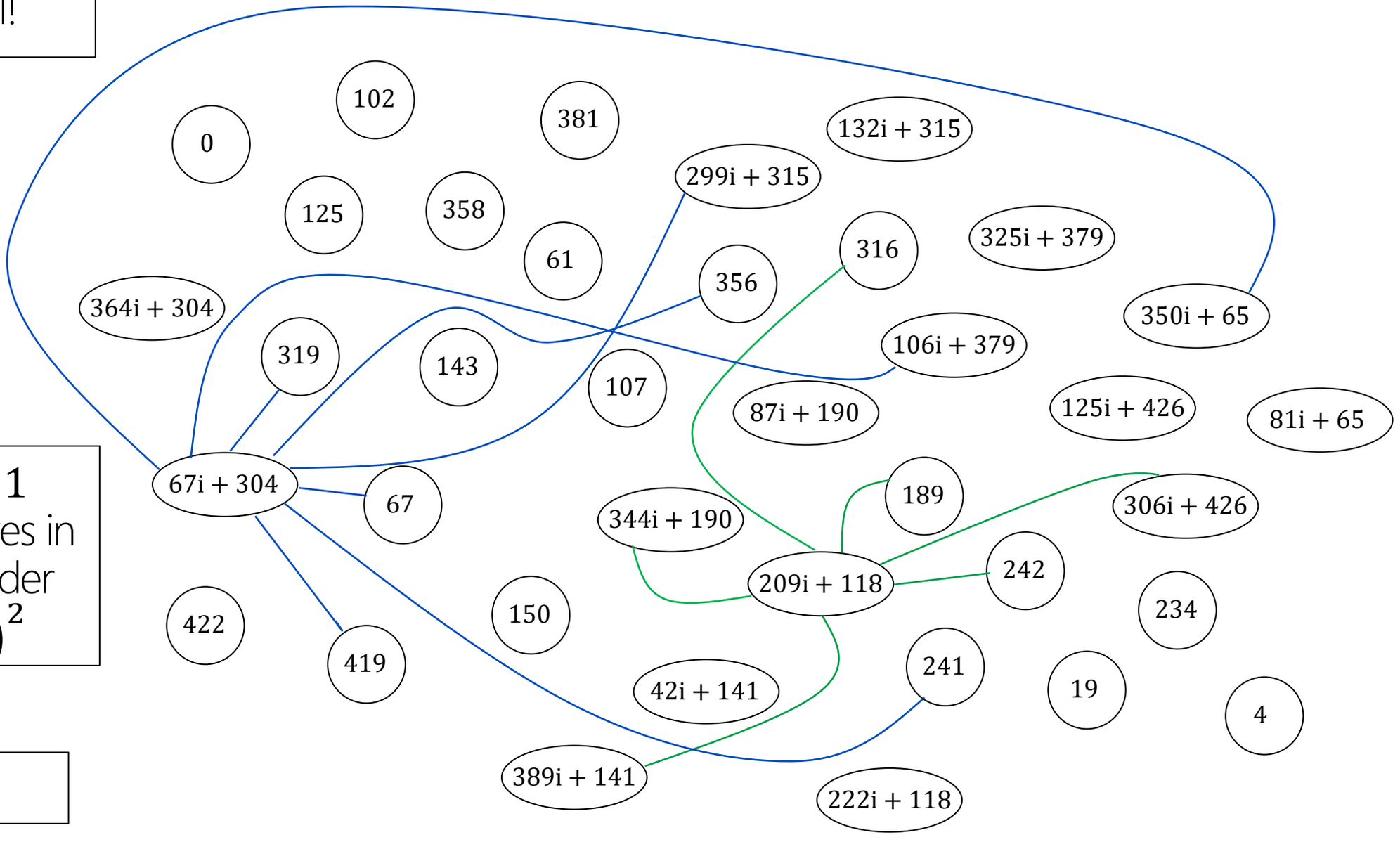


Higher ℓ ?

Could use $\ell = 5$ or $\ell = 7$ … etc, but these isogenies are not $\mathbb{F}_{p^2}$-rational!

$p = 431 = 2^4 3^3 - 1$ chosen so that all curves in graph have group order $(p+1)^2 = (2^4 3^3)^2$

Choose $2^i \approx 3^j$



Params: starting curve and generator points

E_A: $y^2 = x^3 + Ax^2 + x$

$$A = 329i + 423$$

$$j = 87i + 190$$

$$\#E_A(\mathbb{F}_{p^2}) = (p+1)^2 = \left(2^4 3^3\right)^2$$

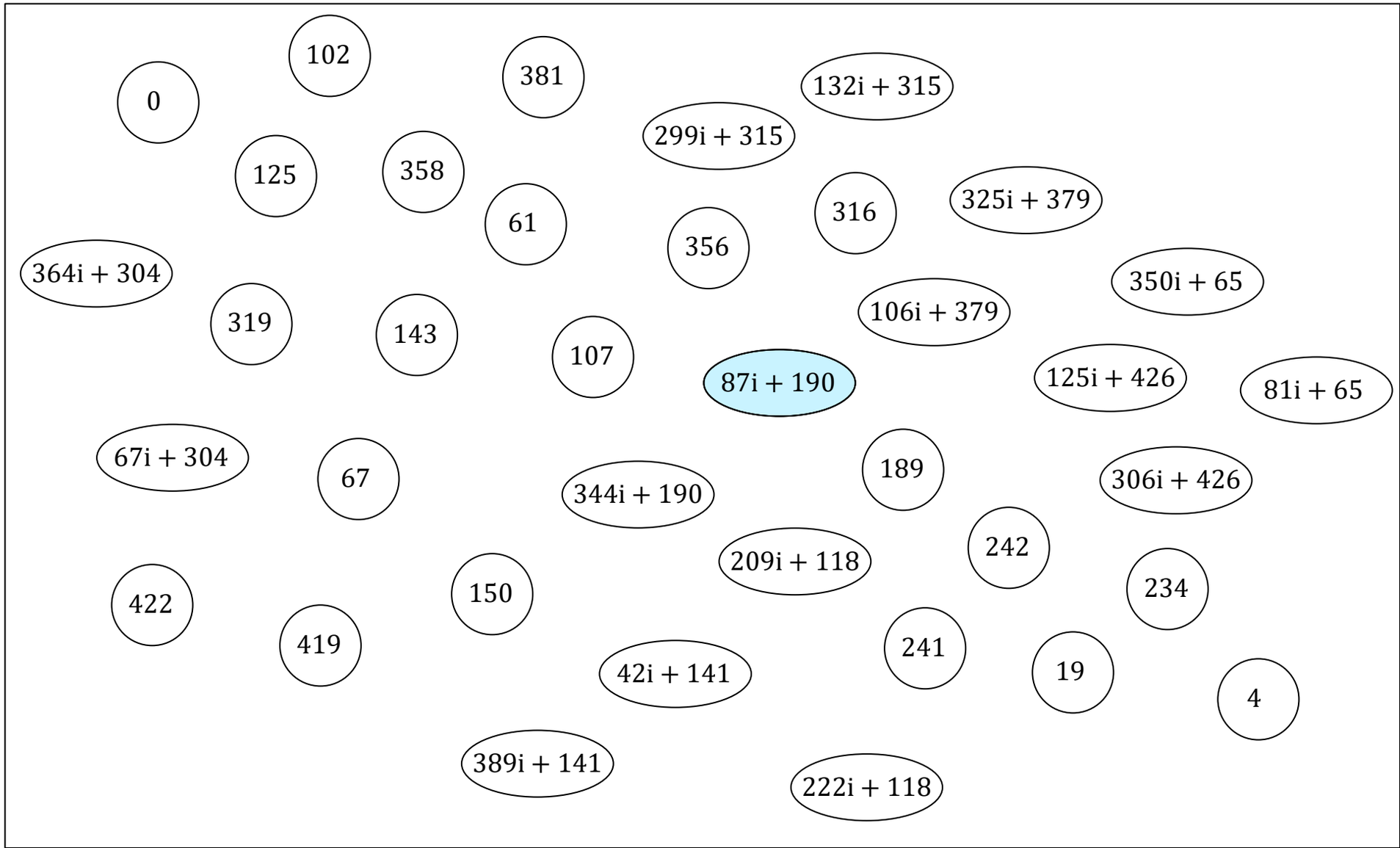
$$E \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$$

$P_A = (100i + 248, 304i + 199)$
$Q_A = (426i + 394, 51i + 79)$

$P_B = (358i + 275, 410i + 104)$
$Q_B = (20i + 185, 281i + 239)$

$$E[2^4] = \langle P_A, Q_A \rangle$$

$$E[3^3] = \langle P_B, Q_B \rangle$$

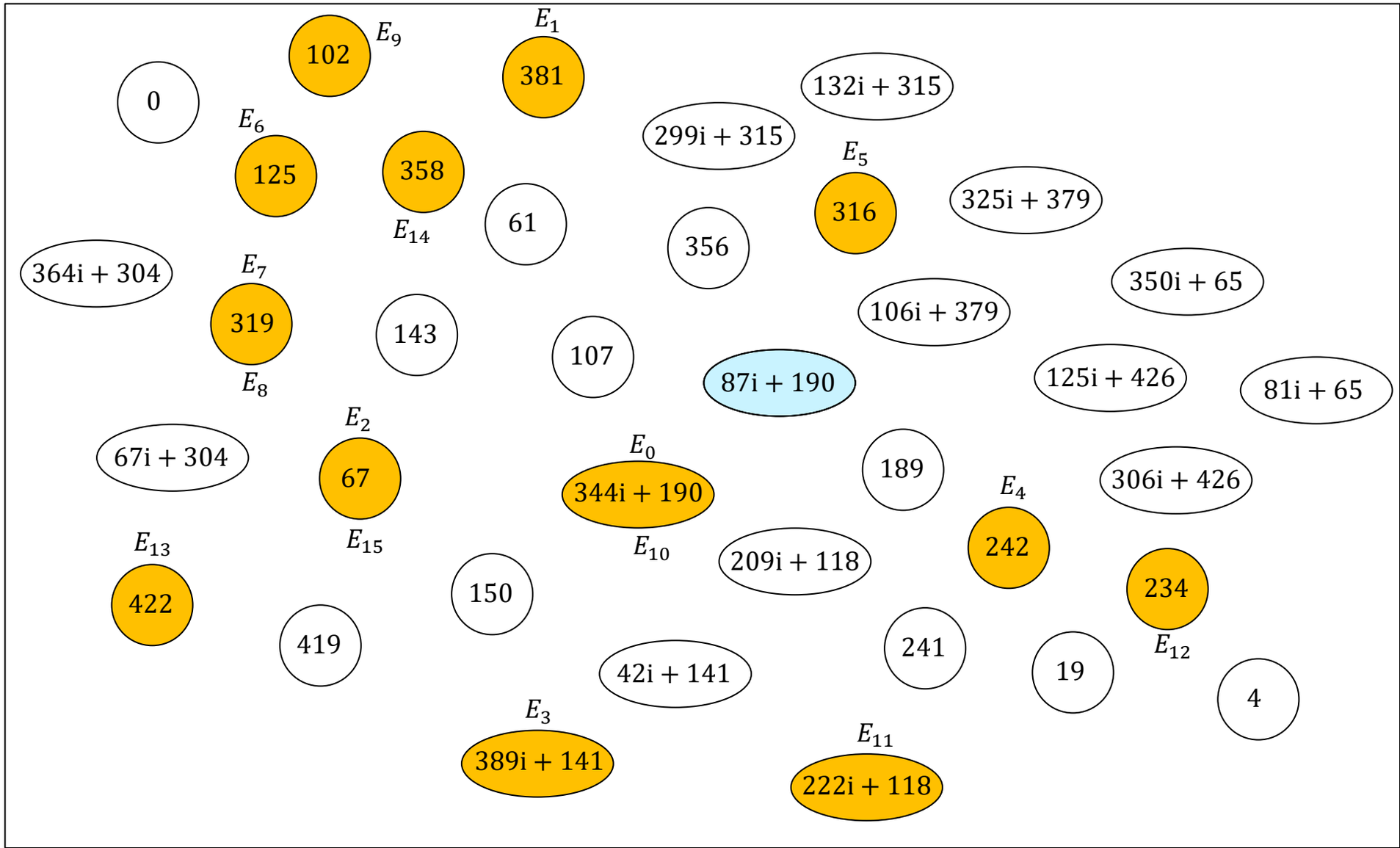


Alice destinations: possible* 2^4-isogenies

$P_A = (100i + 248, 304i + 199)$
$Q_A = (426i + 394, 51i + 79)$

k_A	$S_k = P_A + [k_A]Q_A$
0	$(100i + 248, 304i + 199)$
1	$(430i + 163, 44i + 326)$
2	$(165i + 278, 313i + 113)$
3	$(34i + 202, 310i + 65)$
4	$(320i + 395, 238i + 205)$
5	$(413i + 322, 315i + 91)$
6	$(235i + 98, 316i + 321)$
7	$(59i + 224, 312i + 7)$
8	$(390i + 349, 294i + 408)$
9	$(56i + 391, 289i + 129)$
10	$(183i + 238, 188i + 246)$
11	$(271i + 79, 153i + 430)$
12	$(352i + 382, 154i + 380)$
13	$(63i + 162, 350i + 229)$
14	$(300i + 111, 285i + 10)$
15	$(204i + 139, 166i + 207)$

$$E_{k_A} := E_0/\langle S_{k_A} \rangle$$

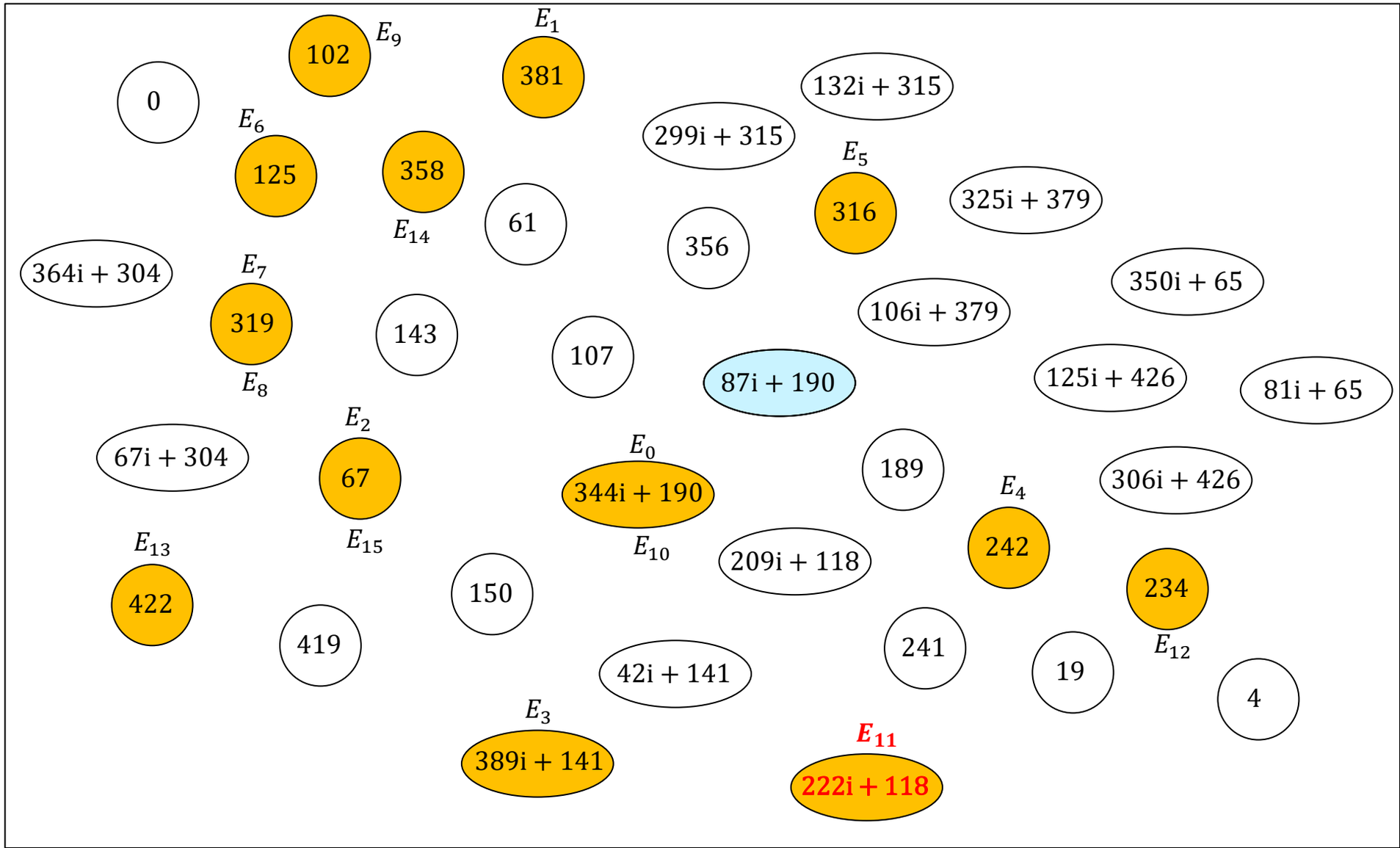


Alice destinations: possible* 2^4-isogenies

$P_A = (100i + 248, 304i + 199)$
$Q_A = (426i + 394, 51i + 79)$

k_A	$S_k = P_A + [k_A]Q_A$
0	$(100i + 248, 304i + 199)$
1	$(430i + 163, 44i + 326)$
2	$(165i + 278, 313i + 113)$
3	$(34i + 202, 310i + 65)$
4	$(320i + 395, 238i + 205)$
5	$(413i + 322, 315i + 91)$
6	$(235i + 98, 316i + 321)$
7	$(59i + 224, 312i + 7)$
8	$(390i + 349, 294i + 408)$
9	$(56i + 391, 289i + 129)$
10	$(183i + 238, 188i + 246)$
11	$\mathbf{(271i + 79, 153i + 430)}$
12	$(352i + 382, 154i + 380)$
13	$(63i + 162, 350i + 229)$
14	$(300i + 111, 285i + 10)$
15	$(204i + 139, 166i + 207)$

$$E_{k_A} := E_0/\langle S_{k_A} \rangle$$

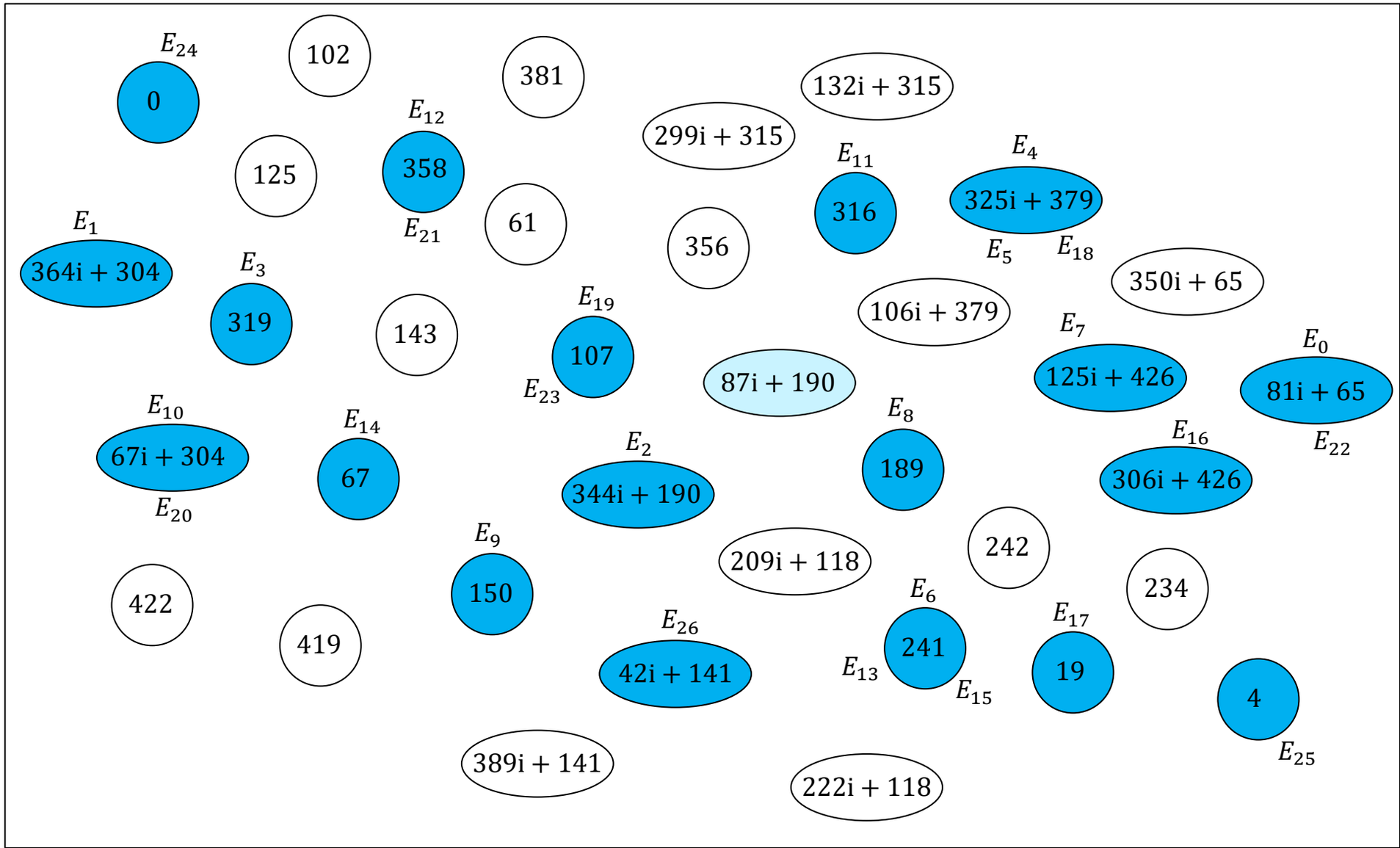


Bob destinations: possible* 3^3-isogenies

$P_A = (358i + 275, 410i + 104)$
$Q_A = (20i + 185, 281i + 239)$

k_B	$S_k = P_B + [k_B]Q_B$
0	$(358i + 275, 410i + 104)$
1	$(150i + 184, 106i + 293)$
2	$(122i + 309, 291i + 374)$
3	$(25i + 70, 254i + 66)$
4	$(47i + 223, 301i + 322)$
⋮	⋮
⋮	⋮
⋮	⋮
21	$(200i + 351, 141i + 361)$
22	$(35i + 417, 183i + 351)$
23	$(327i + 55, 230i + 238)$
24	$(326i + 56, 334i + 220)$
25	$(375i + 404, 378i + 168)$
26	$(333i + 426, 142i + 14)$

$$E_{k_B} := E/\langle S_{k_B} \rangle$$

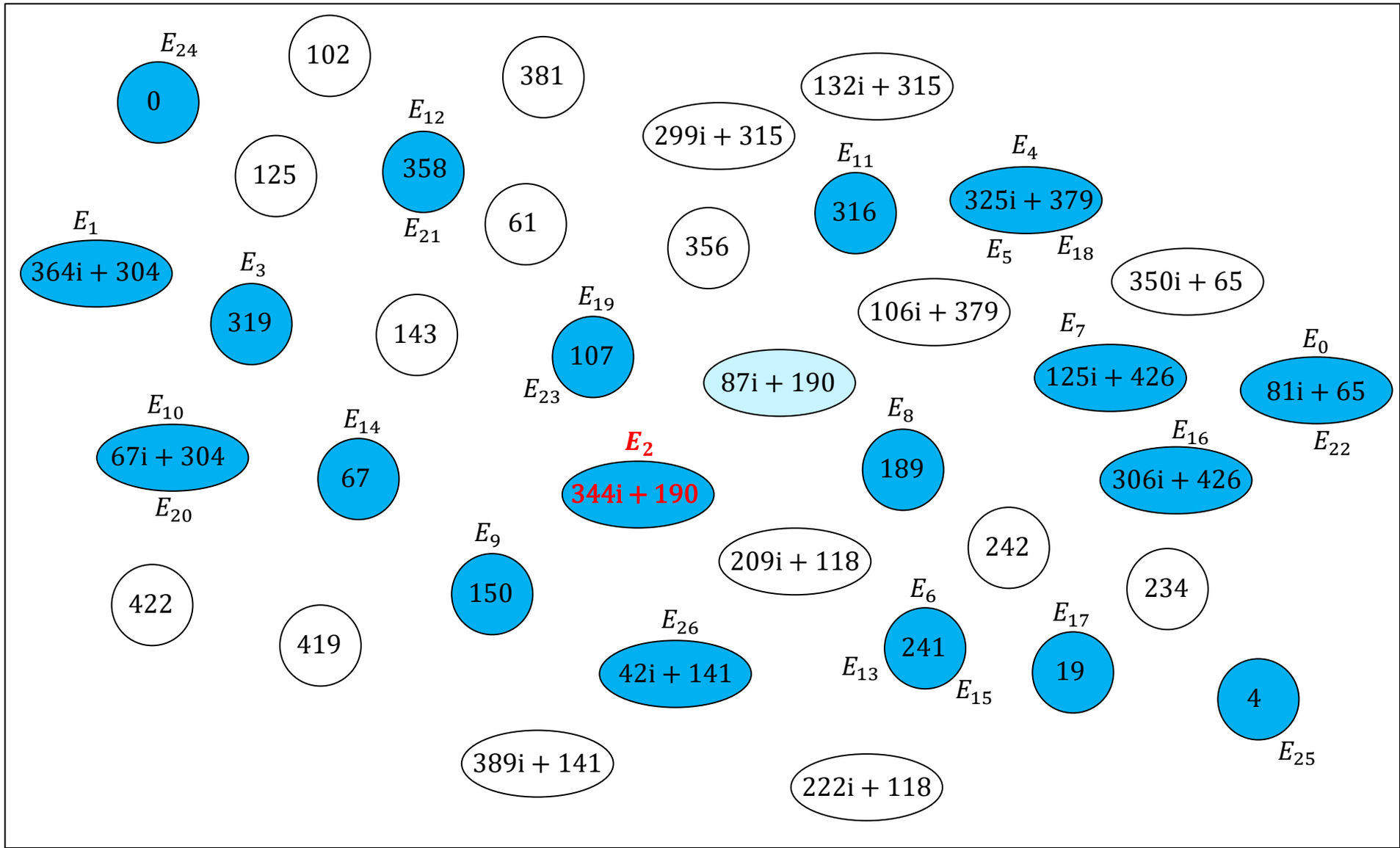


Bob destinations: possible* 3^3-isogenies

$P_A = (358i + 275, 410i + 104)$
$Q_A = (20i + 185, 281i + 239)$

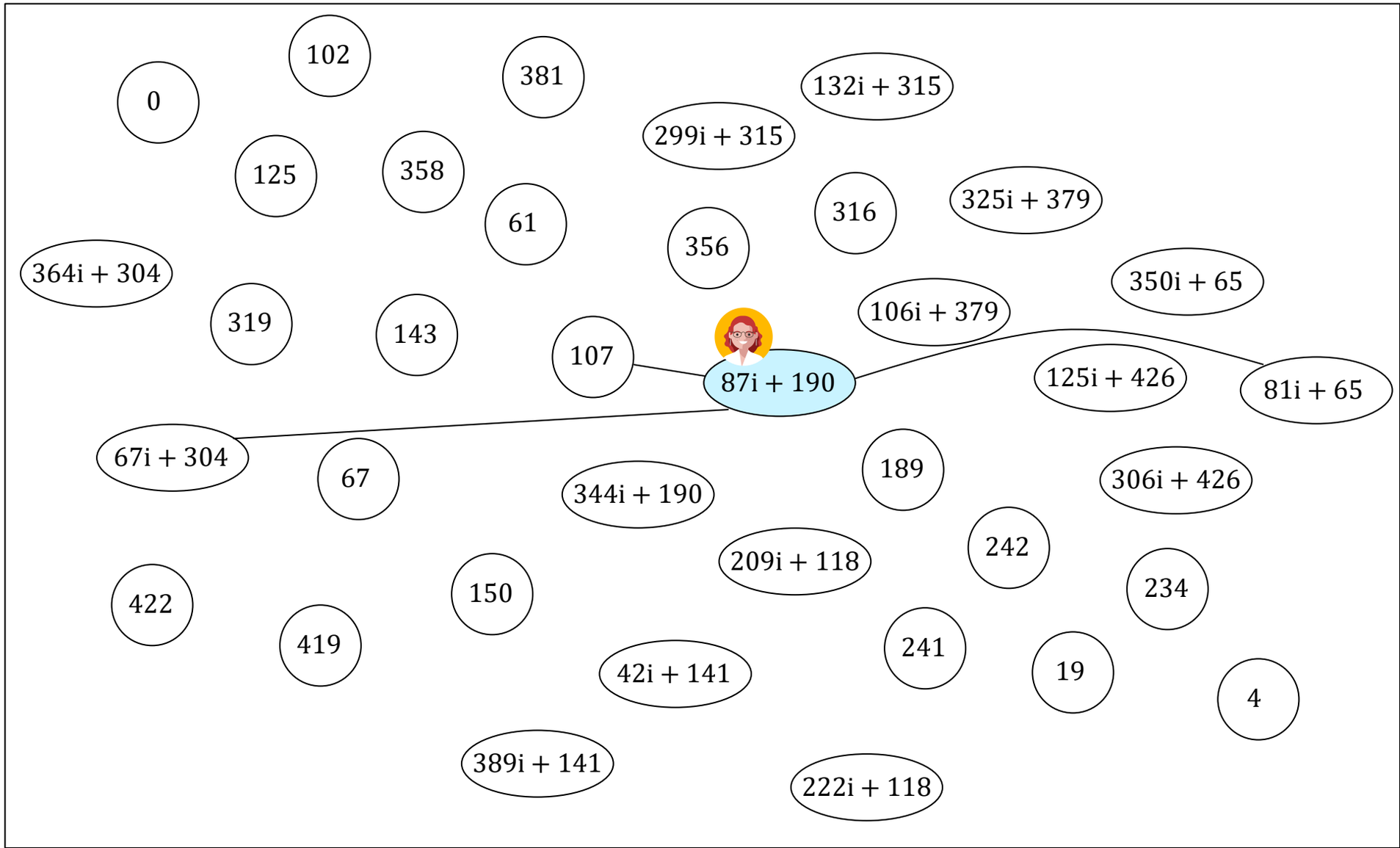
k_B	$S_k = P_B + [k_B]Q_B$
0	$(358i + 275, 410i + 104)$
1	$(150i + 184, 106i + 293)$
2	$\mathbf{(122i + 309, 291i + 374)}$
3	$(25i + 70, 254i + 66)$
4	$(47i + 223, 301i + 322)$
⋮	⋮
⋮	⋮
⋮	⋮
21	$(200i + 351, 141i + 361)$
22	$(35i + 417, 183i + 351)$
23	$(327i + 55, 230i + 238)$
24	$(326i + 56, 334i + 220)$
25	$(375i + 404, 378i + 168)$
26	$(333i + 426, 142i + 14)$

$$E_{k_B} := E/\langle S_{k_B} \rangle$$



Alice's key generation

$S = (271i + 79\ ,\ 153i + 430)$



Alice's key generation

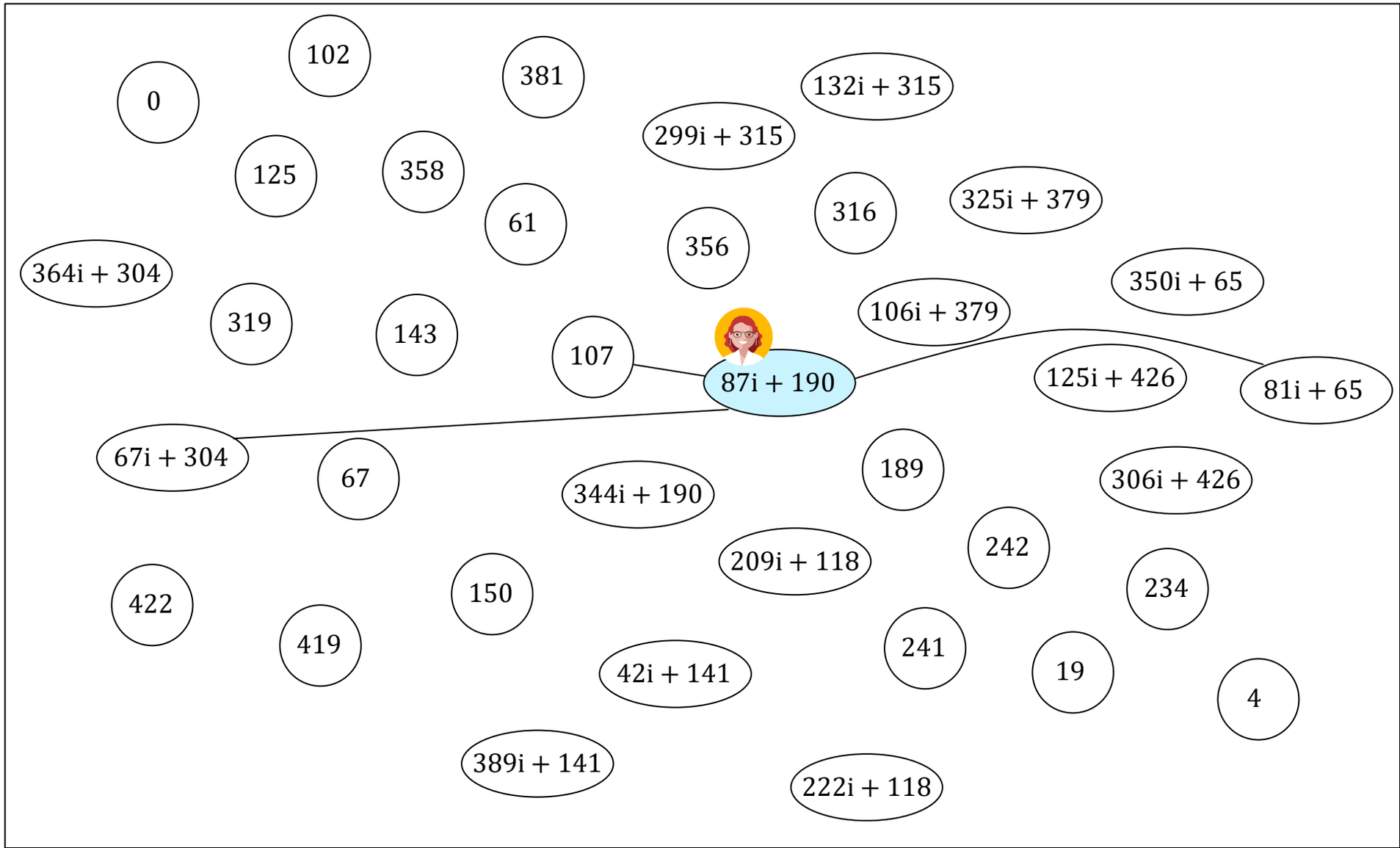
$S = (271i + 79\ ,\ 153i + 430)$

[2]

[2]

[2]

$[8]S = (18i + 37\ ,\ 0)$



Alice's key generation

$S = (271i + 79\ ,\ 153i + 430)$

[2]

[2]

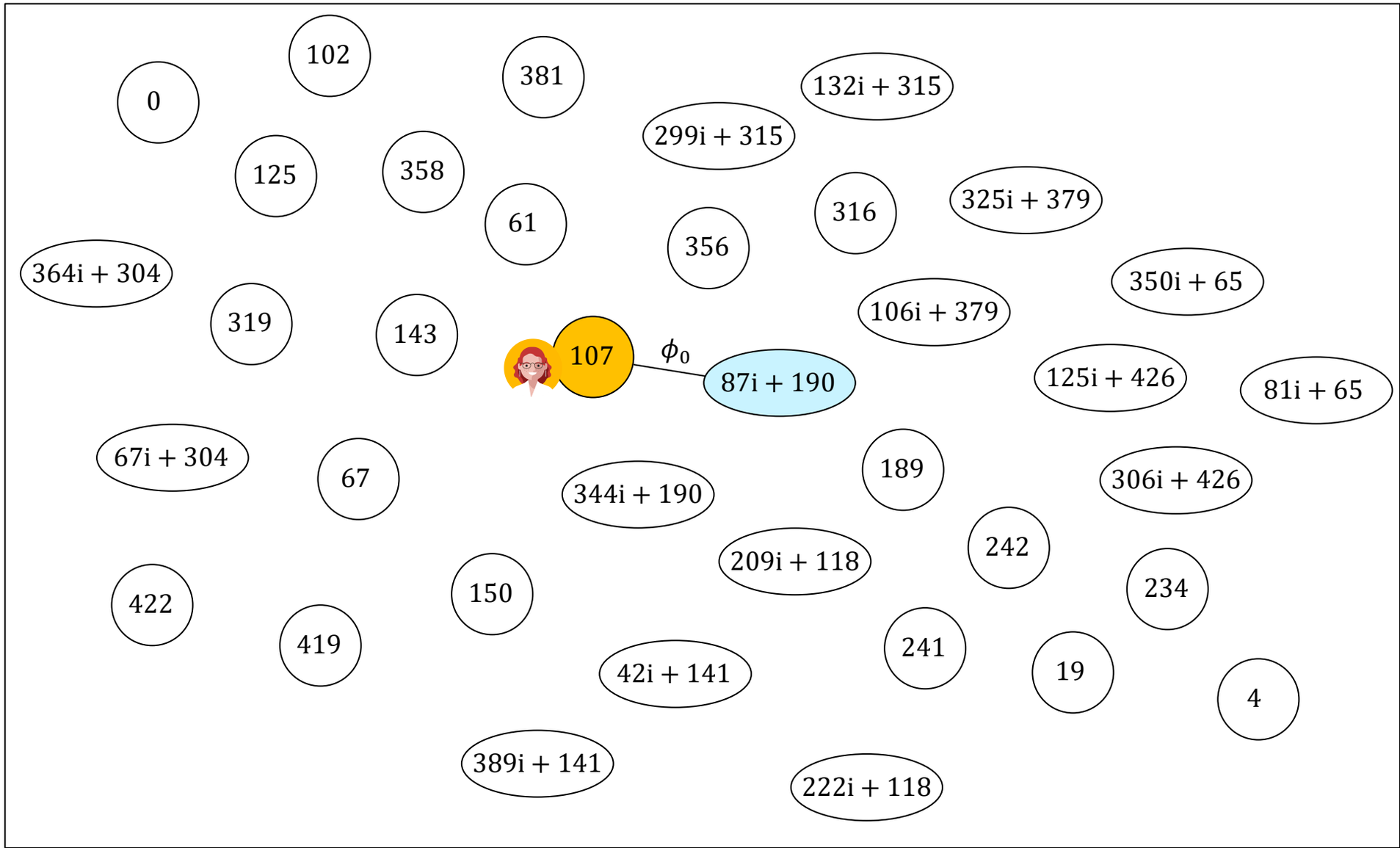
[2]

$[8]S = (18i + 37\ ,\ 0)$

$$\phi_0 : E_0 \to E_1$$

$$\ker(\phi_0) = \langle (18i + 37\ ,\ 0) \rangle$$

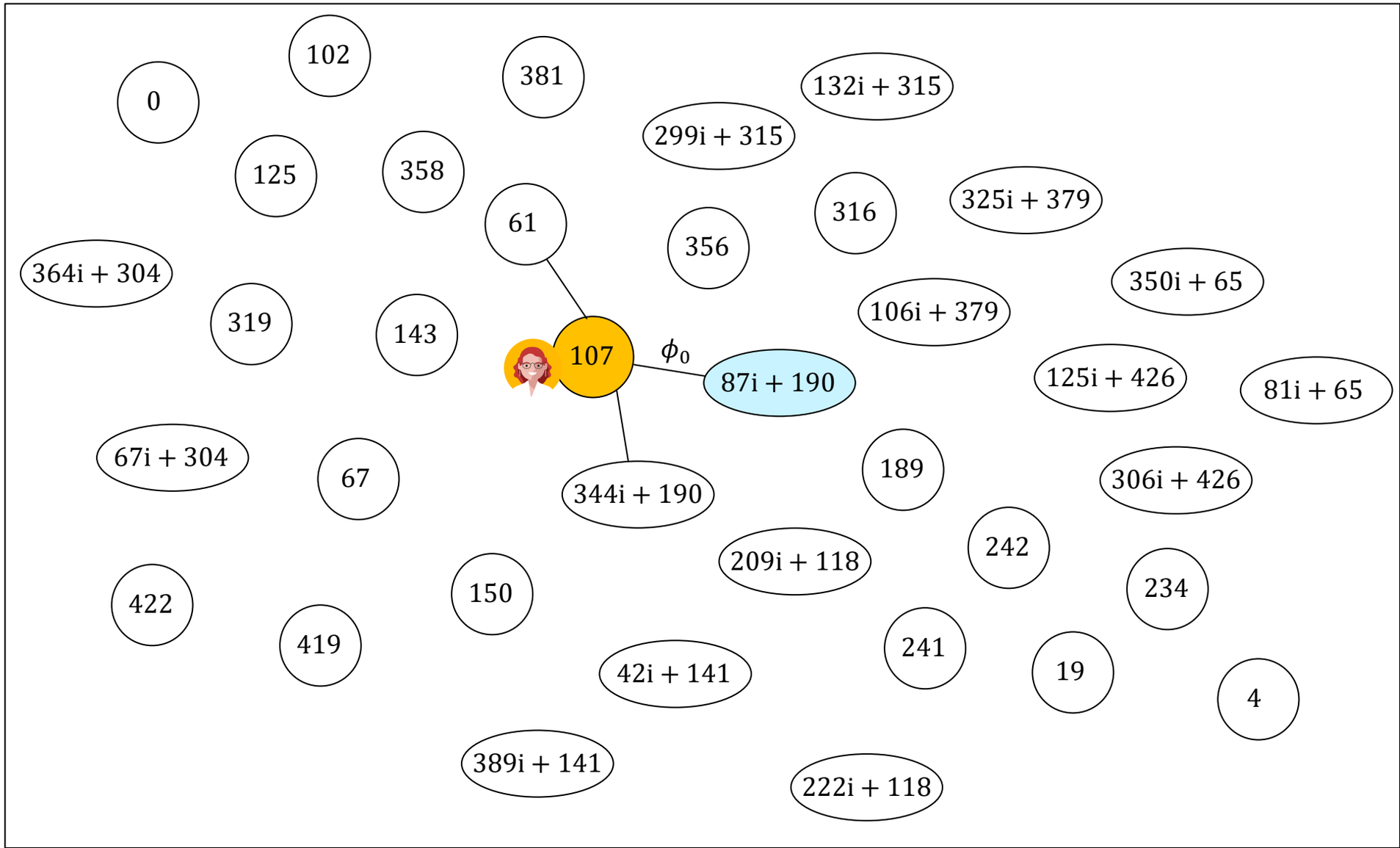
$$j(E_1) = 107$$



Alice's key generation

ϕ_0

$\phi_0(S) = (157i + 156\,,\, 231i + 353)$



Alice's key generation

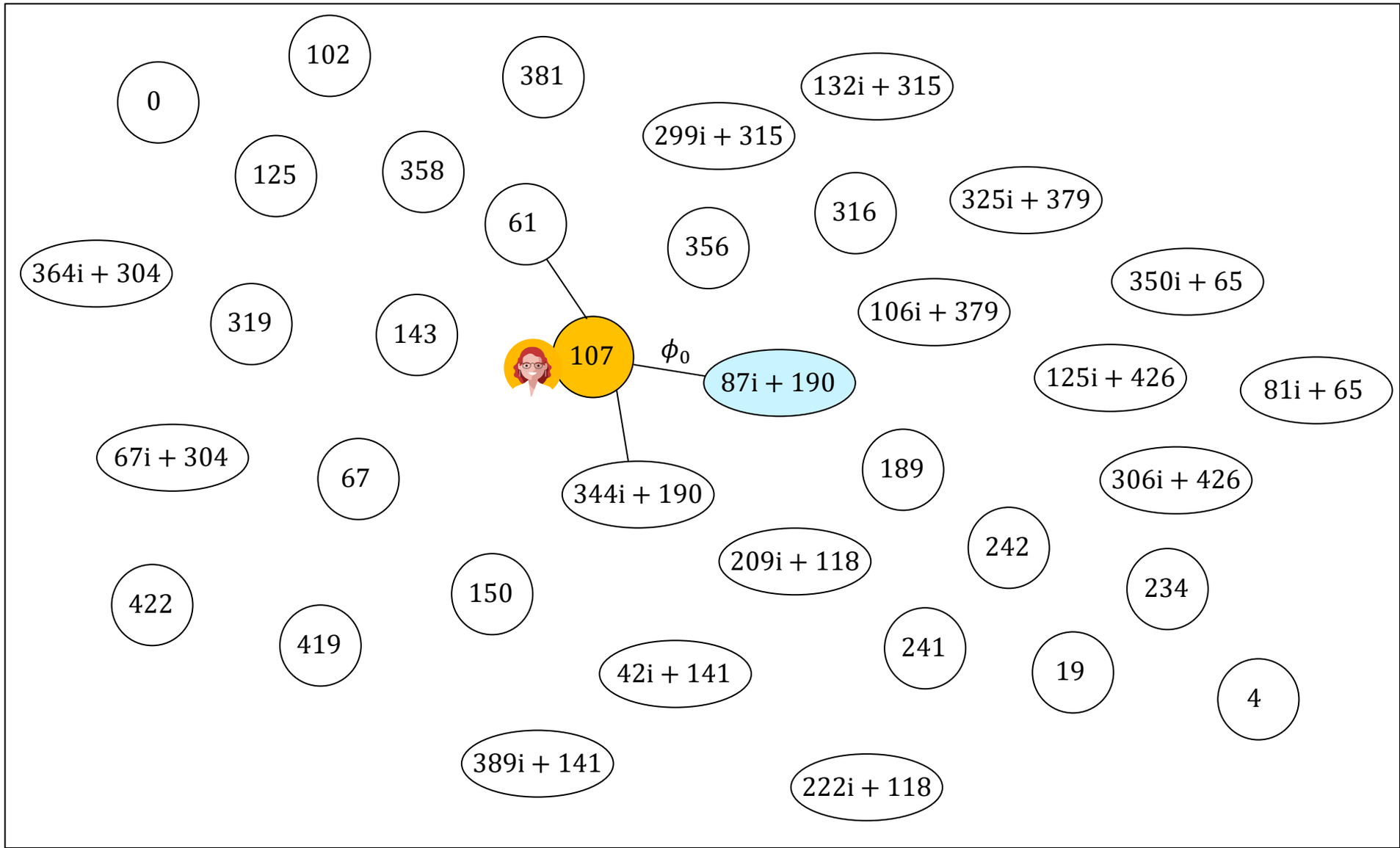
ϕ_0

$\phi_0(S) = (157i + 156\,,\, 231i + 353)$

[2]

[2]

$[4]\phi_0(S) = (100i + 80\,,\, 0)$



Alice's key generation

ϕ_0

$\phi_0(S) = (157i + 156\,,\, 231i + 353)$

[2]

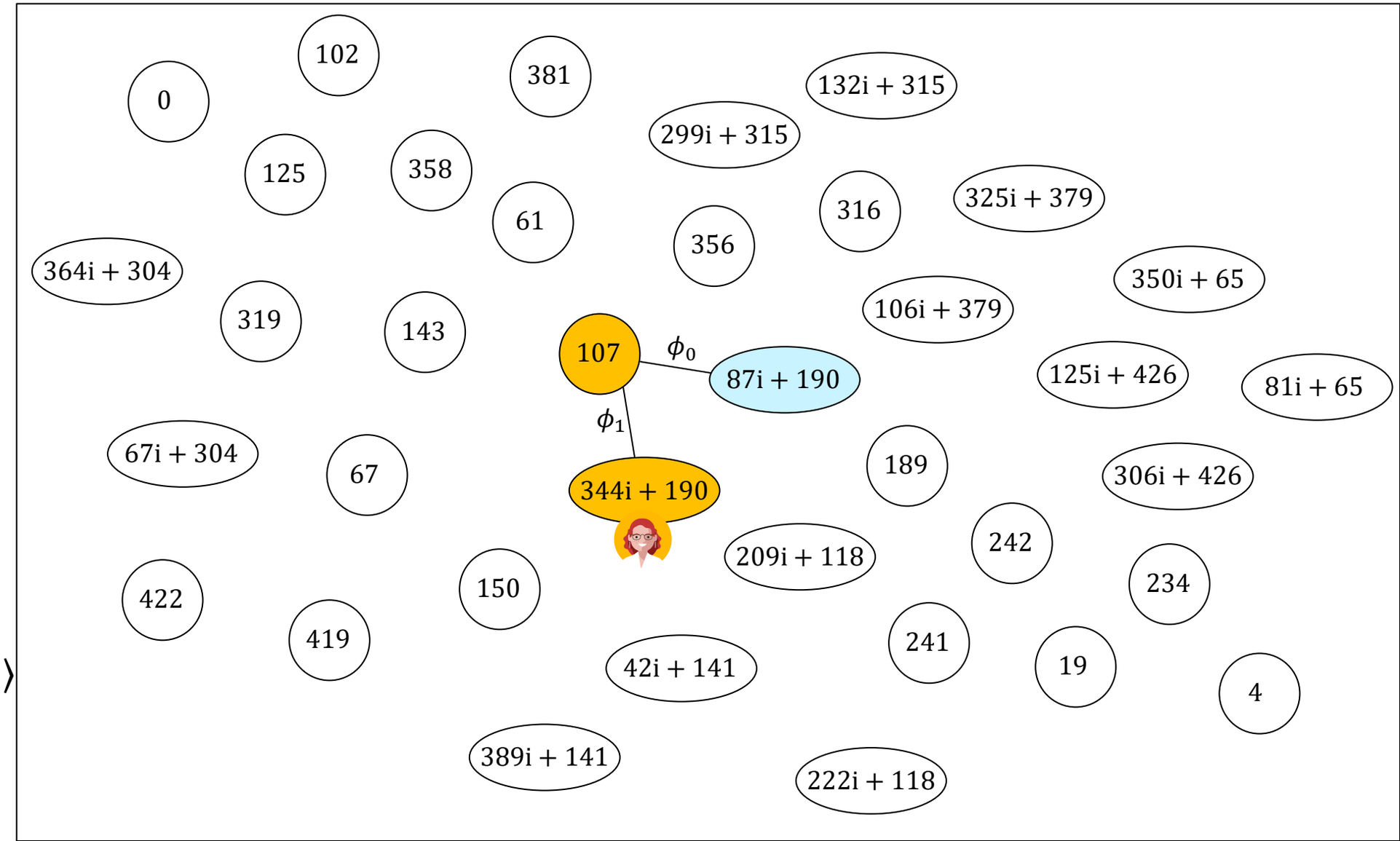
[2]

$[4]\phi_0(S) = (100i + 80\,,\, 0)$

$$\phi_1 : E_1 \to E_2$$

$$\ker(\phi_1) = \langle (100i + 80\,,\, 0) \rangle$$

$$j(E_2) = 344i + 190$$

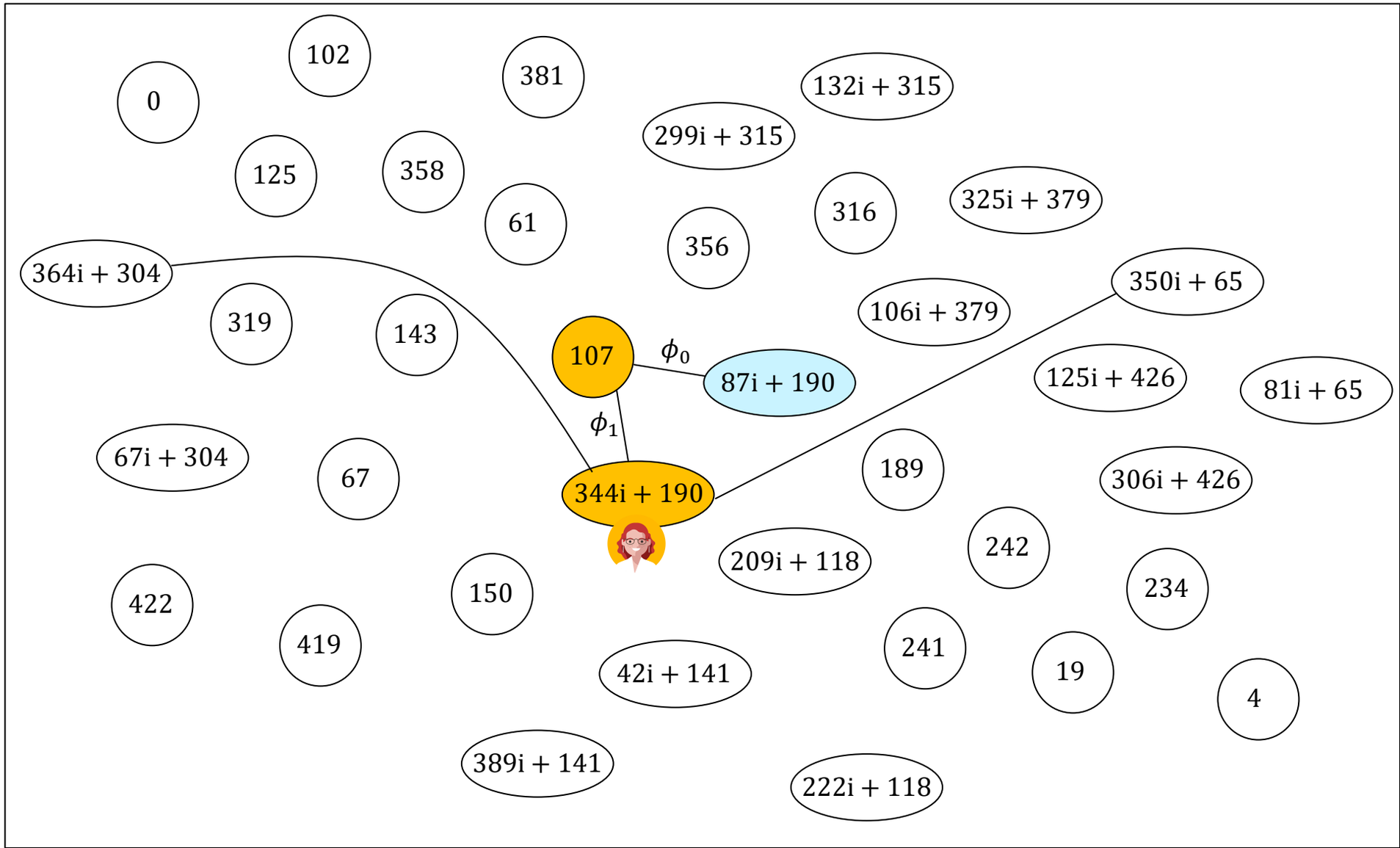


Alice's key generation

ϕ_0

ϕ_1

$\phi_1(\phi_0(S))= (157i + 156\,,\, 231i + 353)$



Alice's key generation

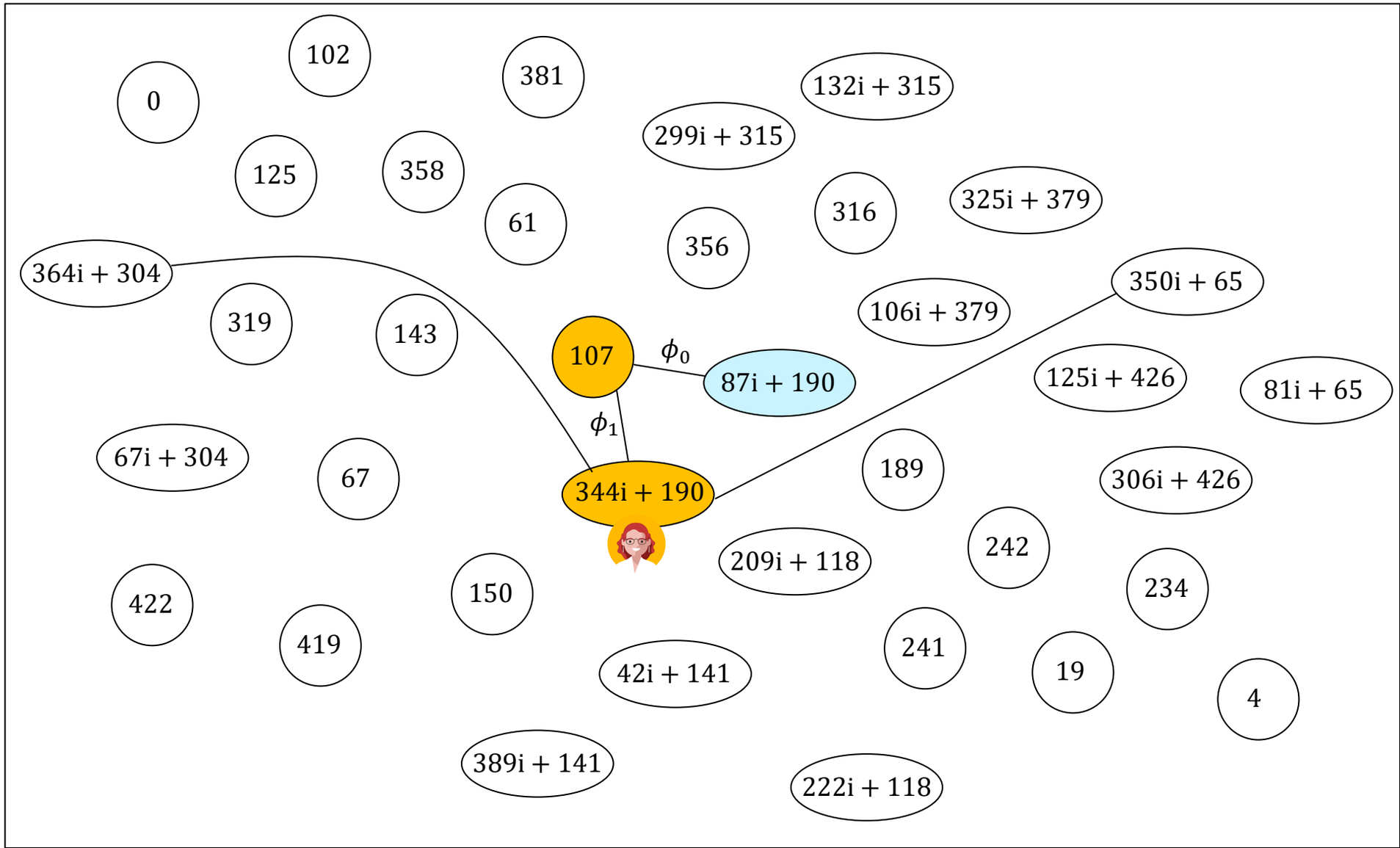
ϕ_0

ϕ_1

$\phi_1(\phi_0(S)) = (157i + 156\ ,\ 231i + 353)$

[2]

$[2]\phi_1(\phi_0(S)) = (317i + 131\ ,\ 0)$



Alice's key generation

ϕ_0

ϕ_1

$\phi_1(\phi_0(S)) = (157i + 156\,,\, 231i + 353)$

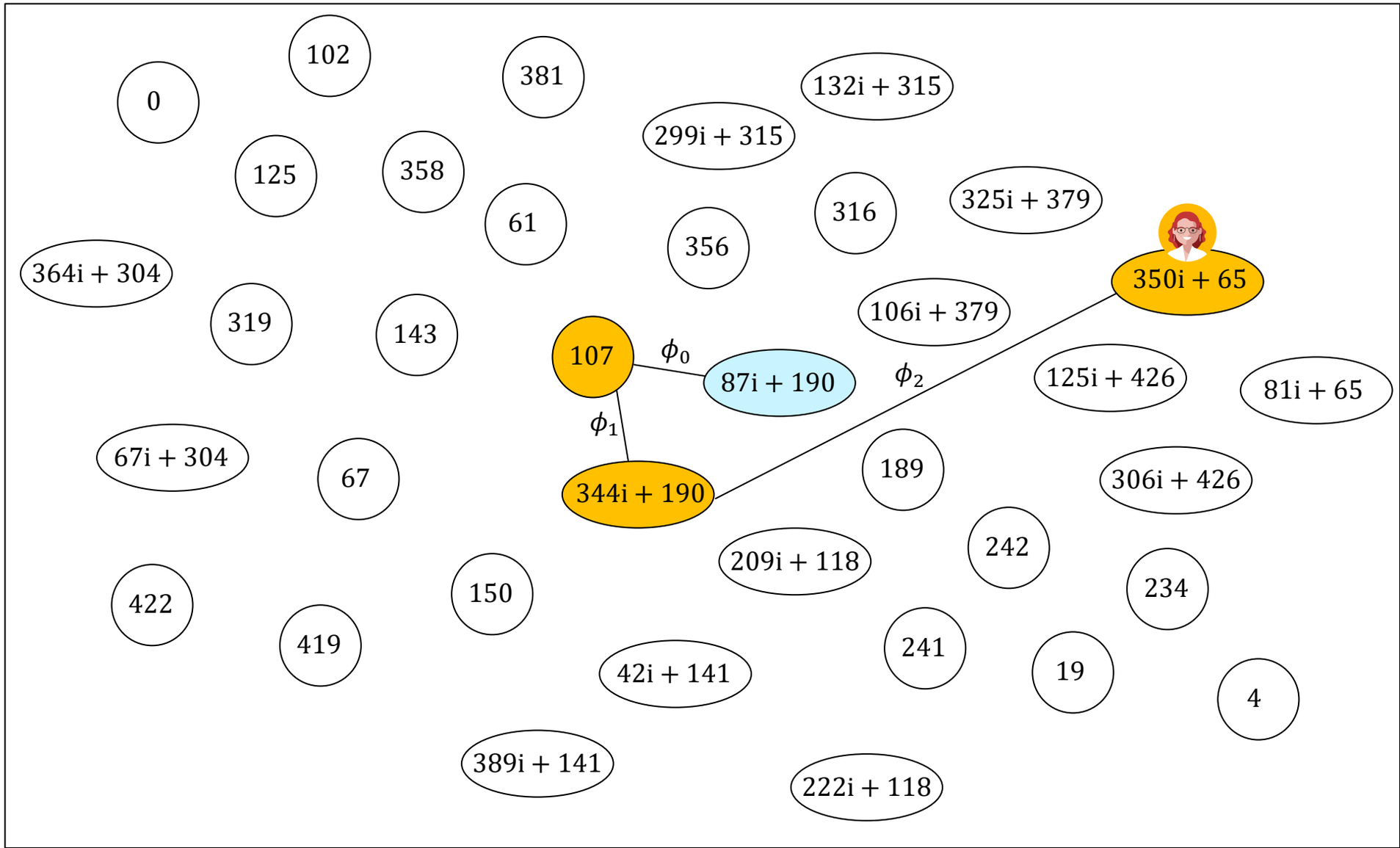
[2]

$[2]\phi_1(\phi_0(S)) = (317i + 131\,,\, 0)$

$$\phi_2 : E_2 \to E_3$$

$$\ker(\phi_2) = \langle (317i + 131, 0) \rangle$$

$$j(E_3) = 350i + 65$$



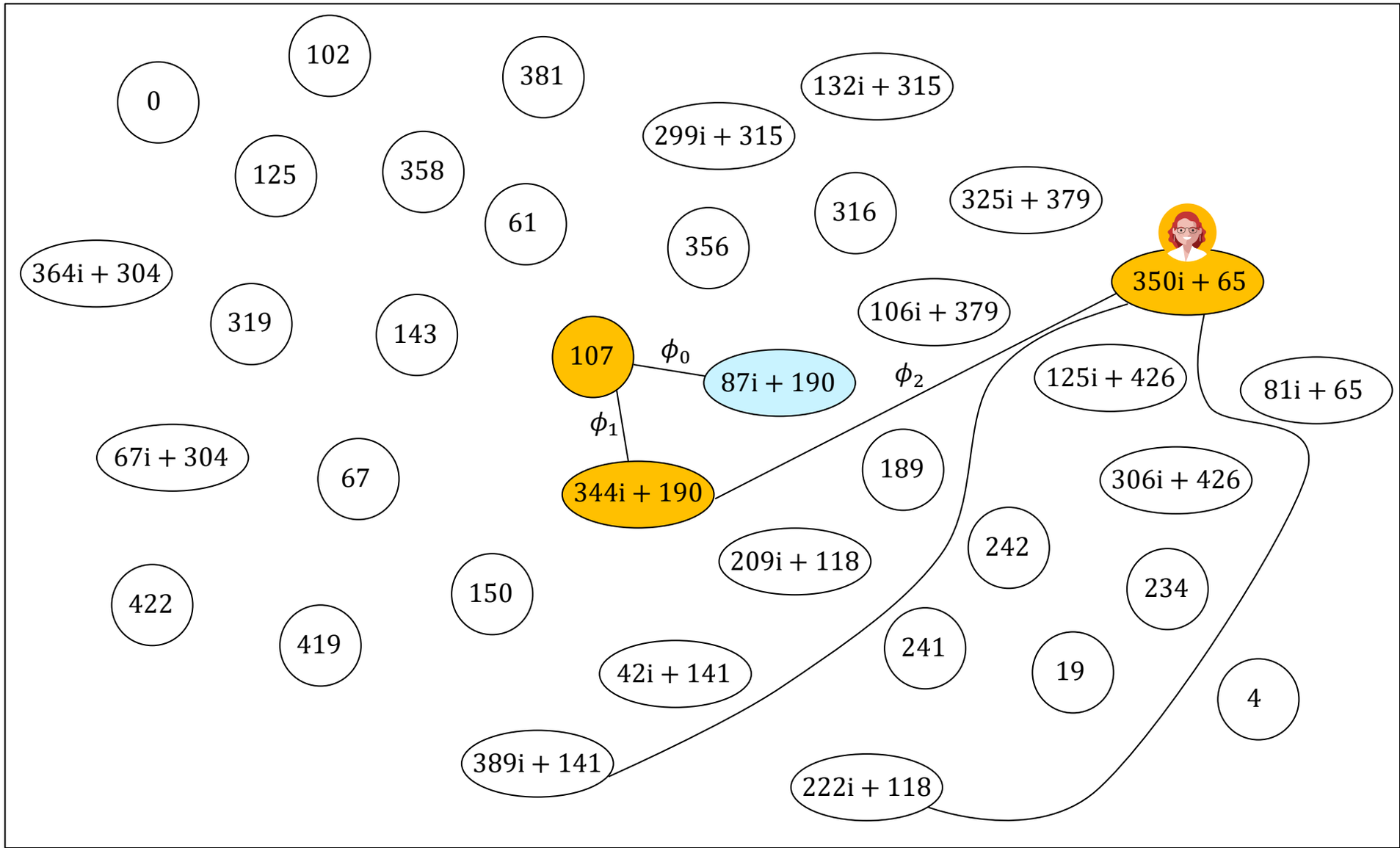
Alice's key generation

ϕ_0

ϕ_1

ϕ_2

$\phi_2(\phi_1(\phi_0(S))) = (208i + 177\ ,\ 0)$



Alice's key generation

ϕ_0

ϕ_1

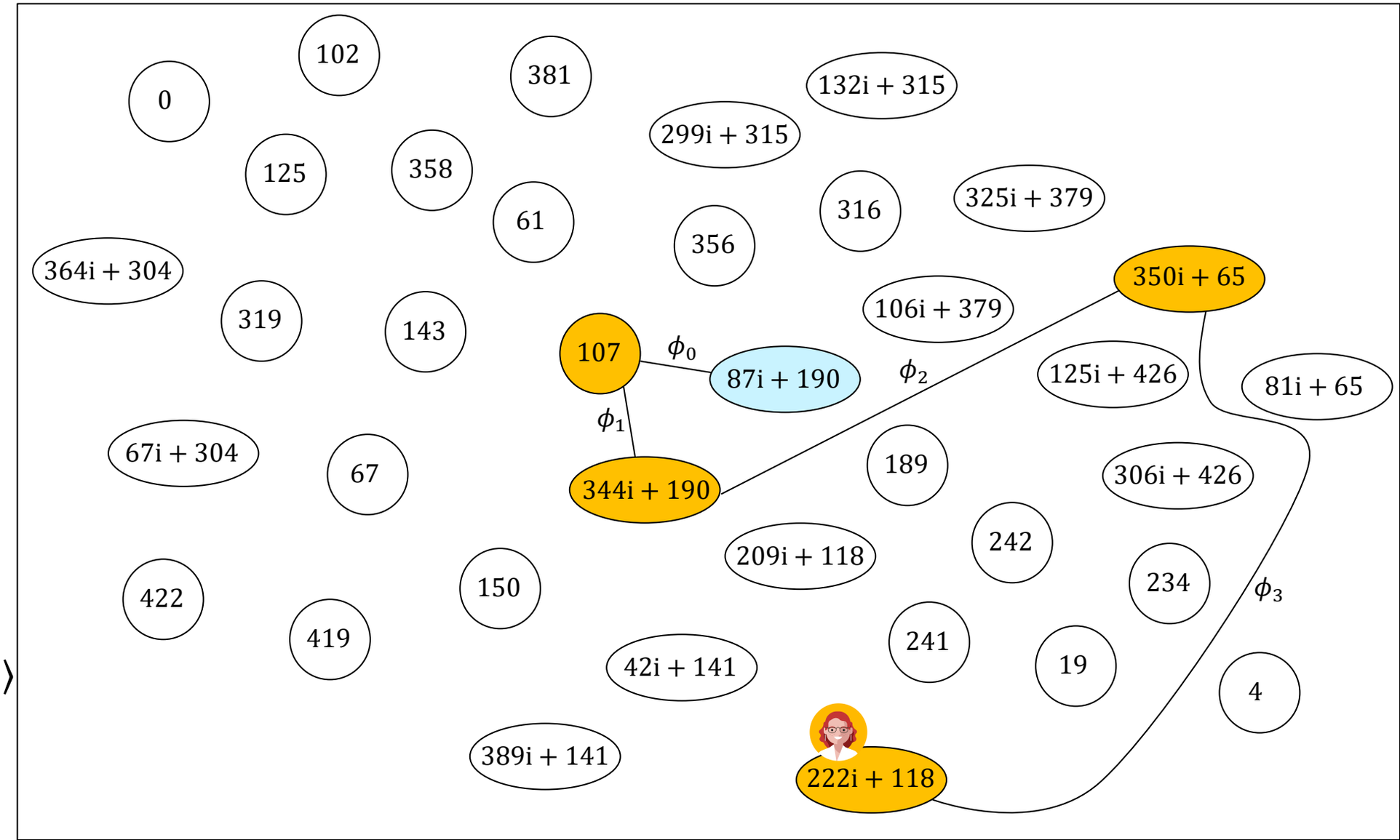
ϕ_2

$\phi_2(\phi_1(\phi_0(S)))= (208i + 177\ , 0)$

$\phi_3 : E_3 \to E_4$

$\ker(\phi_3) = \langle(208i + 177\ , 0)\rangle$

$j(E_4) = 222i + 118$



Summary

in

$k = 11$

Alice's key generation

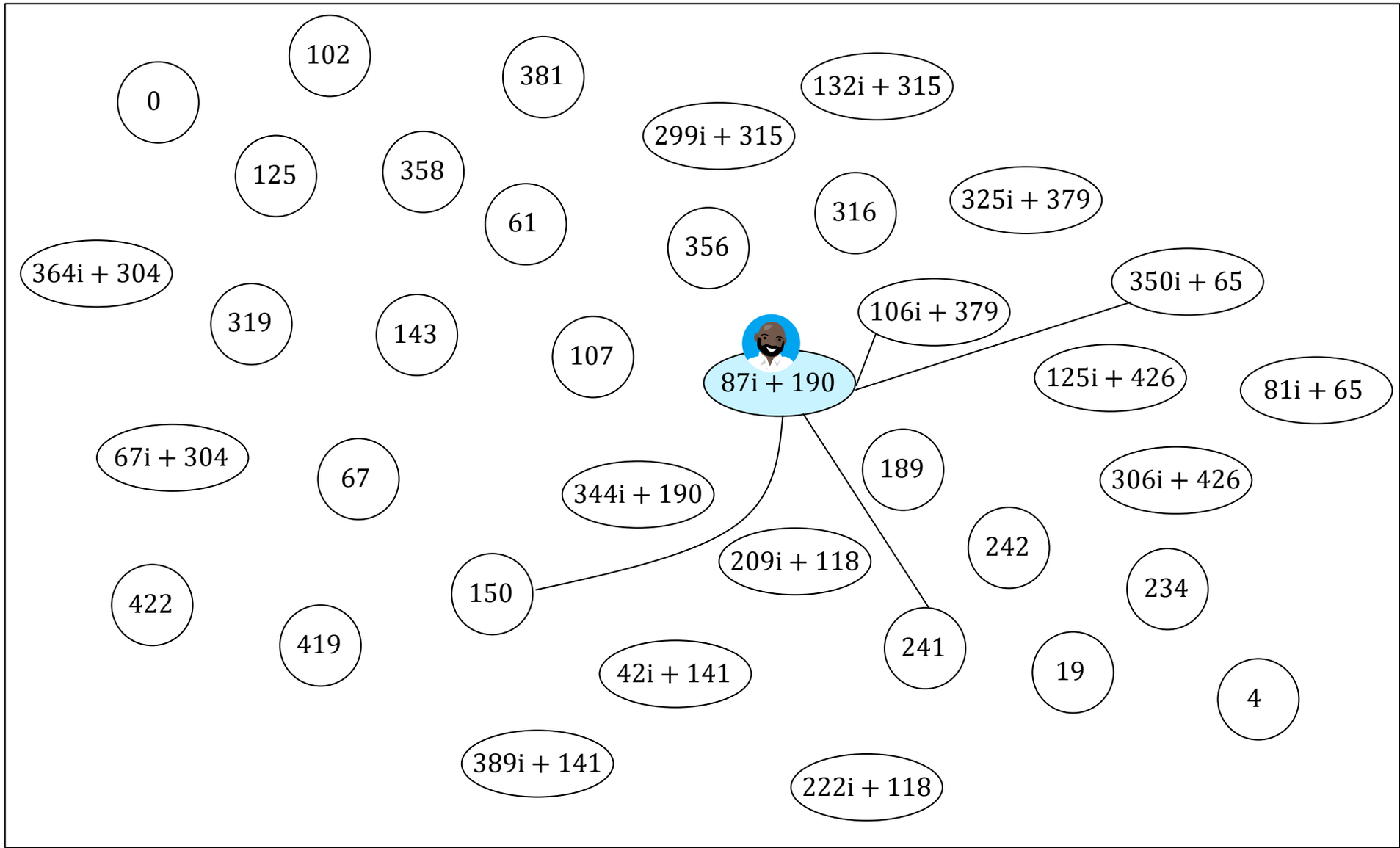
$S_A = P_A + [11]Q_A \longrightarrow E_A = E_0/\langle S_A \rangle$

out

$222i + 118$

Bob's key generation

$S = (122i + 309\ ,\ 291i + 374)$



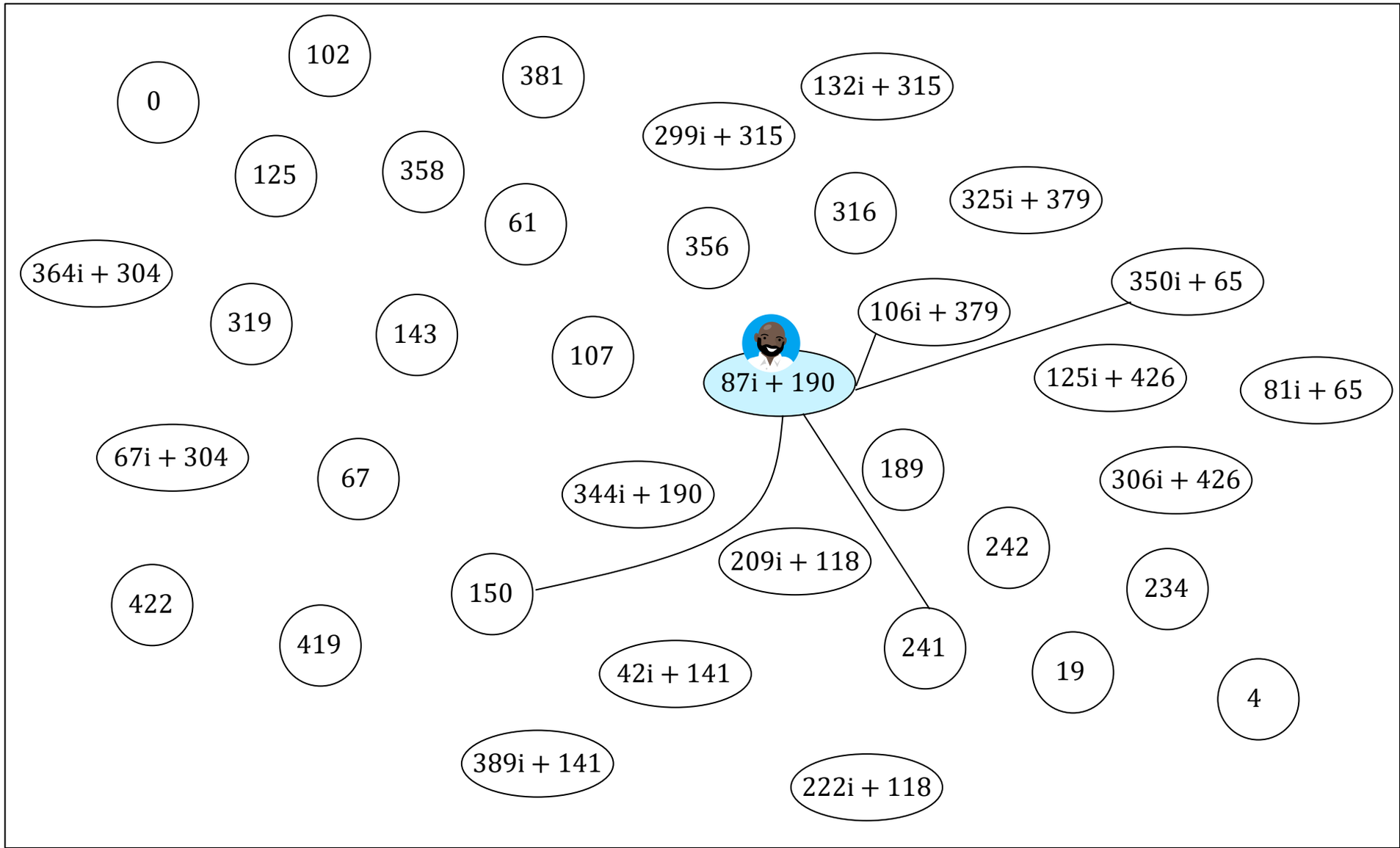
Bob's key generation

$S = (122i + 309\ ,\ 291i + 374)$

[3]

[3]

$S = (23i + 37\ ,\ 4i + 302)$



Bob's key generation

$S = (122i + 309 , 291i + 374)$

[3]

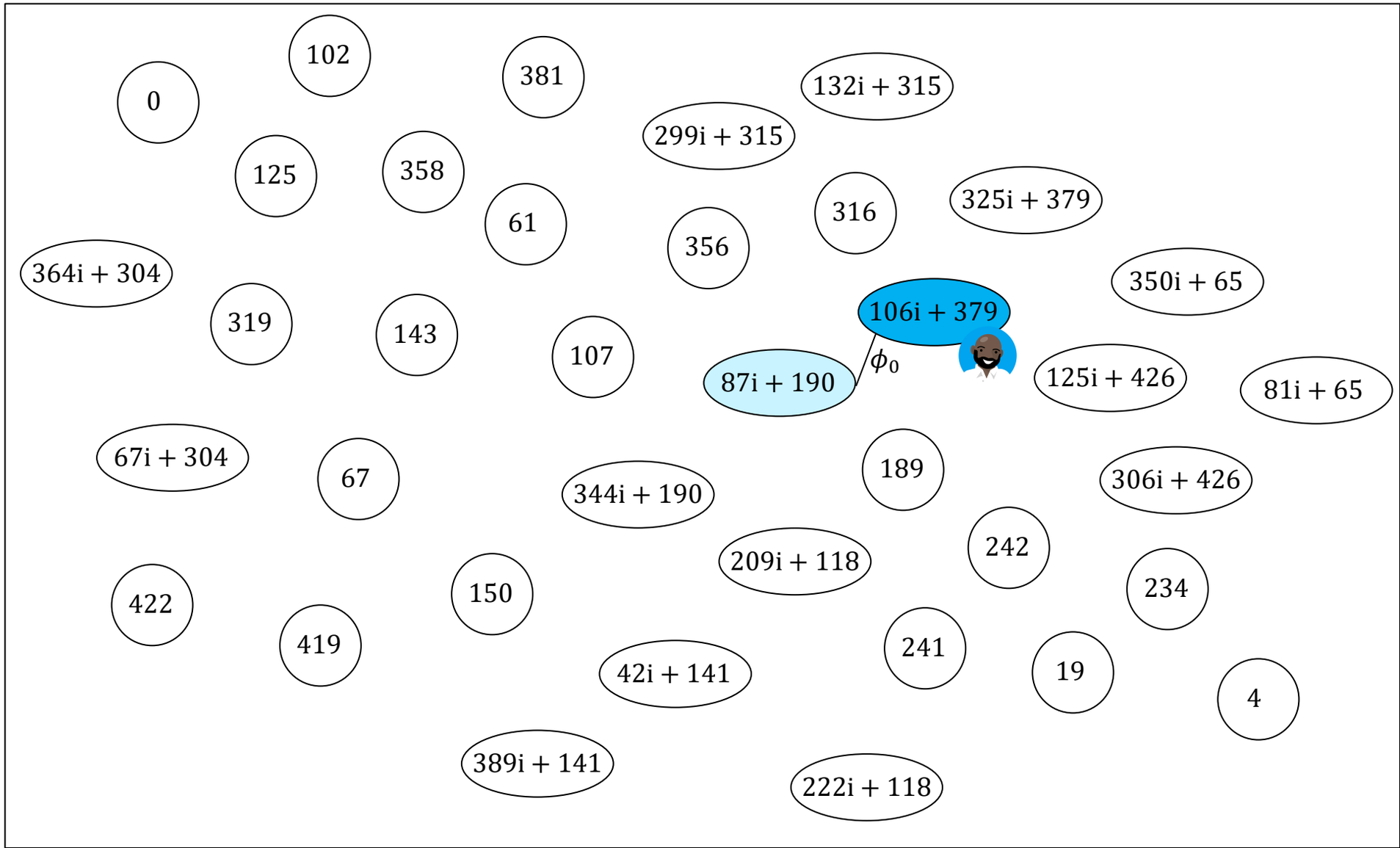
[3]

$[9]S = (23i + 37 , 4i + 302)$

$$\phi_0 : E_0 \to E_1$$

$$\ker(\phi_0) = \langle [9]S \rangle$$

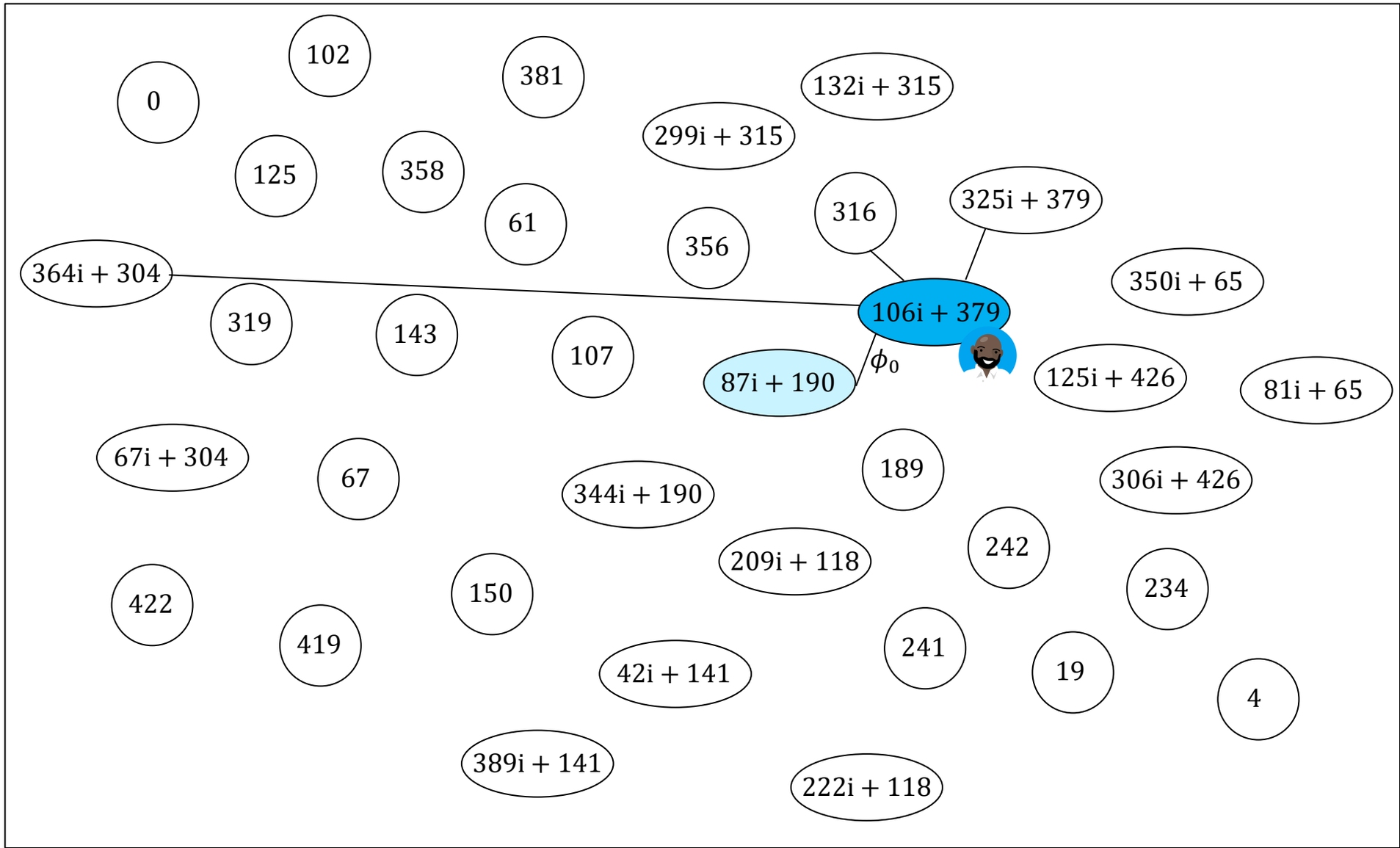
$$j(E_1) = 106i + 379$$



Bob's key generation

ϕ_0

$\phi_0(S) = (277i + 234\ ,\ 183i + 90)$



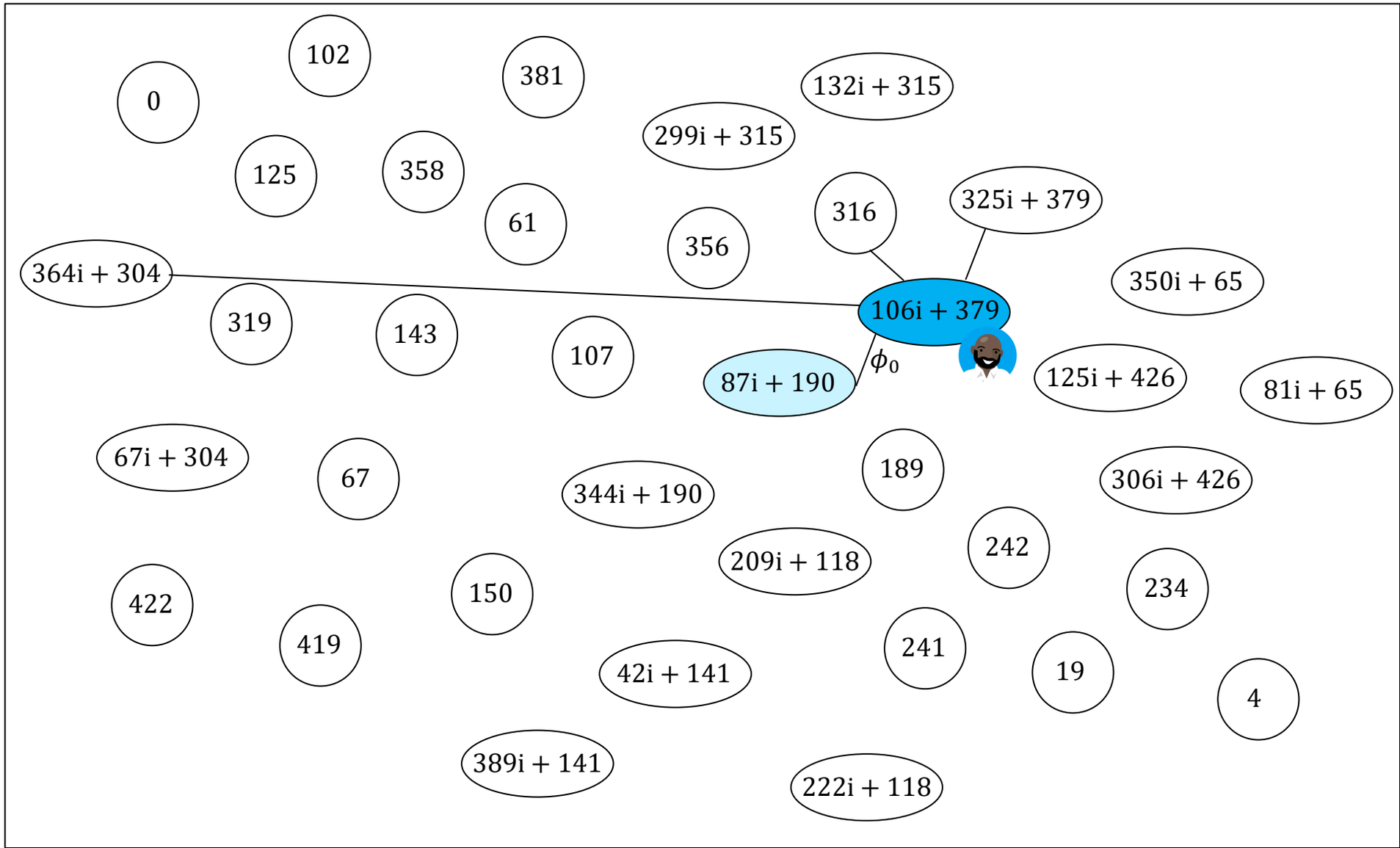
Bob's key generation

ϕ_0

$\phi_0(S) = (277i + 234\ ,\ 183i + 90)$

[3]

$[3]\phi_0(S) = (12i + 410\ ,\ 263i + 350)$



Bob's key generation

ϕ_0

$\phi_0(S) = (277i + 234\ ,\ 183i + 90)$

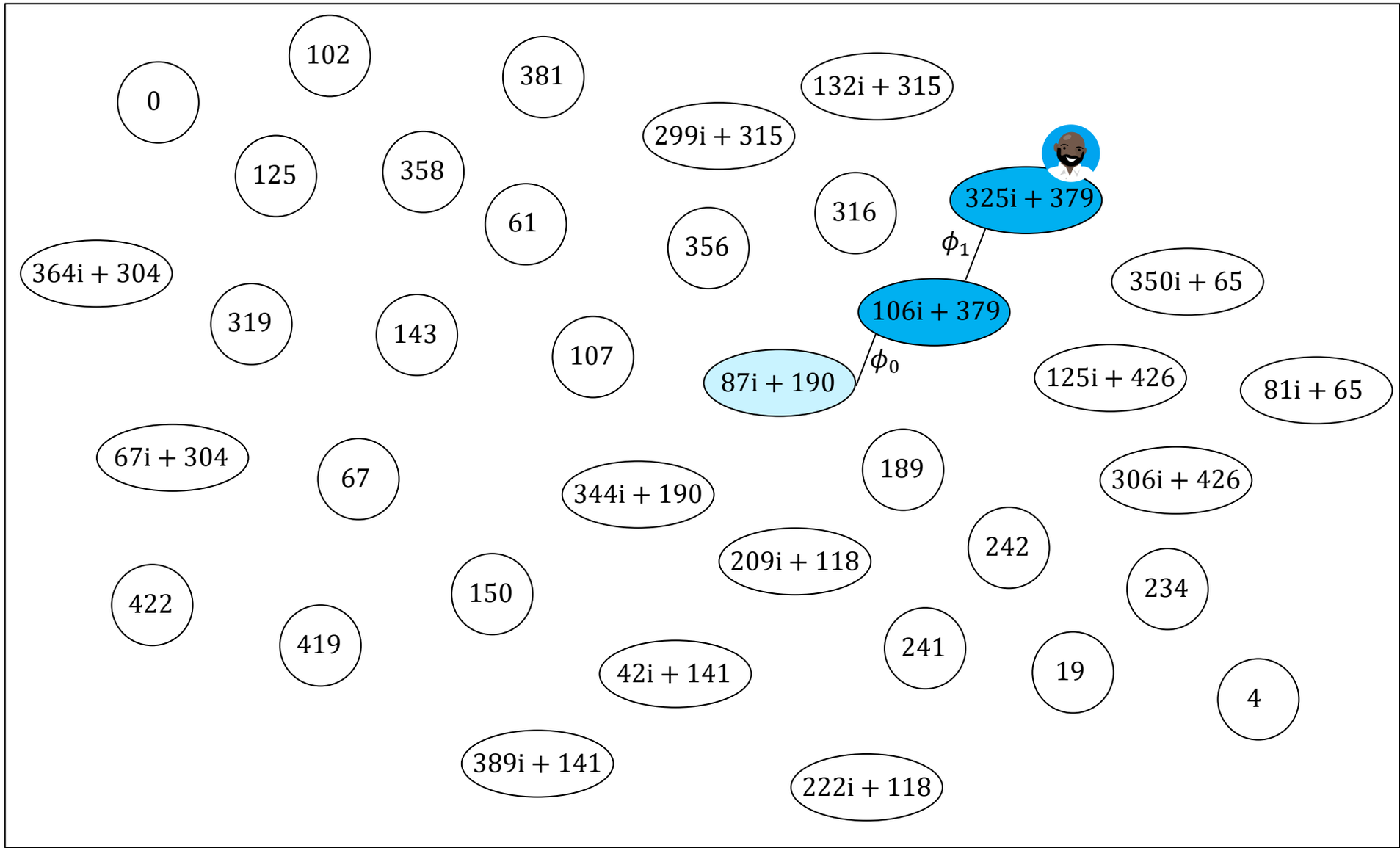
[3]

$[3]\phi_0(S) = (12i + 410\ ,\ 263i + 350)$

$\phi_1 : E_1 \to E_2$

$\ker(\phi_1) = \langle [3]\phi_0(S) \rangle$

$j(E_2) = 325i + 379$



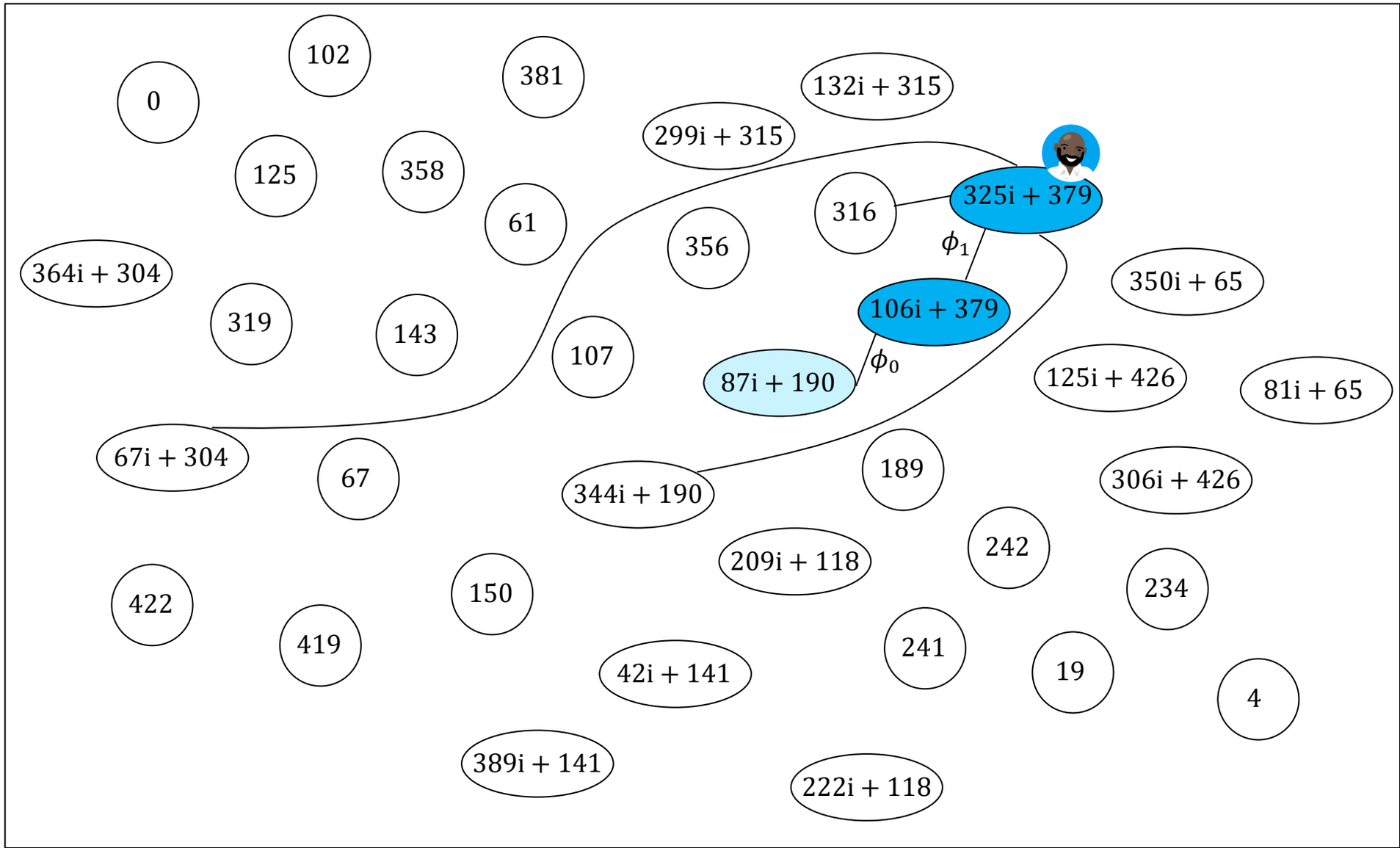
Bob's key generation

ϕ_0

$\phi_0(S) = (277i + 234\,,\, 183i + 90)$

ϕ_1

$\phi_1(\phi_0(S)) = (422i + 207\,,\, 358i + 249)$



Bob's key generation

ϕ_0

$\phi_0(S) = (277i + 234 , 183i + 90)$

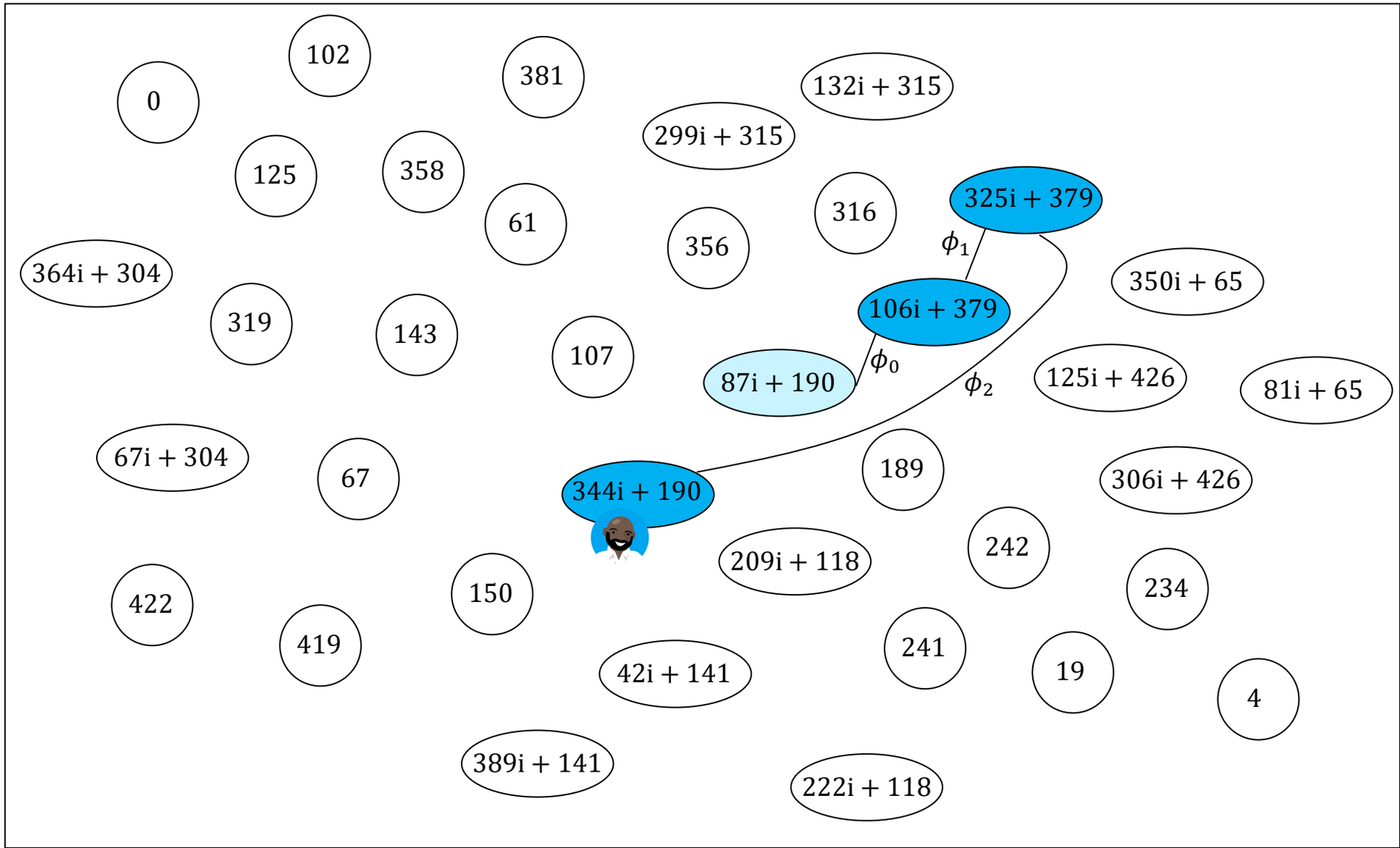
ϕ_1

$\phi_1(\phi_0(S)) = (422i + 207 , 358i + 249)$

$$\phi_2 : E_2 \to E_3$$

$$\ker(\phi_2) = \langle \phi_1(\phi_0(S)) \rangle$$

$$j(E_3) = 344i + 190$$



Summary

in

$k = 2$

Bob's key generation

$S_B = P_B + [2]Q_B \longrightarrow E_B = E_0/\langle S_B \rangle$

out

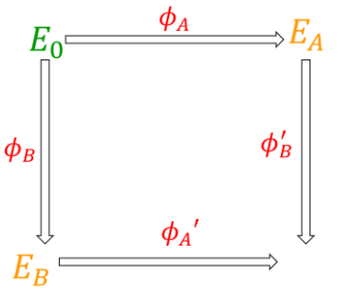
$344i + 190$

Auxiliary points

Alice's public key: $E_A = \phi_A(E_0)$

Bob's public key: $E_B = \phi_B(E_0)$

Auxiliary points



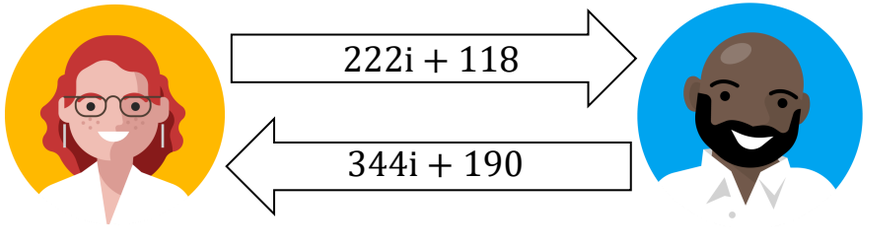
Alice's public key:

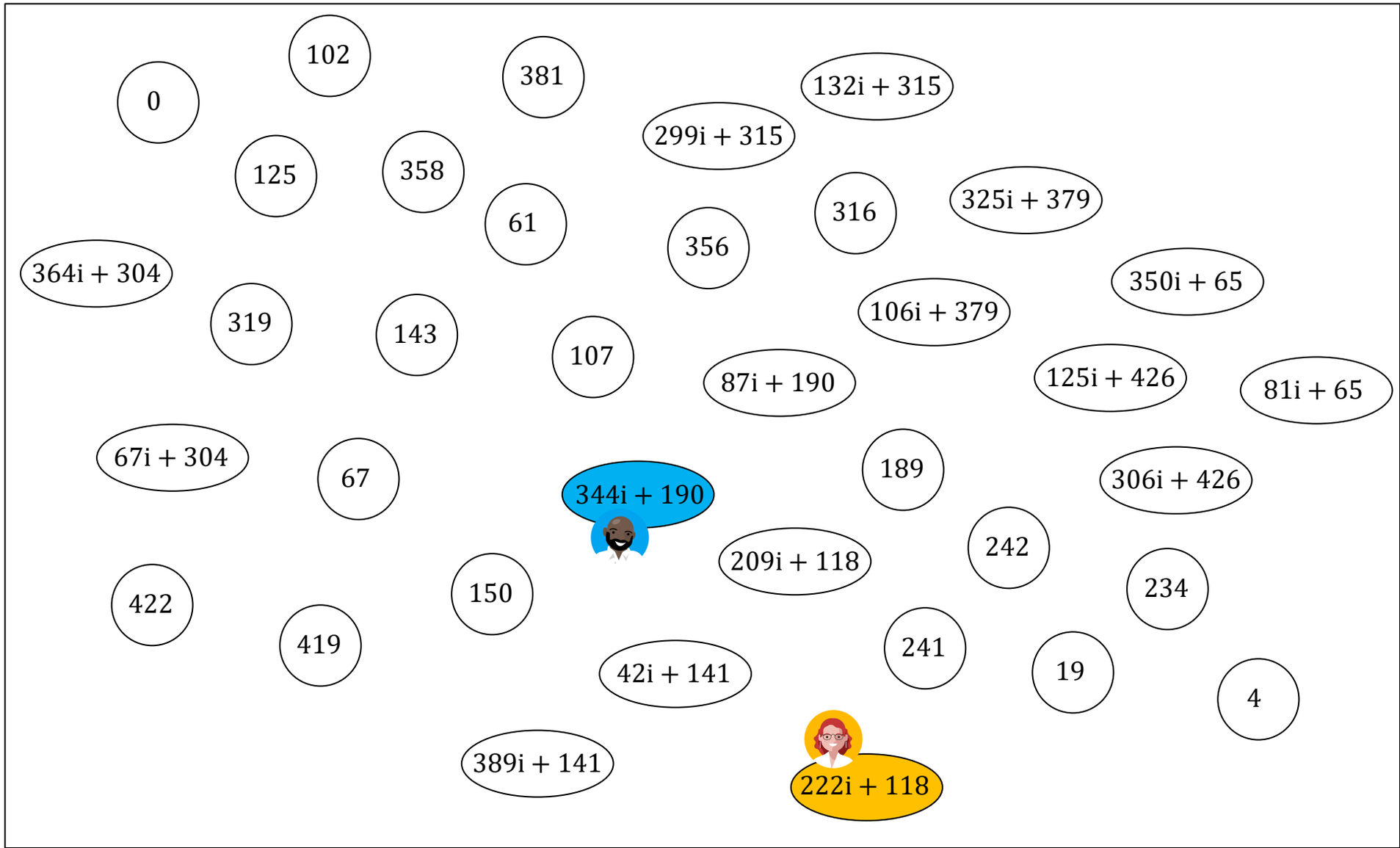
$$E_A = \phi_A(E_0) \qquad P_{AB} = \phi_A(P_B) \qquad Q_{AB} = \phi_A(Q_B)$$

Bob's public key:

$$E_B = \phi_B(E_0) \qquad P_{BA} = \phi_B(P_A) \qquad Q_{BA} = \phi_B(Q_A)$$

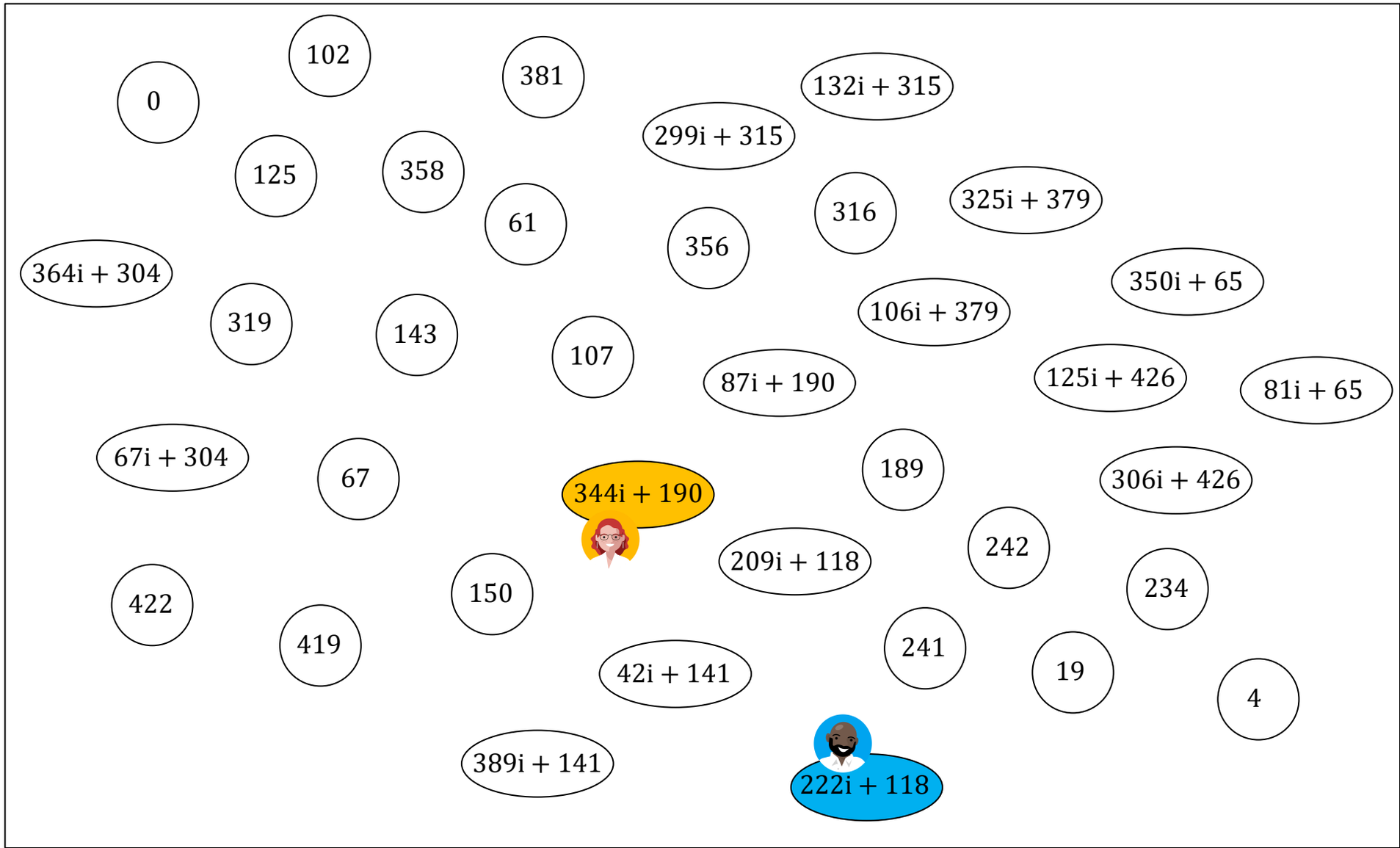
Exchanging public keys





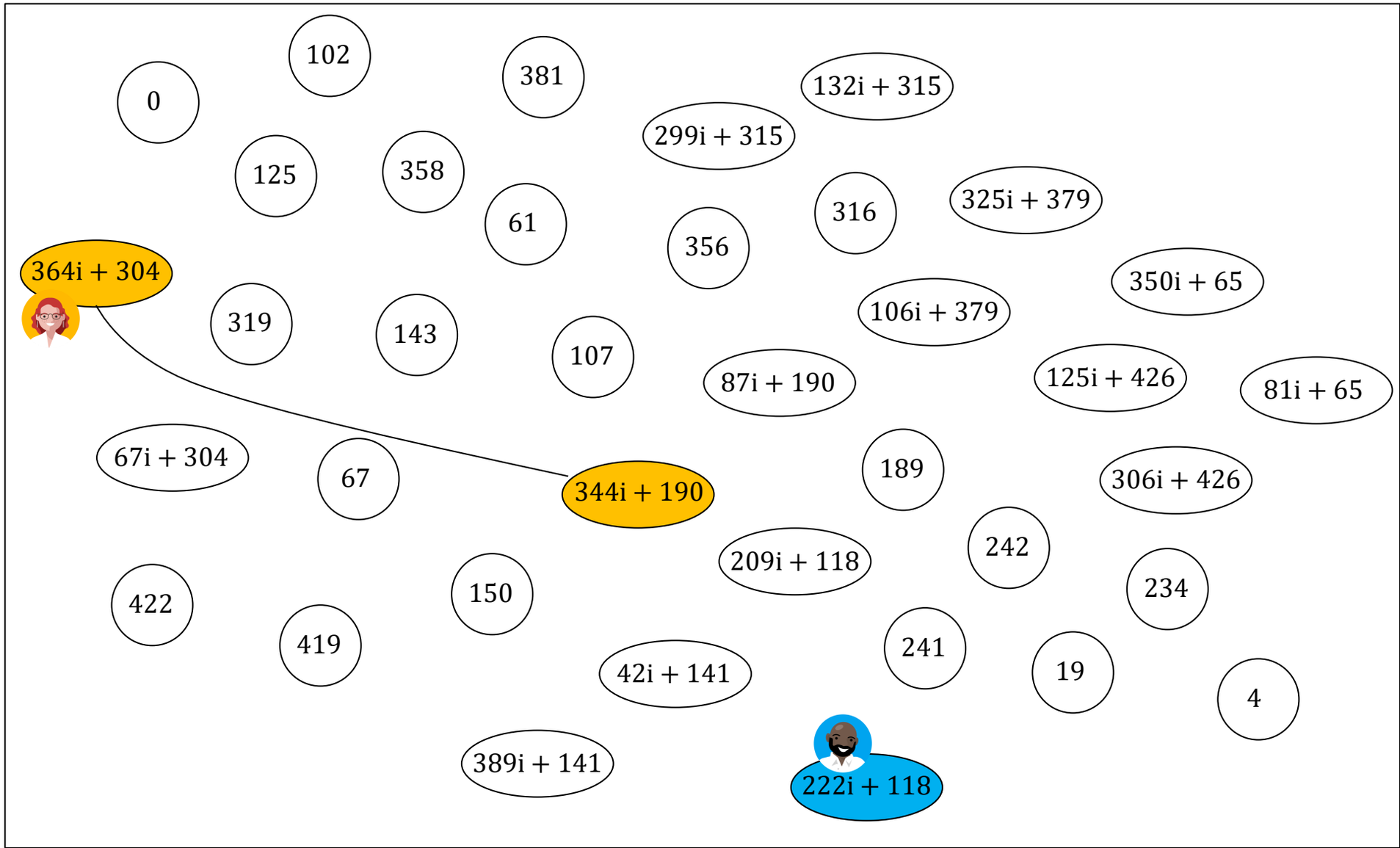
Alice's shared secret

$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$



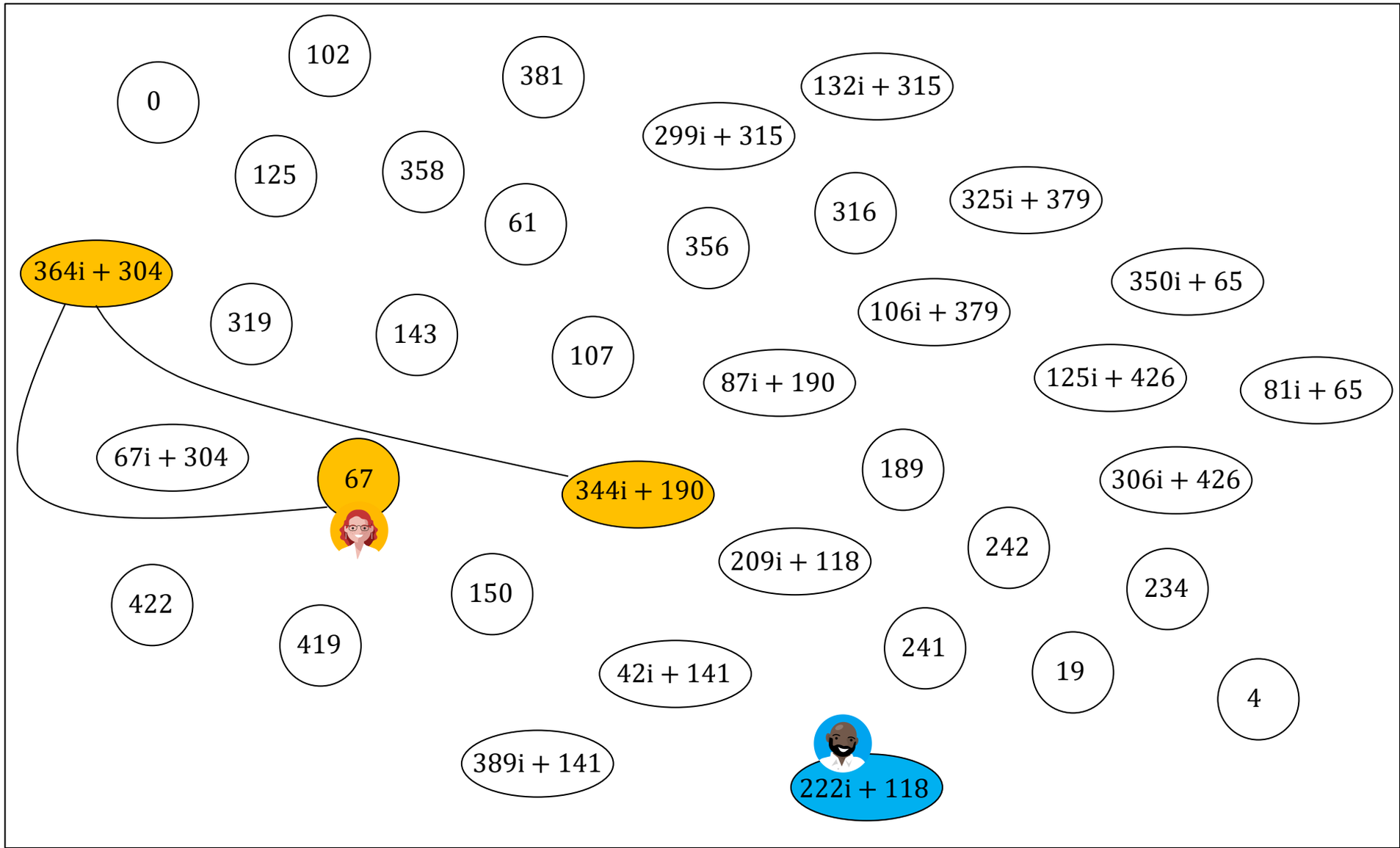
Alice's shared secret

$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$



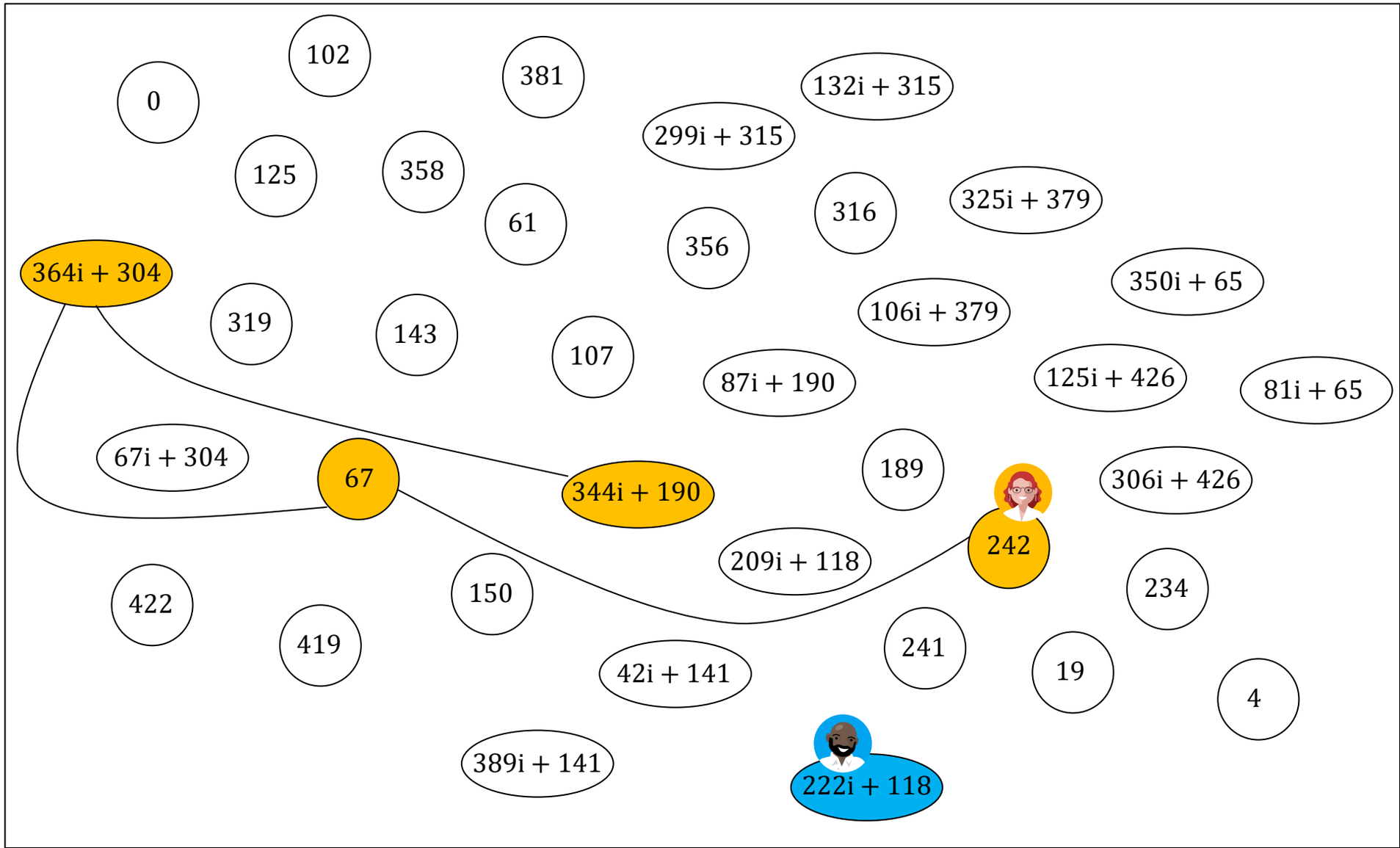
Alice's shared secret

$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$



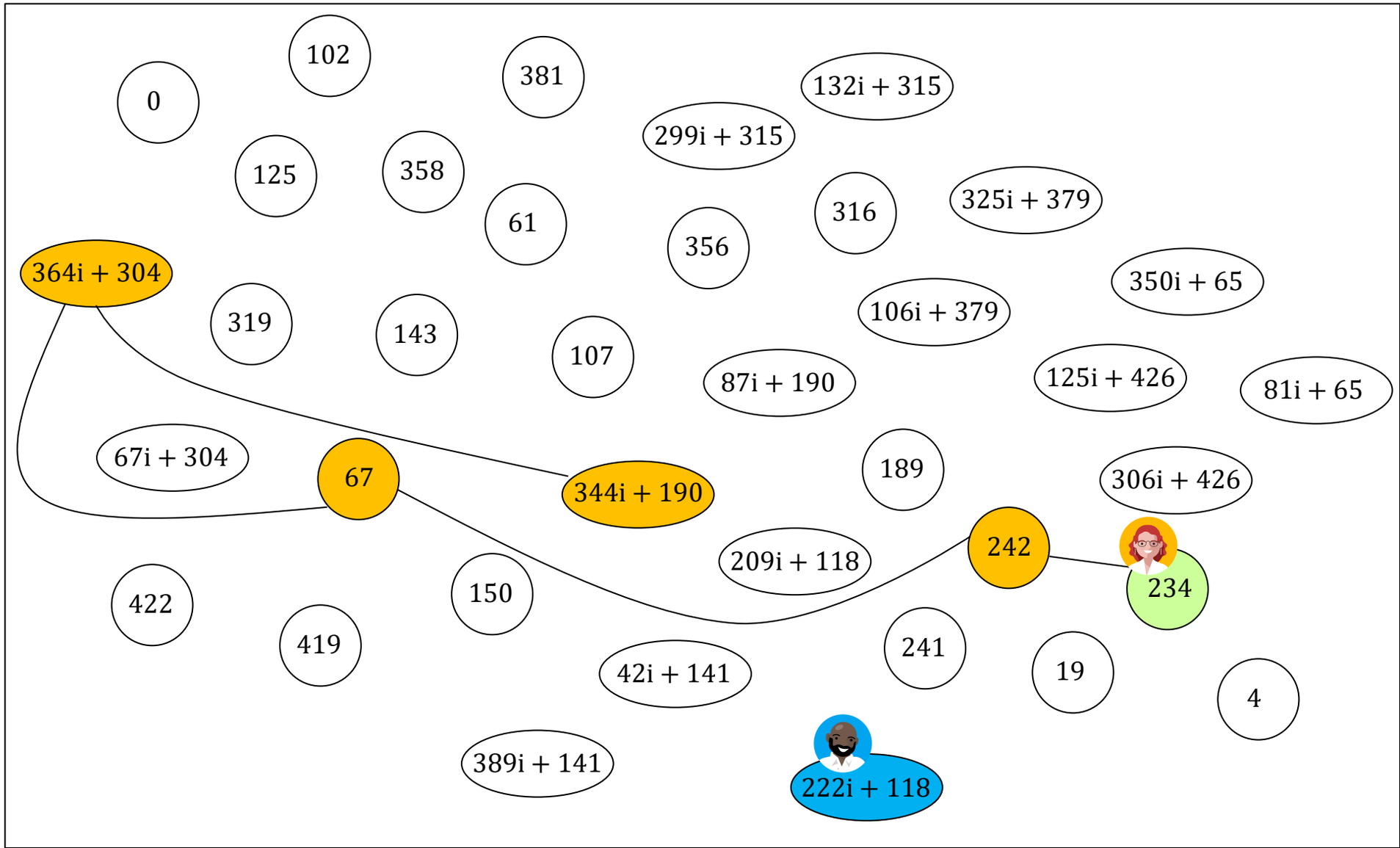
Alice's shared secret

$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$



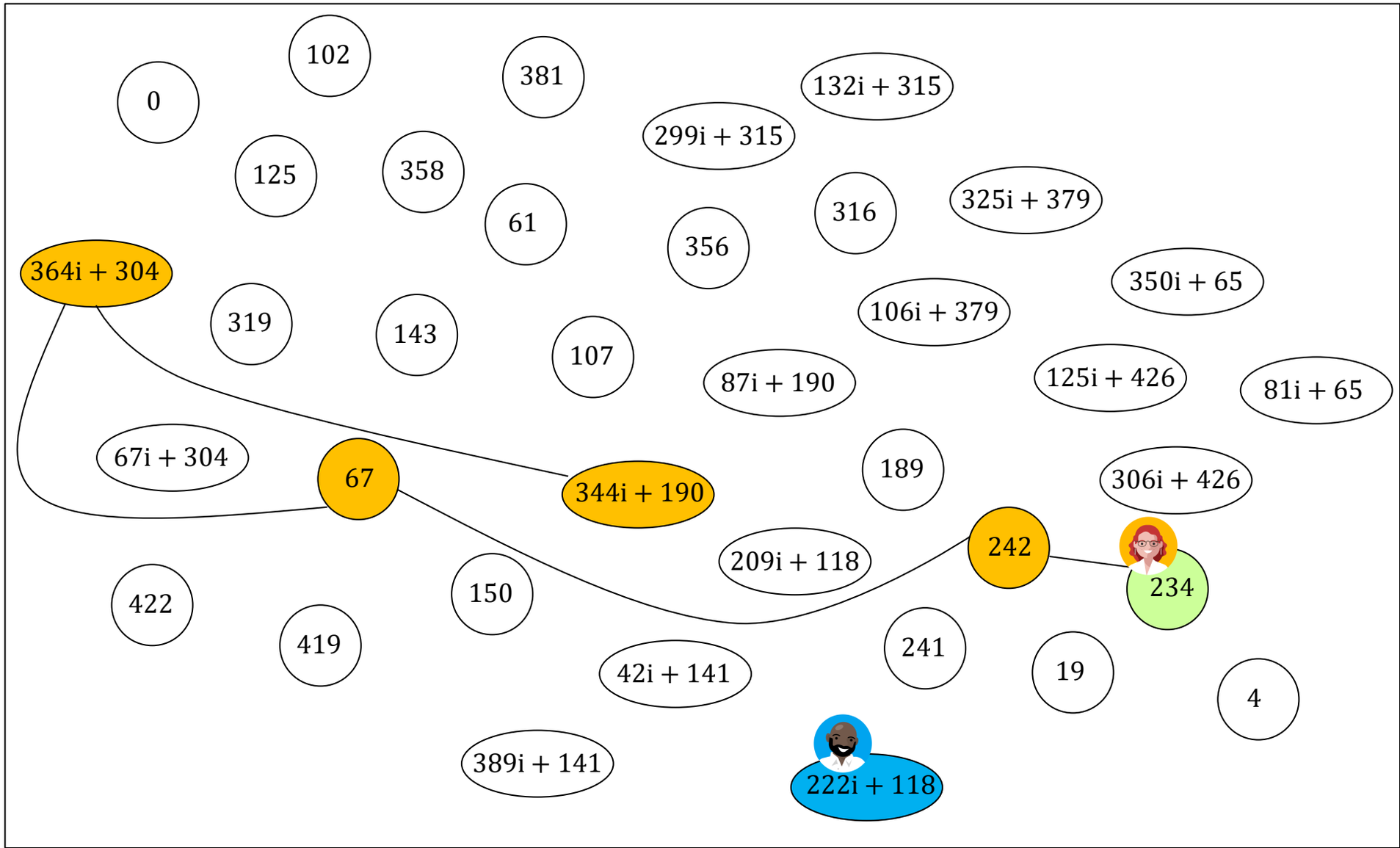
Alice's shared secret

$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$



Bob's shared secret

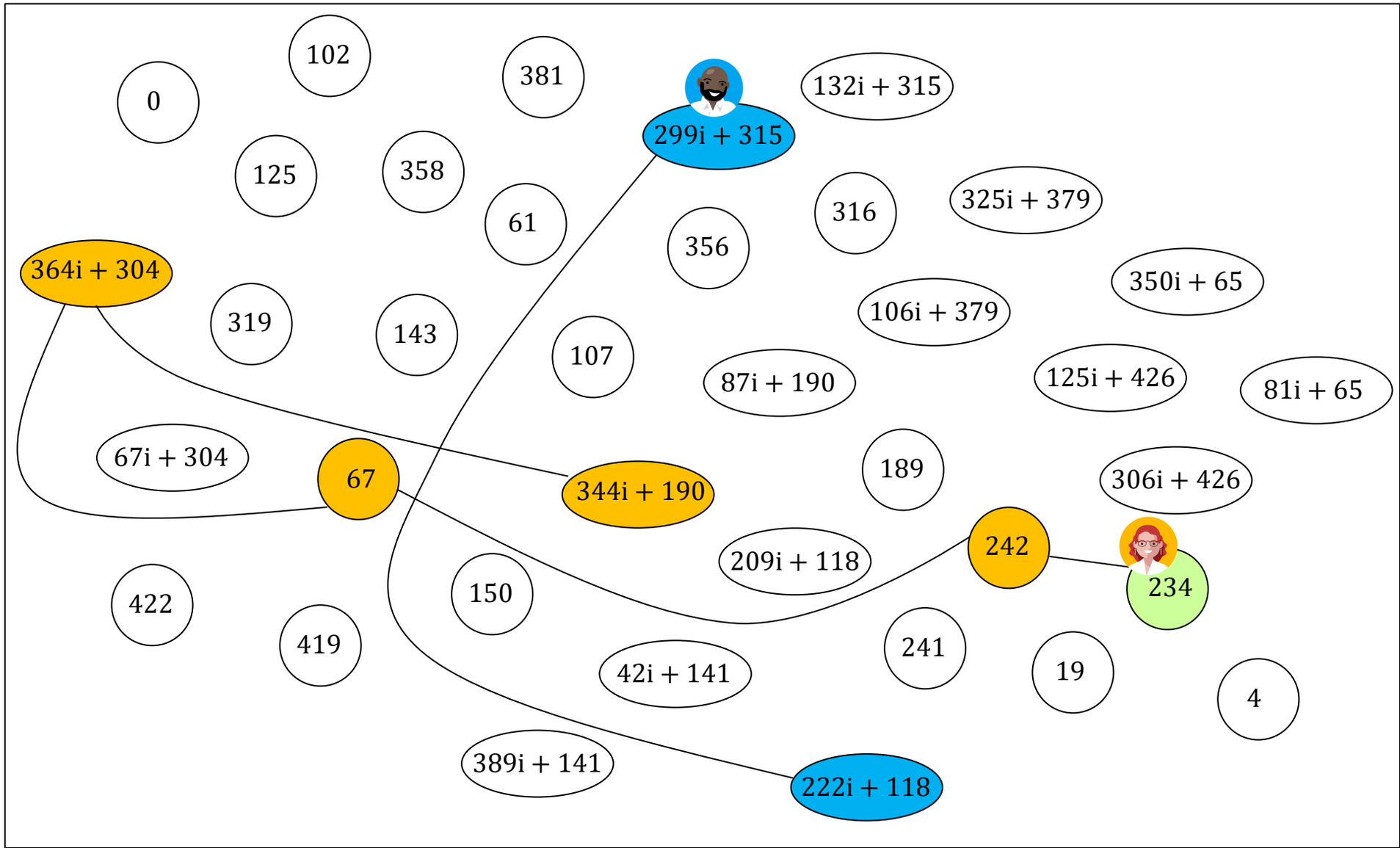
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



$S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B)$

Bob's shared secret

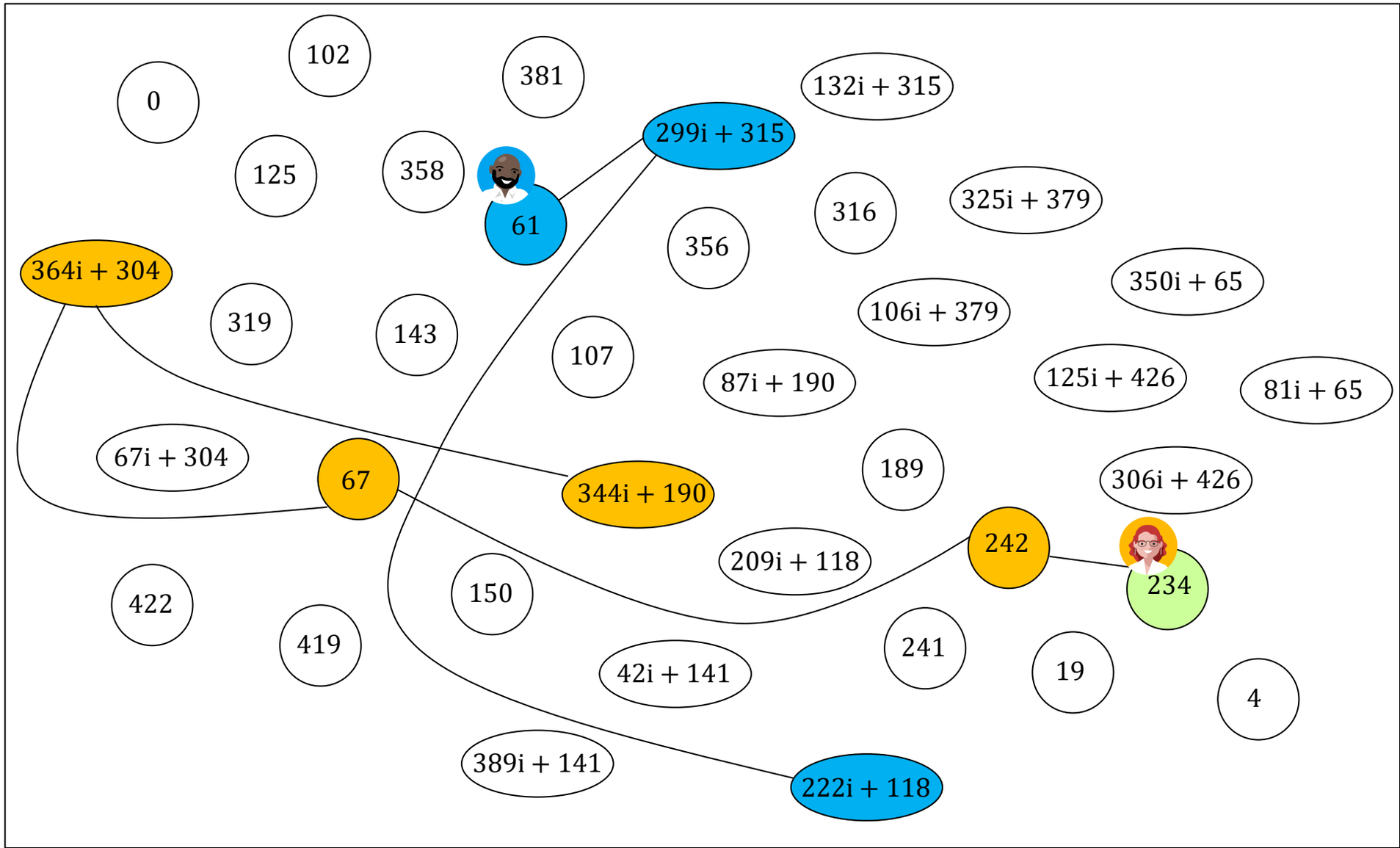
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



$S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B)$

Bob's shared secret

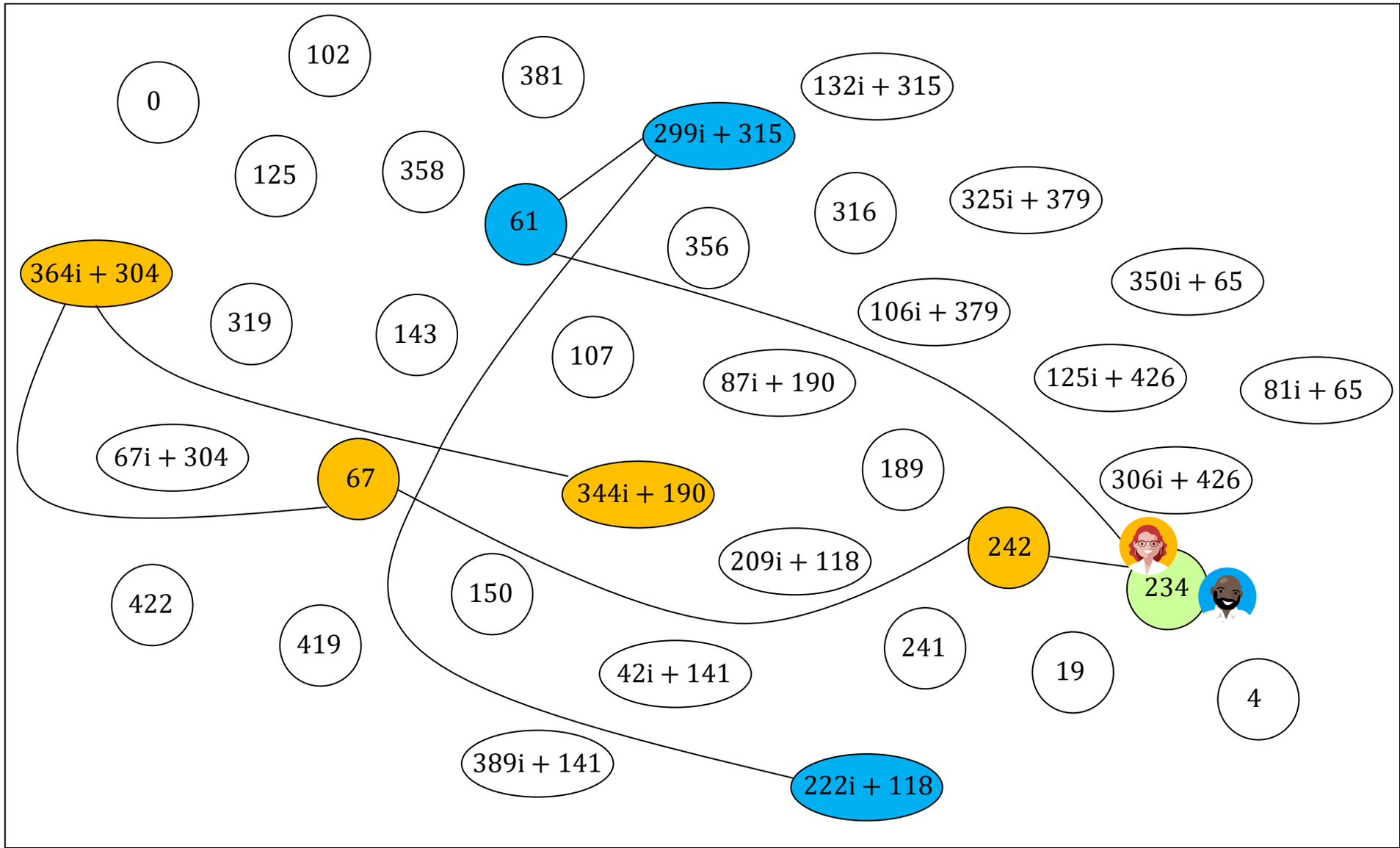
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



$S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B)$

Bob's shared secret

$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



$S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B)$

Why does it work?

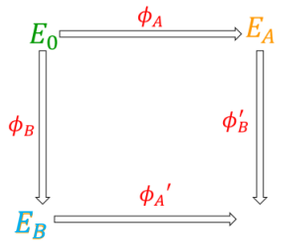
$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$

$$S'_A = \phi_B(P_A) + \phi_B([k_A]Q_A)$$

$$S'_A = \phi_B(P_A + [k_A]Q_A)$$

$$S'_A = \phi_B(S_A)$$

$$\boxed{\phi'_A = E_A/\langle S'_A \rangle}$$



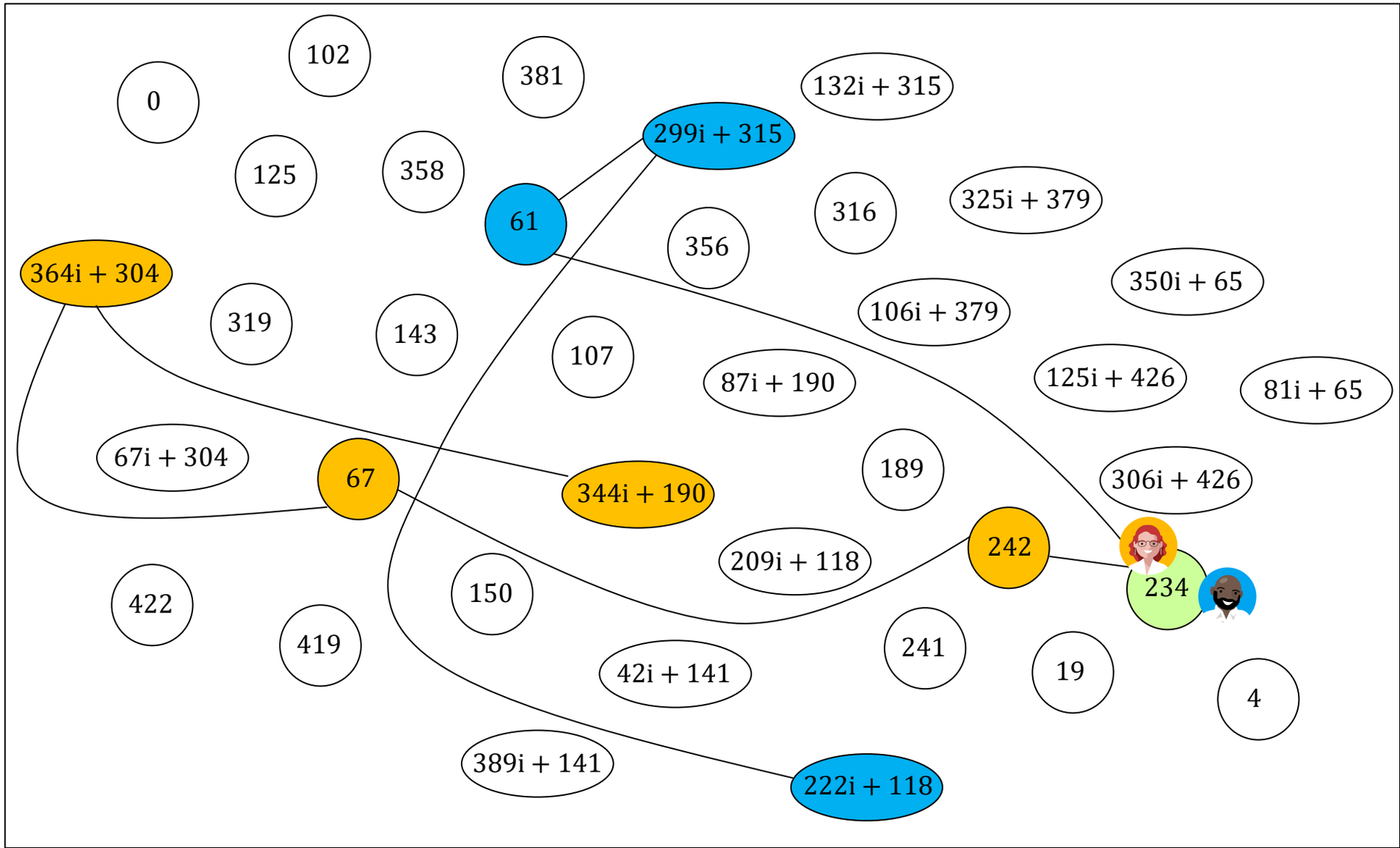
$$\boxed{\phi'_B = E_B/\langle S'_B \rangle}$$

$$S'_B = \phi_A(S_B)$$

$$S'_B = \phi_A(P_B + [k_B]Q_B)$$

$$S'_B = \phi_A(P_B) + \phi_A([k_B]Q_B)$$

$$S'_B = \phi_A(P_B) + [k_B]\phi_A(Q_B)$$



SIDH/SIKE in the real world

	prime p	PK (bytes)	Clock cycles to compute ϕ ($\times 10^6$) i7-6700 Skylake	
				
toy example	$2^4 3^3 - 1$	7	ϵ	ϵ'
SIKEp434	$2^{216} 3^{137} - 1$	330	92	98
SIKEp503	$2^{250} 3^{159} - 1$	378	142	151
SIKEp610	$2^{305} 3^{192} - 1$	462	295	297
SIKEp751	$2^{372} 3^{239} - 1$	564	468	503

https://sike.org/

https://www.microsoft.com/en-us/research/project/sike/

https://csrc.nist.gov/projects/post-quantum-cryptography

Questions?