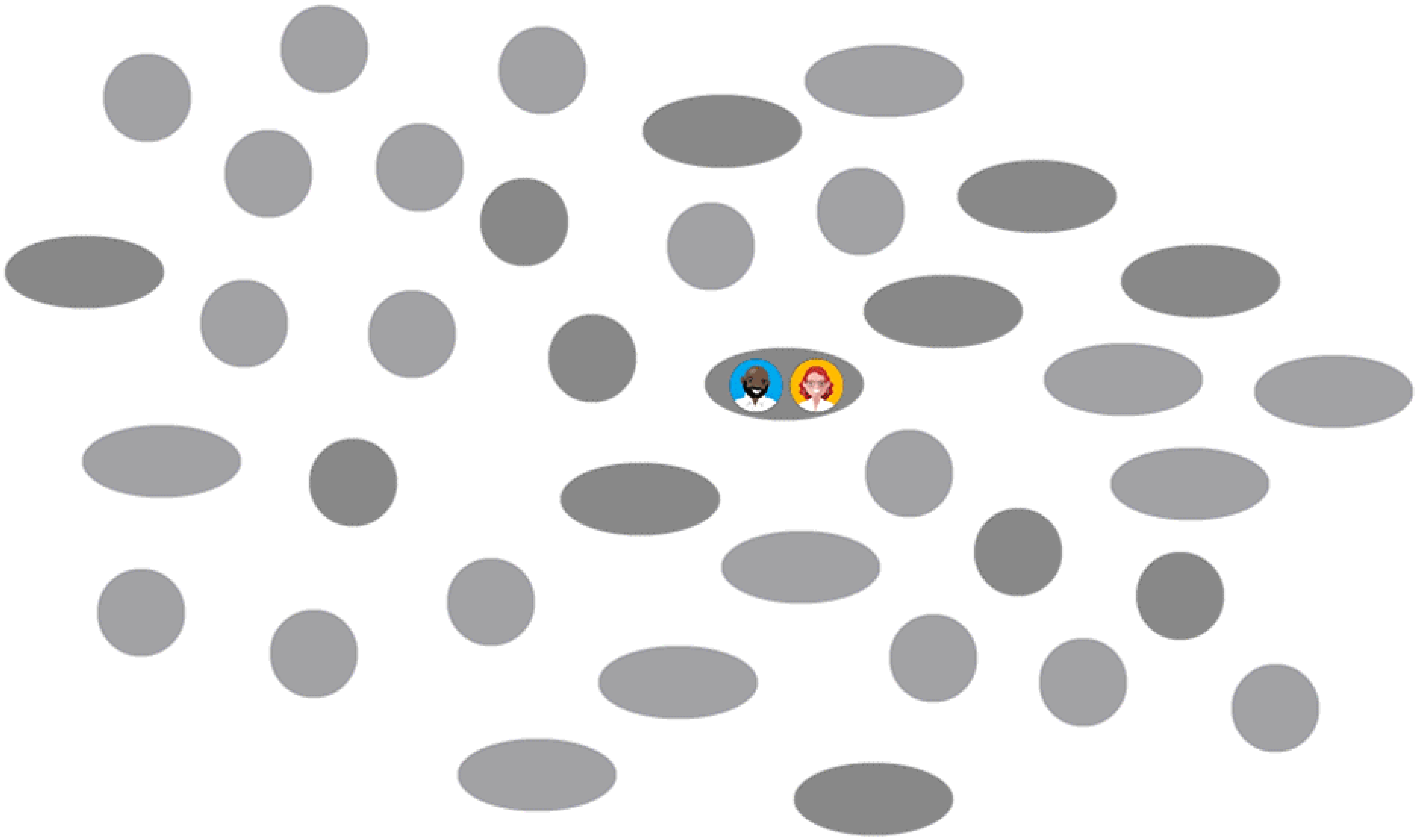
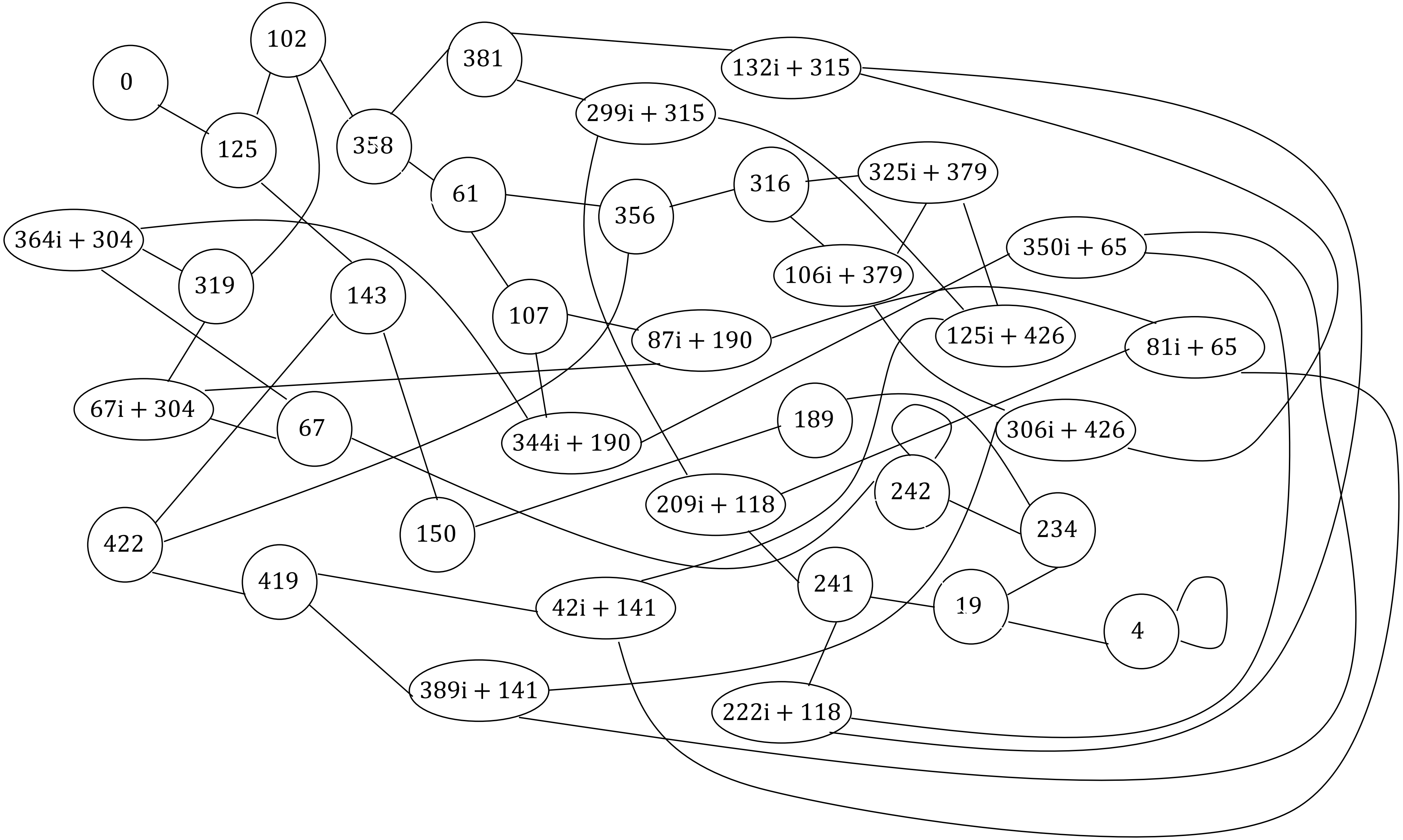
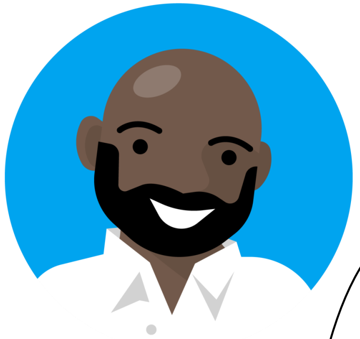
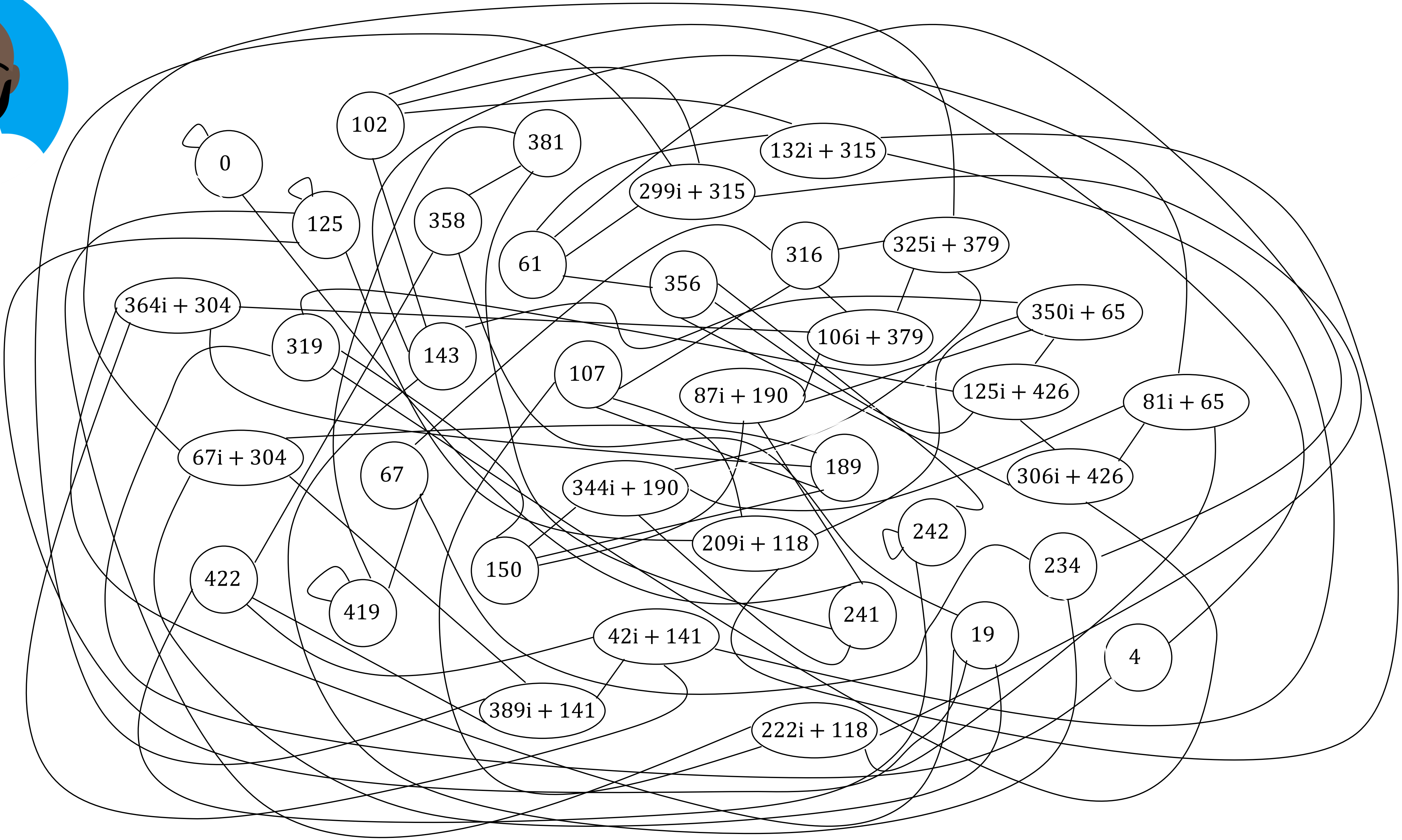
Post-quantum key exchange from supersingular isogenies



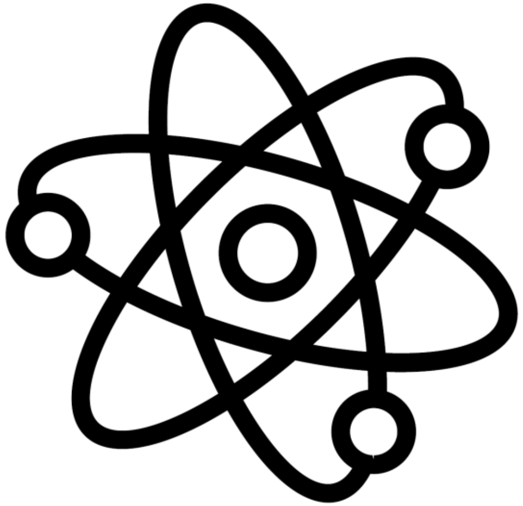
Craig Costello


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
242
209i + 118
234
422
150
419
42i + 141
241
19
4
389i + 141
222i + 118




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

Why?



Question: if a large-scale quantum computer is not built yet, why do we need these schemes deployed now?

Started from the bottom (in 2016), now (exactly 3 weeks ago) we here...

NIST IR 8413

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Gorjan Alagic
Daniel Apon*
David Cooper
Quynh Dang
Thinh Dang
John Kelsey
Jacob Lichtinger
Yi-Kai Liu
Carl Miller
Dustin Moody
Rene Peralta
Ray Perlner
Angela Robinson
Daniel Smith-Tone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8413

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Table 4. Algorithms to be Standardized

Public-Key Encryption/KEMs	**Digital Signatures**
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	**Digital Signatures**
BIKE	
Classic McEliece	
HQC	
SIKE	

Question: how do we know these schemes are all quantum secure?

A brief history of Diffie-Hellman key exchange

Question: why do we need public key cryptography?

Diffie-Hellman key exchange (circa 1976)

$q = 160693804425899027554196209234116260252220299378279283530 1301$

$g = 123456789$

$g^a \text{ mod } q = 7846737452942265357975459631985270257549969298008577 7948593$

$5600481042932181286674410213424831338026262713942994101287 98 = g^b \text{ mod } q$

$a =$
685408003627063
761059275919665
781694368639459
527871881531452

$b =$
362059131912941
987637880257325
269696682836735
524942246807440

$g^{ab} \text{ mod } q = 437452857085801785219961443000845969831329749878767465041215$

Index calculus

$$\text{solve} \quad g^x \equiv h \pmod p$$
$$\text{e.g.} \quad 3^x \equiv 37 \pmod{1217}$$

- factor base $p_i = \{2,3,5,7,11,13,17,19\}$, $\#p_i = 8$
- Find 8 values of k where 3^k splits over p_i, i.e., $3^k \equiv \pm\prod p_i \bmod p$

$(\text{mod } 1217)$

$$\begin{aligned}
3^1 &\equiv 3 \\
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \\
3^{25} &\equiv 5^3 \\
3^{30} &\equiv -2 \cdot 5^2 \\
3^{34} &\equiv -3 \cdot 7 \cdot 19 \\
3^{54} &\equiv -5 \cdot 11 \\
3^{71} &\equiv -17 \\
3^{87} &\equiv 13
\end{aligned}$$

$(\text{mod } 1216)$

$$\begin{aligned}
1 &\equiv L(3) \\
24 &\equiv 608 + 2 \cdot L(2) + L(7) + L(13) \\
25 &\equiv 3 \cdot L(5) \\
30 &\equiv 608 + L(2) + 2 \cdot L(5) \\
34 &\equiv 608 + L(3) + L(7) + L(19) \\
54 &\equiv 608 + L(5) + L(11) \\
71 &\equiv 608 + L(17) \\
87 &\equiv L(13)
\end{aligned}$$

$(\text{mod } 1216)$

$$\begin{aligned}
L(2) &\equiv 216 \\
L(3) &\equiv 1 \\
L(5) &\equiv 819 \\
L(7) &\equiv 113 \\
L(11) &\equiv 1059 \\
L(13) &\equiv 87 \\
L(17) &\equiv 679 \\
L(19) &\equiv 528
\end{aligned}$$

Index calculus

solve $g^x \equiv h \pmod{p}$

e.g. $3^x \equiv 37 \pmod{1217}$

$L(2) \equiv 216$
$L(3) \equiv 1$
$L(5) \equiv 819$
$L(7) \equiv 113$
$L(11) \equiv 1059$
$L(13) \equiv 87$
$L(17) \equiv 679$
$L(19) \equiv 528$

Now search for j such that $g^j \cdot h = 3^j \cdot 37$ factors over p_i

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}$$

$$L(37) \equiv 3 \cdot L(2) + L(7) + L(11) - 16 \pmod{1216}$$
$$\equiv 3 \cdot 216 + 113 + 1059 - 1$$
$$\equiv 588$$

Subexponential complexity $L_p[1/3, (64/9)^{1/3}] = e^{\left((64/9)^{1/3} + o(1)\right)(\ln(p))^{1/3} \cdot (\ln\ln(p))^{2/3}}$

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
6052422101474898256696660124195726100495725510022002932814218768060112310763455404567248761396399633344901857872119208518550803791724

411604662069593306683228525653441872410777999220572079993574397237156368762038378332742471939666544968793817819321495269833613169937
986164811320795616949957400518206385310292475529284550626247132930124027703140131220968771142788394846592816111078275196955258045178
705254016469773509936925361994895894163065551105161929613139219782198757542984826465893457768888915561514505048091856159412977576049
073563225572809880970058396501719665853110101308432647427786565525121328772587167842037624190143909787938665842005691911199739672645 5
110758448552553744288464337906540312125397571803103278271979007681841394534114315726120595749993896347981789310754194864577435905673
172970033596584445206671223874399576560291954856168126236657381519414592942037018351232440467191228145585909045861278091800166330876
40732384471994880701268730488602792217616292819610462552195843277148172486262439624136130759567700180173857249994951177791494168821 88

$= g^b \pmod q$

$a =$

7147687166405;957187905360554739658 2
692405186145916522354912615715297097
100679170037904924330116019497881089
087696131592831386326210951294944584
400497488929803858493191812844757232 1
023987160439062006177648318875457556
233770853912505292364631833219121732 1
464134655845254917228378772756695589
845219962202945089226966507426526912
7802446416400\9025927104004338958261
141986237587898819361218794559180286 4
062679\8648395781392730436849555977 64
1300972122182491581096457937635455 6\6
554629883777859568089157882151127357
4220422646379170599917677567\30420698
422392494816906777896174923072071297
603455802621072109220\54662739697748
553543758990879608882627763290293452
560094576029847\3913613887675543866
224792652999780598864724145304621 94
52761811989\974647725290887806049 3
179541951463829228890455778045929 43
73052654\104851802640020794151939 83
851143425084273119820368274789460 58
7100\304977477069244278989689910572
120963577252034804024499138445834 48

$b =$

655456209464694;93360682685816031704
969423104727624468251177438749706128
879957701\93698826859762790479113062
308975863428283798589097017957365590
672\83571386389571224667609499300898
554802446403039544300748002507962036
386619315229886063541005322448463915
897986412102737725583739 65\486539312
854838650709031919742048649235894391
903529930326769610 05\088404319792729
916038927477470940948581926791161465
02863521484987\08623286193422239171 7
121545686125300672760188085915004248
49476686\70678405106871539770685266 4
532638332403983747338379697022624261
377163163204493828299206039808703403
575100467337085017748387148822224875
309641791879395483731754620034884930
5403999505191916794712 24\05558557093
219350747155777569598163700850920394
70528193639241108 4\43600686183528465
724969562186437214972625833222544865
99616046455 8\546299370165894704252 64
445624157899586972652935647856967092
689604\42796501209877036845001246792
761563917639959736383038665362727158

$g^{ab} =$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880006673 9
419999231378970715307039317876258453876701124543849520979430233302777503265010724513551209279573183234934359636696506
968325769489511028943698821518689496597758218540767517885836464160289471651364552490713961456608536013301649753975875
610659655755567474438180357958360226708742348175045563437075840969230826767034061119437657466993989389348289599600338
950372251336932673571743428823026014699232071116171392219599691096846714133643382745709376112500514300983651201961186
613464267685926563624589817259637248558104903657371981684417053993082671827345252841433337325420088380059232089174946
086536664984836041334031650438692639106287627157575758383128971053401037407031731509582807639509448704617983930135028
759658938329275199307916131883904312132911893000994819789990758698610895359142027942687477942356022103846 8

Diffie-Hellman key exchange (cont.)

- Individual secret keys secure under Discrete Log Problem (DLP): $g, g^x \mapsto x$
- Shared secret secure under Diffie-Hellman Problem (DHP): $g, g^a, g^b \mapsto g^{ab}$
- Fundamental operation in DH is group exponentiation: $g, x \mapsto g^x$
  … done via "square-and-multiply", e.g., $(x)_2 = (1,0,1,1,0,0,0,1 \ldots)$
- We are working "$\mathbf{mod}\ q$", but only with <u>one operation</u>: multiplication
- Main reason for fields being so big: (sub-exponential) index calculus attacks!

DH key exchange (Koblitz-Miller style)

If all we need is a group, why not use elliptic curve groups?

MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 203–209

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over $GF(2^n)$. We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

1. Introduction. The earliest public key cryptosystems using number theory were based on the structure either of the multiplicative group $(\mathbf{Z}/N\mathbf{Z})^*$ or the multiplicative group of a finite field $GF(q)$, $q = p^n$. The subsequent construction of analogous systems based on other finite Abelian groups, together with H. W. Lenstra's success in using elliptic curves for integer factorization, make it natural to study the possibility of public key cryptography based on the structure of the group of points of an elliptic curve over a large finite field. We first briefly recall the facts we need about such elliptic curves (for more details, see [4] or [5]). We then describe elliptic curve analogs of the Massey-Omura and ElGamal systems. We give some concrete examples, discuss the question of primitive points, and conclude with a theorem concerning the probability that the order of a cyclic subgroup is nonsmooth.

I would like to thank A. Odlyzko for valuable discussions and correspondence, and for sending me a preprint by V. S. Miller, who independently arrived at some similar ideas about elliptic curves and cryptography.

2. Elliptic Curves. An elliptic curve E_K defined over a field K of characteristic $\neq 2$ or 3 is the set of solutions $(x, y) \in K^2$ to the equation

$$y^2 = x^3 + ax + b, \qquad a, b \in K \tag{1}$$

(where the cubic on the right has no multiple roots). More precisely, it is the set of such solutions together with a "point at infinity" (with homogeneous coordinates $(0, 1, 0)$; if K is the real numbers, this corresponds to the vertical direction which the tangent line to E_K approaches as $x \to \infty$). One can start out with a more complicated general formula for E_K which can easily be reduced to (1) by a linear change of variables whenever $\operatorname{char} K \neq 2, 3$. If $\operatorname{char} K = 2$—an important case in

---

Received October 29, 1985; revised June 5, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T71, 94A60; Secondary 68P25, 11Y11, 11Y40.

Use of Elliptic Curves in Cryptography

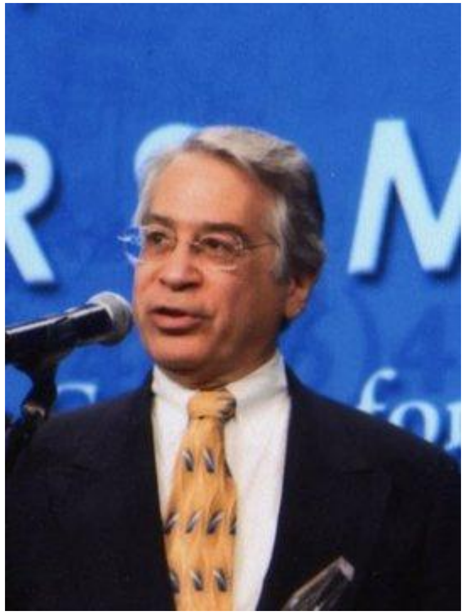
Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 417-426, 1986.
© Springer-Verlag Berlin Heidelberg 1986



Rationale: "it is extremely unlikely that an index calculus attack on the elliptic curve method will ever be able to work" [Miller, 85]

NIST Curve P-256

NIST NISTReCur.pdf

csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf

RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE

July 1999

This collection of elliptic curves is recommended for Federal government use and contains choices of private key length and underlying fields.

§1. Parameter Choices

§2. Curves over Prime Fields

For each prime p, a pseudo-random curve

$$E: \quad y^2 \equiv x^3 - 3x + b \pmod{p}$$

National Institute of Standards and Technology

Curve P-256

$p =$ 115792089210356248762697446949407573530086143415290314195533631308867097853951

$r =$ 115792089210356248762697446949407573529996955224135760342422259061068512044369

$s =$ c49d3608 86e70493 6a6678e1 139d26b7 819f7e90

$c =$ 7efba166 2985be94 03cb055c 75d4f7e0 ce8d84a9 c5114abc af317768 0104fa0d

$b =$ 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

$G_x =$ 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

$G_y =$ 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

ECDH key exchange (1999 – nowish)

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

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

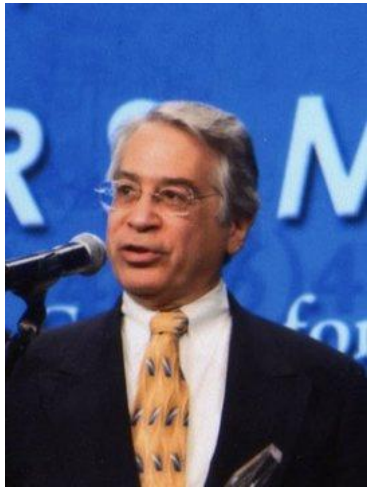
$$E/\mathbb{F}_p : y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,$
$36134250956749795798585127919587881956611106672985015071877198253568414405109)$

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

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



$a =$
89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

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

$b =$
10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

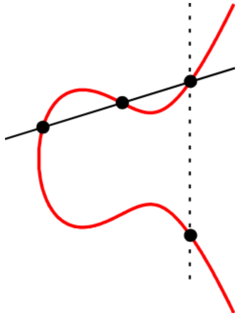
Diffie-Hellman instantiations

$\mathbb{Z}_q$

$g^a \bmod q$

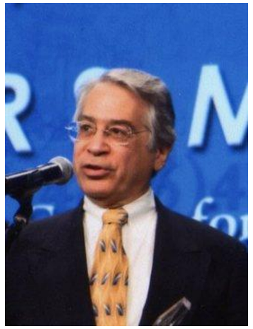
$g^b \bmod q$

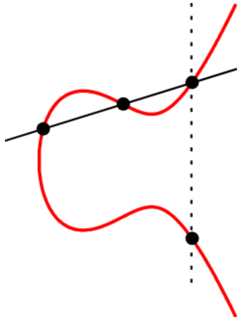
$\mathbb{Z}_q$

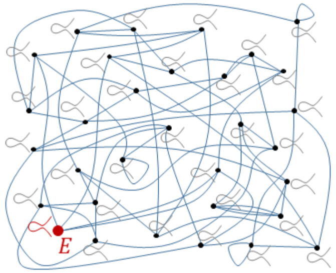


$[a]P$

$[b]P$

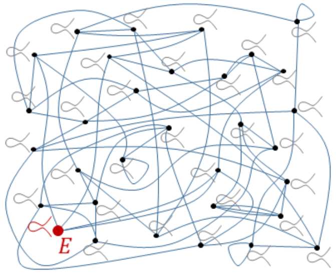






$\phi_A(E)$

$\phi_B(E)$

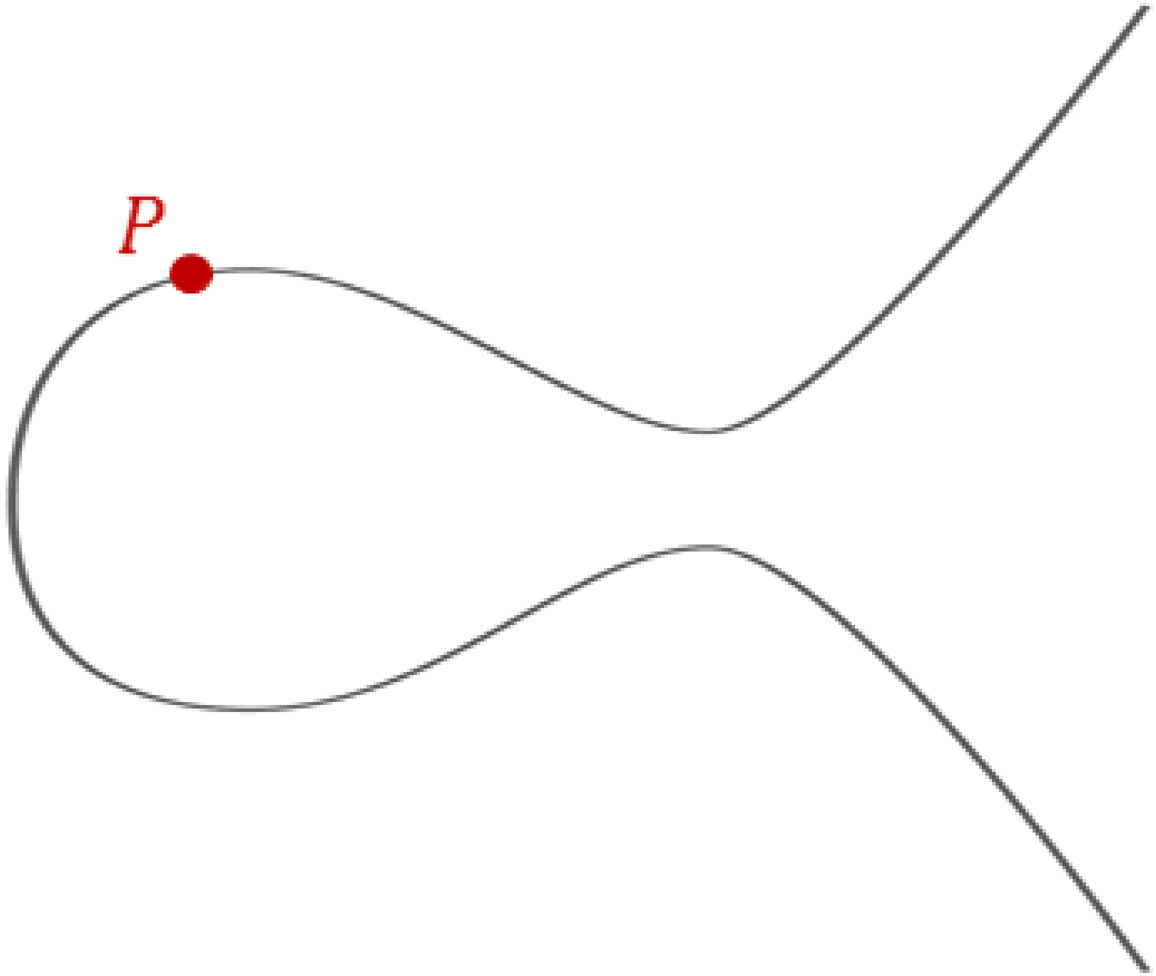


Diffie-Hellman instantiations

	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

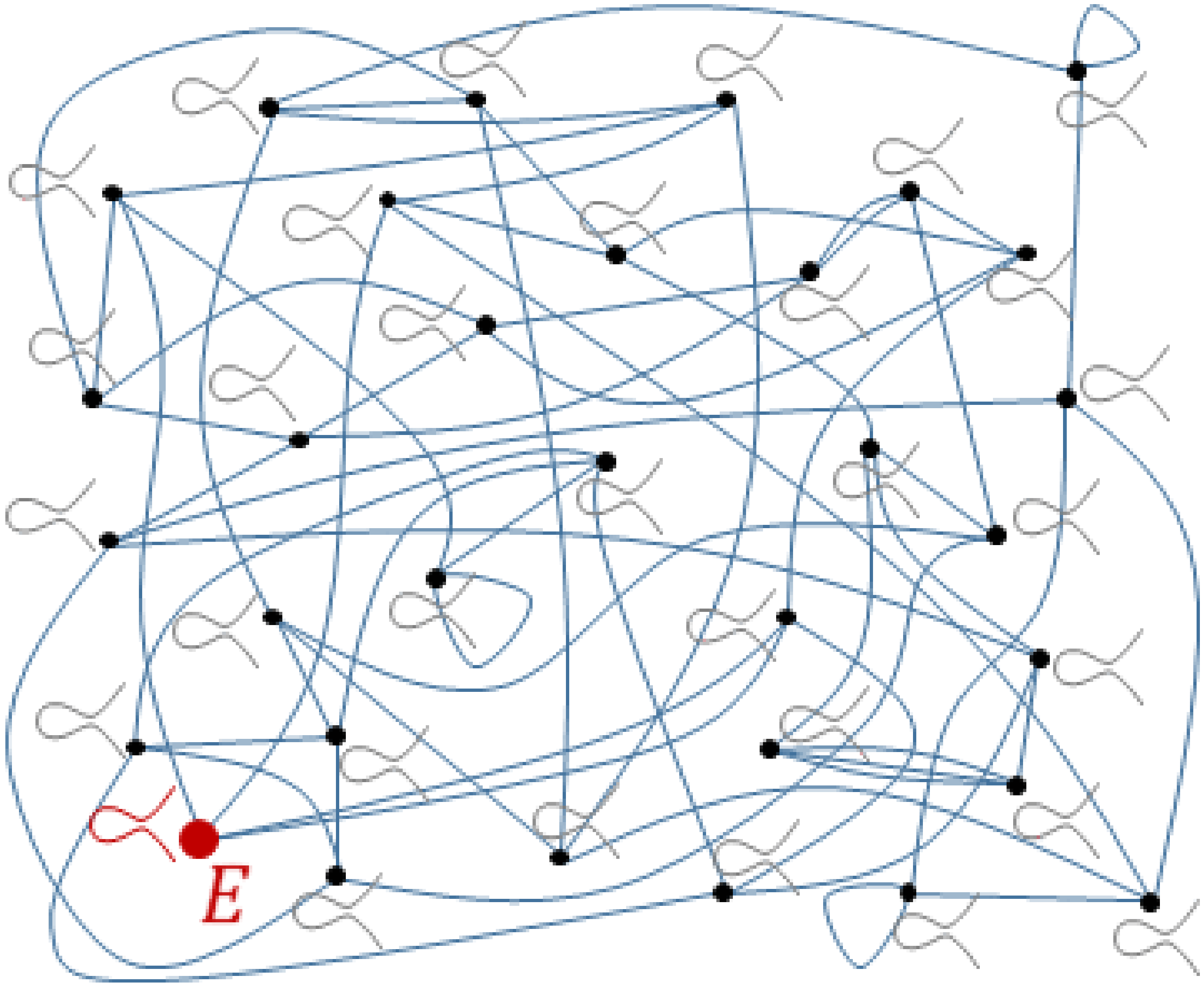
Pre-quantum (classical) ECC

$$P, k \mapsto [k]P$$



GIF: Wouter Castryck

Post-quantum ECC



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

Elliptic curves and isogenies

group	$(G,+)$	can do $+\ -$
ring	$(R,+,\times)$	can do $+\ -\ \times$
field	$(F,+,\times)$	can do $+\ -\ \times\ \div$

If you've never seen an elliptic curve before....

Remember: an elliptic curve is a group defined over a field

elliptic curve group	$(\boldsymbol{E}, \oplus)$	can do $\oplus$ $\ominus$
underlying field	$(\boldsymbol{K}, +, \times)$	can do $+$ $-$ $\times$ $\div$

operations in underlying field are used and combined to compute the elliptic curve operation $\oplus$

Boring curves

$$f(x,y) = 0 \quad \text{or} \quad f(X,Y,Z) = 0$$

Degree 1 (lines)

$$ax + by = c \qquad ab \neq 0$$

Degree 2 (conic sections)

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \qquad abc \neq 0$$

e.g., ellipses, hyperbolas, parabolas

- “Genus” measures geometric complexity, and both are genus 0
- We know how to describe all solutions to these, e.g., over (exts of) $\mathbb{Q}$
- Not cryptographically interesting

Elliptic curves

- Degree 3 is where all the fun begins…

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

$$\Big\Downarrow \; ch(K) \neq 2,3$$

$$E/K: \quad y^2 = x^3 + ax + b$$

⟵ E specified by K, a, b

- Elliptic curves ↔ genus 1 curves
- Set is ≈ points $(x, y) \in K \times K$ satisfying above equation
- Geometrically/arithmetically/cryptographically interesting
- Fermat's last theorem/BSD conjecture/ …

Elliptic curves

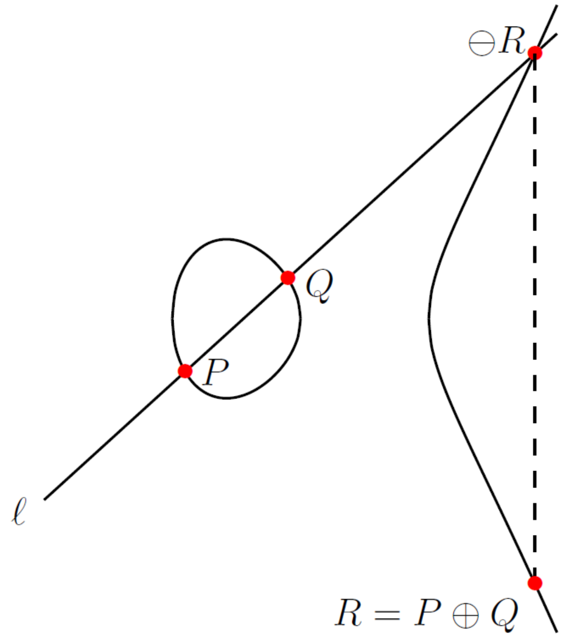
- Cubic curves E/K : $y^2 = x^3 + \ ...$

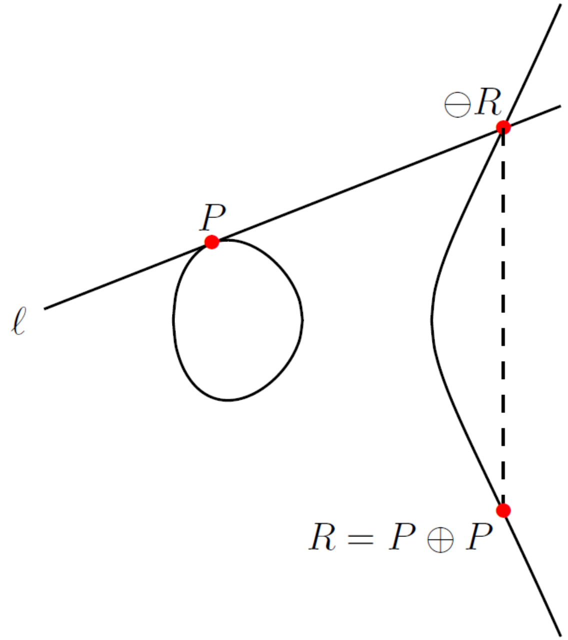
- Old school ECC
  - K is a finite field $\mathbb{F}_q$
  - Curve fixed once-and-for-all
  - Group elements are points e.g. $P = (x_P, y_P)$ and $\mathcal{O}_E$

- 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...

$$E \cong E'$$

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

$\psi(\mathcal{O}_E) = \mathcal{O}_{E'}$, 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 $\mathbf{ker}(\phi) = \{\mathcal{O}_E, \big((350i + 68), 0\big)\}$ and $j(E_a) \neq j(E_{a'})$ in general!

- Seperable isogenies $\leftrightarrow$ 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

$$(x, y) \mapsto \big(f(x), c\, y\, f'(x)\big)$$

  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!

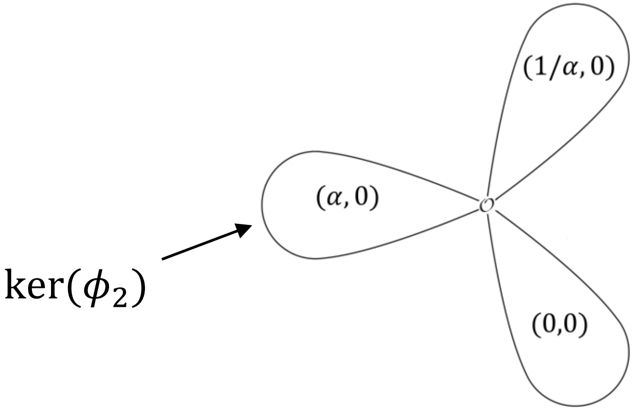
- Fortunately, we only need $n = 2$ and $n = 3$ to do SIDH!

Explicit formulas

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

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

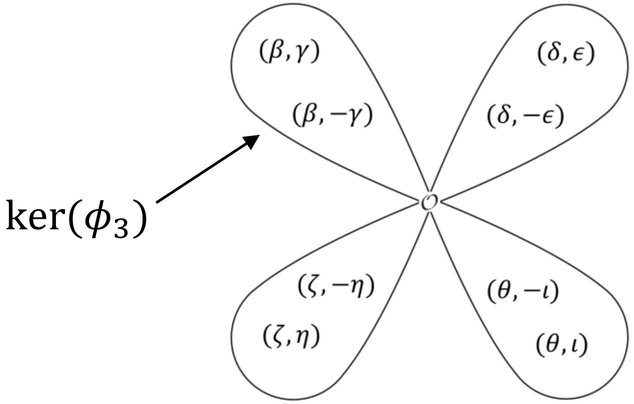
$$a' = 2\left(1 - 2\alpha^2\right)$$



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

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

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

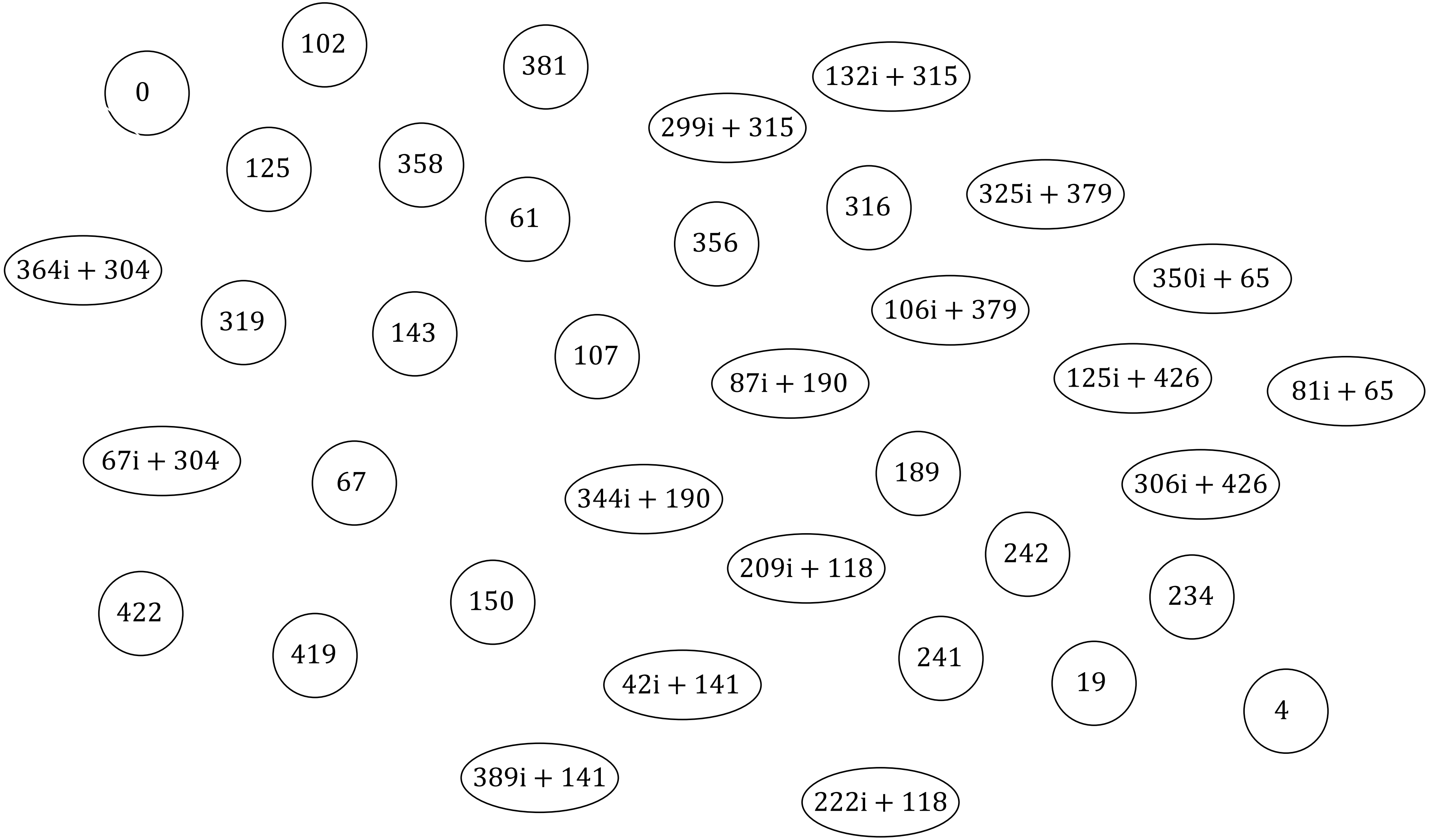


SIDH
(Supersingular Isogeny Diffie Hellman)

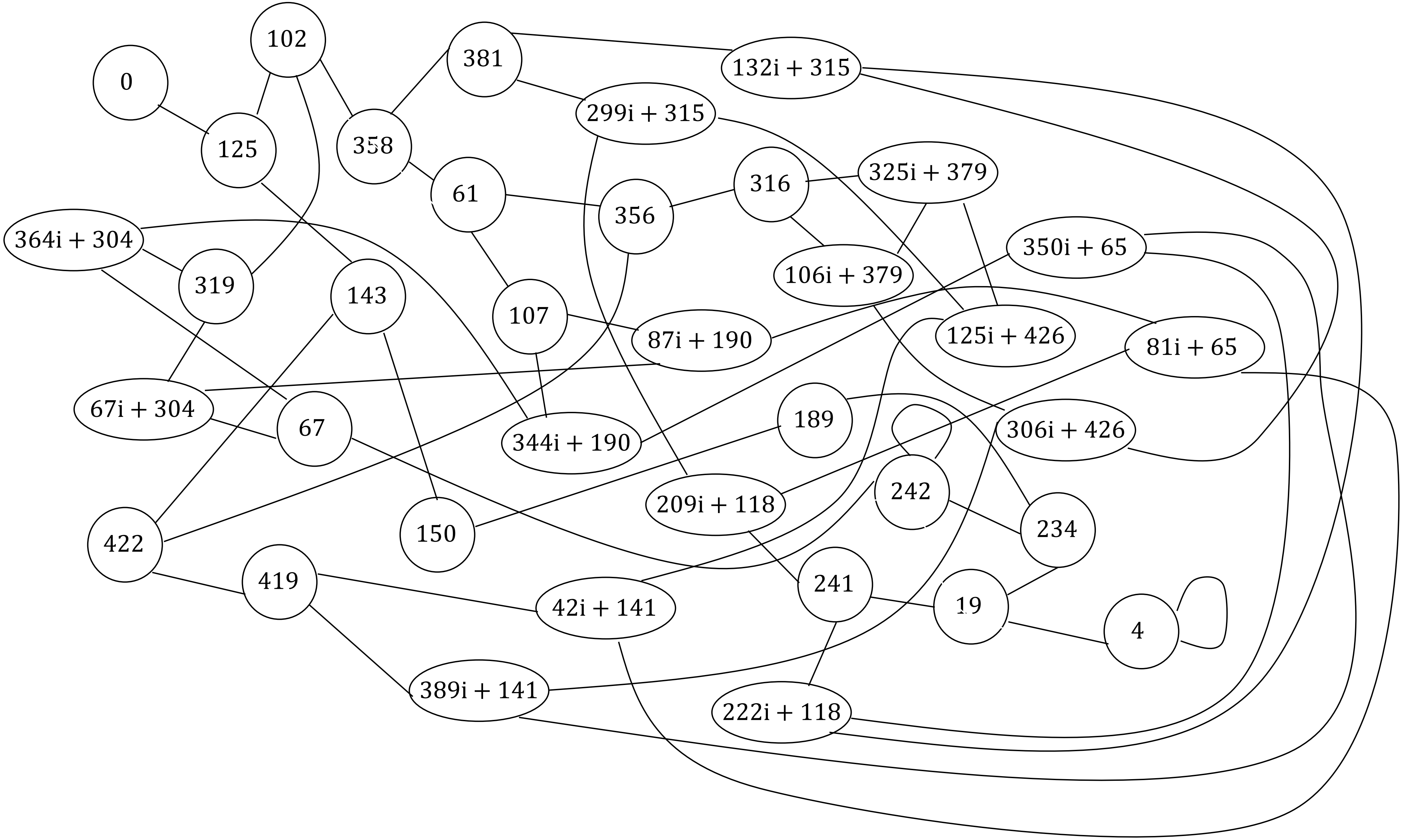
https://eprint.iacr.org/2019/1321.pdf

Question: why do we need elliptic curves and isogenies if all we need is expander graphs?

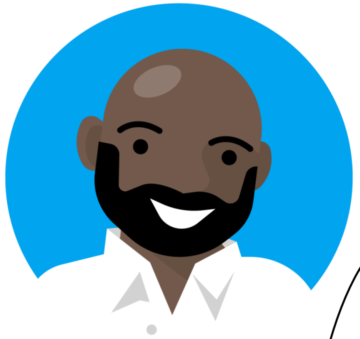
e.g. supersingular isogeny graph – the nodes

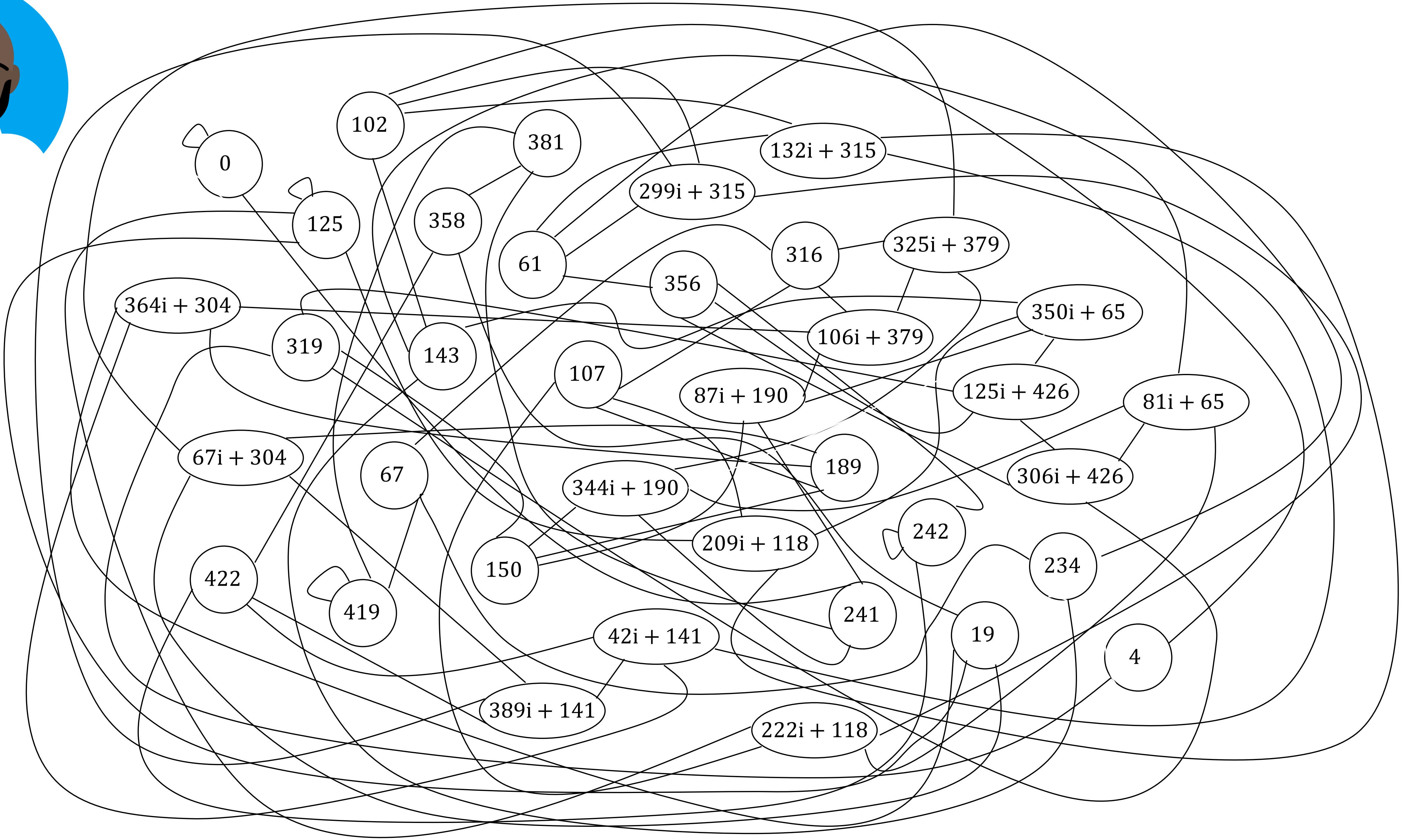


$p := 431$: there are 37 supersingular j's (all over $\mathbb{F}_{p^2} := \mathbb{F}_p(i)$, $i^2 + 1 = 0$)



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
242
209i + 118
234
422
150
419
42i + 141
241
19
4
389i + 141
222i + 118

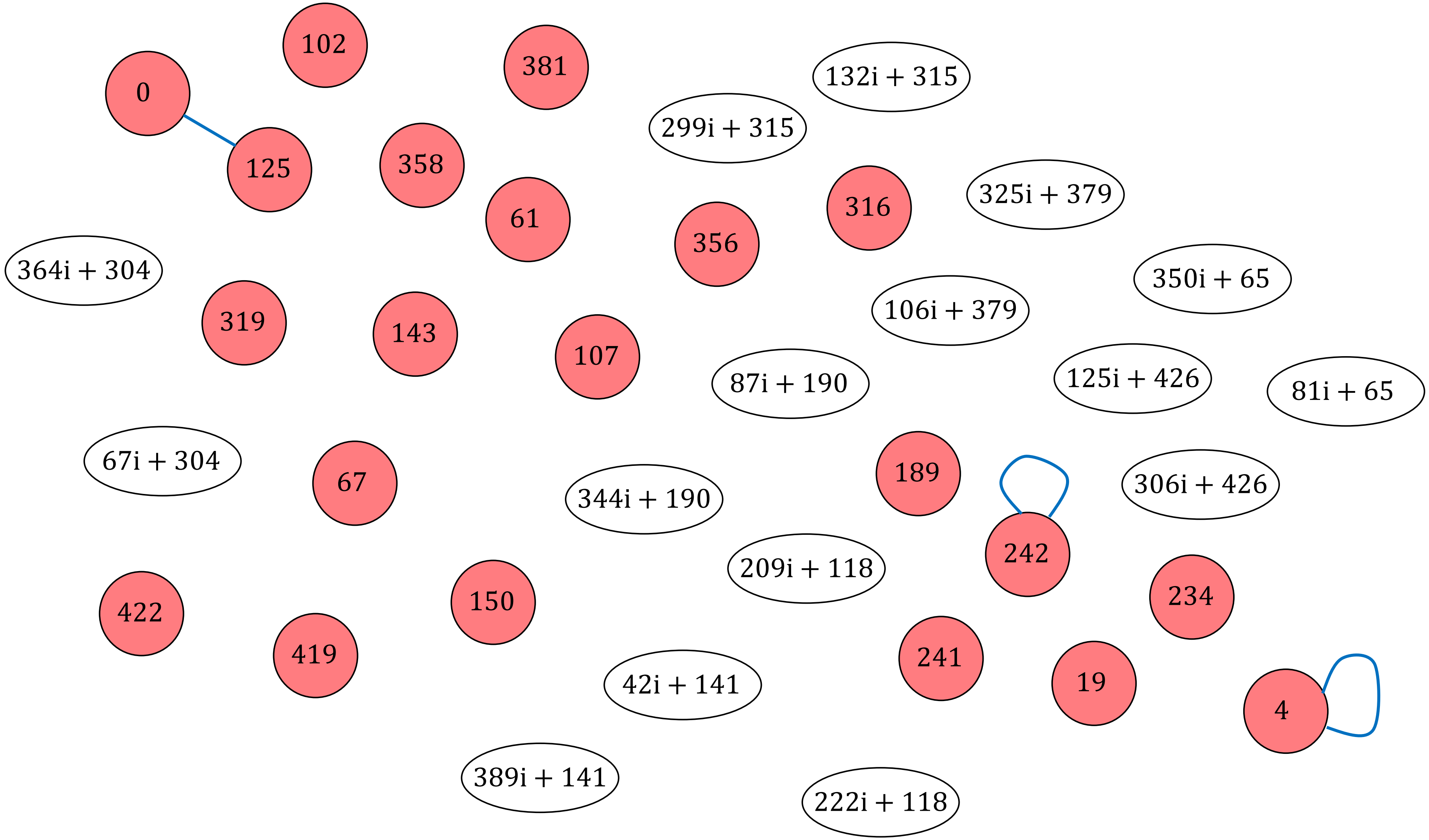



102
381
0
132i + 315
299i + 315
125
358
61
316
325i + 379
356
364i + 304
319
143
350i + 65
106i + 379
107
87i + 190
125i + 426
81i + 65
67i + 304
67
189
344i + 190
306i + 426
242
209i + 118
150
234
422
419
241
19
4
42i + 141
389i + 141
222i + 118

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 $\mathbb{F}_p$.

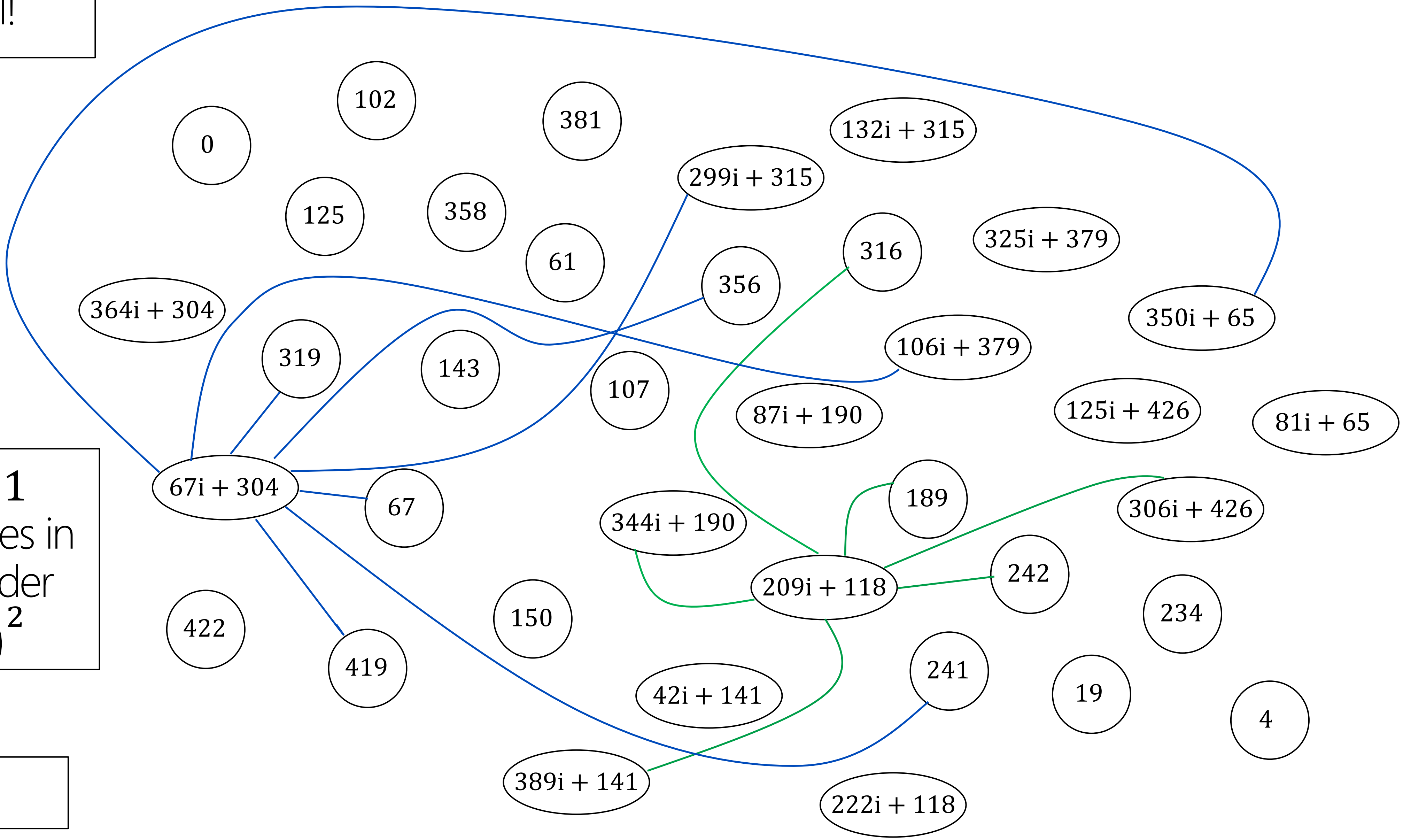
These (self edges, double/triple edges) look relatively common here, but as $p \to \infty$, they aren't



$p = 431$

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 $(p+1)^2 = \left(2^4 3^3\right)^2$

Choose $2^i \approx 3^j$

Params: starting curve and generator points

$E_A\colon\ y^2 = x^3 + Ax^2 + x$

$$A = 329i + 423$$

$$j = 87i + 190$$

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

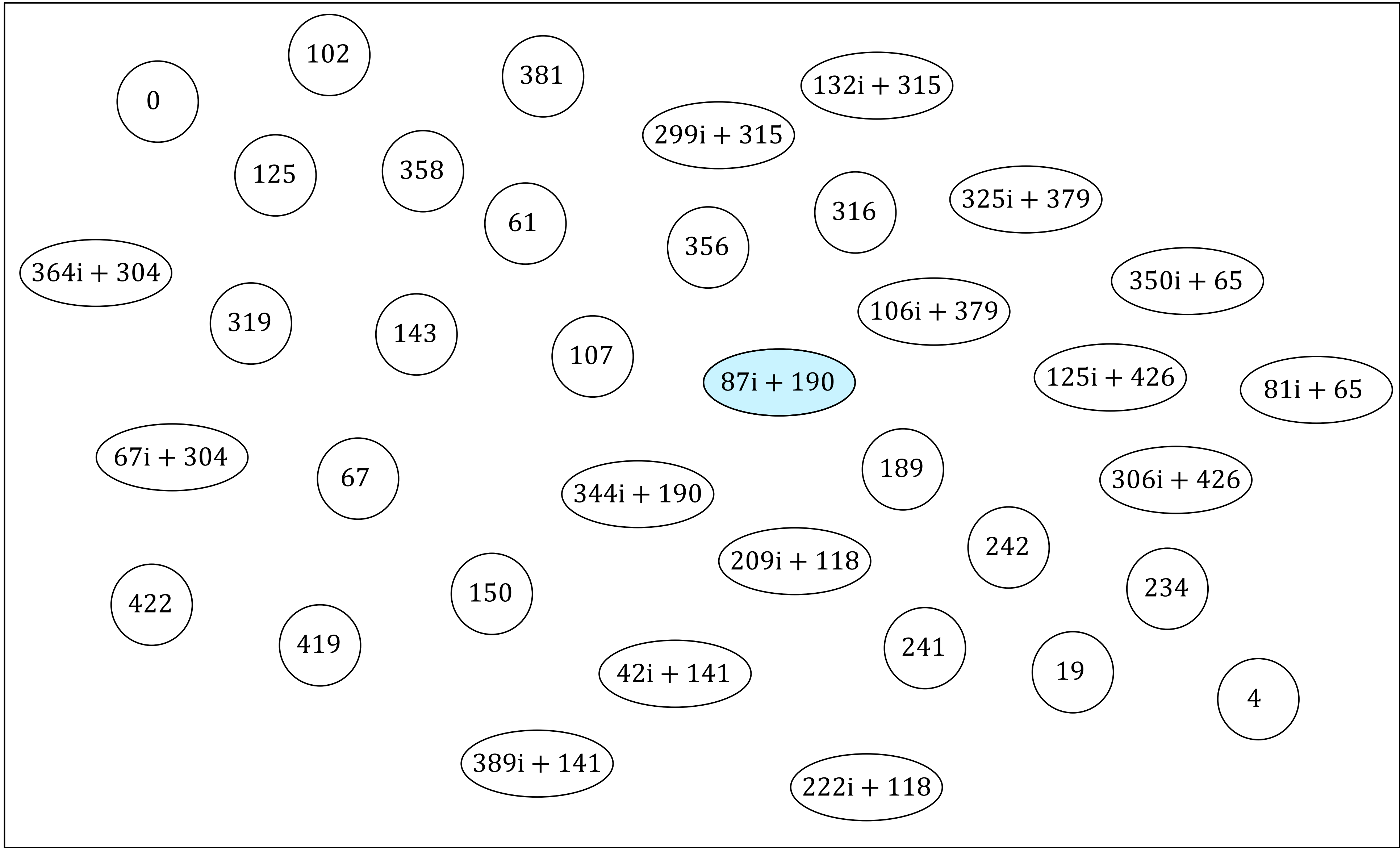
$$E \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$$

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

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

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

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

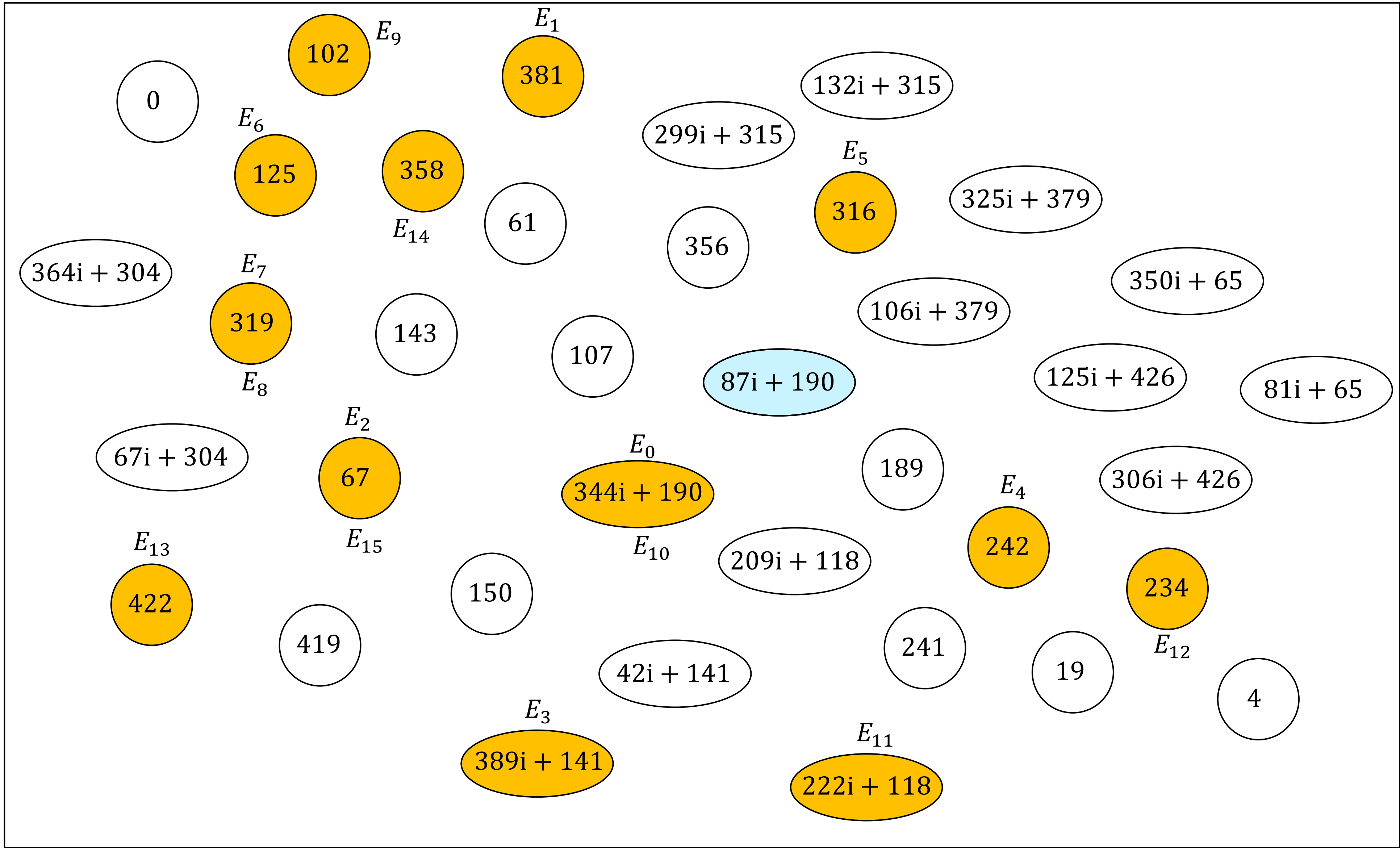


Alice destinations: possible* 2^4-isogenies

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

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	$(204i + 139, 166i + 207)$

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

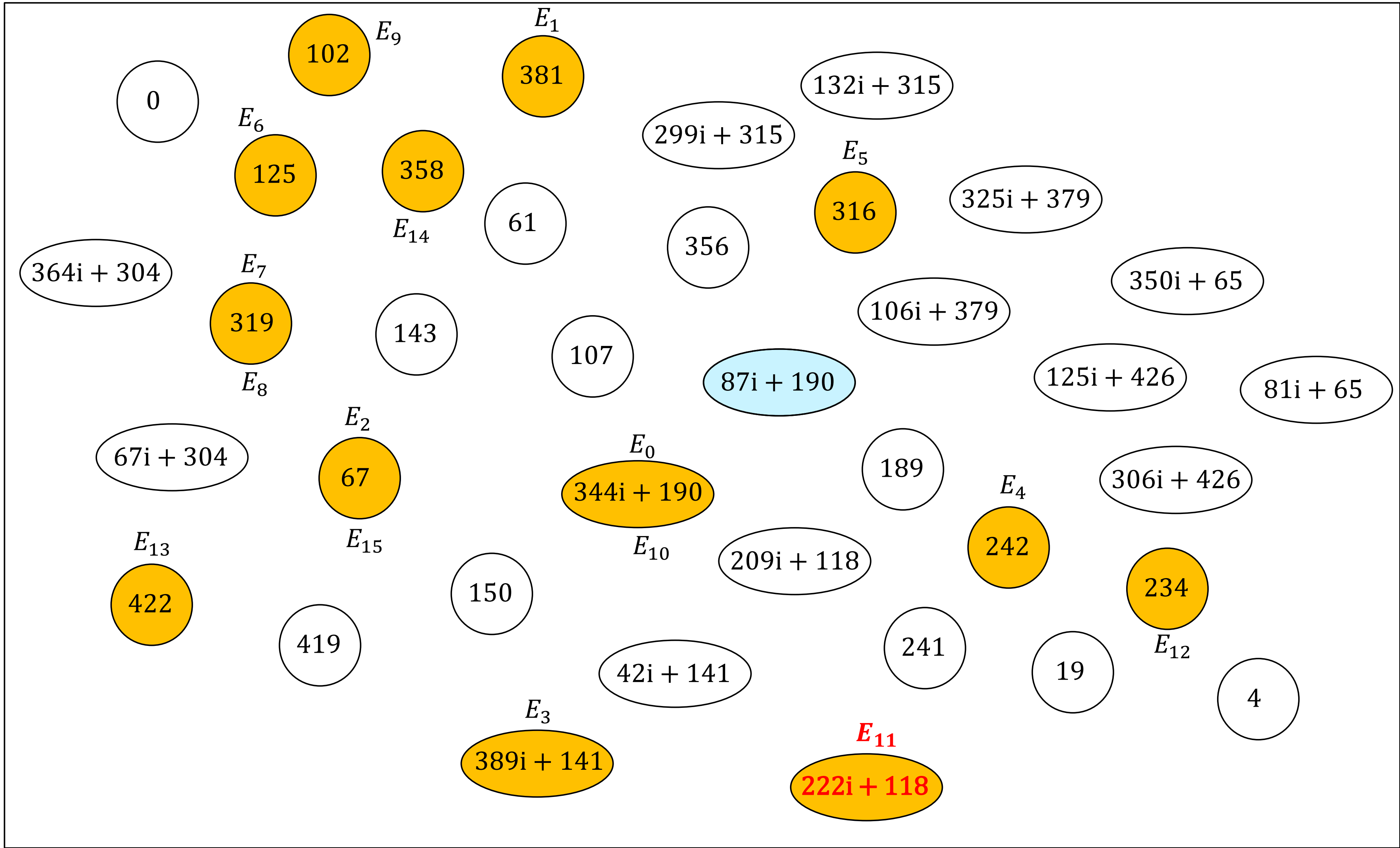


Alice destinations: possible* 2^4-isogenies

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

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	$(271i + 79\,, 153i + 430)$
12	$(352i + 382\,, 154i + 380)$
13	$(63i + 162\,, 350i + 229)$
14	$(300i + 111\,, 285i + 10)$
15	$(204i + 139\,, 166i + 207)$

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

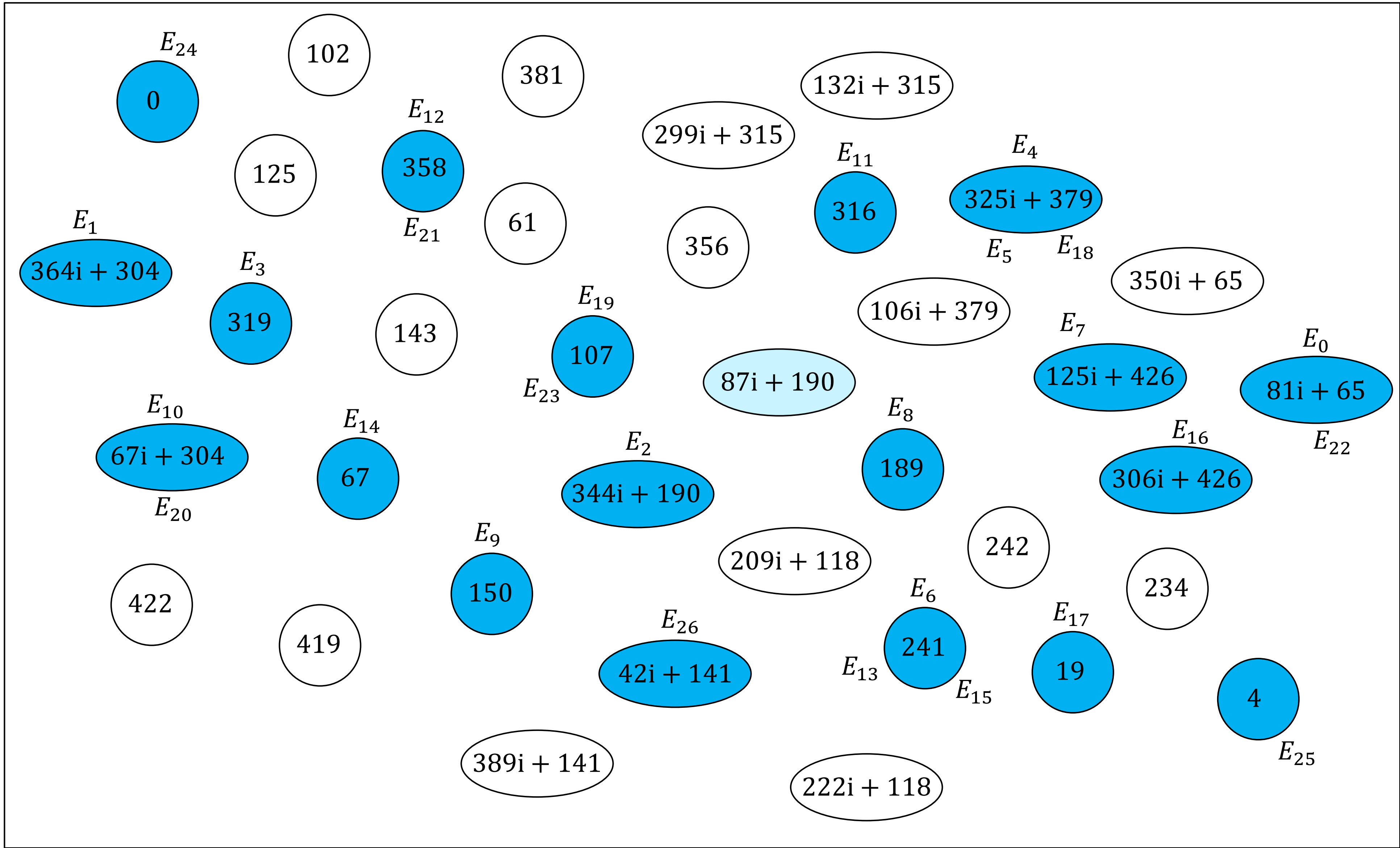


Bob destinations: possible* 3^3-isogenies

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

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	$(333i + 426, 142i + 14)$

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

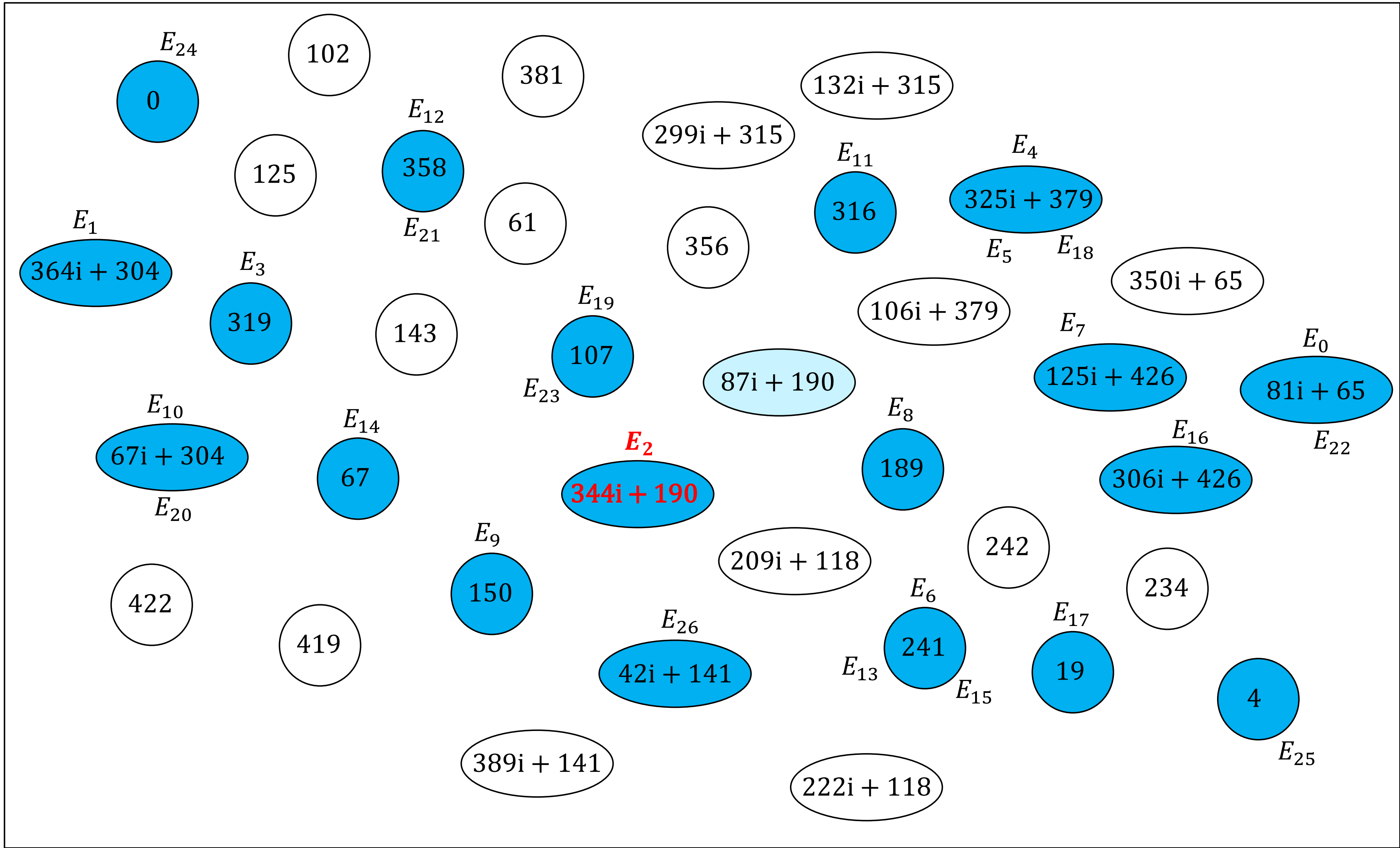


Bob destinations: possible* 3^3-isogenies

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

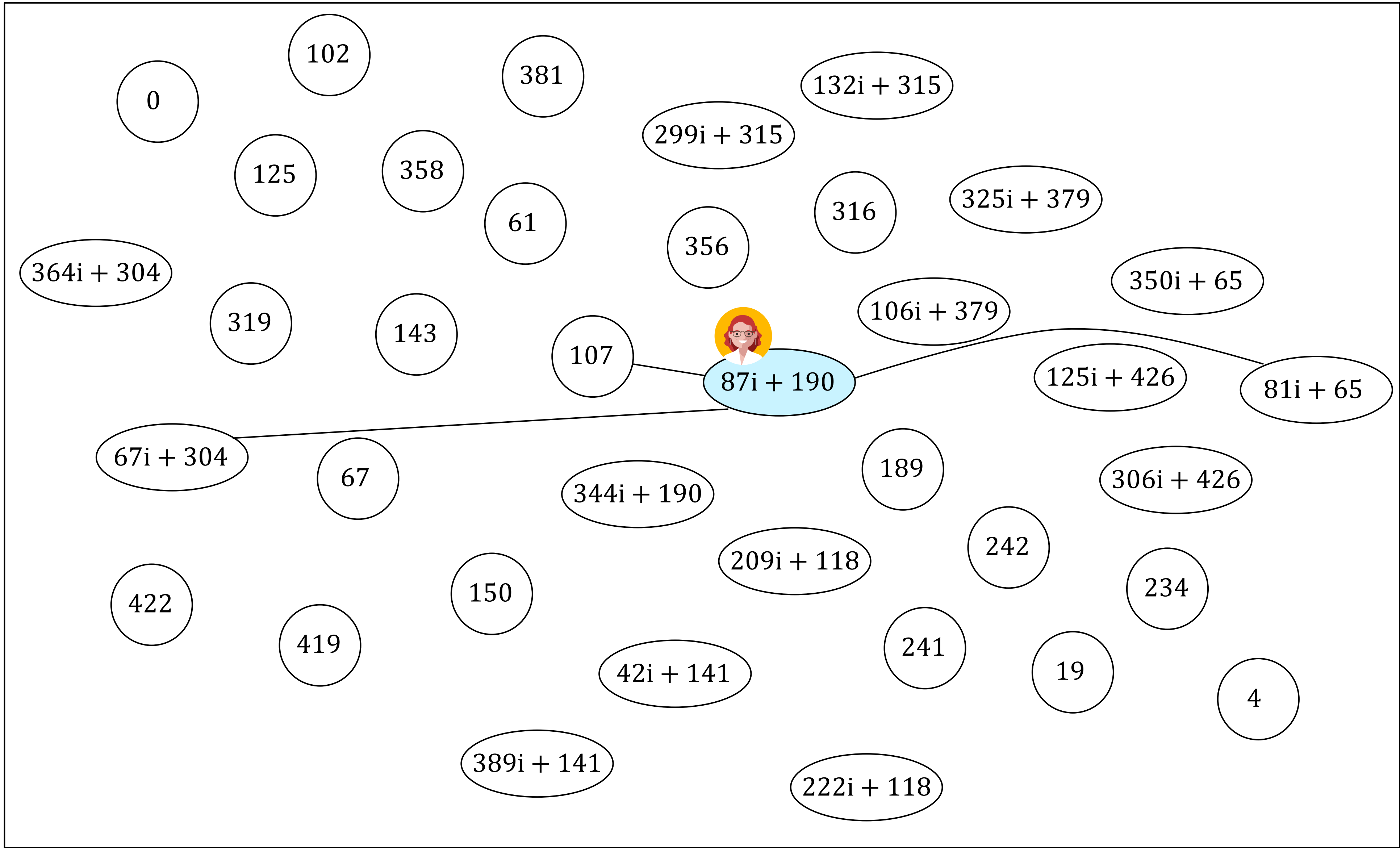
k_B	$S_k = P_B + [k_B]Q_B$
0	$(358i + 275, 410i + 104)$
1	$(150i + 184, 106i + 293)$
2	**$(122i + 309, 291i + 374)$**
3	$(25i + 70, 254i + 66)$
4	$(47i + 223, 301i + 322)$
⋮	⋮
⋮	⋮
⋮	⋮
21	$(200i + 351, 141i + 361)$
22	$(35i + 417, 183i + 351)$
23	$(327i + 55, 230i + 238)$
24	$(326i + 56, 334i + 220)$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

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



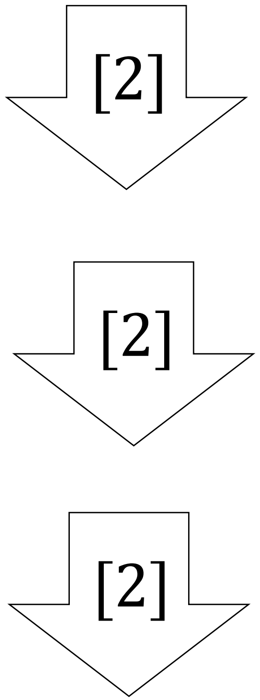
Alice's key generation

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

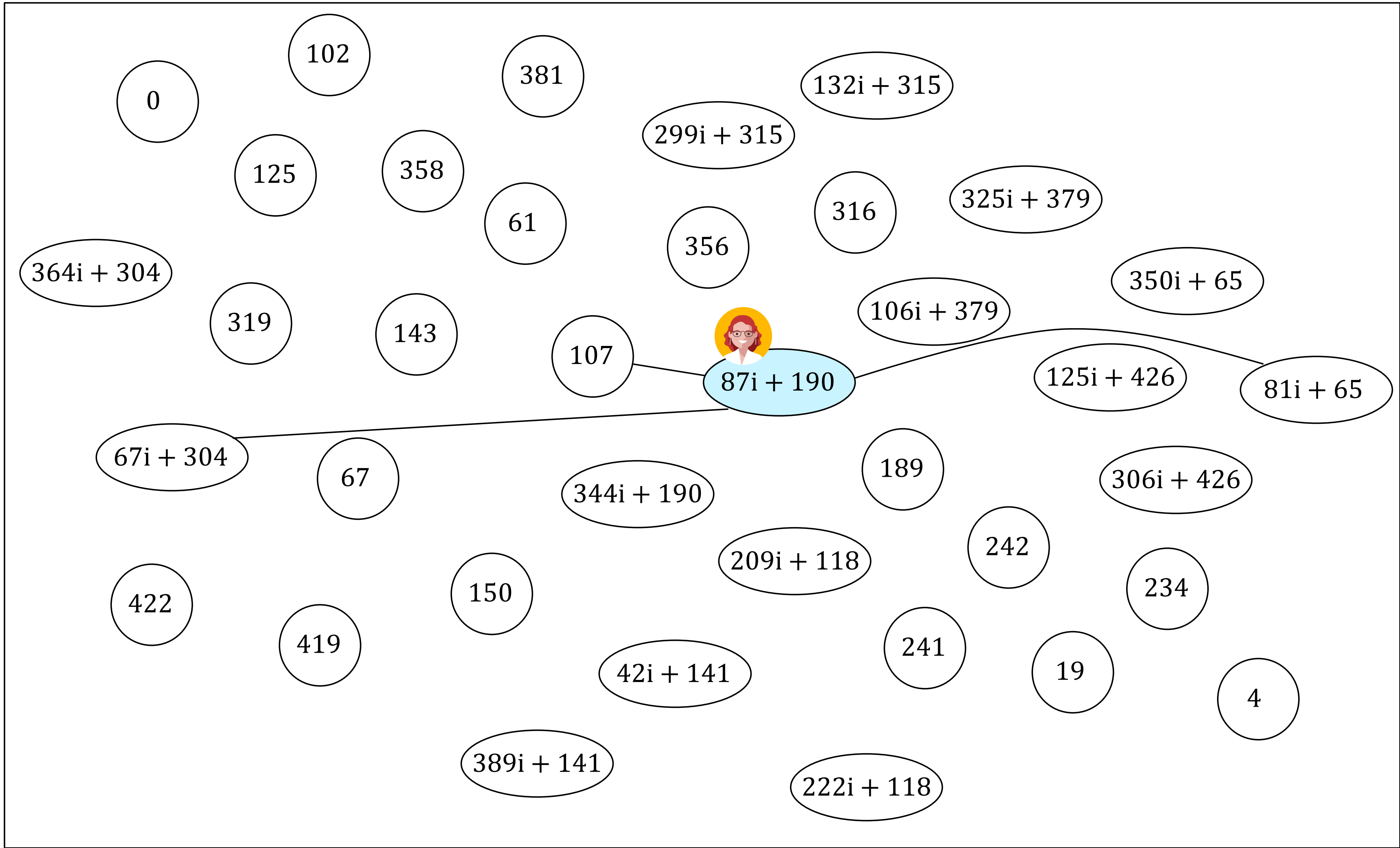


Alice's key generation

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



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



Alice's key generation

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

[2]

[2]

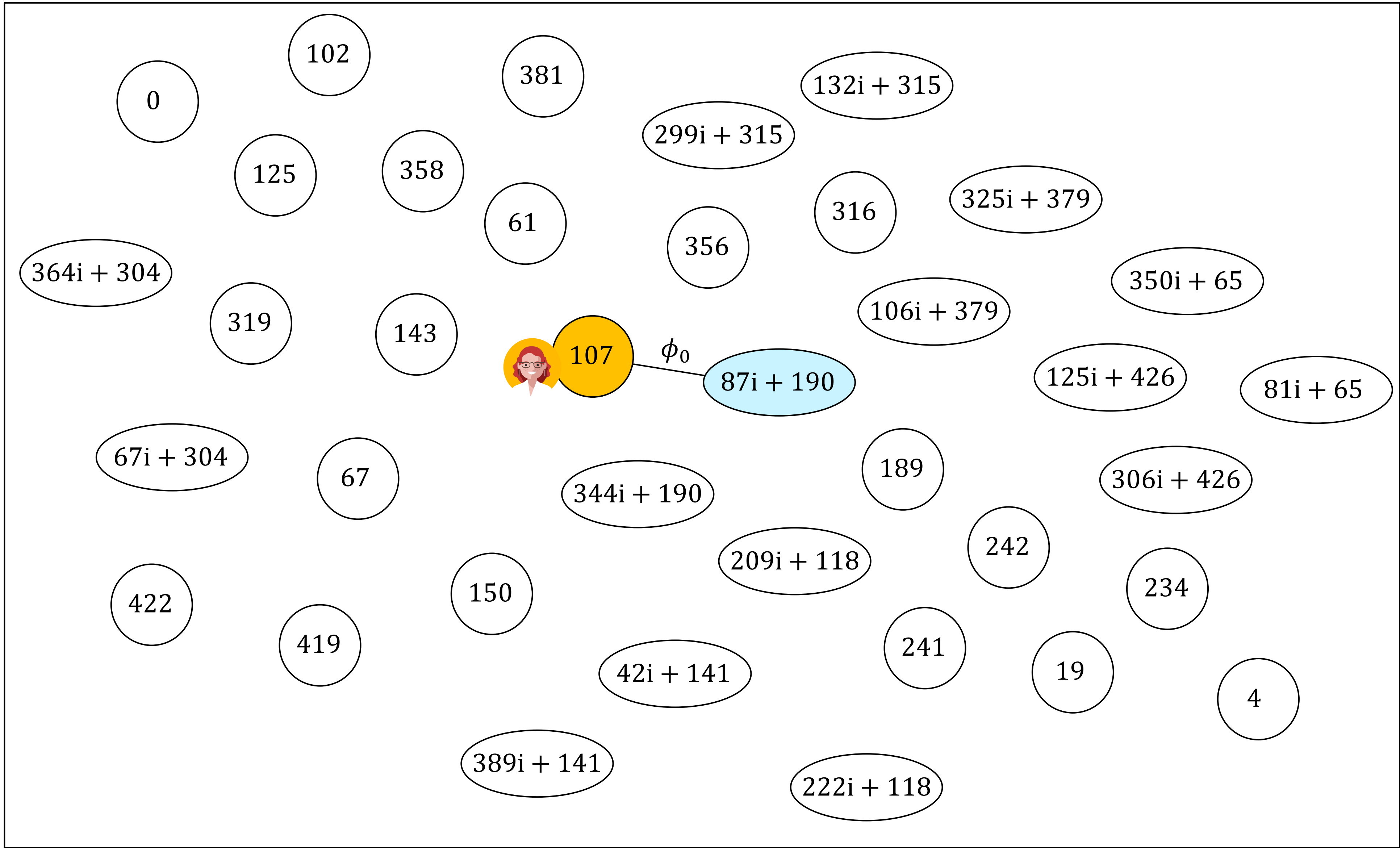
[2]

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

$$\phi_0 : E_0 \rightarrow E_1$$

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

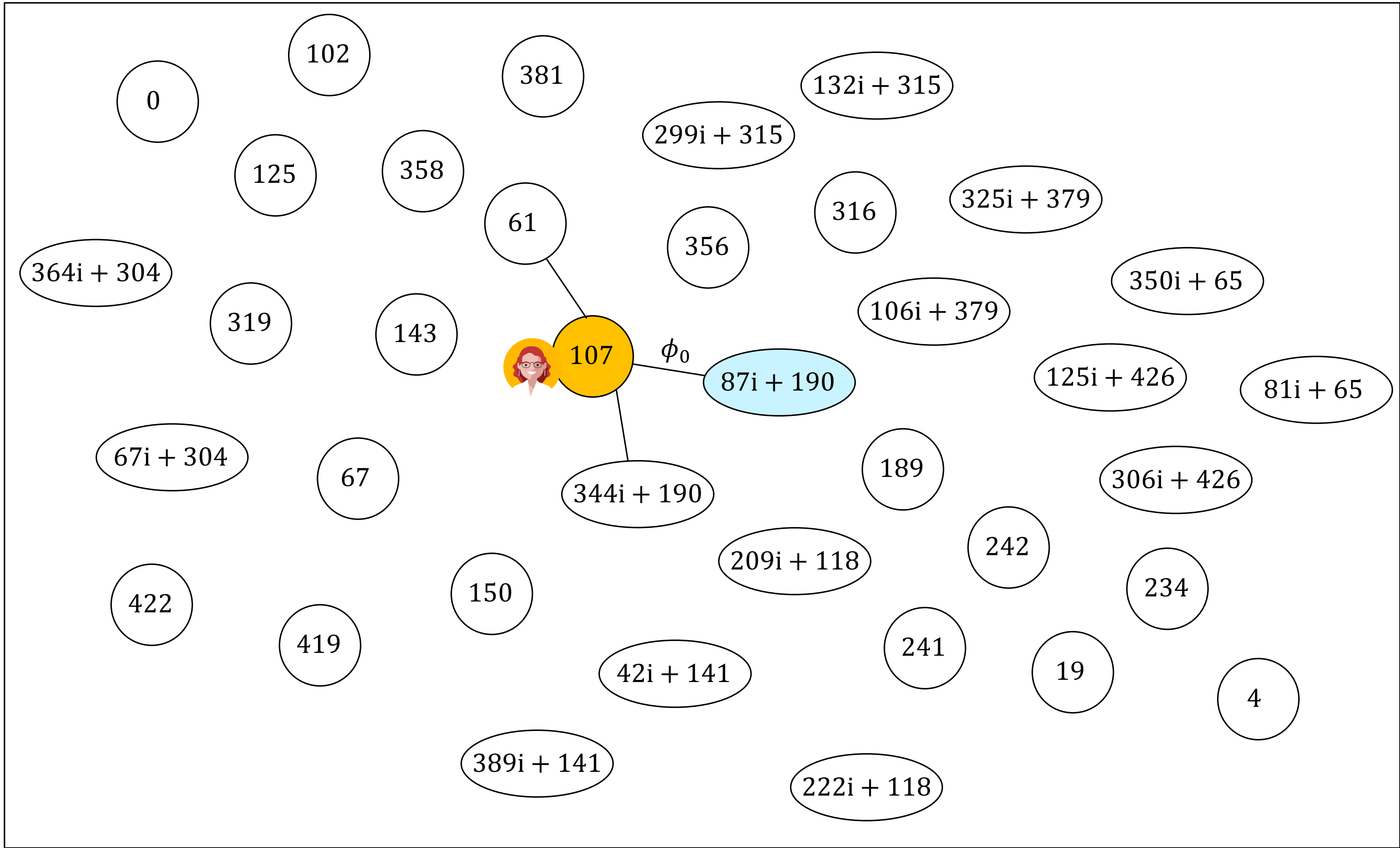
$$j(E_1) = 107$$



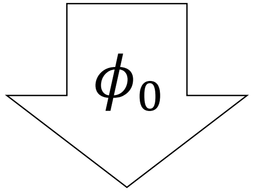
Alice's key generation

ϕ_0

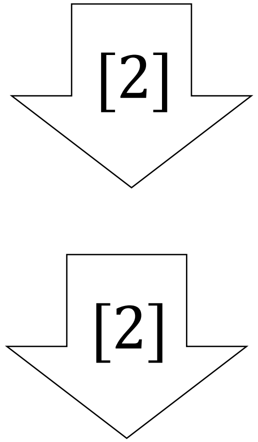
$\phi_0(S)= (157i + 156\,, 231i + 353)$



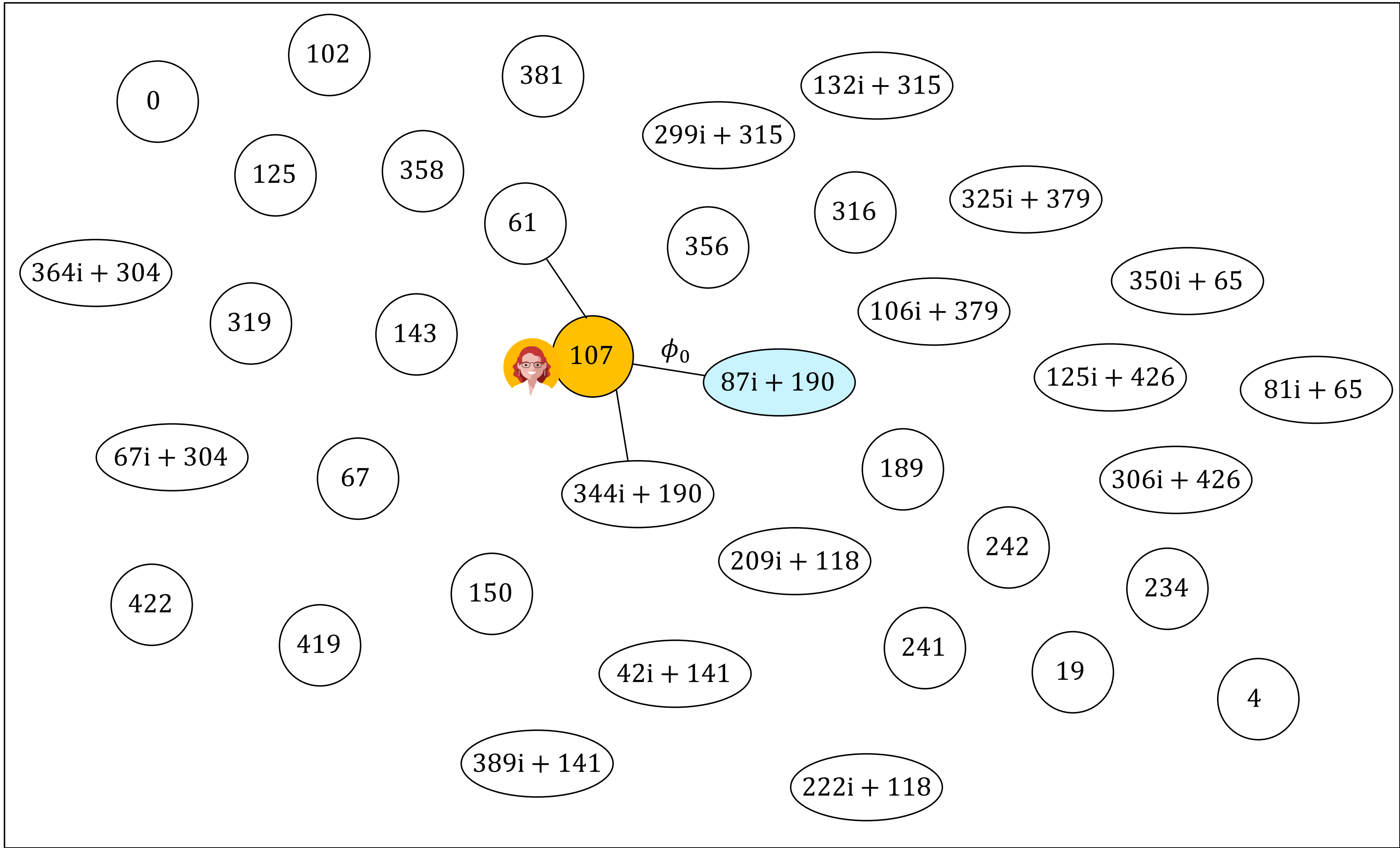
Alice’s key generation



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



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



Alice's key generation

ϕ_0

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

$[2]$

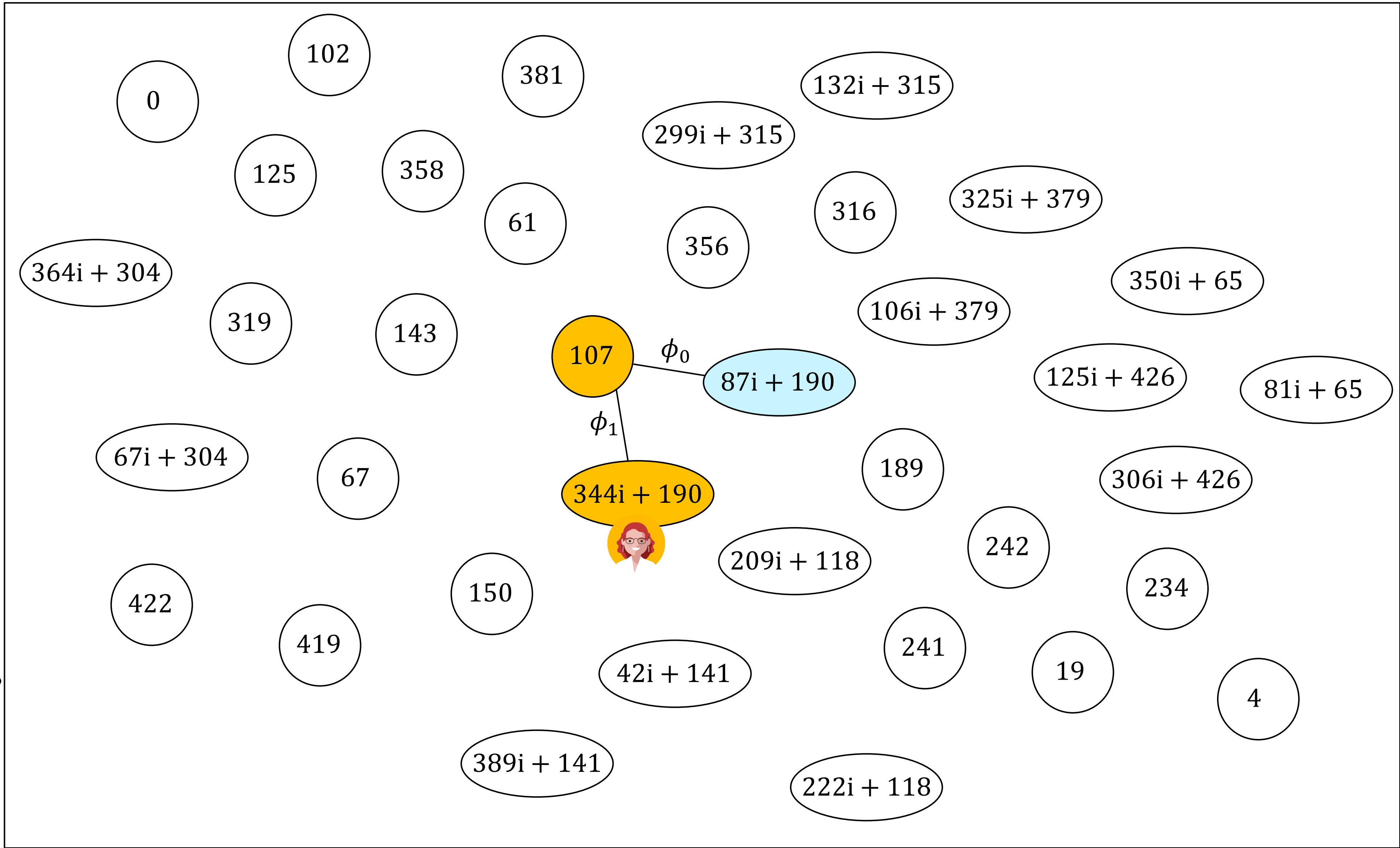
$[2]$

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

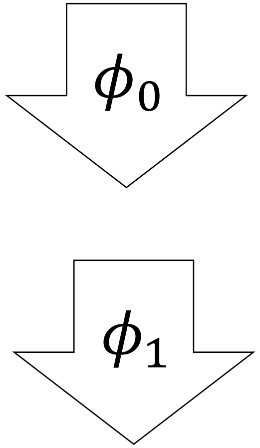
$$\phi_1 : E_1 \to E_2$$

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

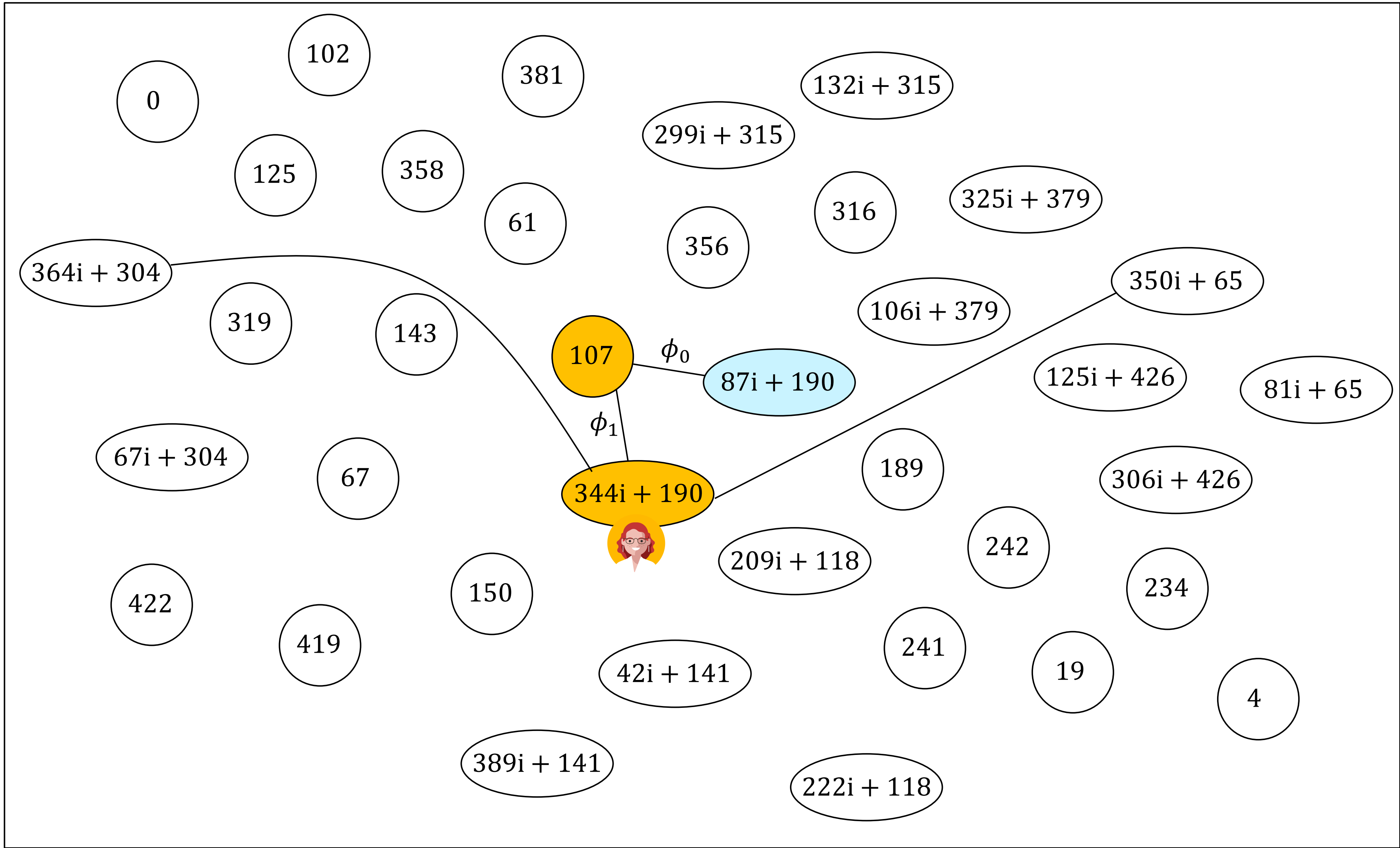
$$j(E_2) = 344i + 190$$



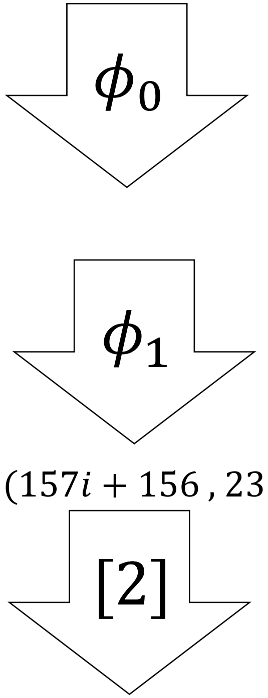
Alice's key generation



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

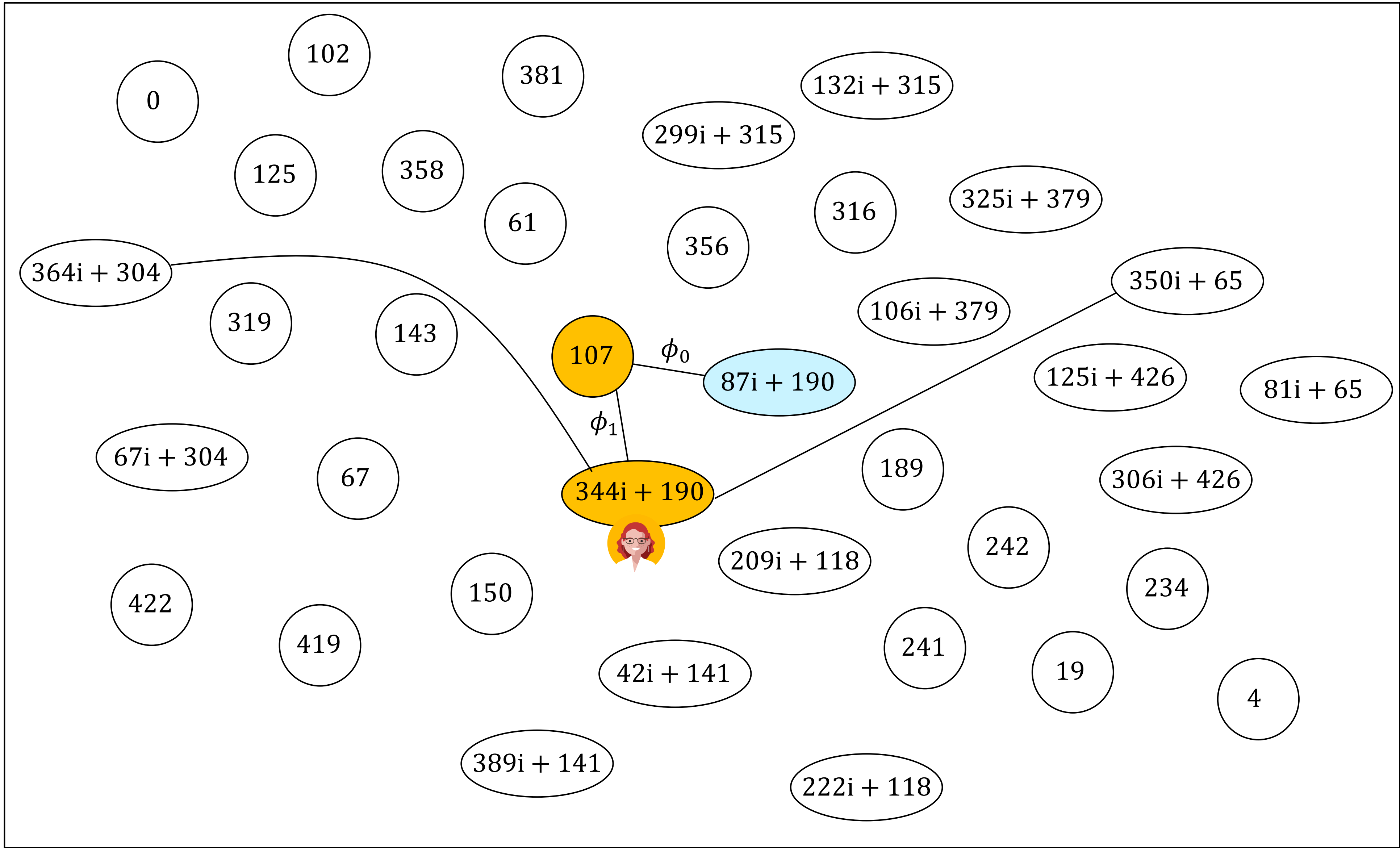


Alice's key generation



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

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



Alice's key generation

ϕ_0

ϕ_1

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

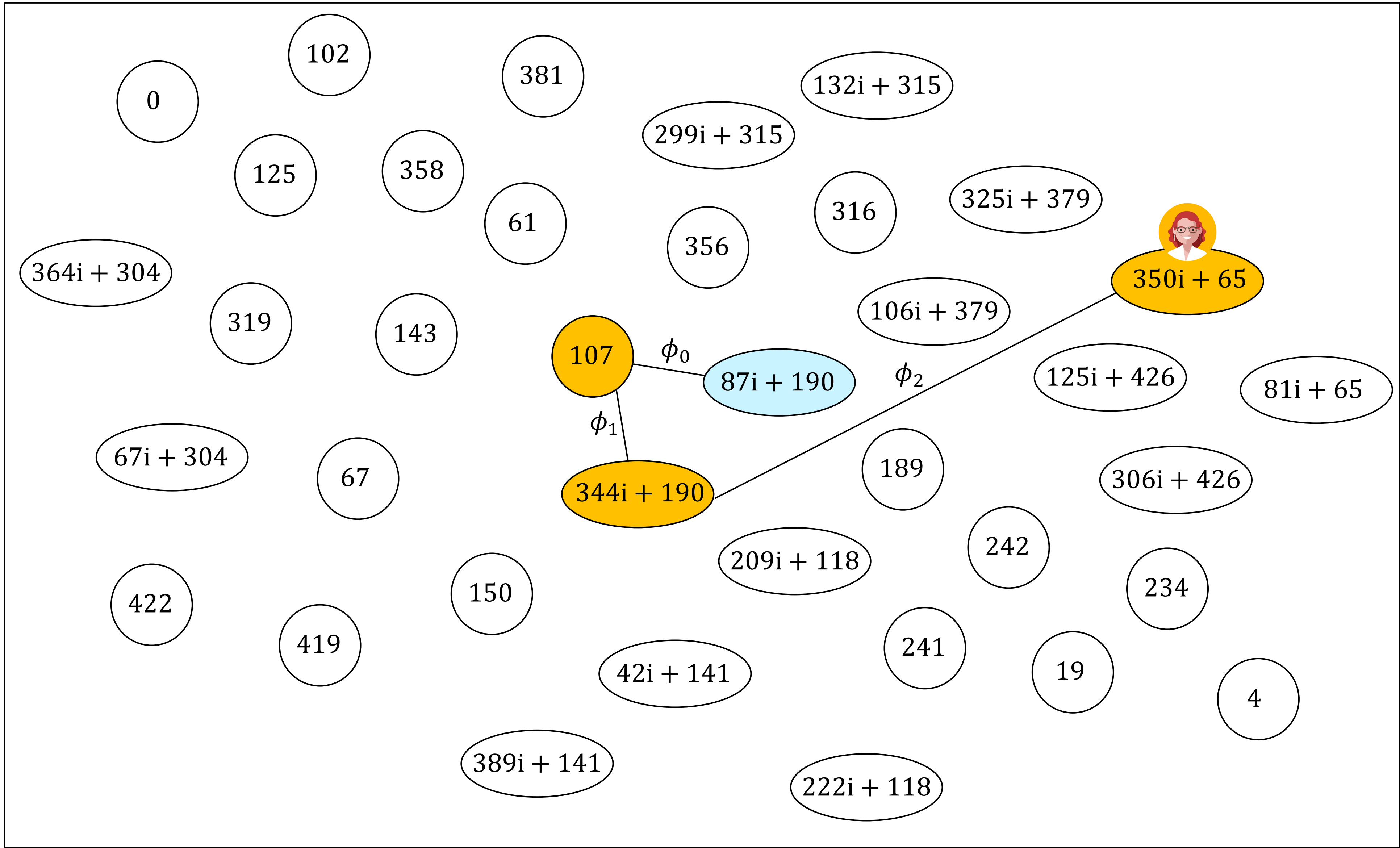
$[2]$

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

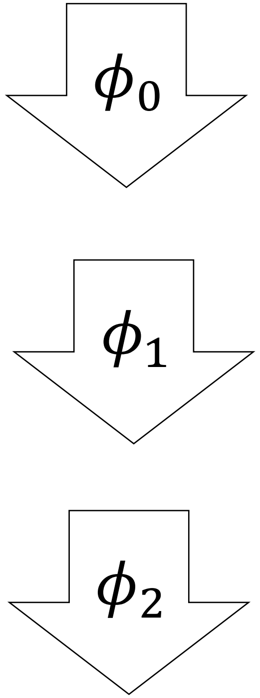
$$\phi_2 : E_2 \to E_3$$

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

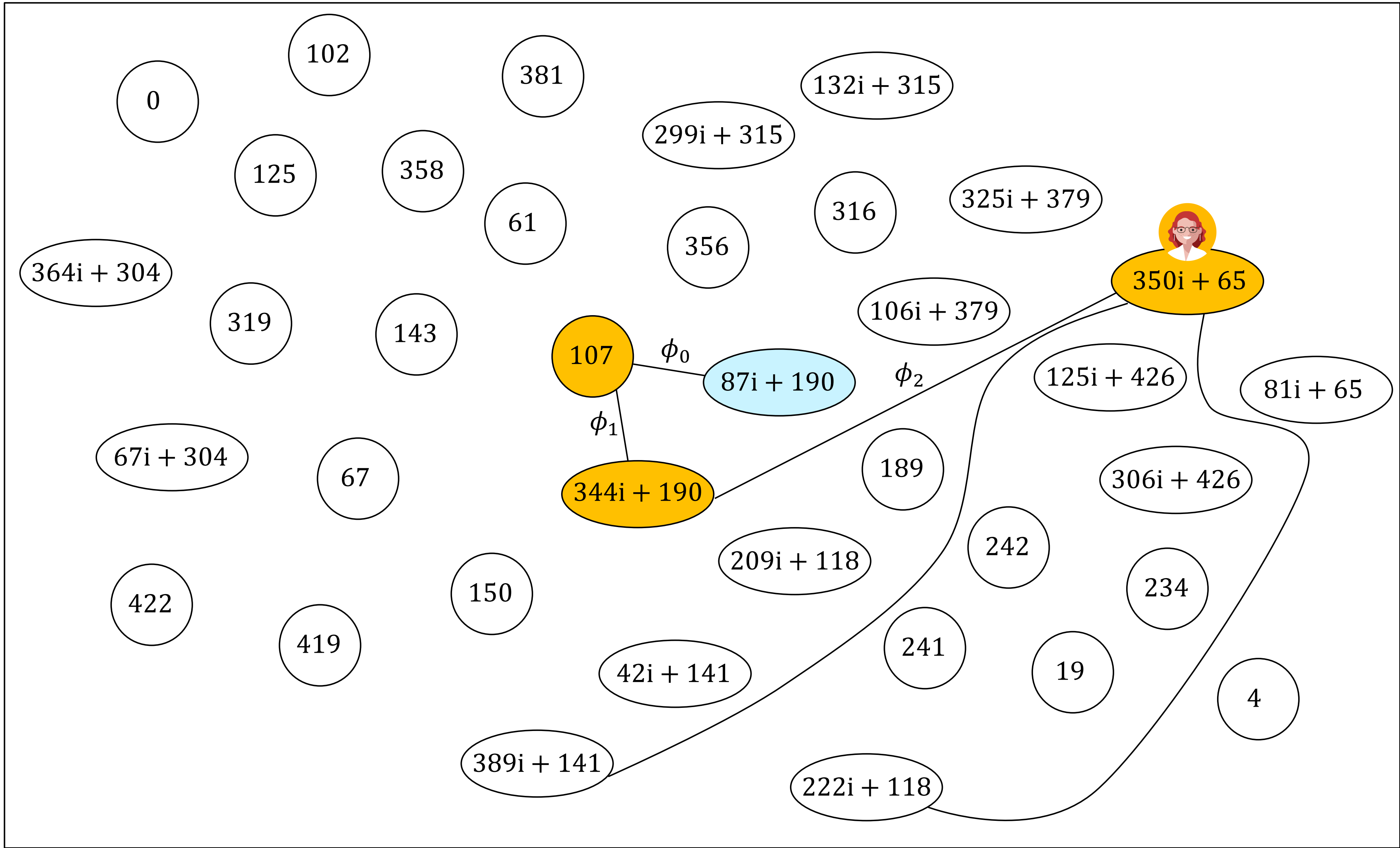
$$j(E_3) = 350i + 65$$



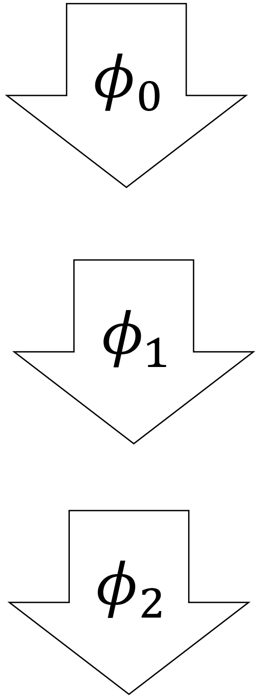
Alice's key generation



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



Alice's key generation

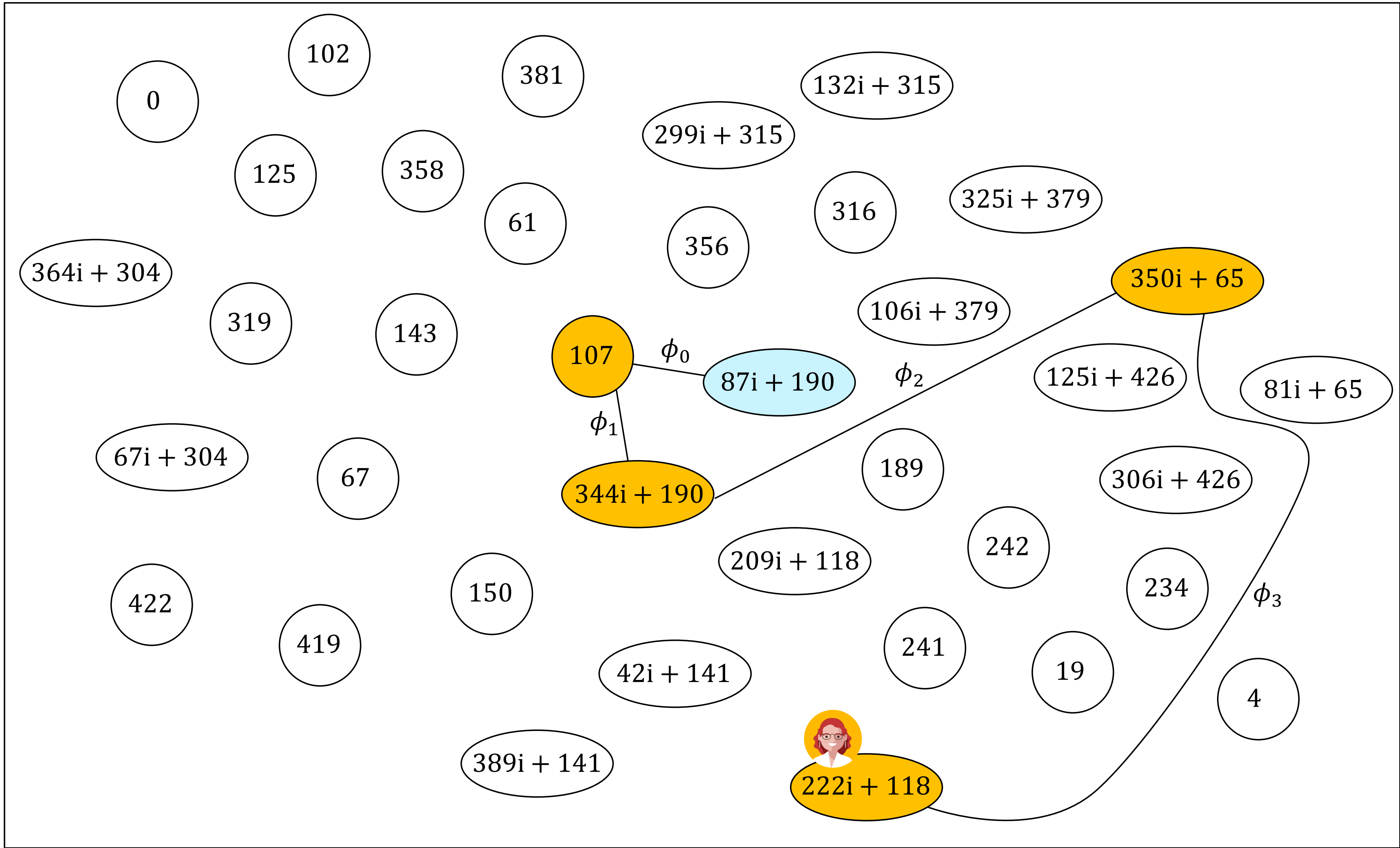


$\phi_2(\phi_1(\phi_0(S)))= (208i + 177\,, 0)$

$$\phi_3 : E_3 \to E_4$$

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

$$j(E_4) = 222i + 118$$



Summary

in

$k = 11$

Alice's key generation

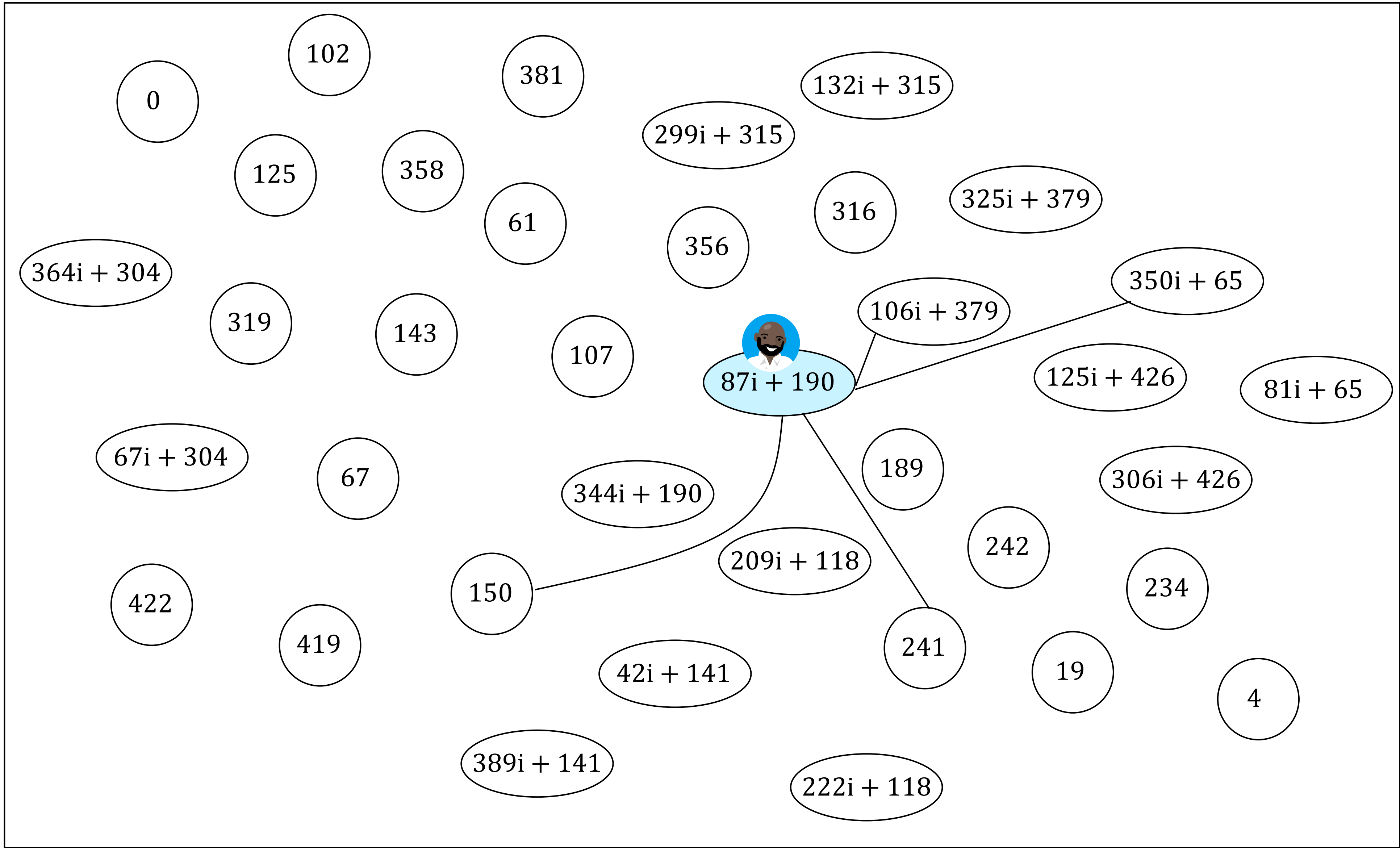
$S_A = P_A + [11]Q_A \Longrightarrow E_A = E_0/\langle S_A \rangle$

out

$222i + 118$

Bob's key generation

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



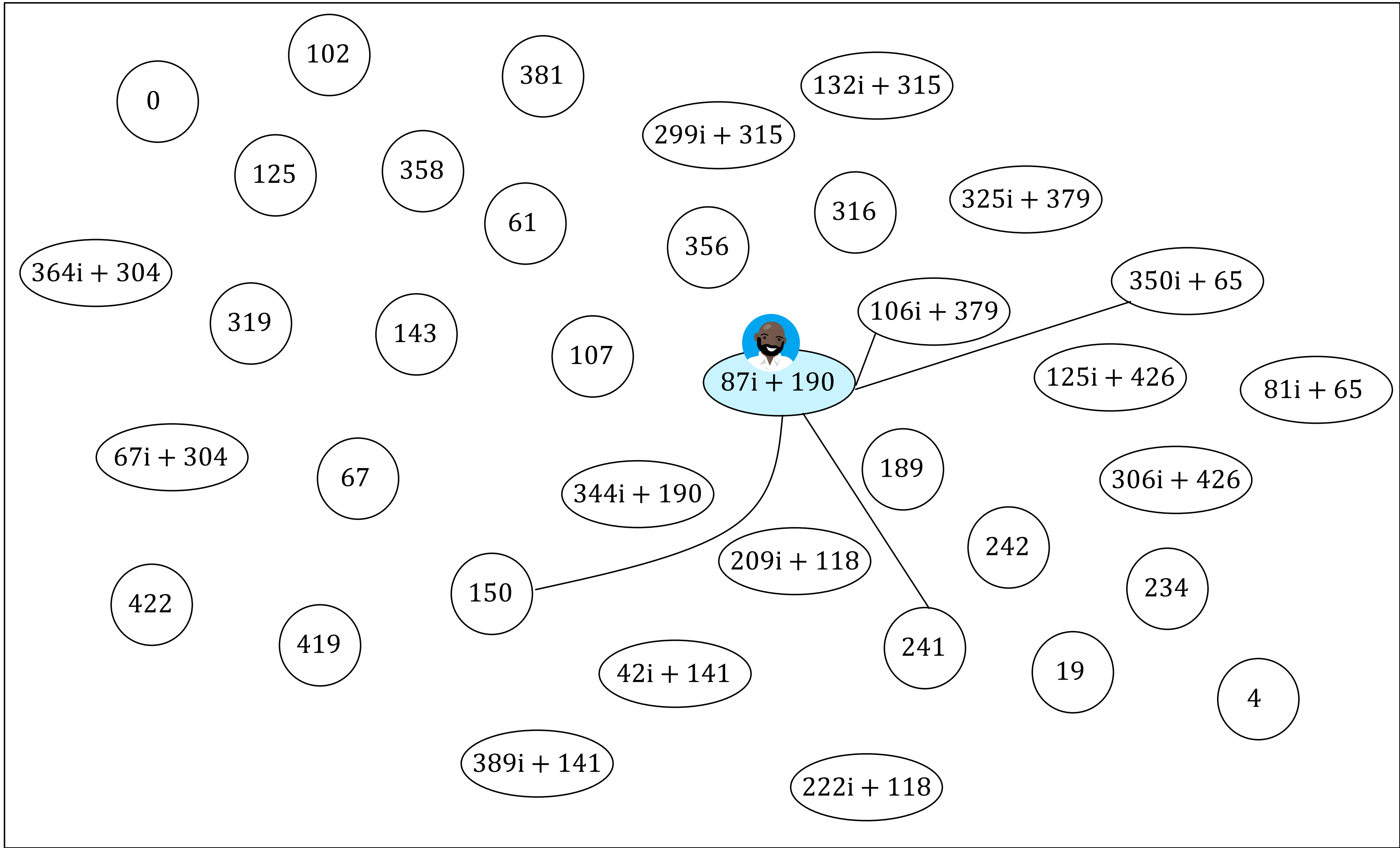
Bob's key generation

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

[3]

[3]

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



Bob's key generation

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

[3]

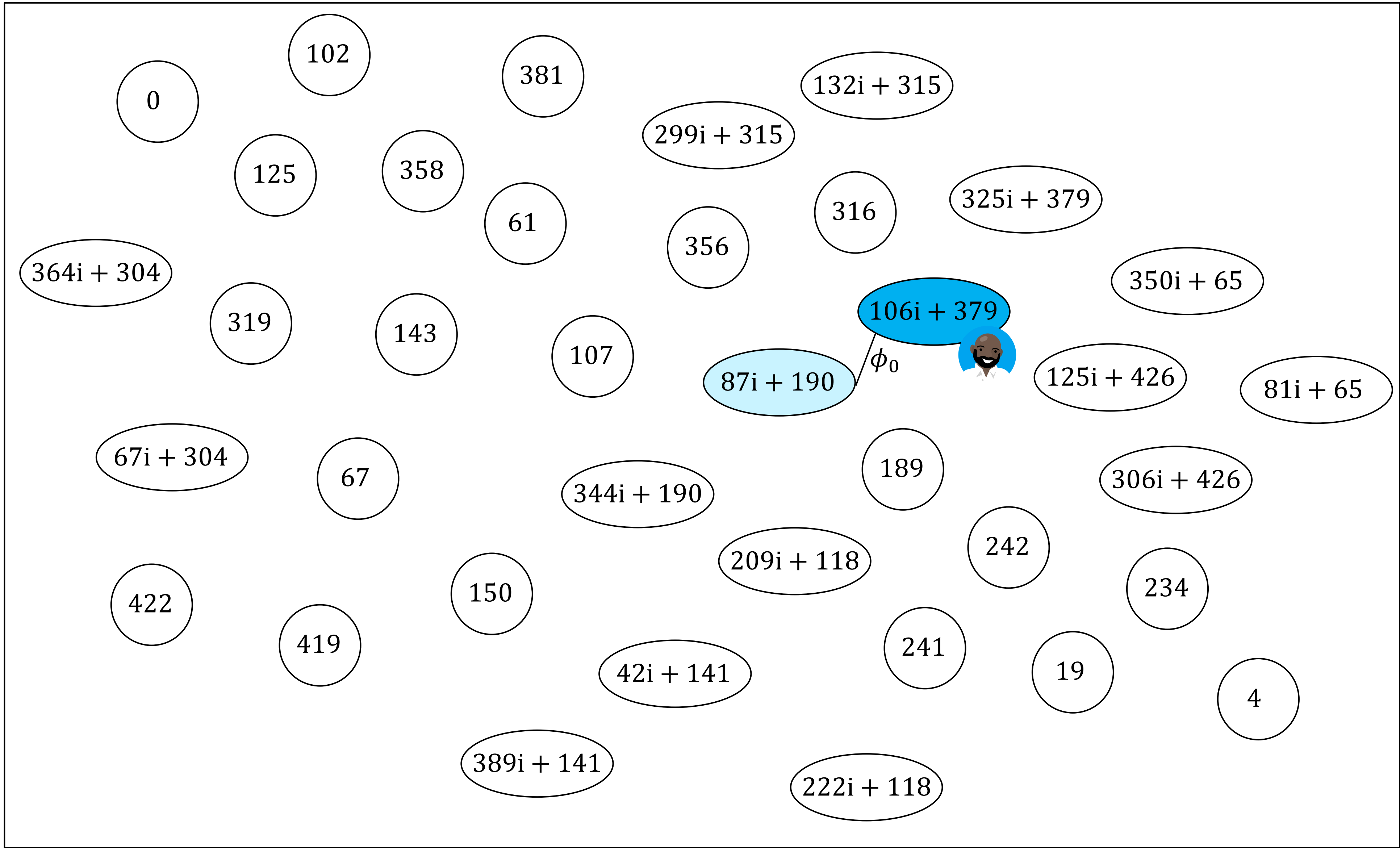
[3]

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

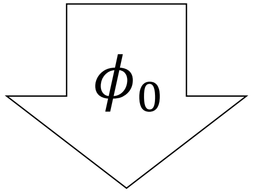
$$\phi_0 : E_0 \to E_1$$

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

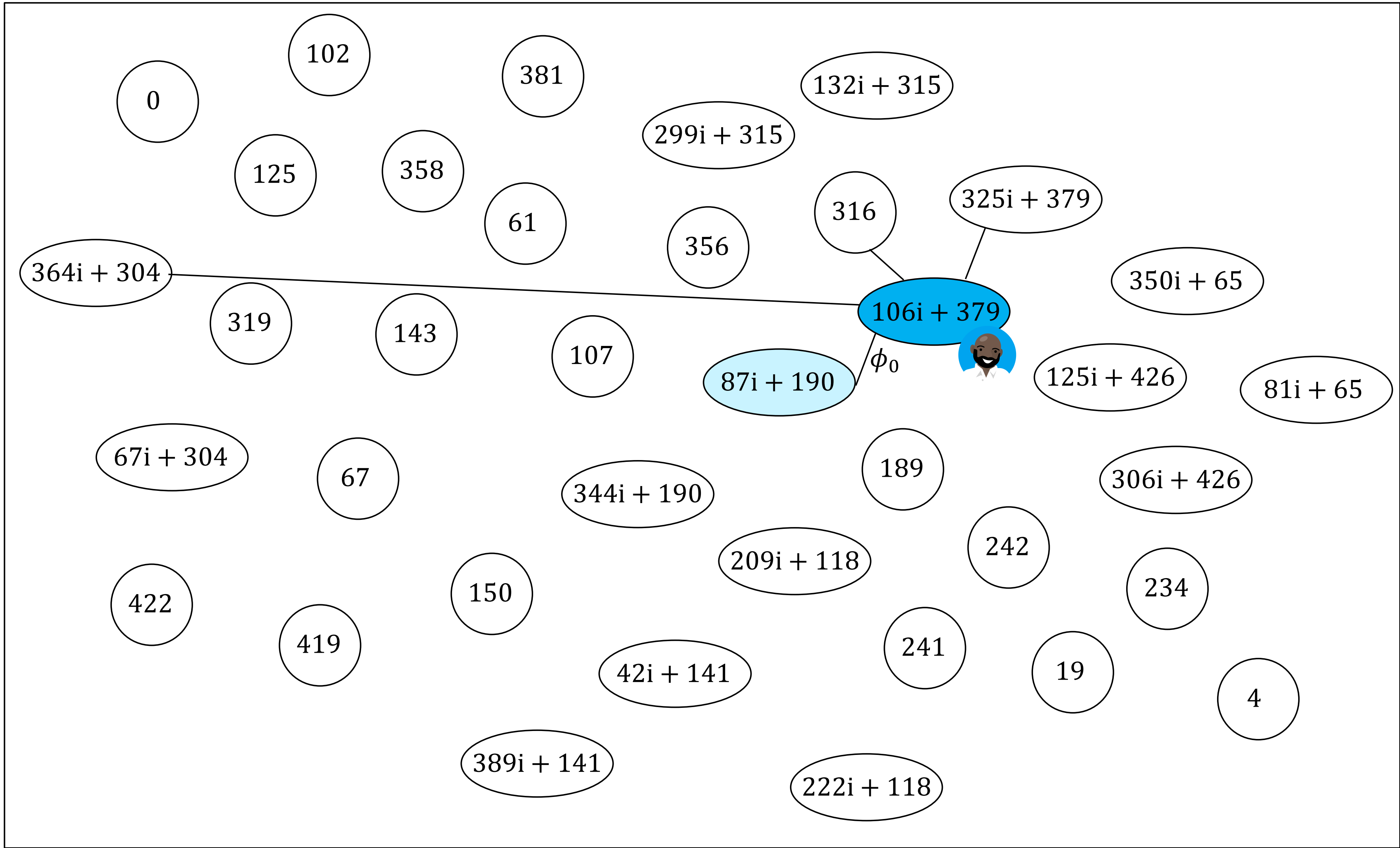
$$j(E_1) = 106i + 379$$



Bob's key generation



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



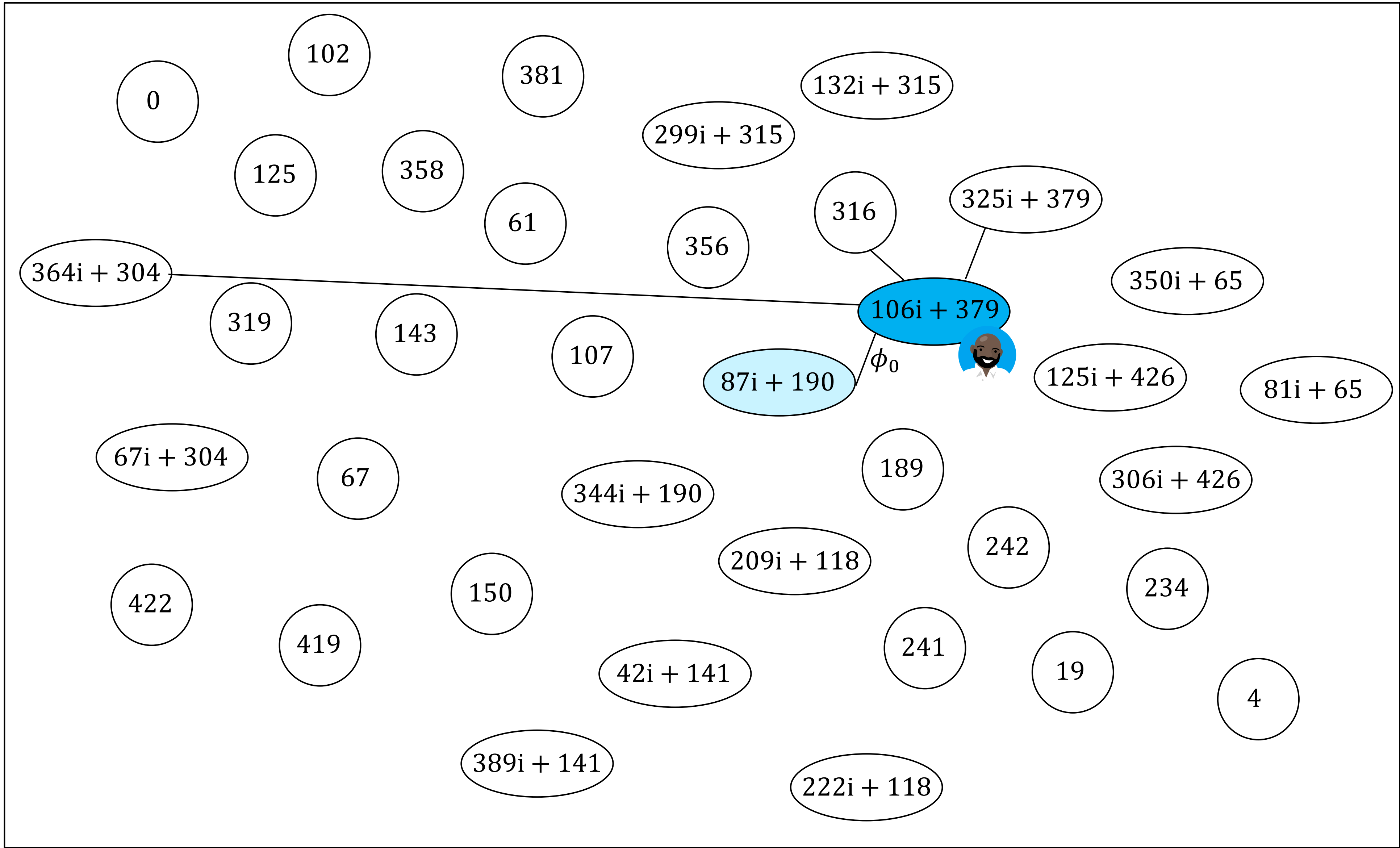
Bob’s key generation

ϕ_0

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

$[3]$

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



Bob’s key generation

ϕ_0

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

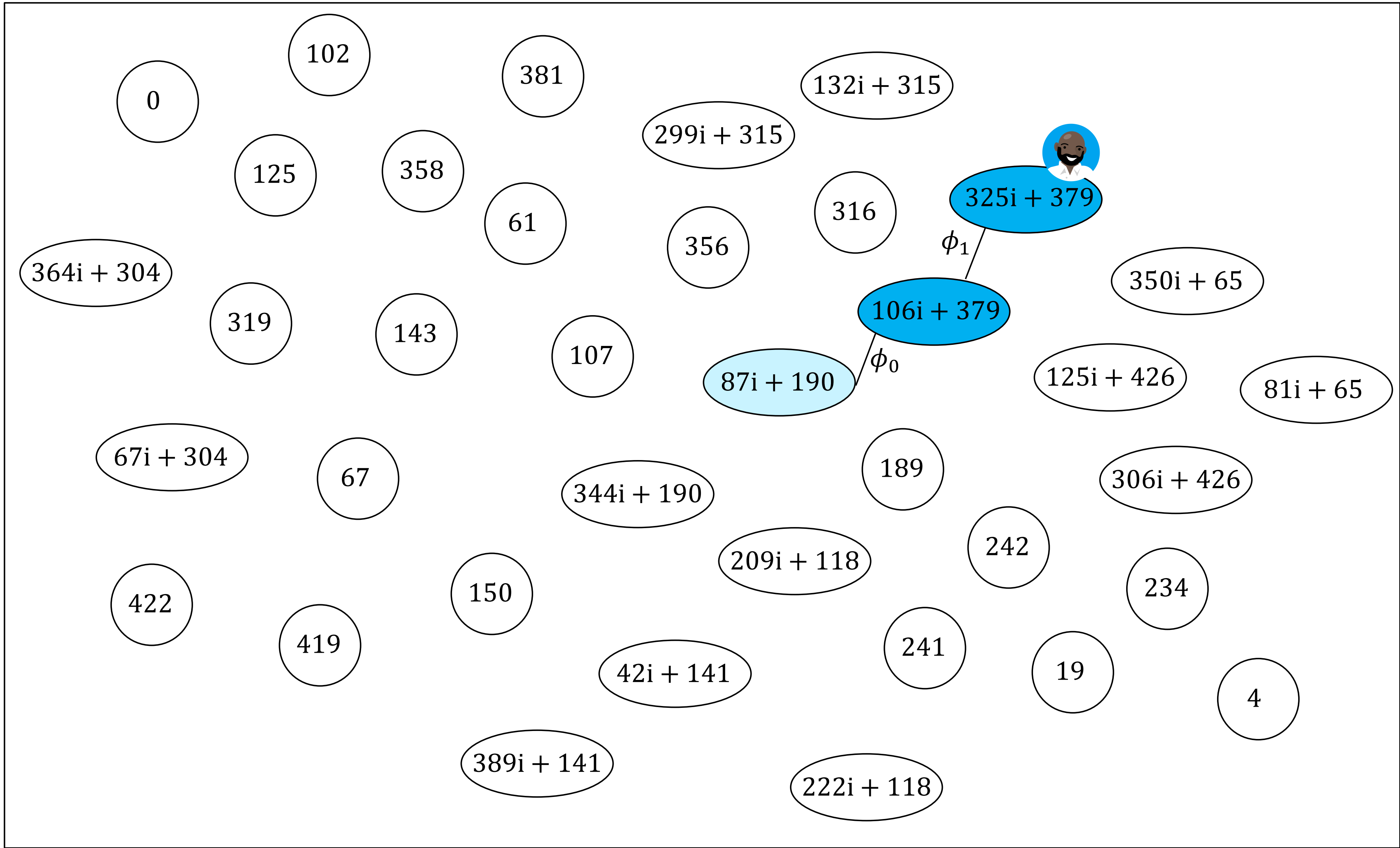
$[3]$

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

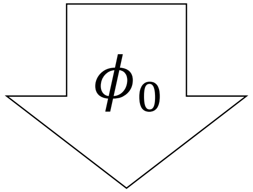
$$\phi_1 : E_1 \rightarrow E_2$$

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

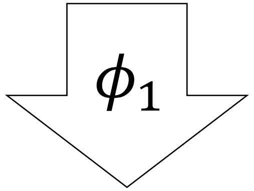
$$j(E_2) = 325i + 379$$



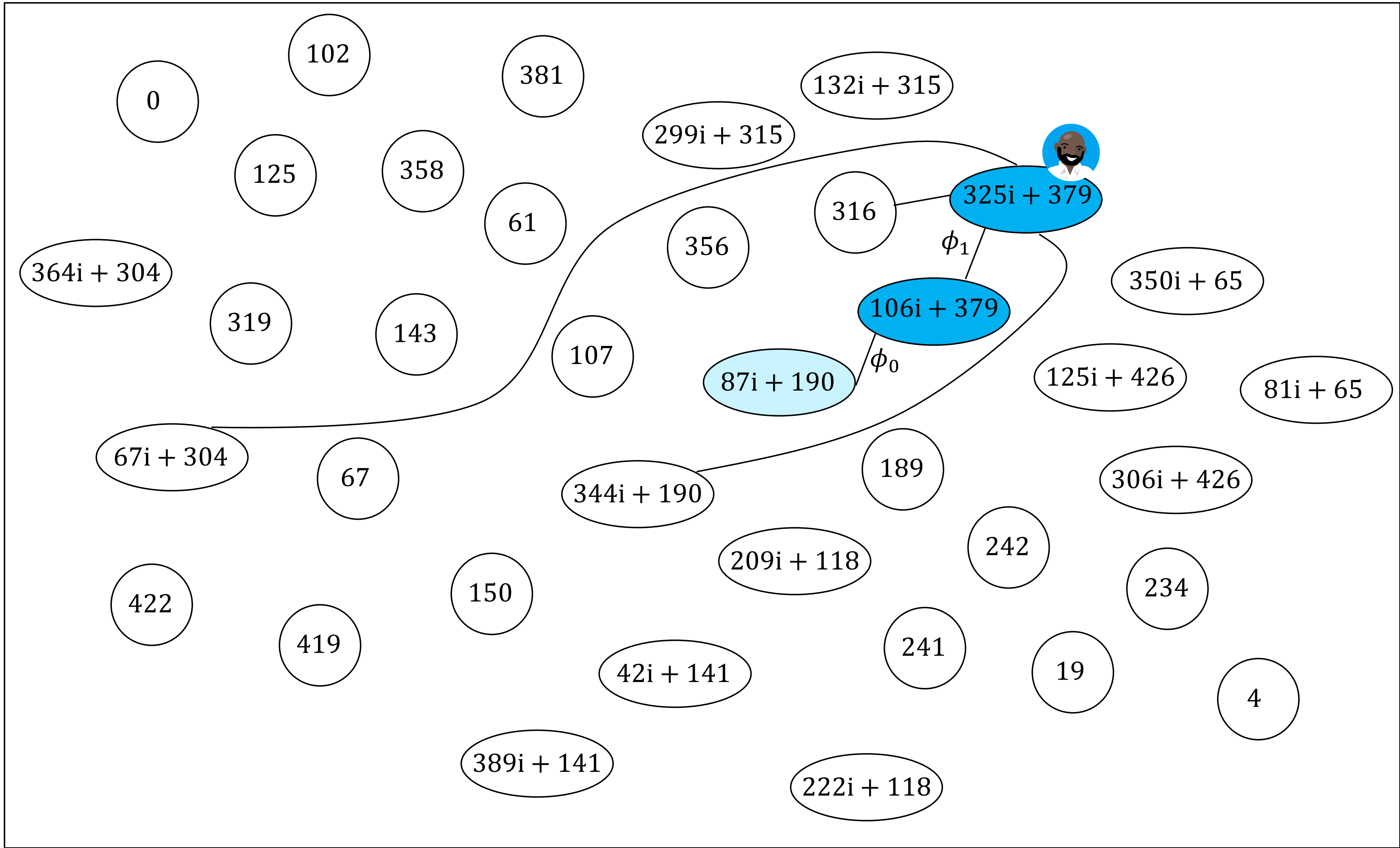
Bob’s key generation



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



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



Bob's key generation

ϕ_0

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

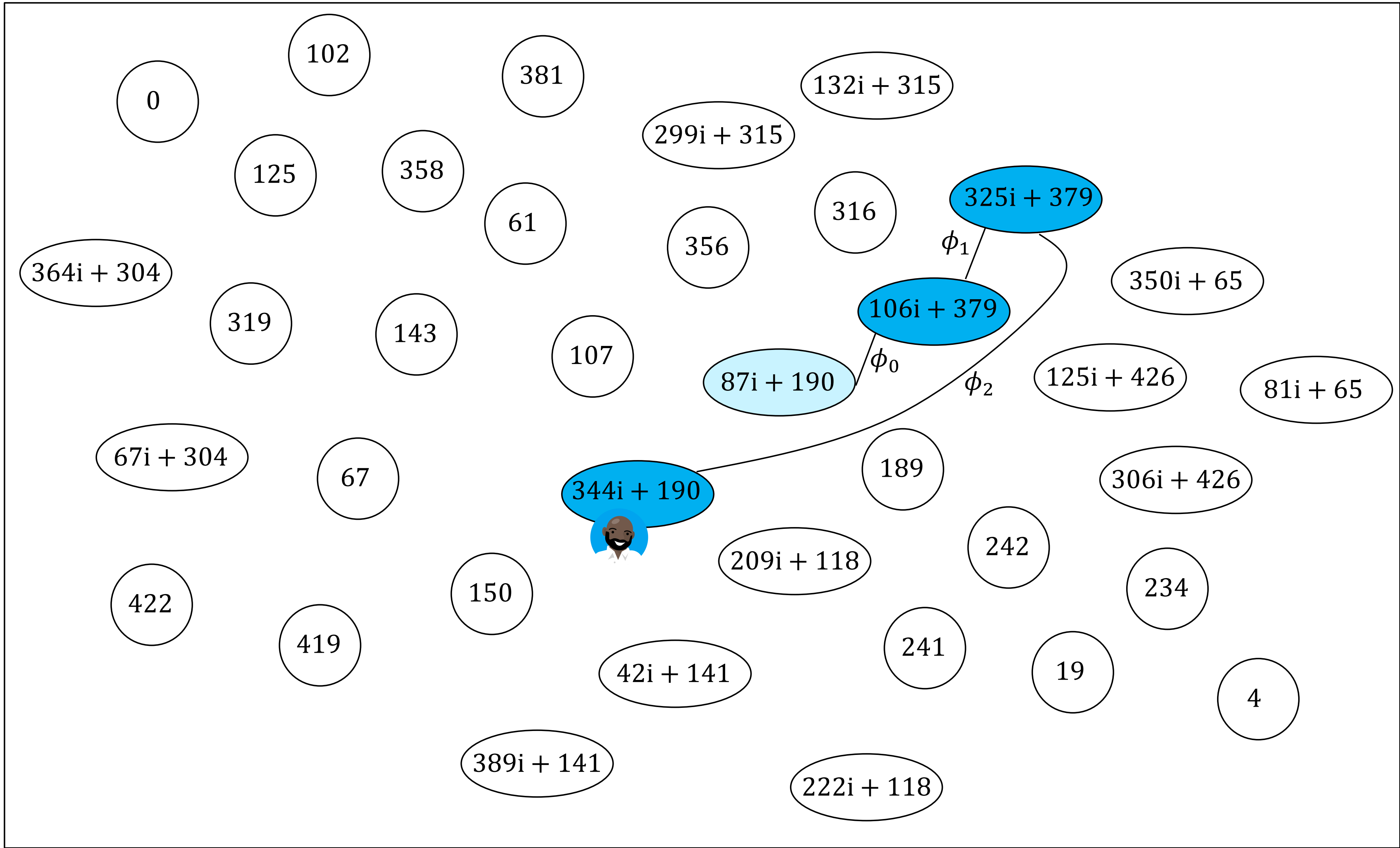
ϕ_1

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

$$\phi_2 : E_2 \to E_3$$

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

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



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

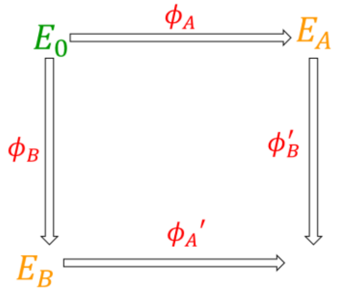
$344i + 190$

Auxiliary points

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

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

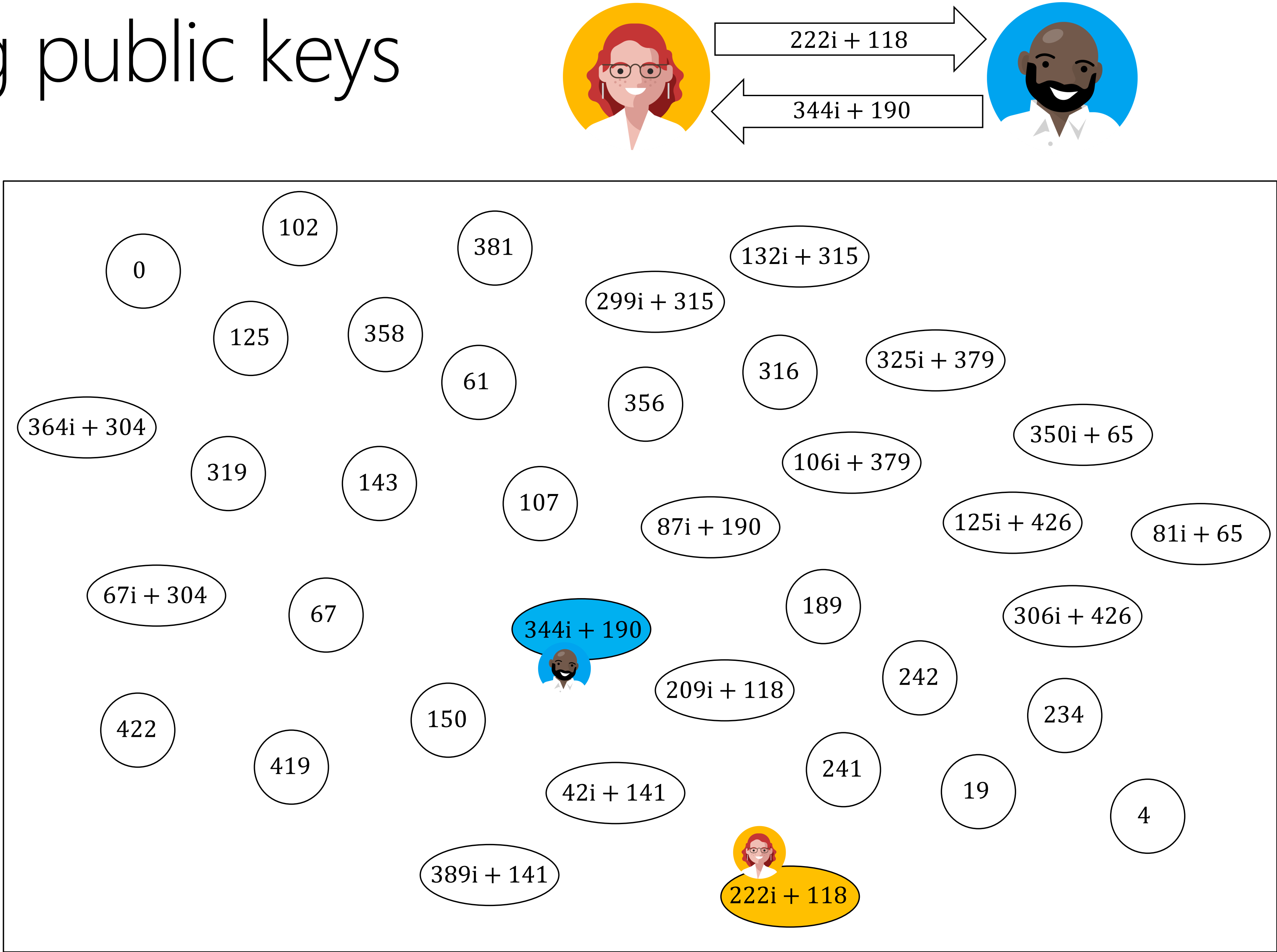
Auxiliary points



Alice's public key:	E_A	P_{AB}	Q_{AB}
	$=$	$=$	$=$
	$\phi_A(E_0)$	$\phi_A(P_B)$	$\phi_A(Q_B)$

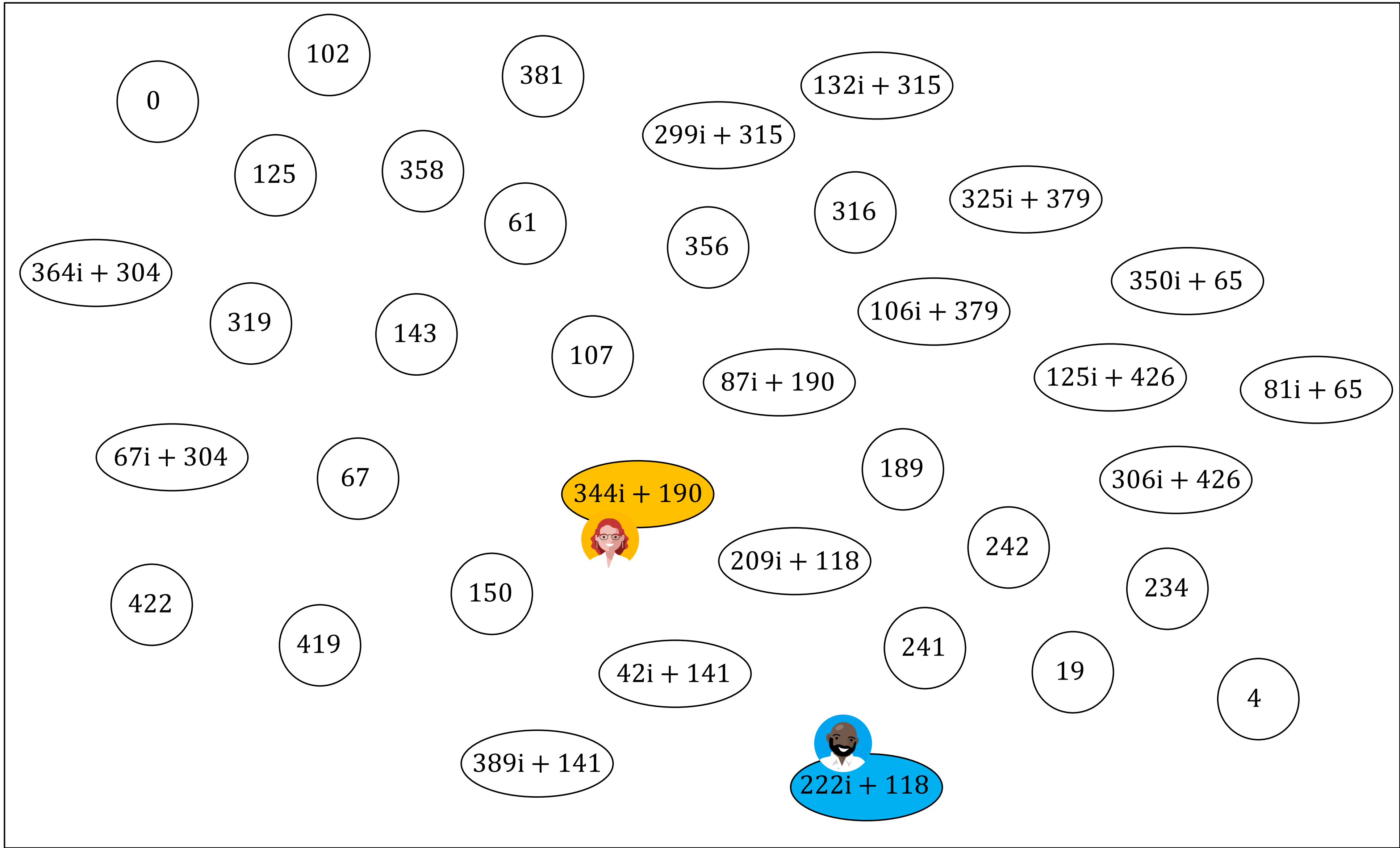
Bob's public key:	E_B	P_{BA}	Q_{BA}
	$=$	$=$	$=$
	$\phi_B(E_0)$	$\phi_B(P_A)$	$\phi_B(Q_A)$

Exchanging public keys



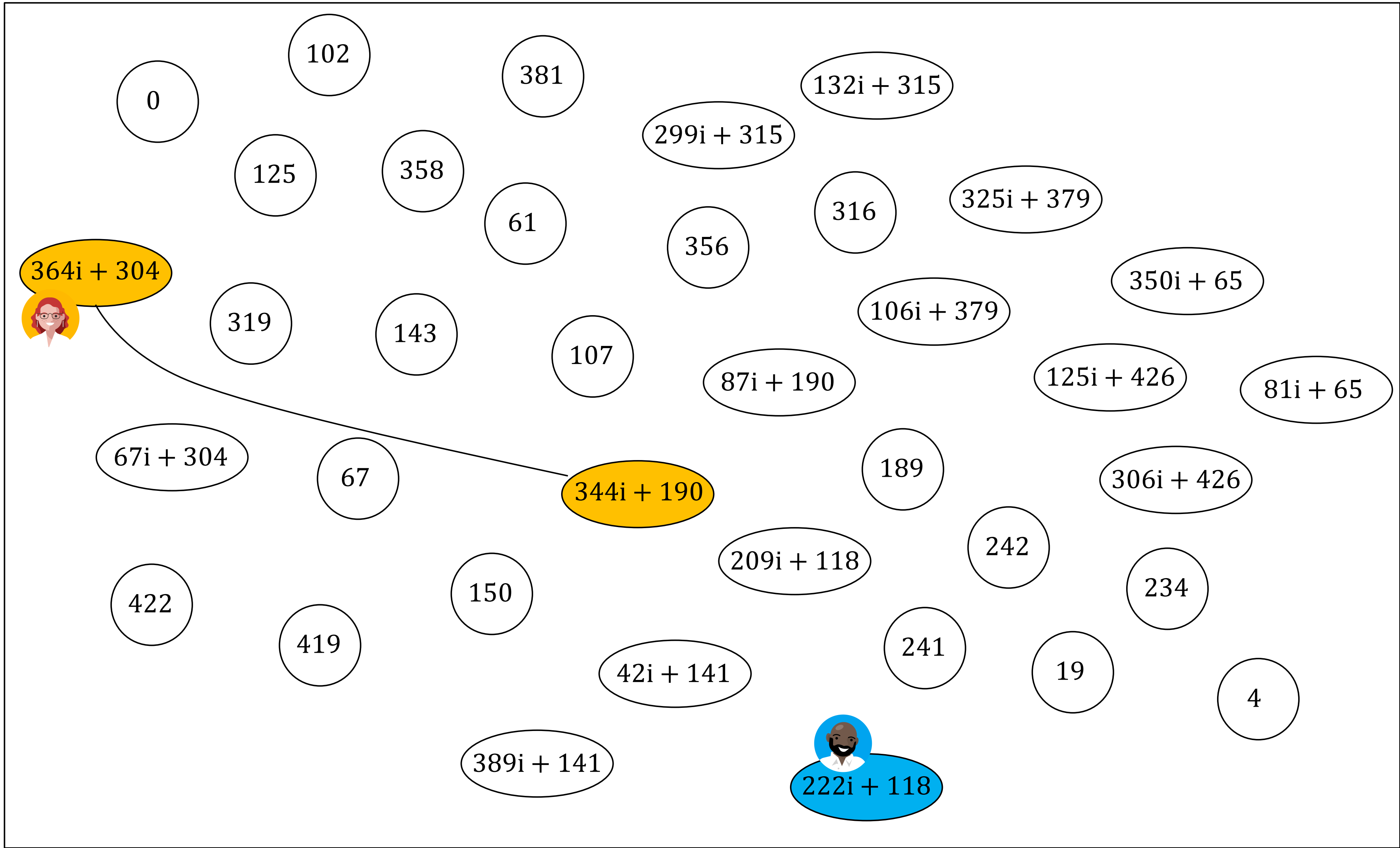
Alice's shared secret

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



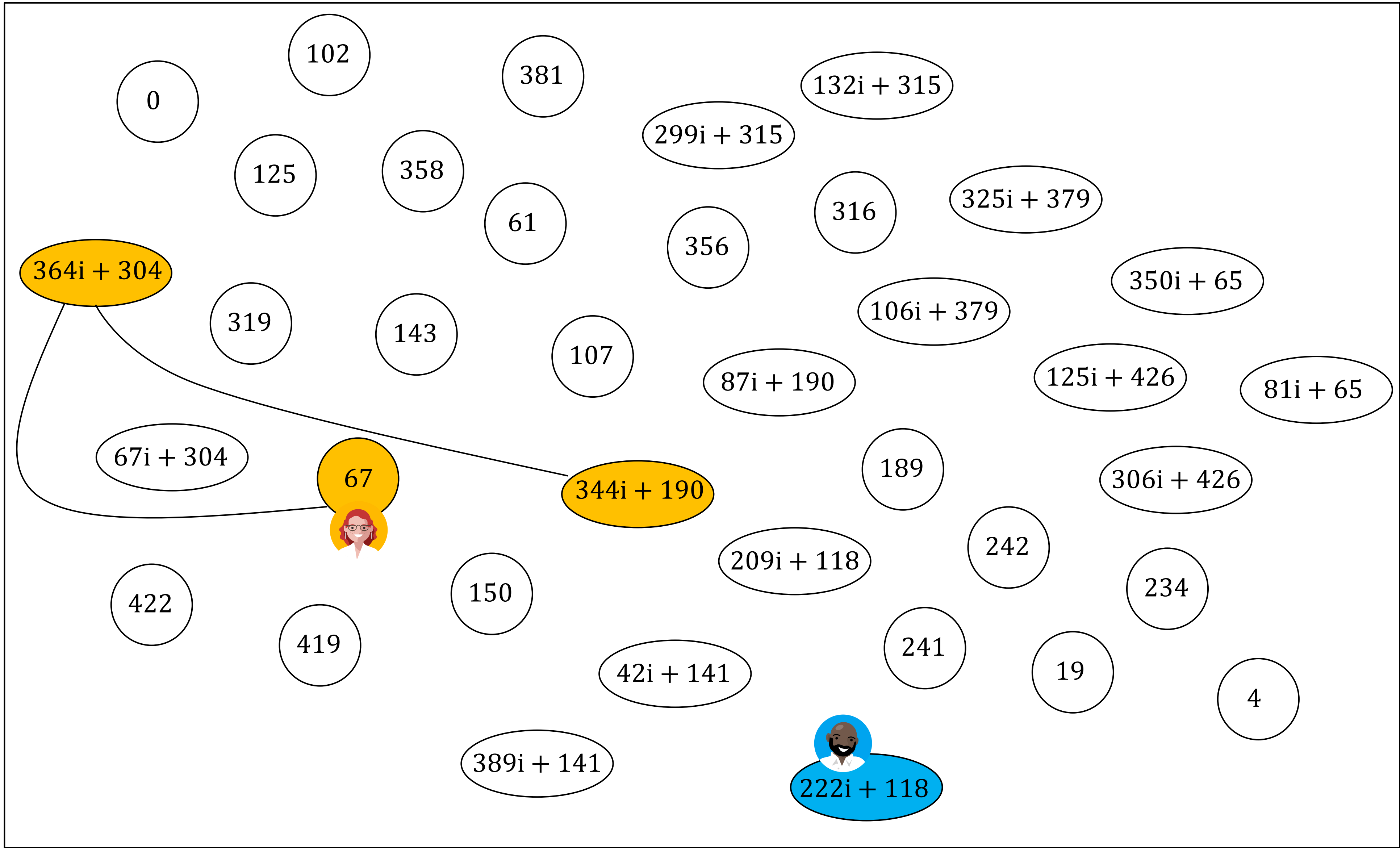
Alice's shared secret

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



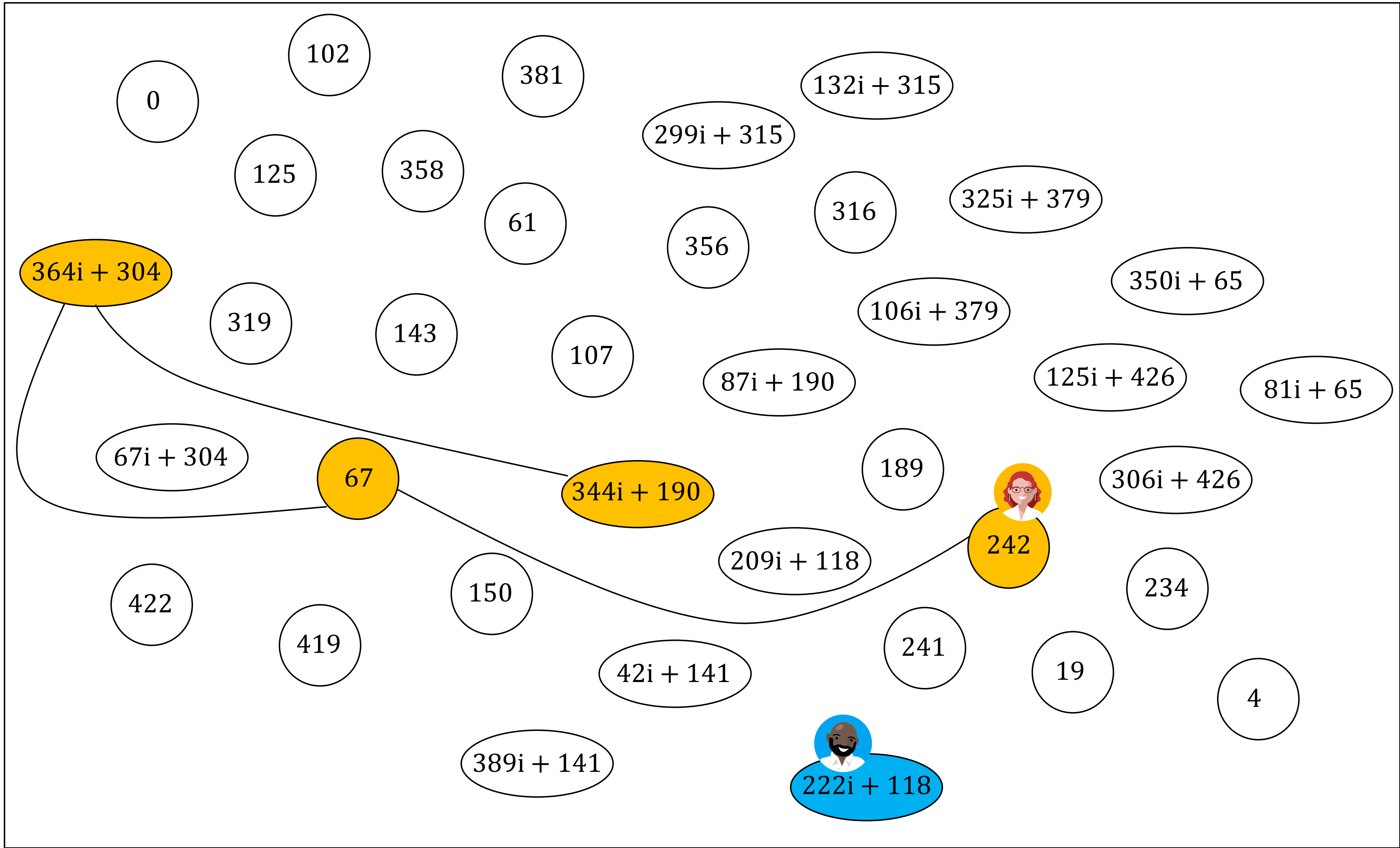
Alice's shared secret

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



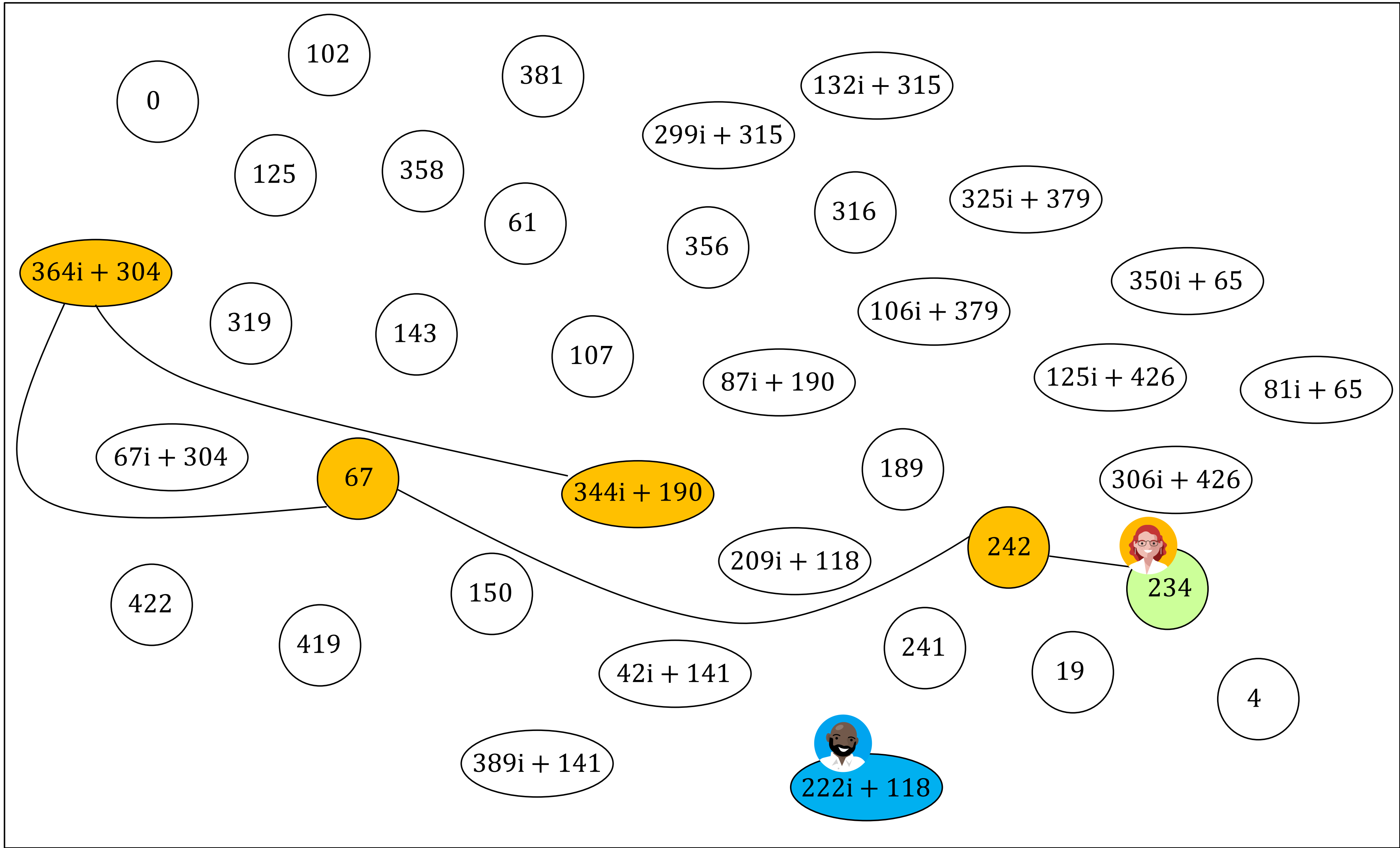
Alice's shared secret

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



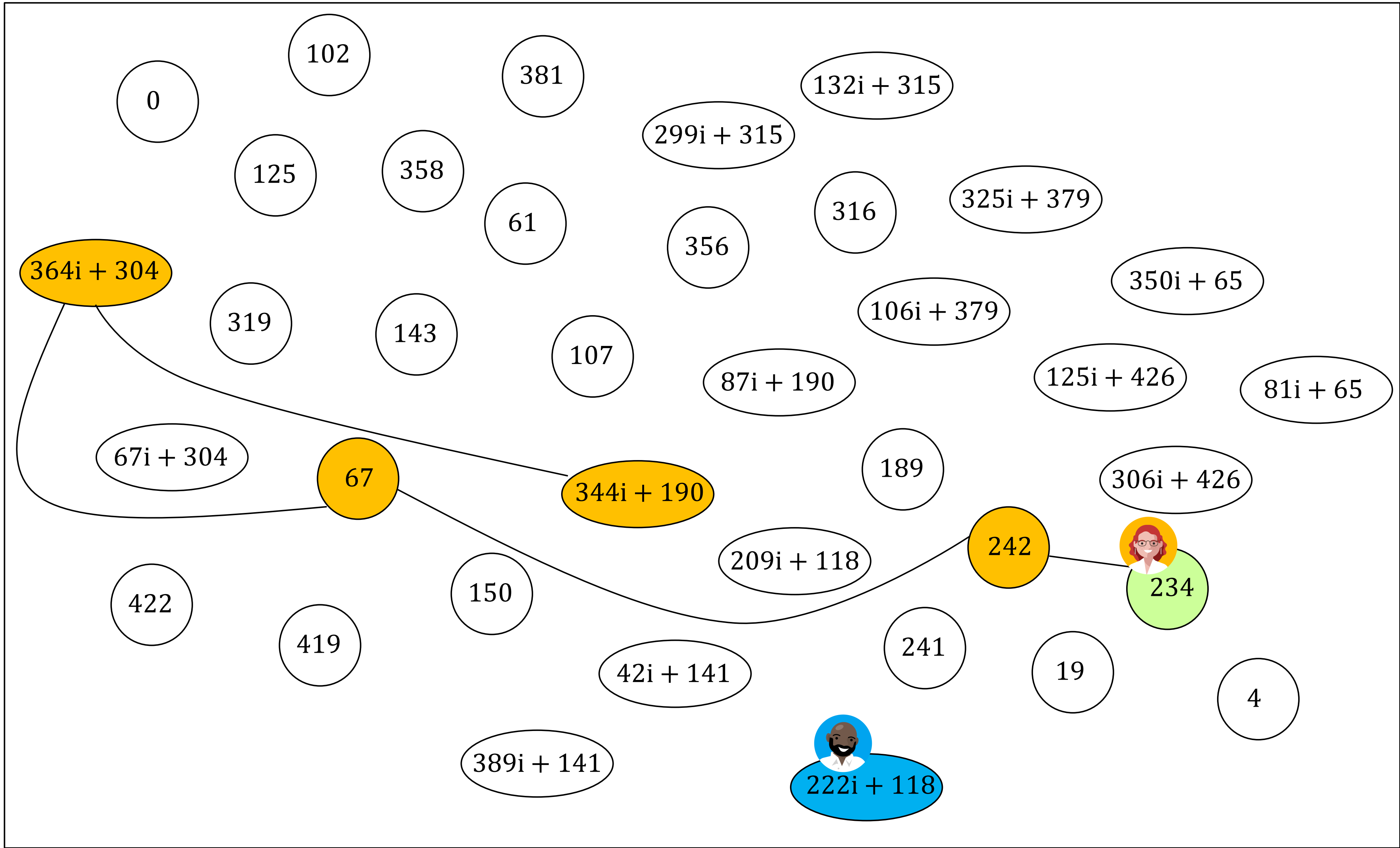
Alice's shared secret

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



Bob's shared secret

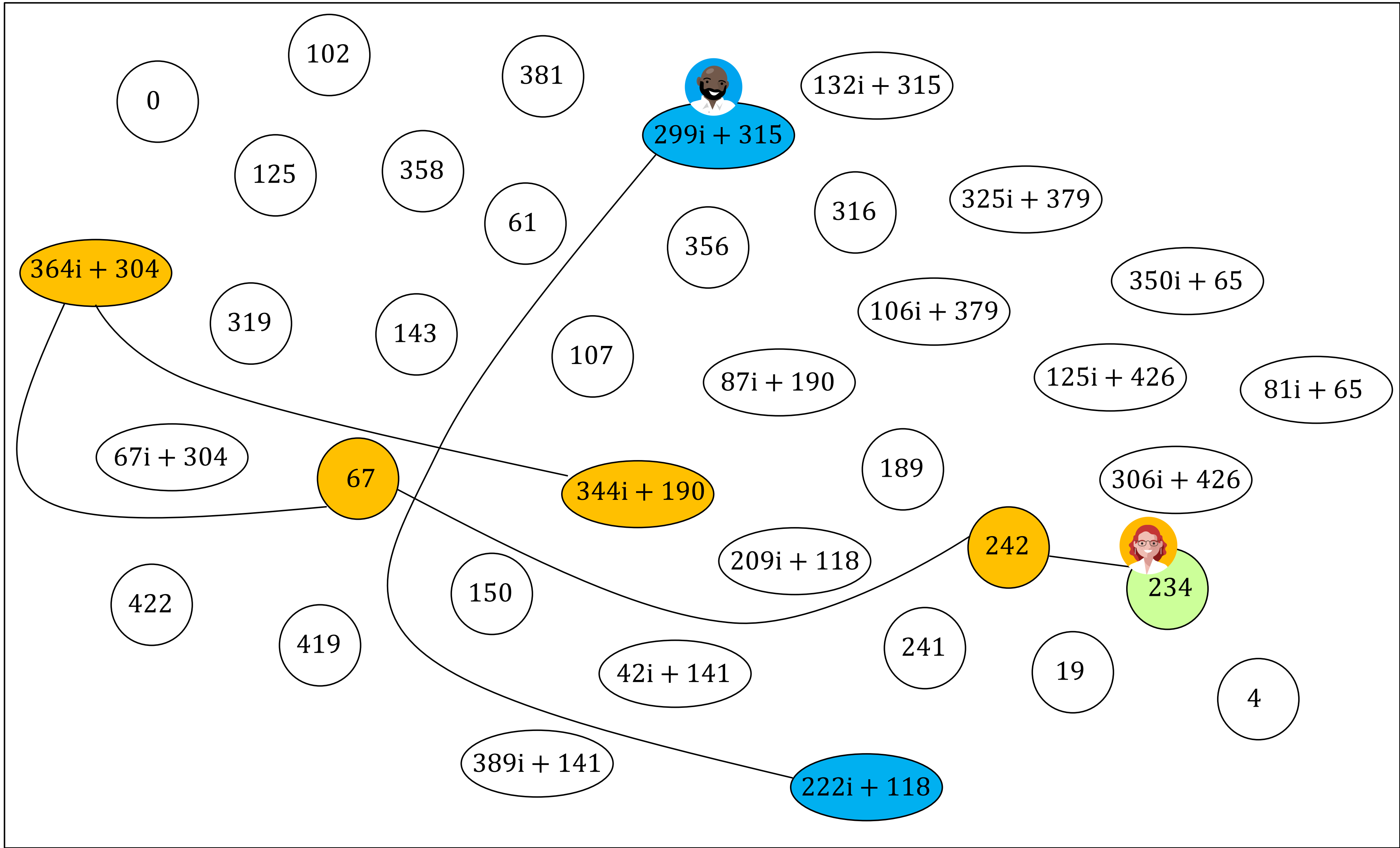
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

Bob's shared secret

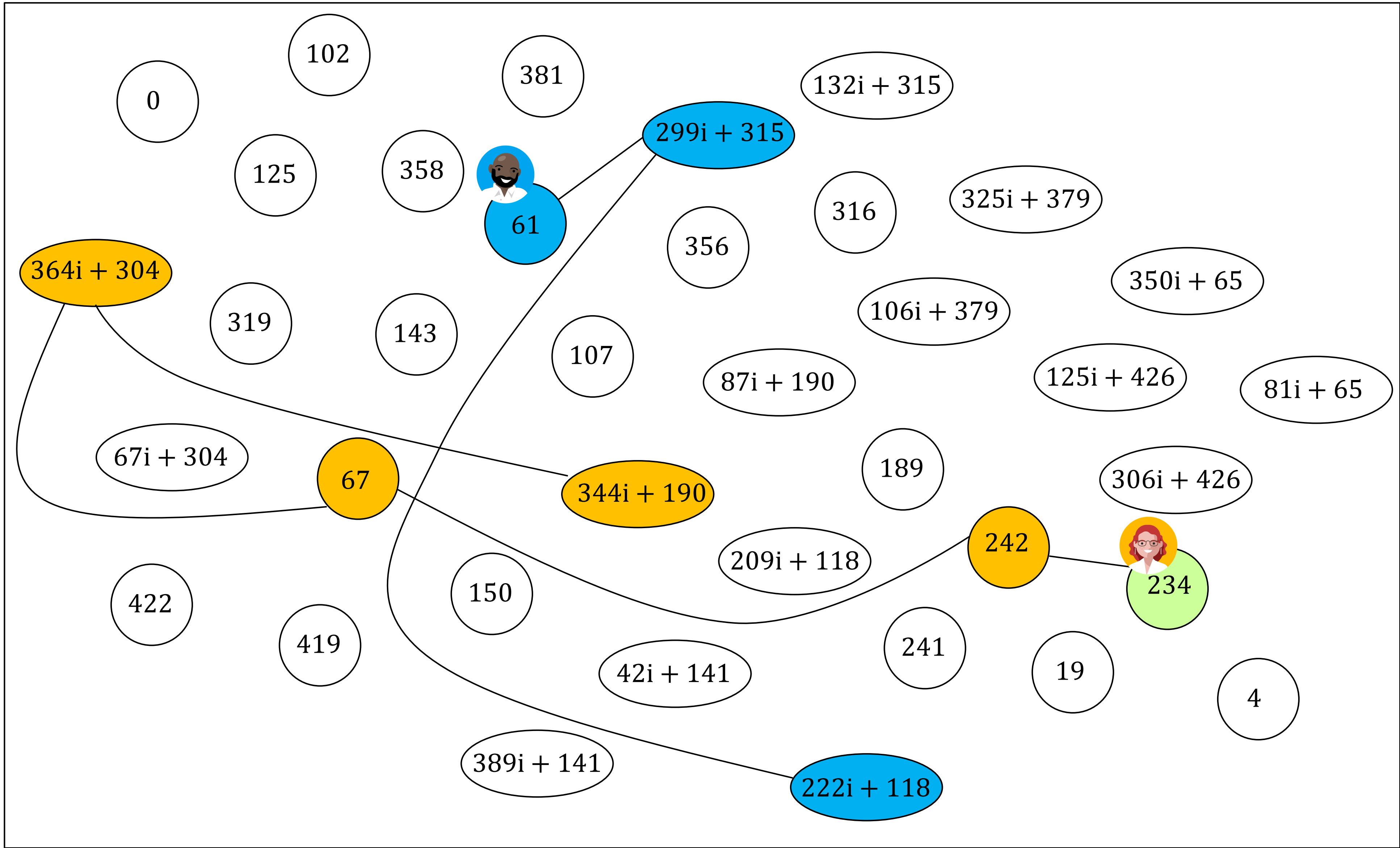
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

Bob’s shared secret

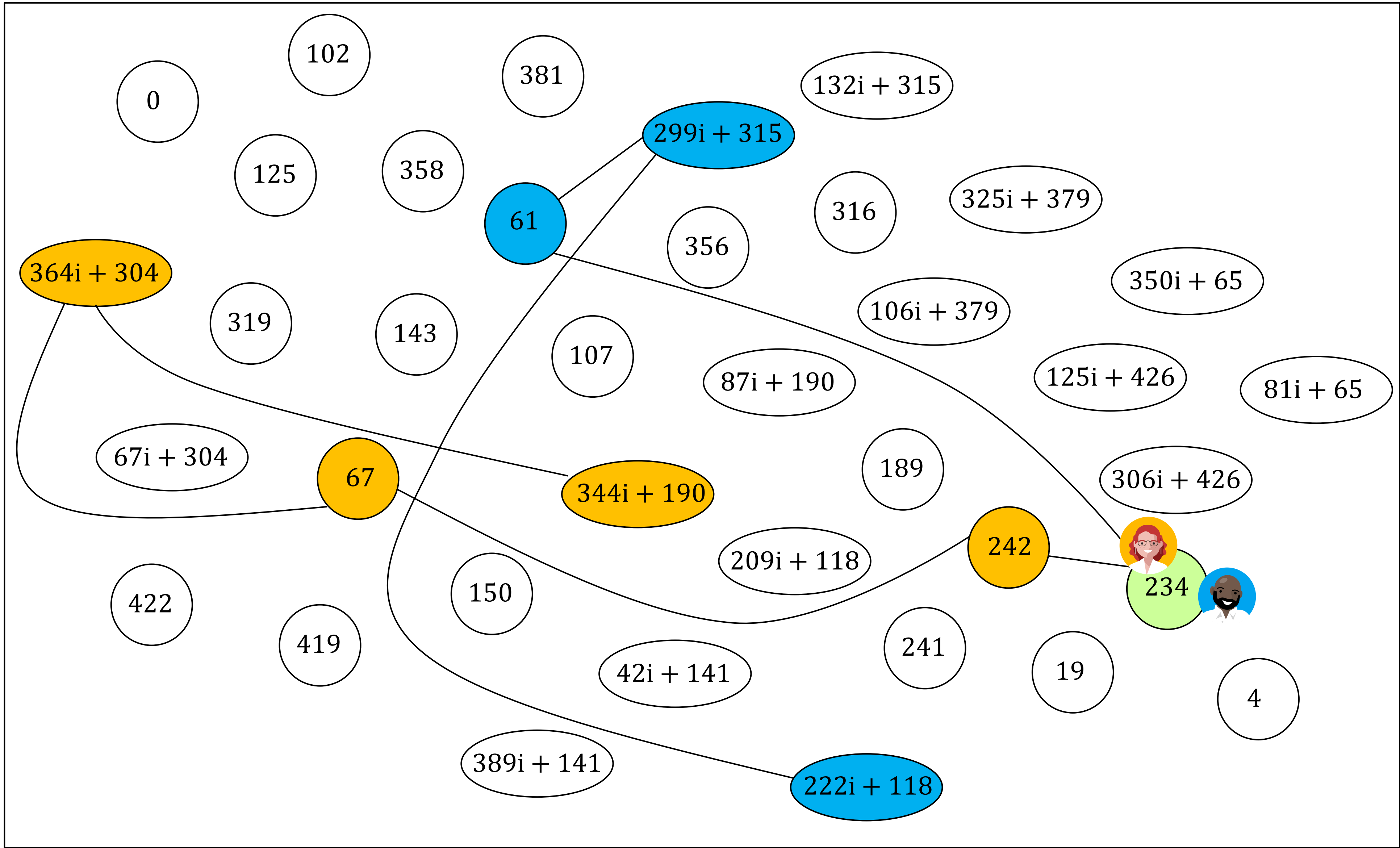
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

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?

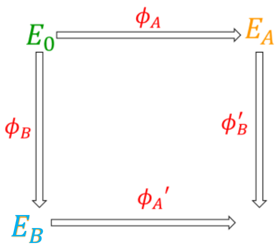
$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$

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

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

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

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



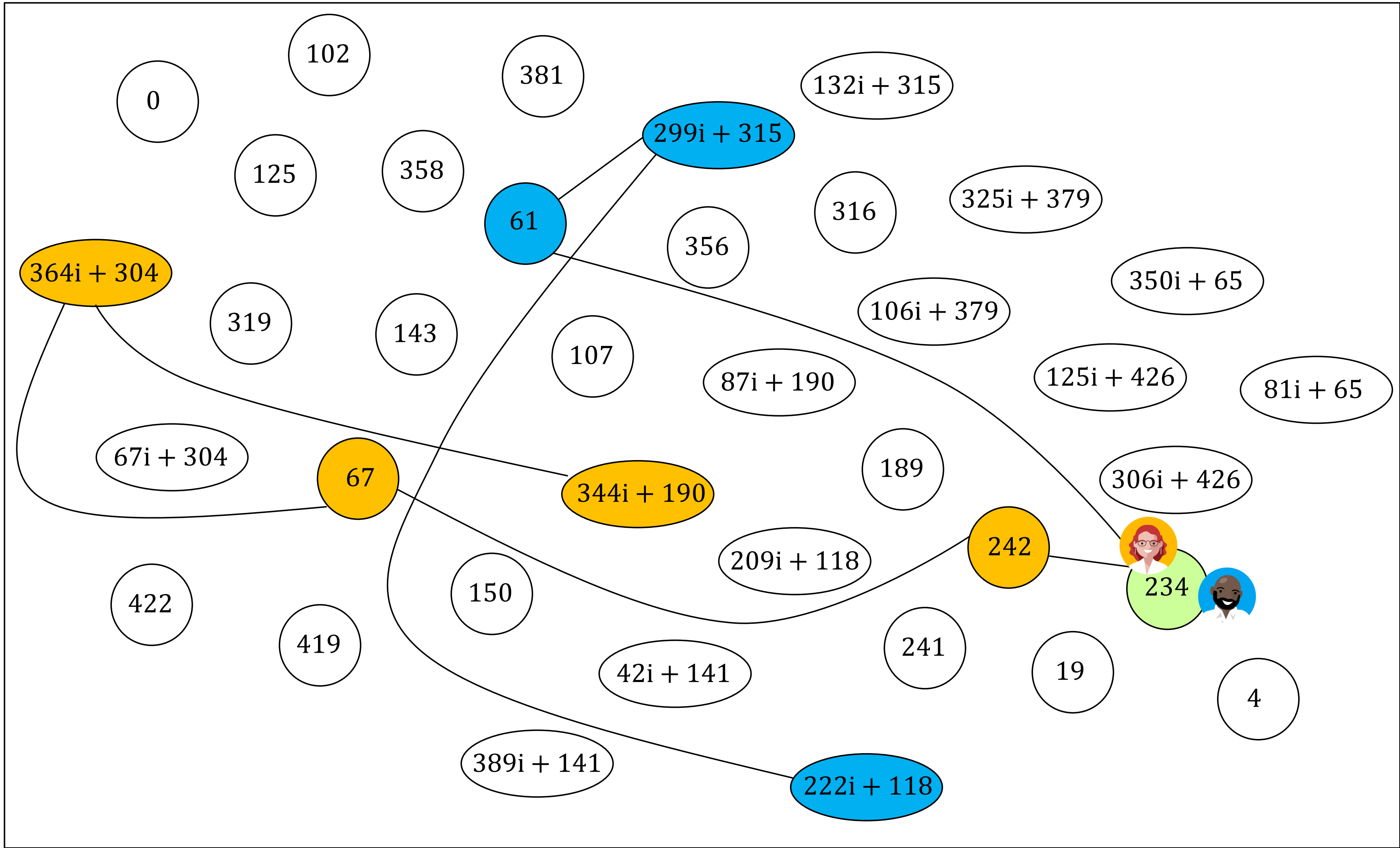
$$\boxed{\phi'_B = E_B/\langle S'_B\rangle}$$

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

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

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

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



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

Cryptanalysis of the SSI problem


E
?
E′

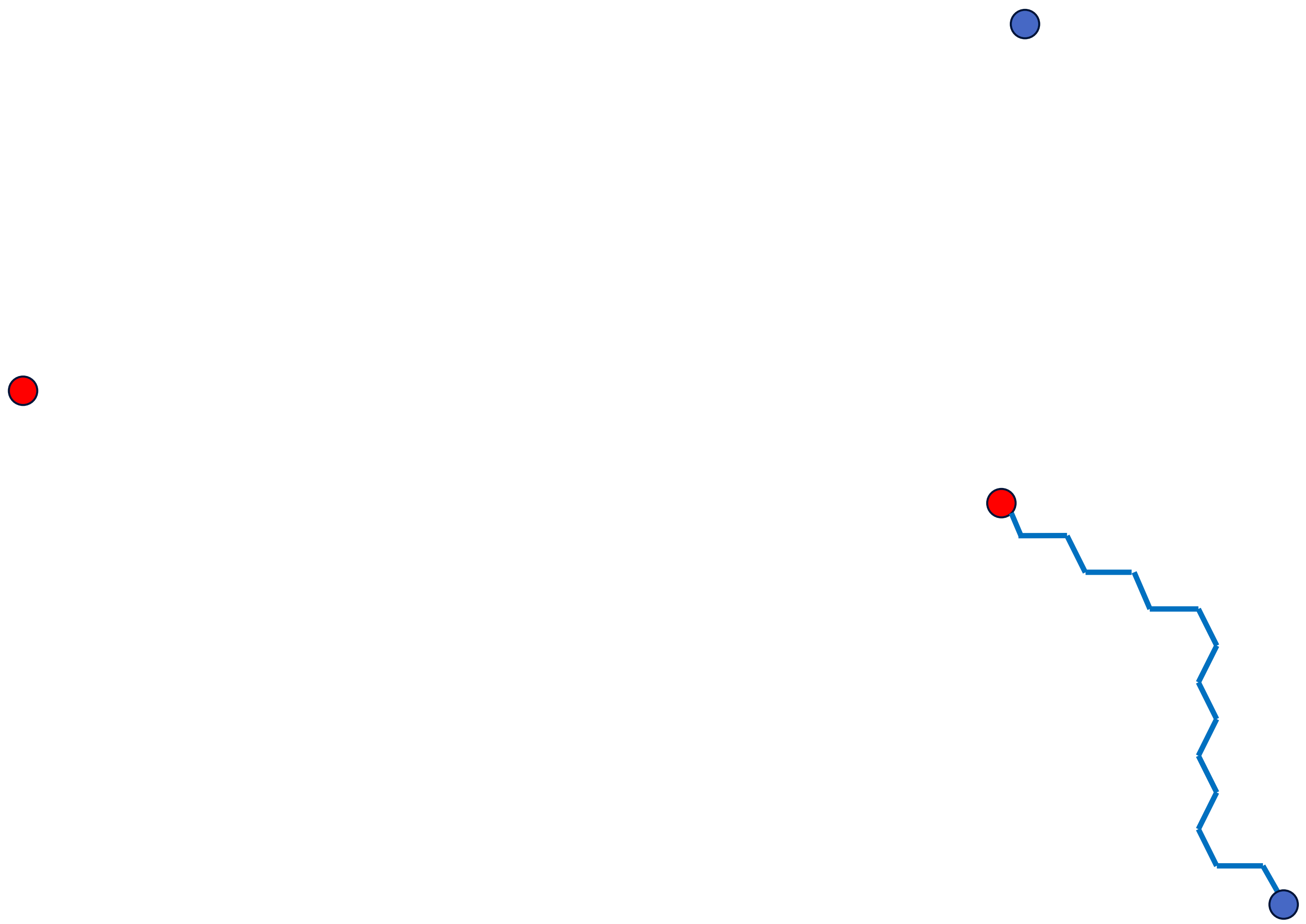
Claw algorithm

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

Claw algorithm

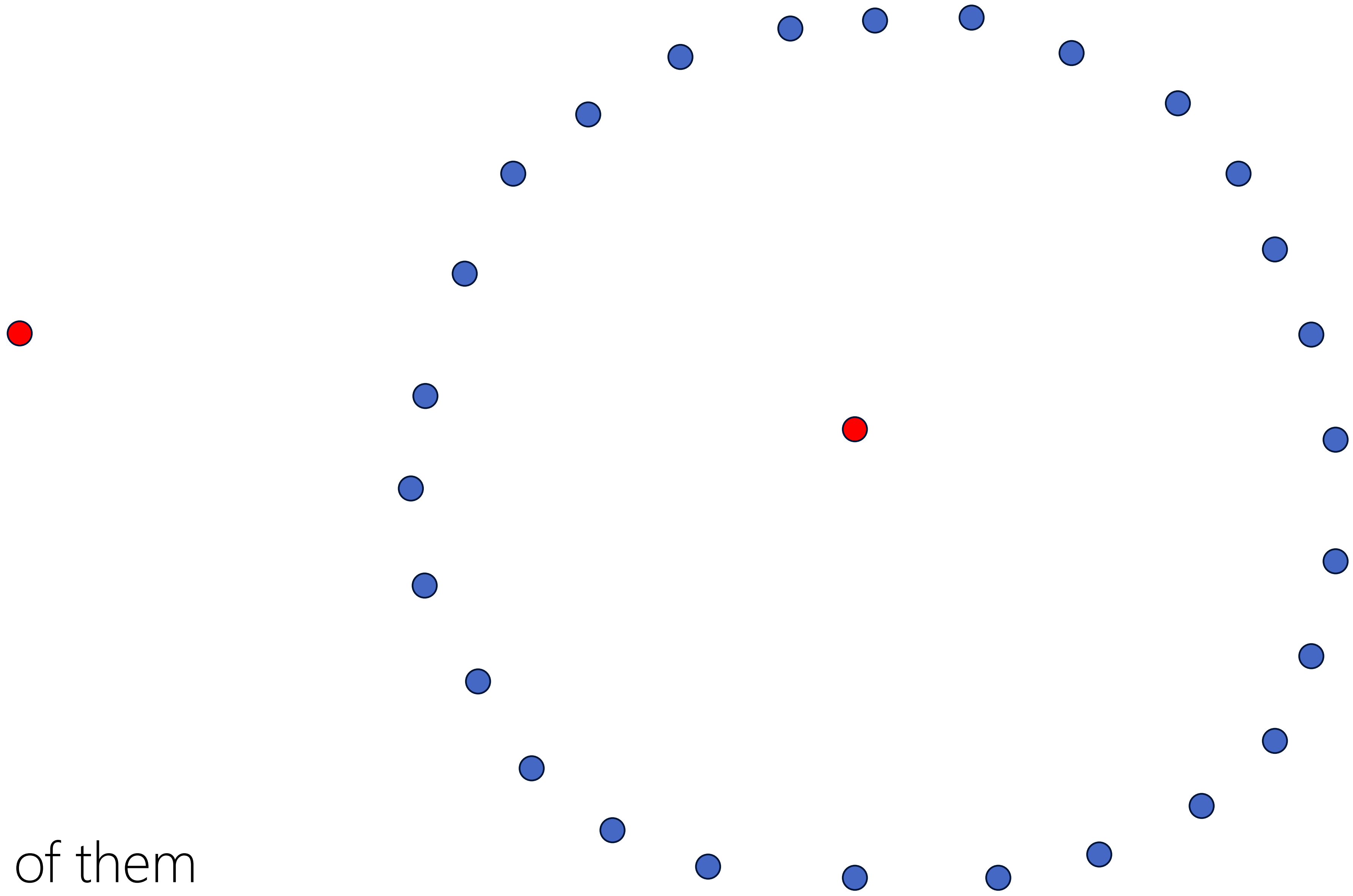
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



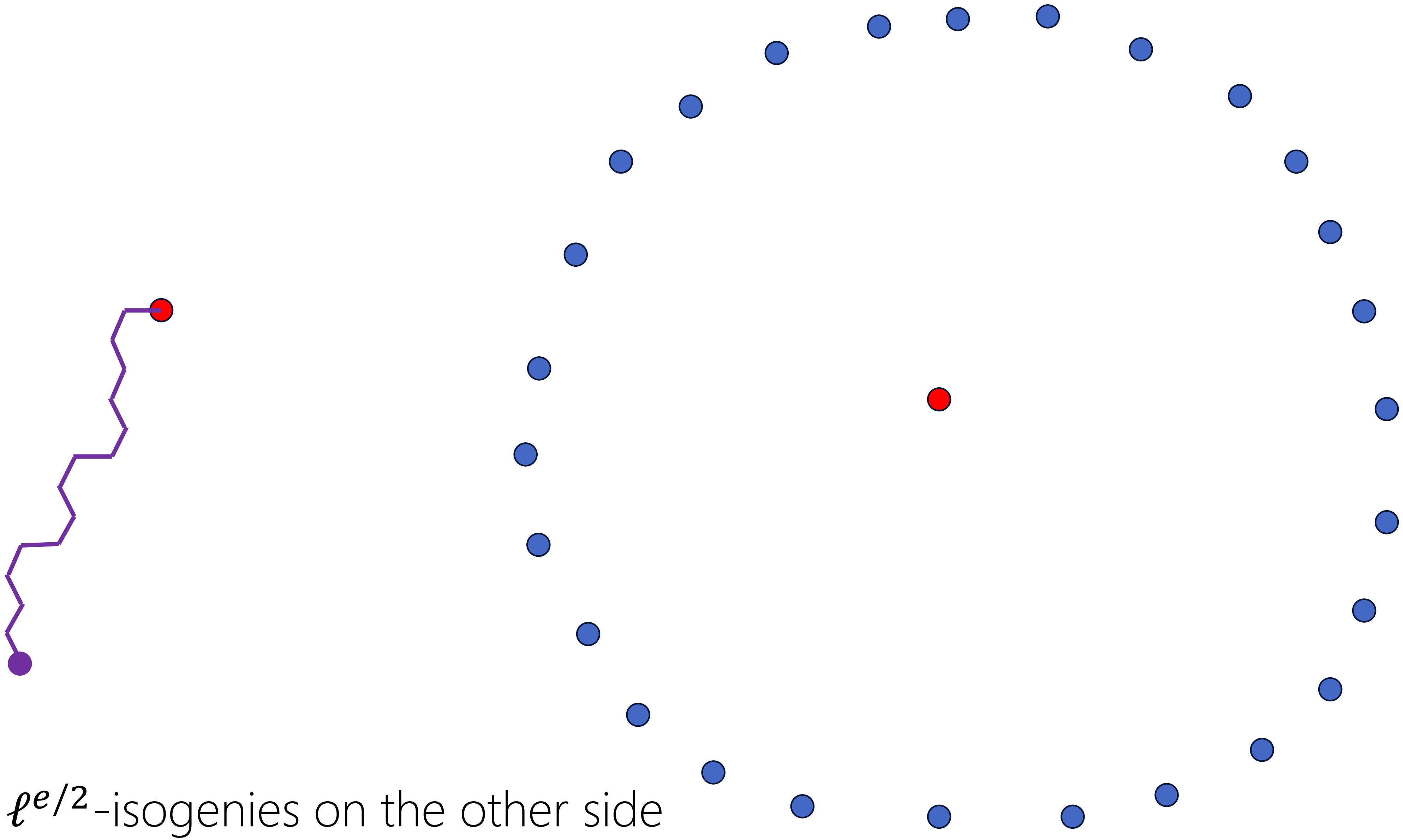
Compute and store $\ell^{e/2}$-isogenies on one side

Claw algorithm



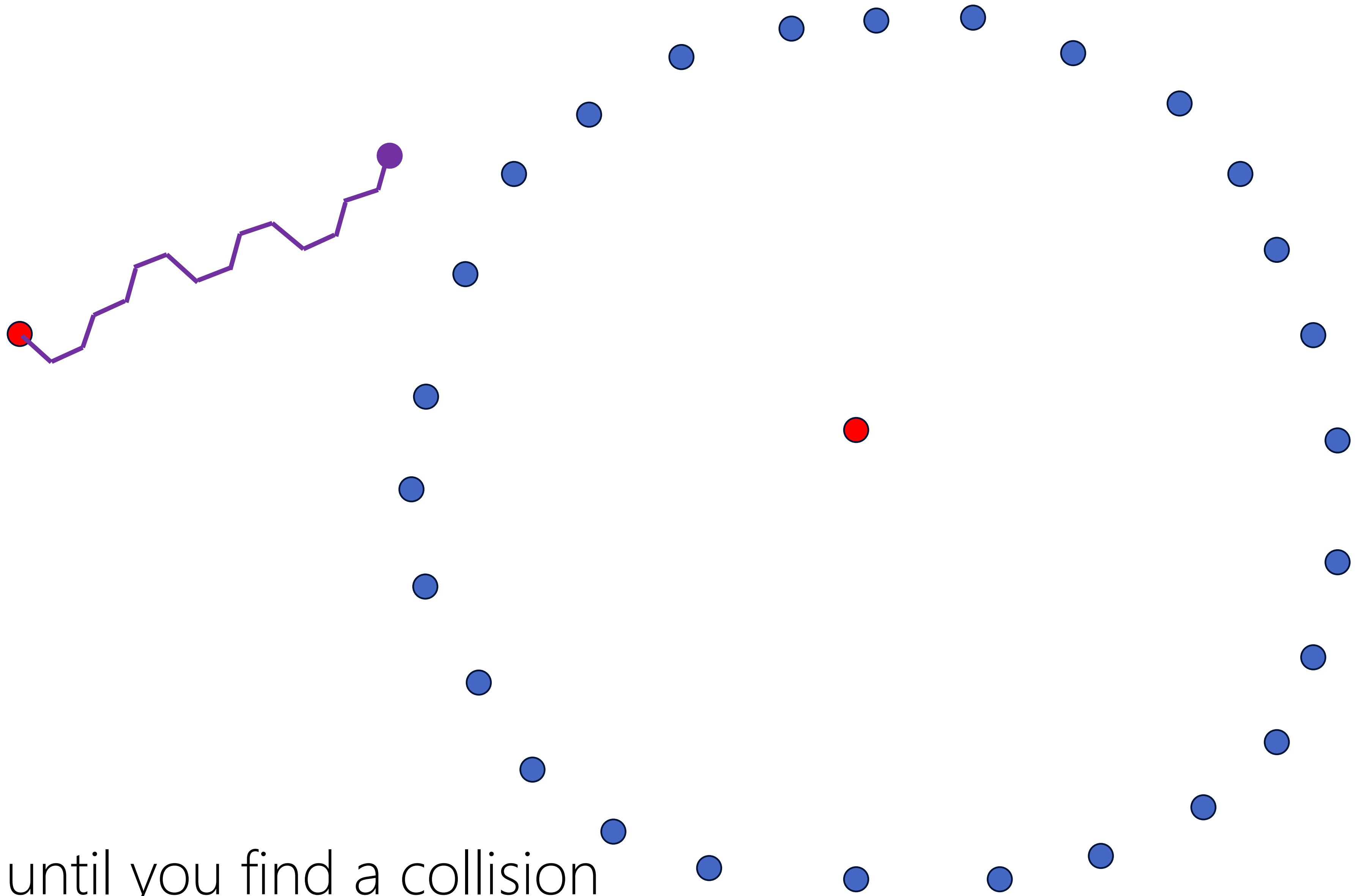
… until you have all of them

Claw algorithm



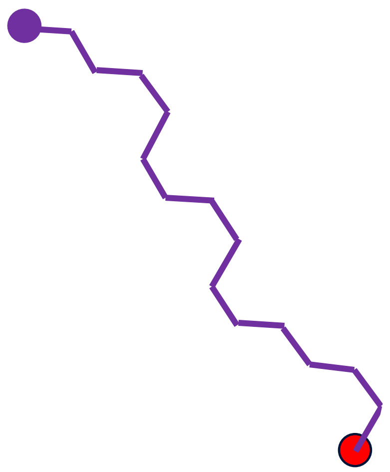
Now compute $\ell^{e/2}$-isogenies on the other side

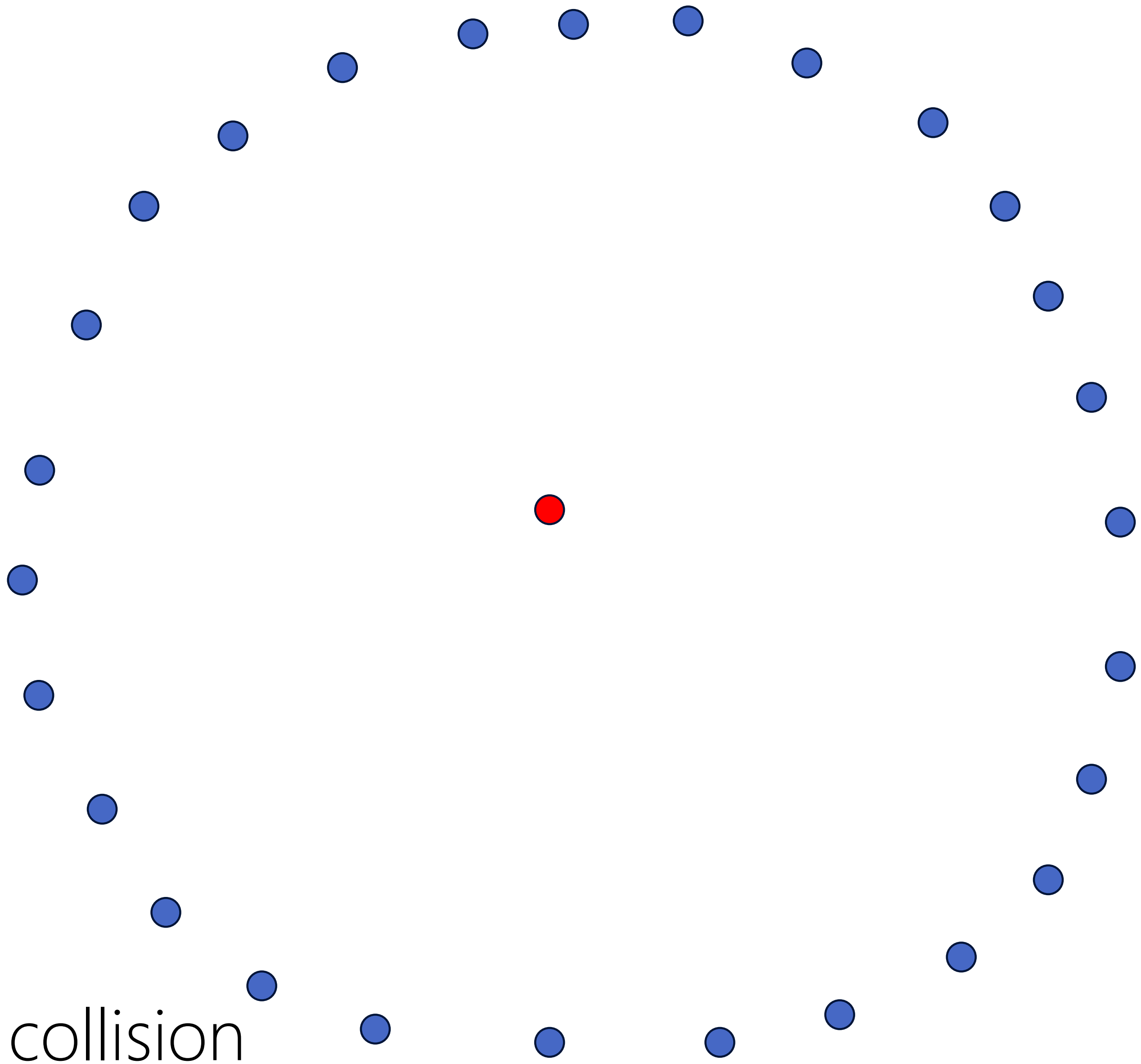
Claw algorithm



… discarding them until you find a collision

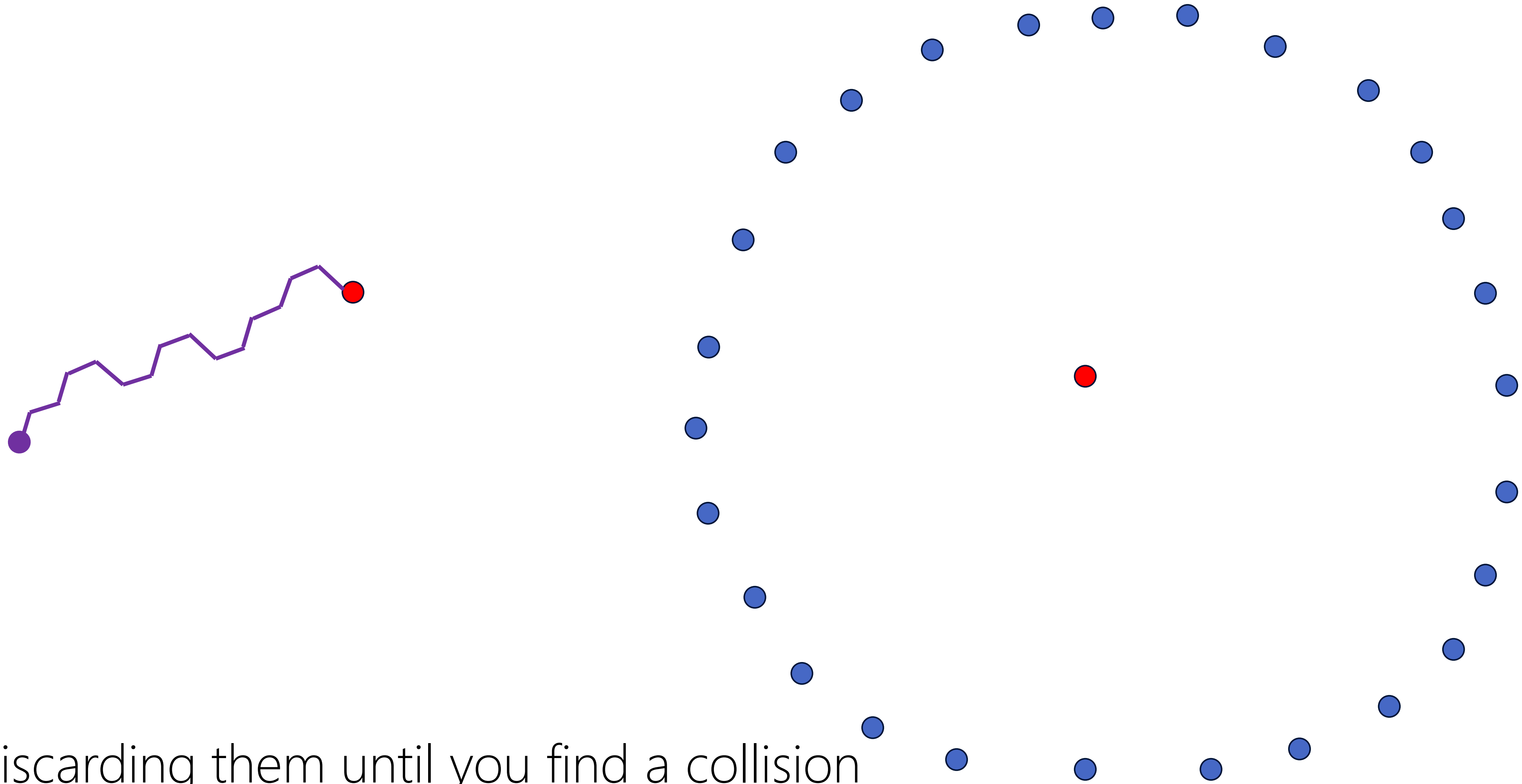
Claw algorithm





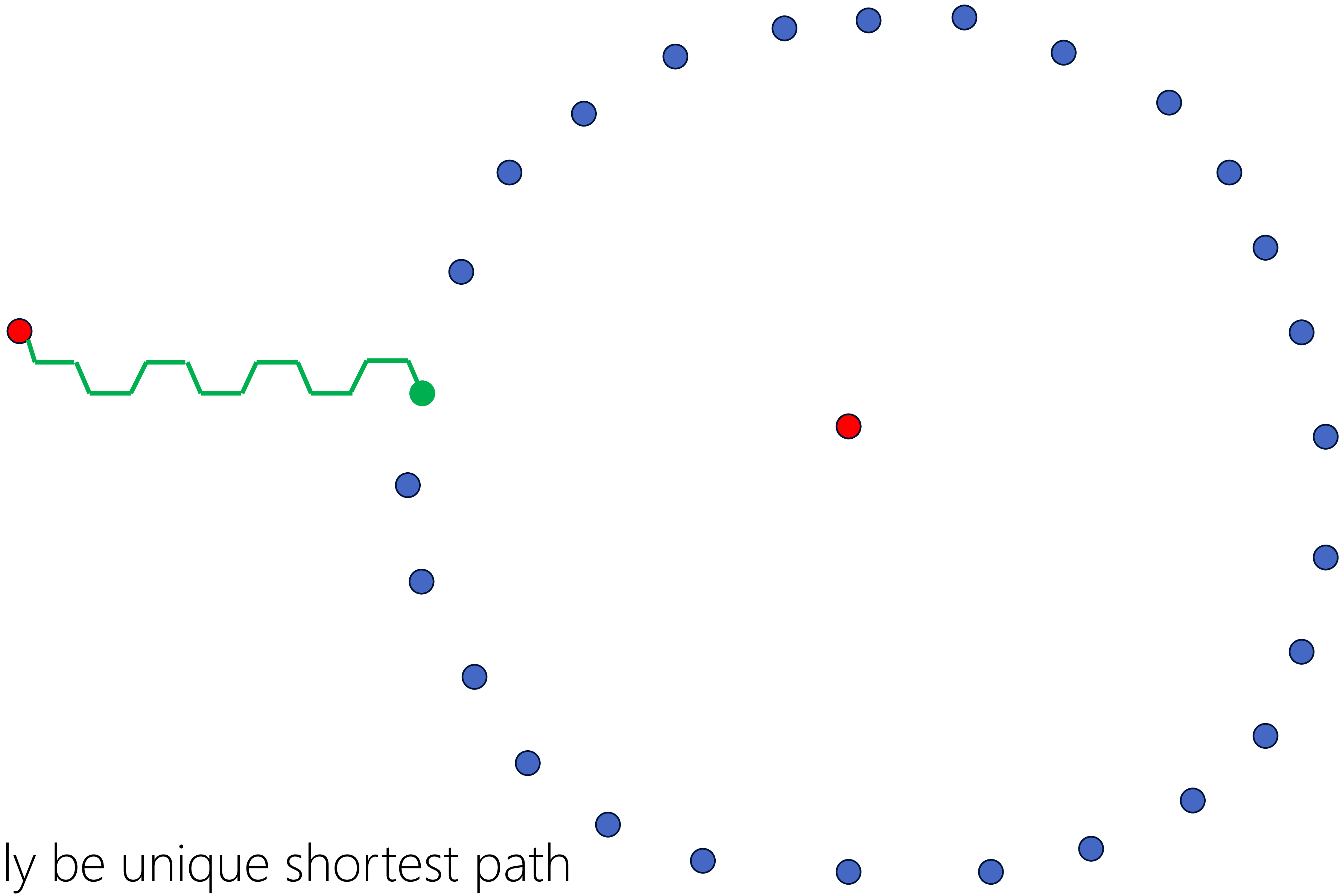
... discarding them until you find a collision

Claw algorithm



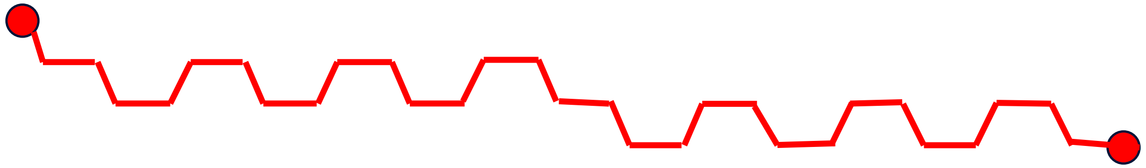
… discarding them until you find a collision

Claw algorithm



Collision will most likely be unique shortest path

Claw algorithm



This path describes secret isogeny $\phi : E \to E'$

Claw algorithm: theoretical 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

Claw algorithm: practical analysis

- In practice we do not have $O(p^{1/4})$ storage (combining the whole planet's storage capabilities

- **vOW algorithm:** meet-in-the-middle with a fixed memory bound

- **vOW runtime:** very close to $\frac{2.5}{m} \cdot \frac{p^{3/8}}{\sqrt{w}} \cdot t$ on average

  (m processors, w storage units, t time to compute isogeny)

- **Quantum in practice:** does not help!

SIDH/SIKE 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)

- **Theoretical best (known) attacks:** classical $O(p^{1/4})$ and quantum $O(p^{1/6})$

- **... but in practice:** vOW classical attack is best (quantum doesn't help)

Questions?