The state-of-the-art in supersingular isogenies: the SIKE protocol and its cryptanalysis

Craig Costello

Microsoft® Research

The state-of-the-art in supersingular isogenies: the SIKE protocol and its cryptanalysis

- First half
- Monday's tutorials help
- Some jargon/math
- Main takeaway:

  high-level view of how SIDH/SIKE works

- Second half
- No background needed
- The fun part
- Main takeaway:

  SIKE cryptanalysis has subtleties

Talk based on works mainly done here…

SIKE protocol

"Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" – Jao & De Feo. PQCRYPTO 2011.

"SIKE: Supersingular Isogeny Key Encapsulation" – Jao et al. Submission to the NIST PQC standardization effort. 2017.

its cryptanalysis

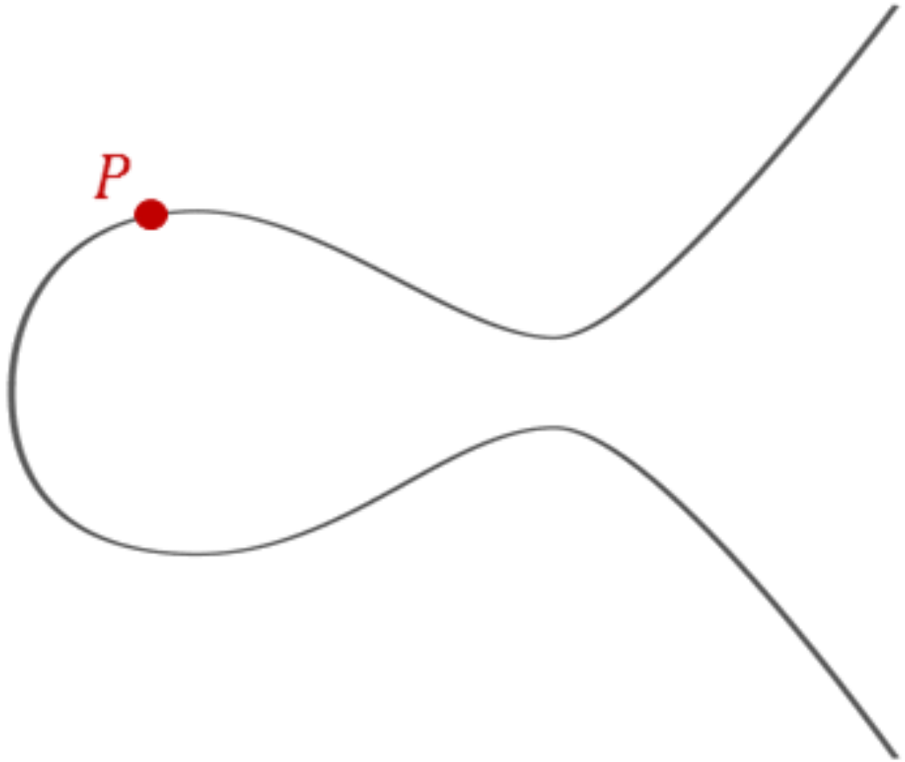
"On the cost of computing isogenies on supersingular elliptic curves" – Adj, Cervantes-Vazquez, Chi-Dominguez, Menezes, Rodriguez-Henriquez. SAC 2018.

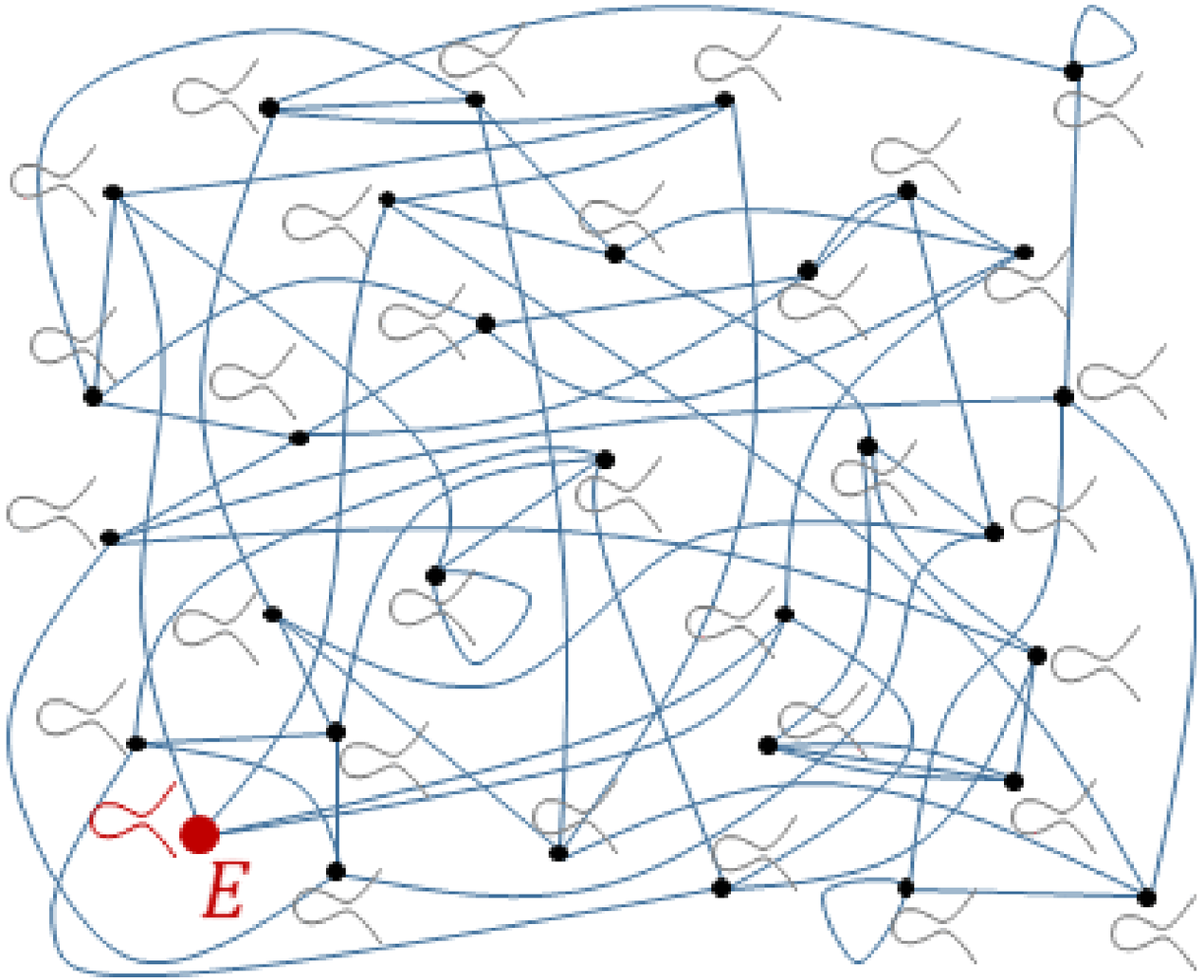
"Quantum cryptanalysis in the RAM model: claw-finding attacks on SIKE" – Jaques and Schanck. CRYPTO 2019.

"Improved classical cryptanalysis of the computational supersingular isogeny problem" – C-Longa-Naehrig-Renes-Virdia. Preprint.

SIKE protocol

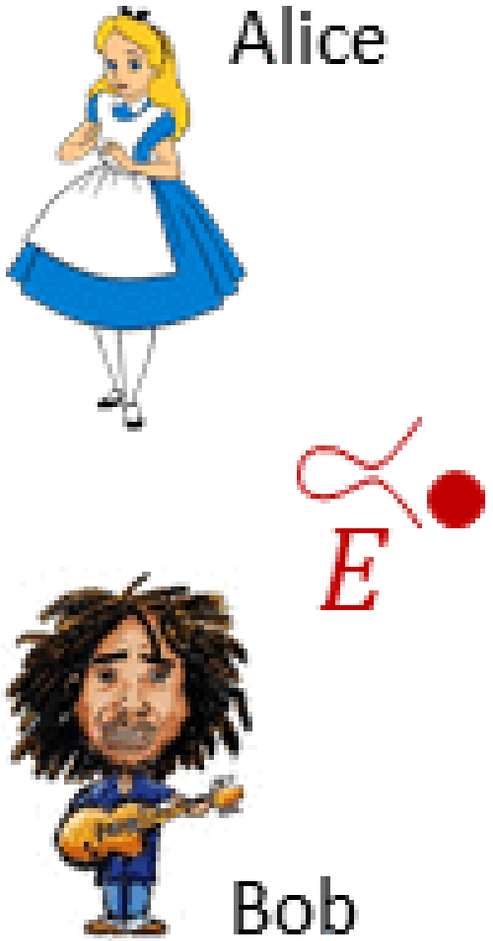
ECC vs. post-quantum ECC





W. Castryck (GIF): https://www.esat.kuleuven.be/cosic/?p=7404

Alice 2^e-isogenies, Bob 3^f-isogenies



W. Castryck (GIF): https://www.esat.kuleuven.be/cosic/?p=7404

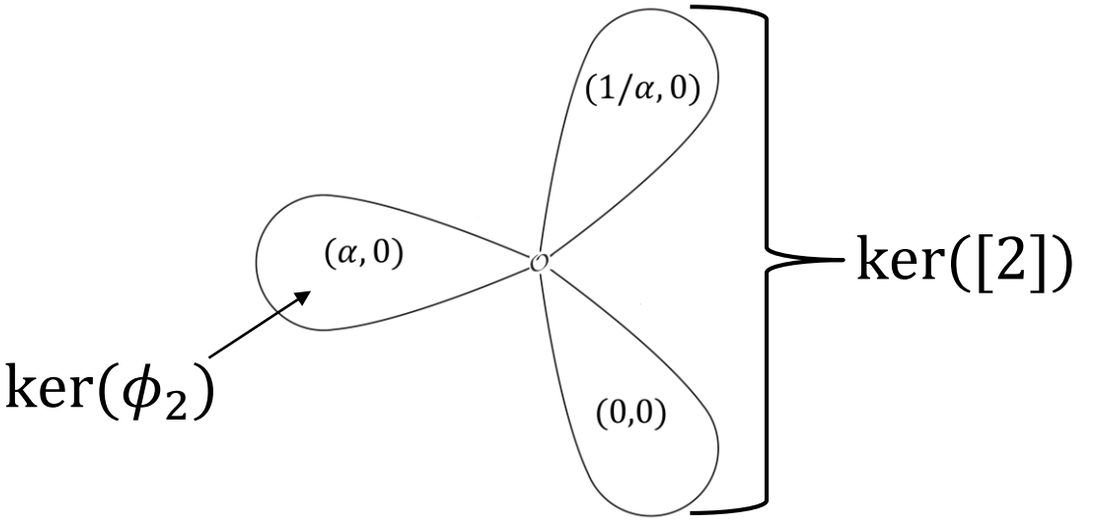
Montgomery curves everywhere!

$$E:\ y^2 = x^3 + Ax^2 + x \qquad E':\ y^2 = x^3 + A'x^2 + x$$

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

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

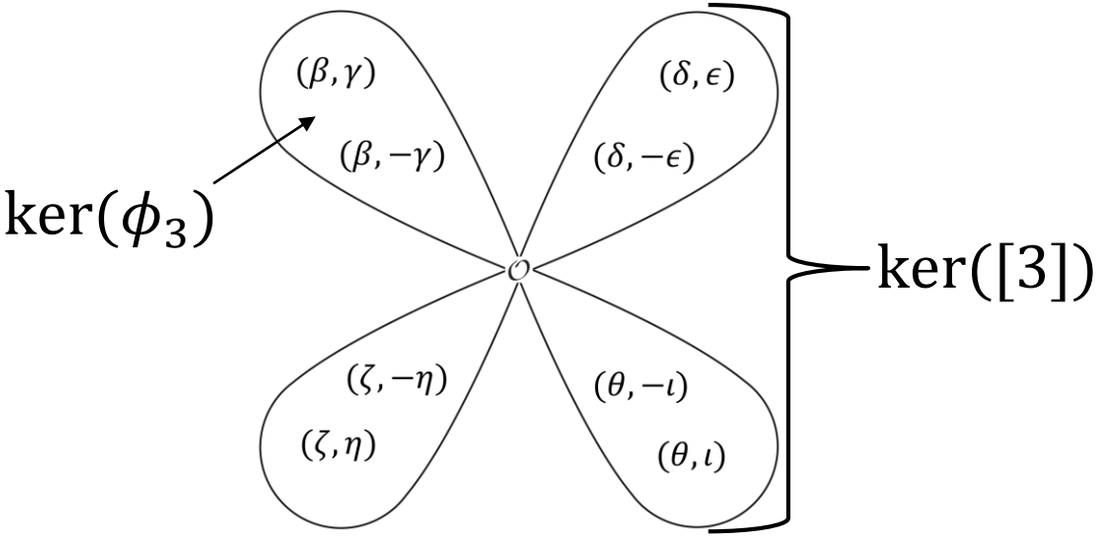
$$A' = 2\left(1 - 2\alpha^2\right)$$



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

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

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

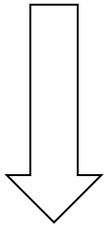


$\mathbb{P}^1$ everywhere!

$$\phi_2 : E \to E'$$

Pushing points through ϕ_2

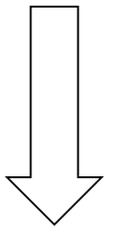
$$x \mapsto x \cdot \left(\frac{\alpha x - 1}{x - \alpha}\right)$$



$$(X:Z) \mapsto \left(X(X_\alpha X - Z_\alpha Z) : Z(Z_\alpha X - X_\alpha Z)\right)$$

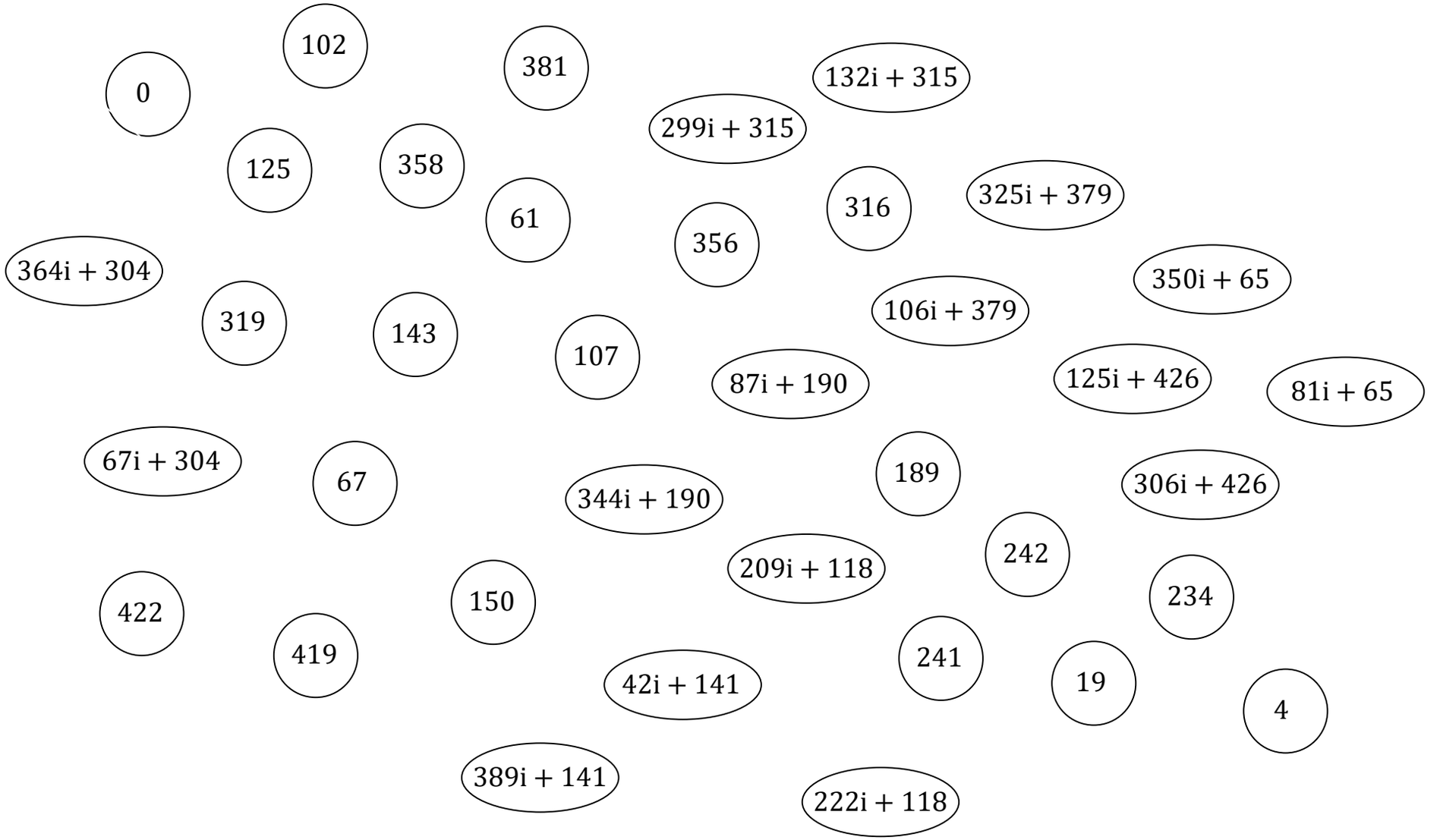
Pushing curves through ϕ_2

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



$$(A':1) = \left(2\left(Z_\alpha^2 - 2X_\alpha^2\right) : Z_\alpha^2\right)$$

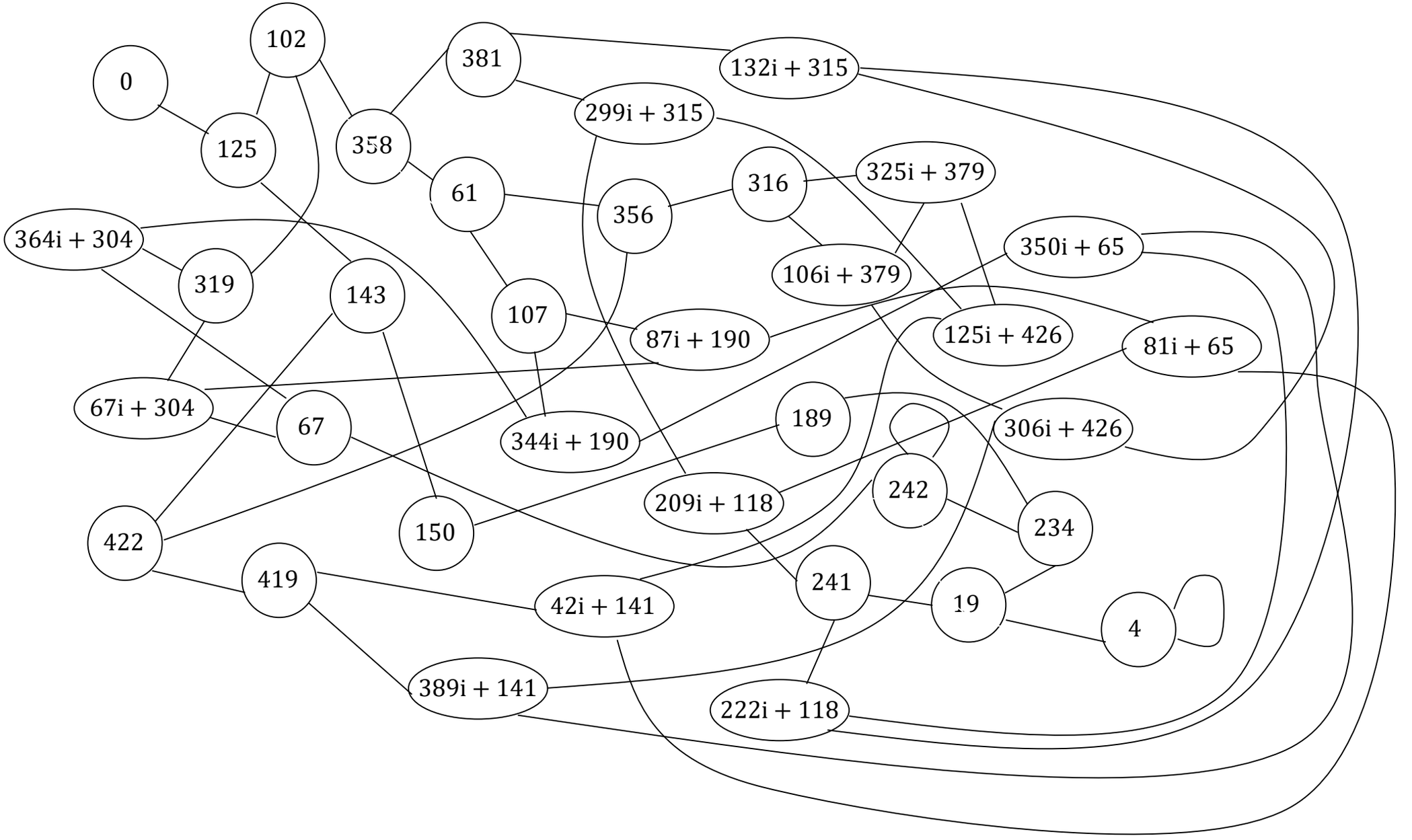
E.g. supersingular isogeny graph – the nodes



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

Alice's graph

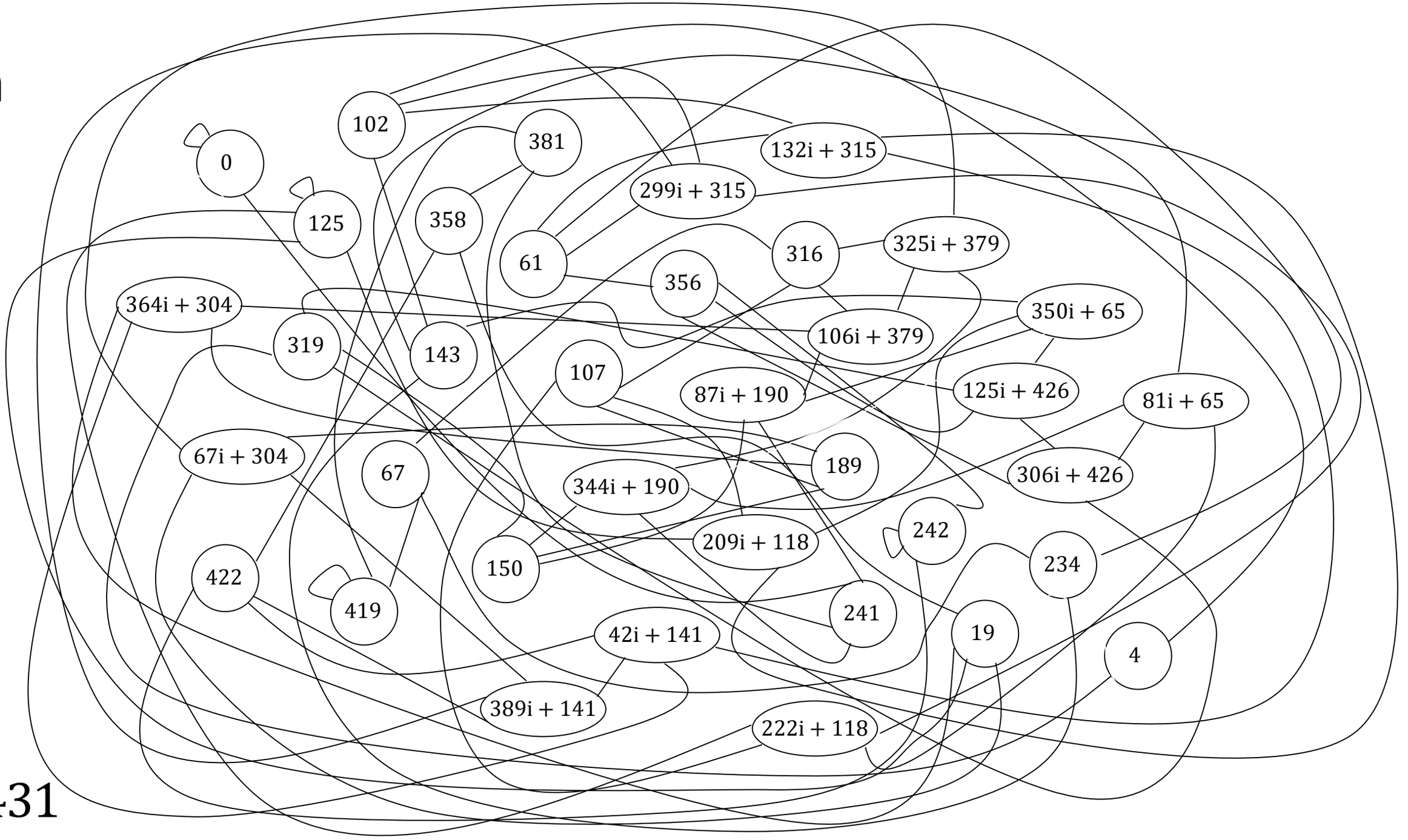
$\ell = 2$



$p := 431$

Bob's graph

$\ell = 3$



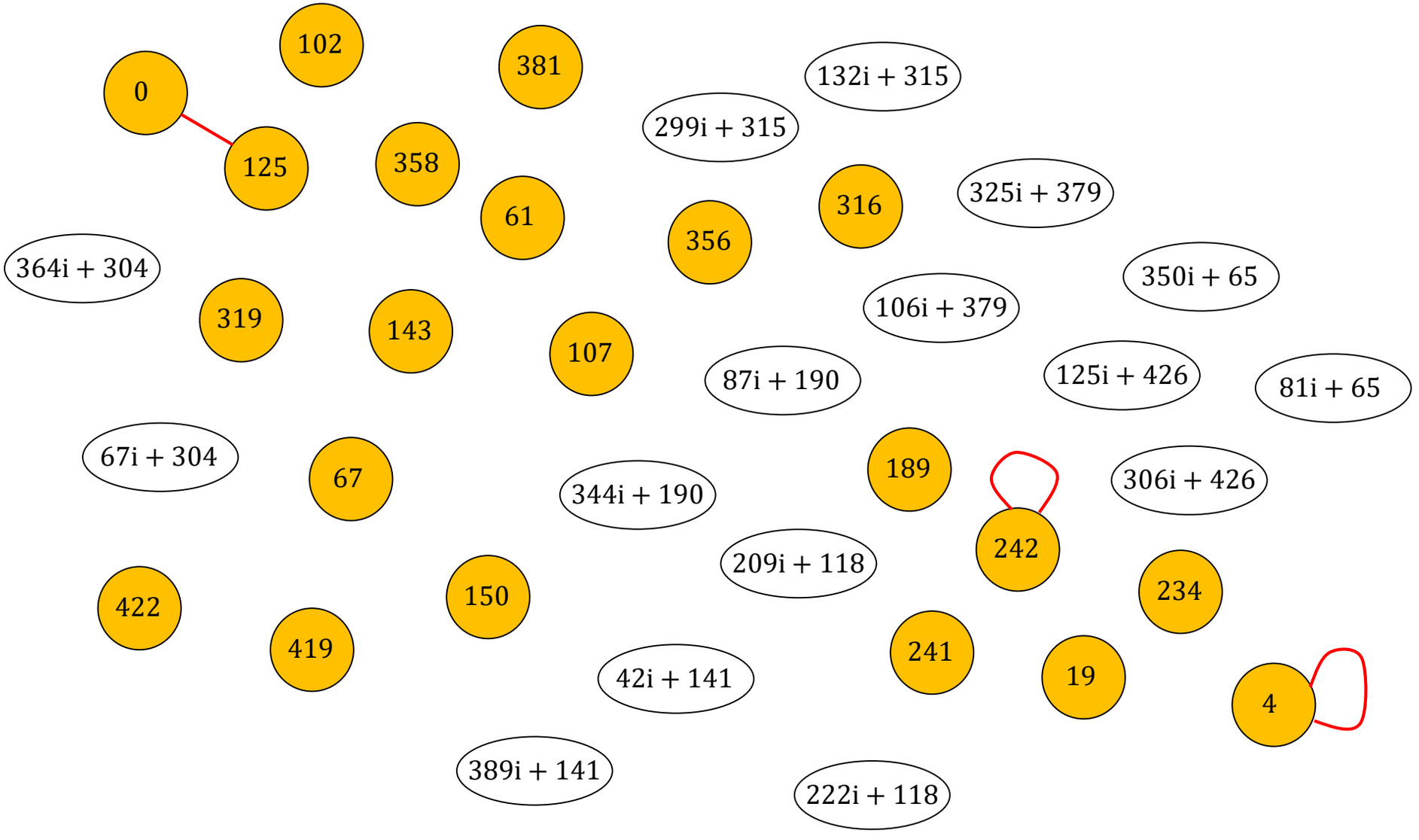
$p := 431$

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

$p := 431$

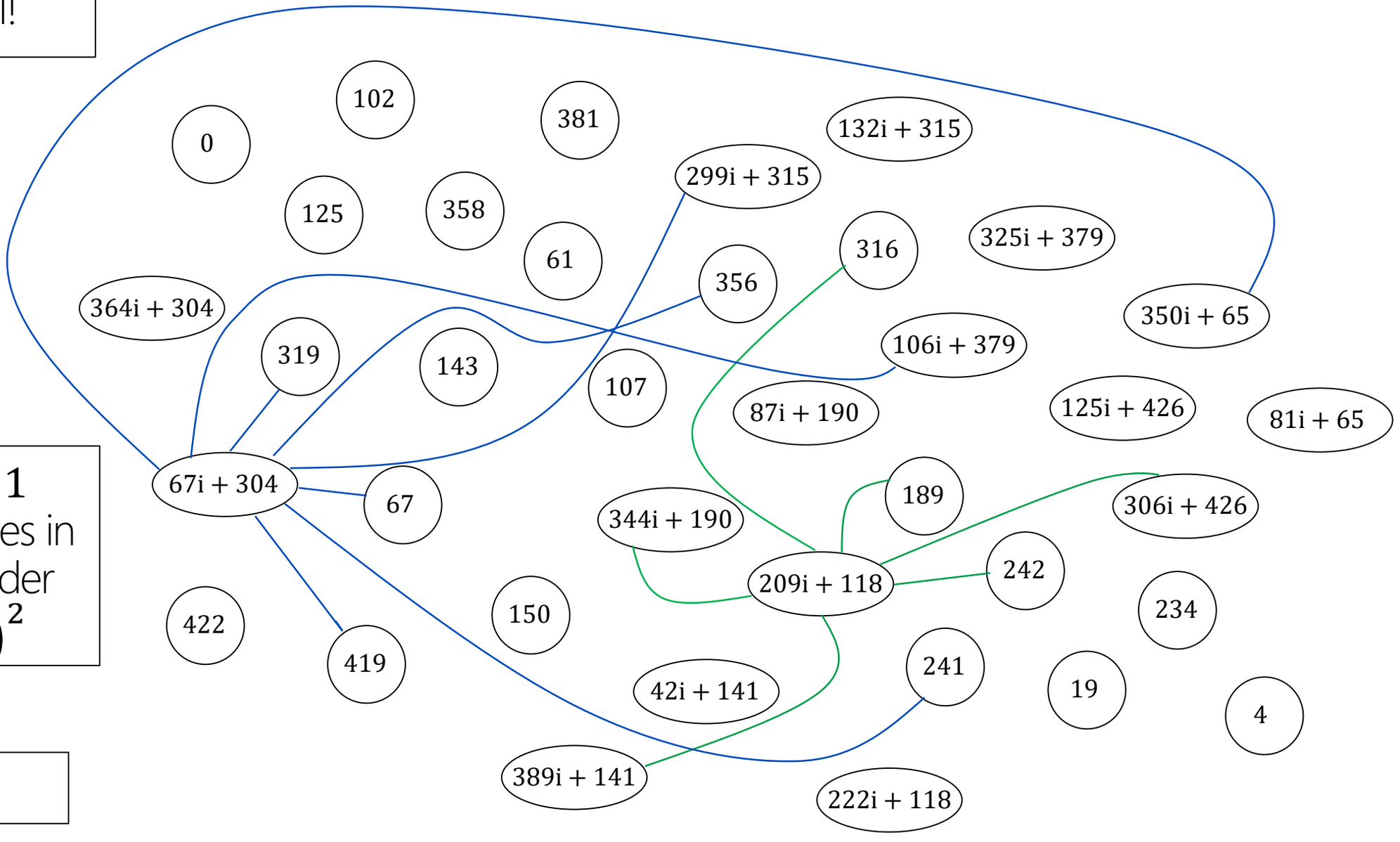


Higher ℓ ?

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

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

$$A = 329i + 423$$

$$j = 87i + 190$$

$$\#E_0(\mathbb{F}_{p^2}) = (p+1)^2 = \left(2^4 3^3\right)^2$$

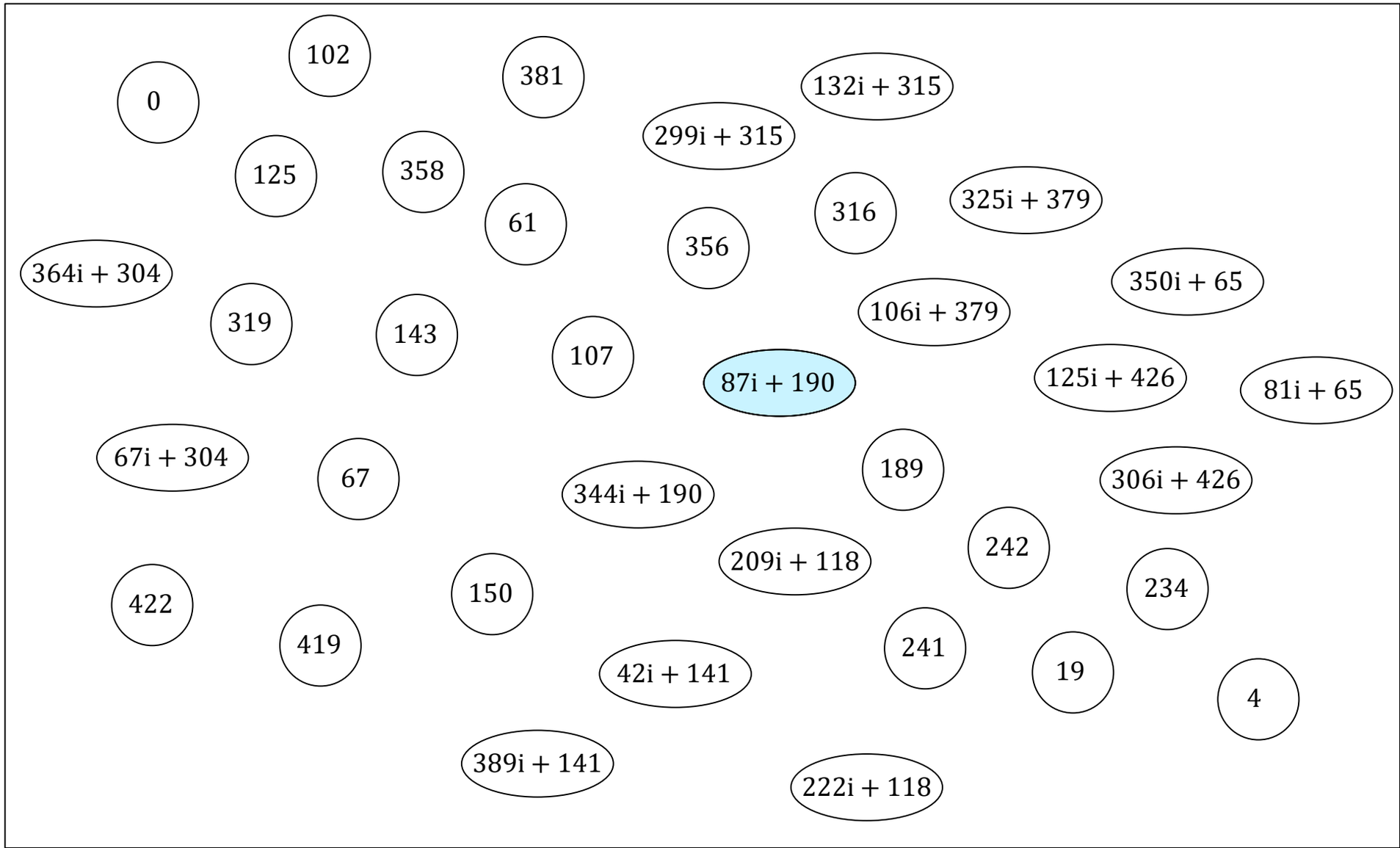
$$E \cong\ \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$$

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

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

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

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

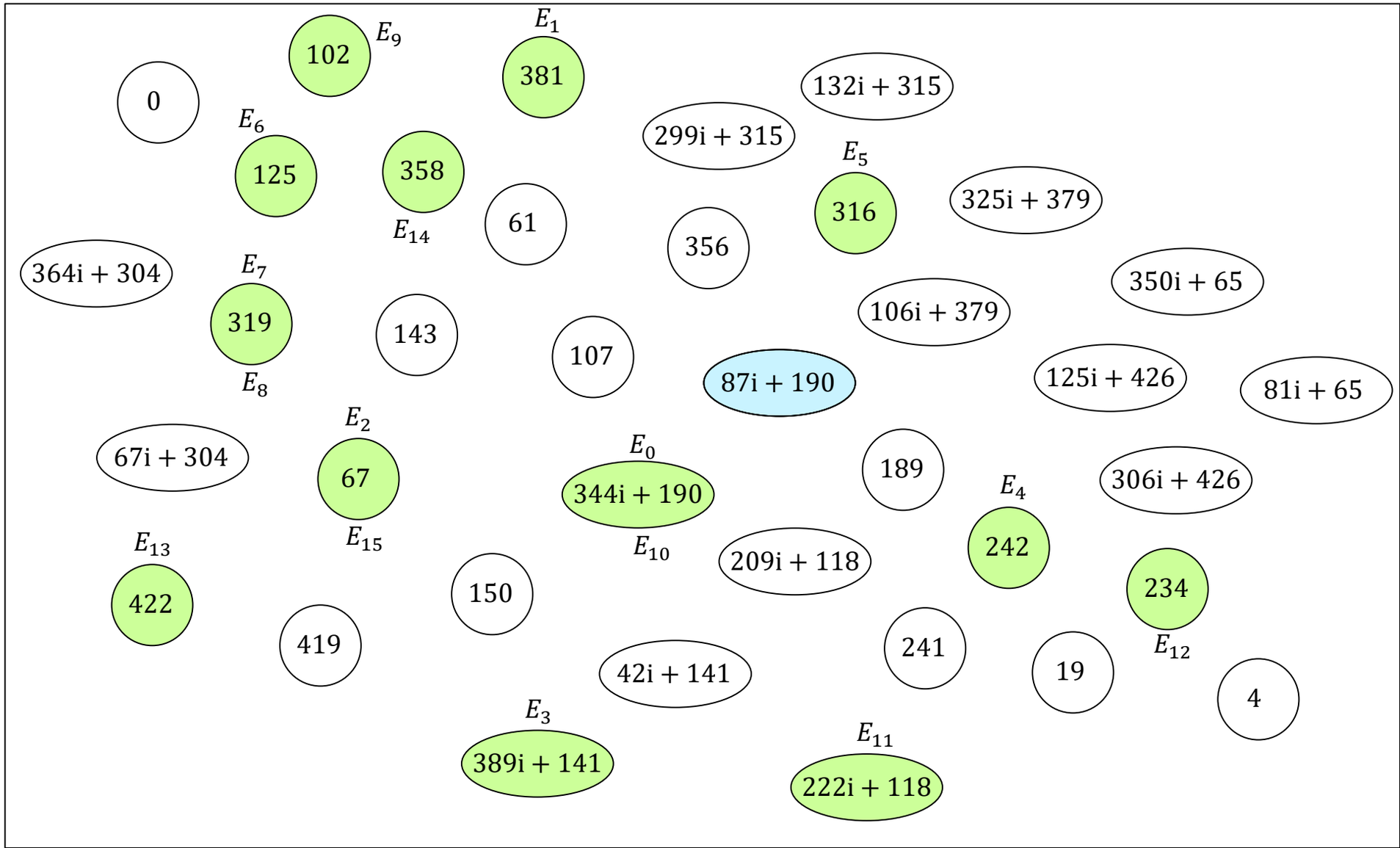


Alice destinations: possible* 2^4-isogenies

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

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

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

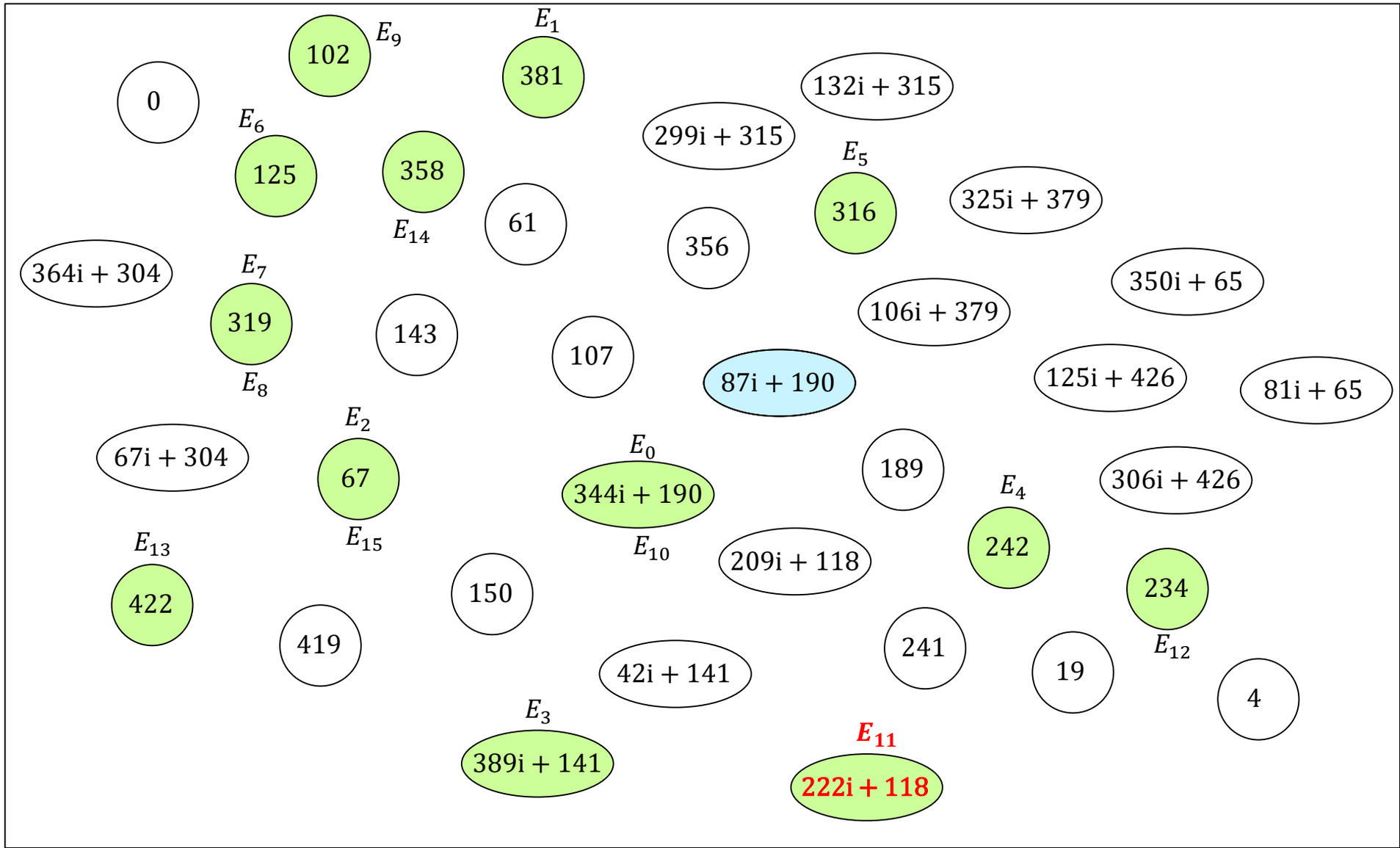


Alice destinations: possible* 2^4-isogenies

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

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

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

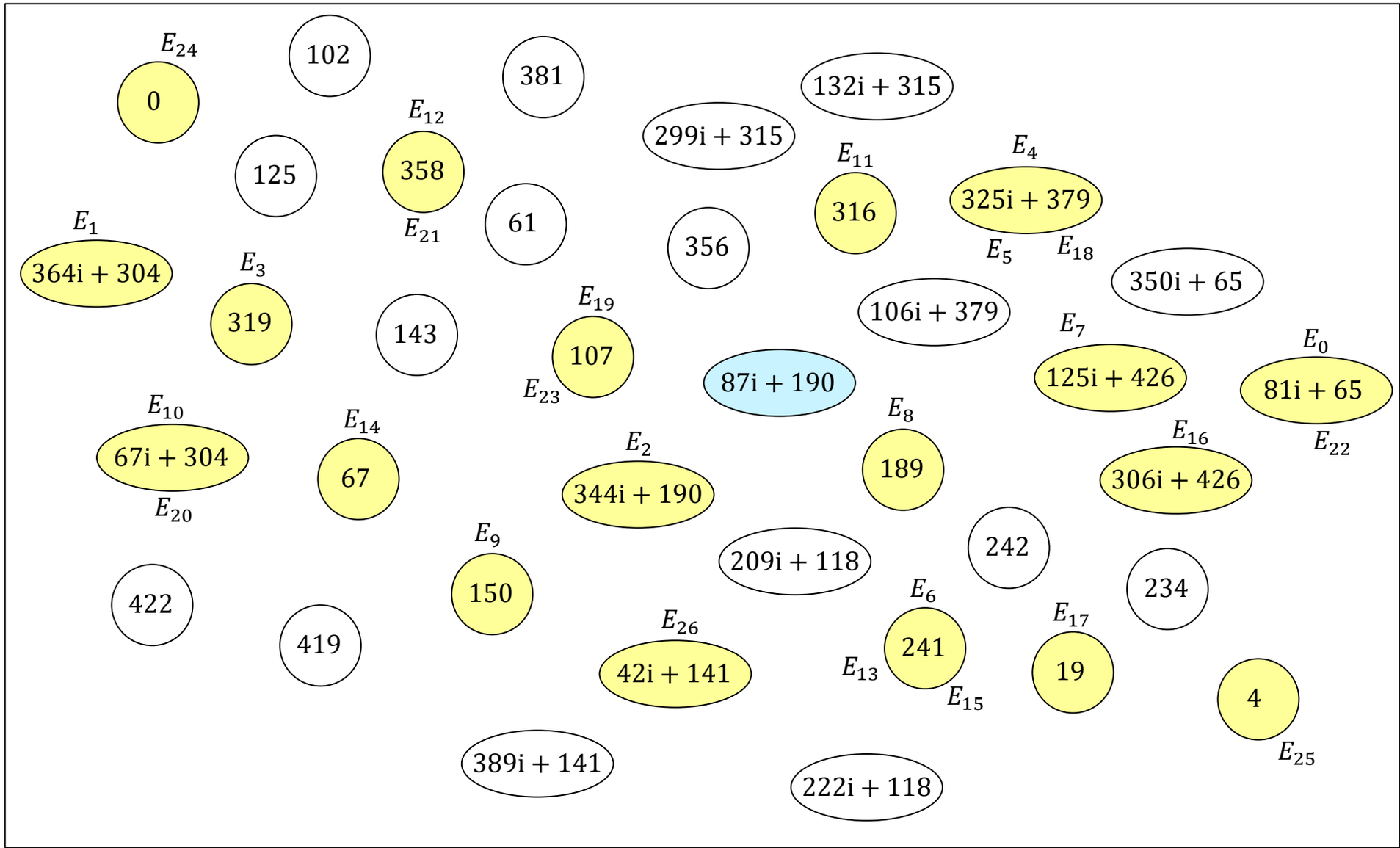


Bob destinations: possible* 3^3-isogenies

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

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

$$E_k := E/\langle S_k \rangle$$

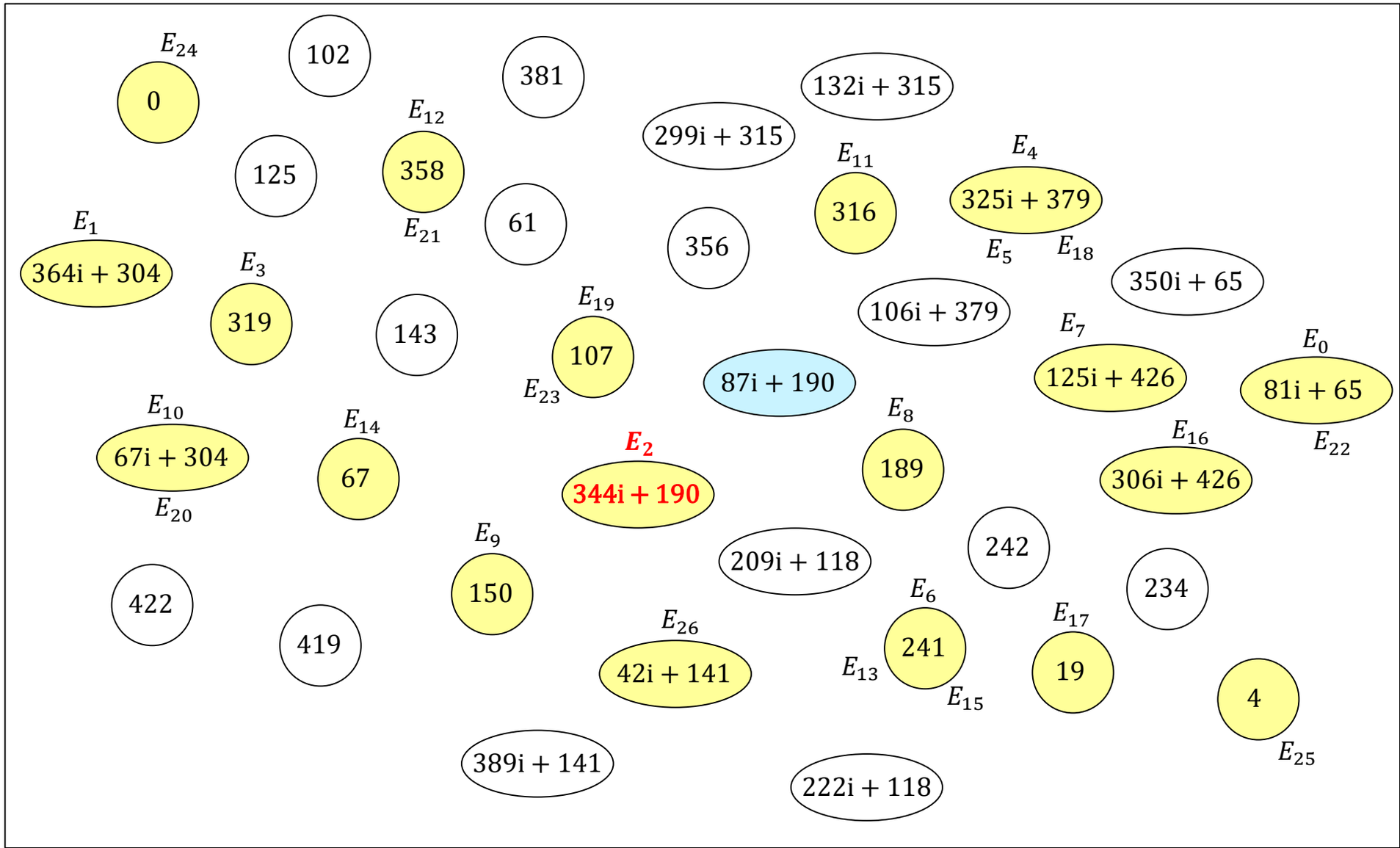


Bob destinations: possible* 3^3-isogenies

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

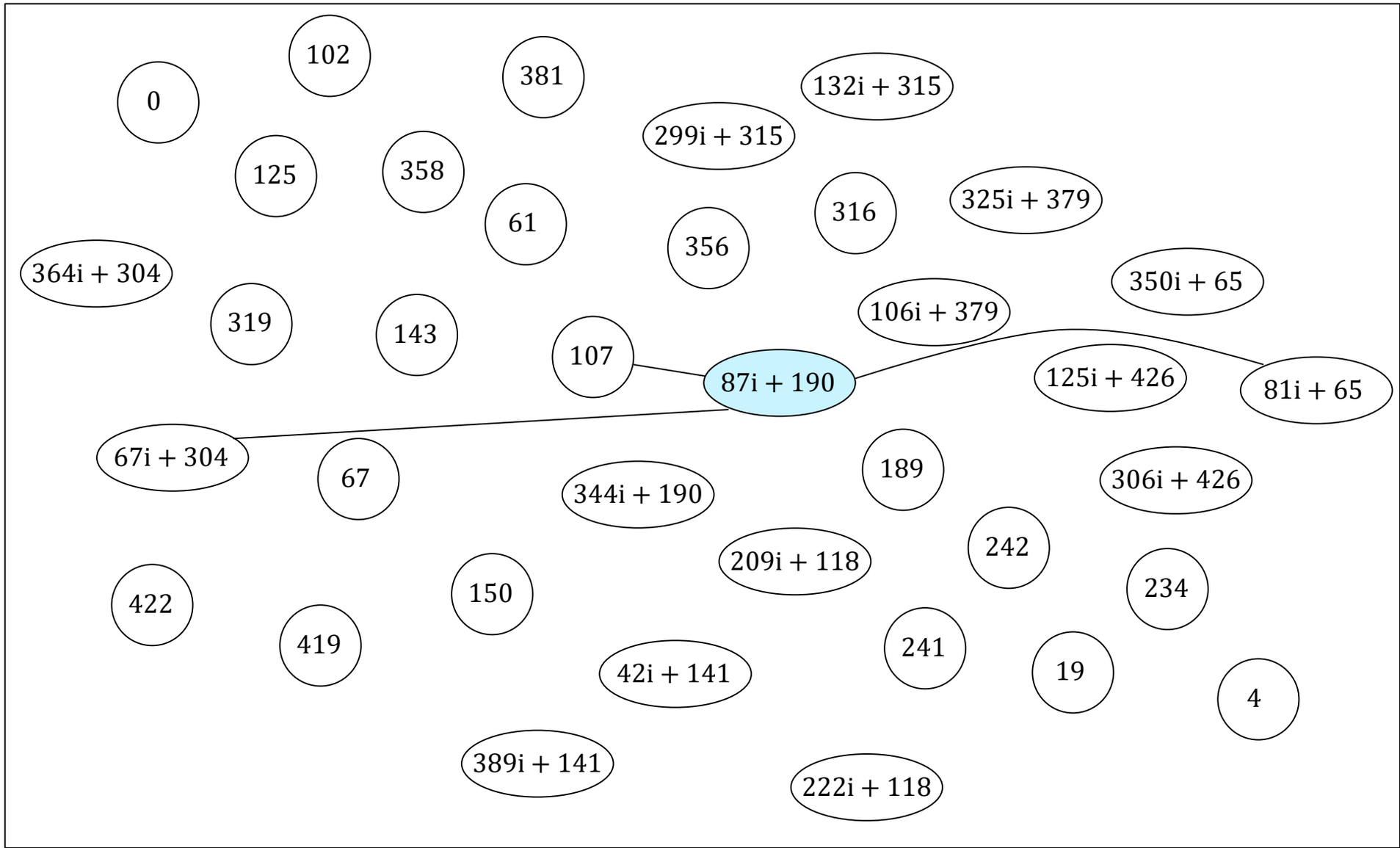
k_B	$S_{k_B} = P_B + [k_B]Q_B$
0	$(358i + 275, 410i + 104)$
1	$(150i + 184, 106i + 293)$
2	$\mathbf{(122i + 309, 291i + 374)}$
3	$(25i + 70, 254i + 66)$
4	$(47i + 223, 301i + 322)$
⋮	⋮
⋮	⋮
⋮	⋮
21	$(200i + 351, 141i + 361)$
22	$(35i + 417, 183i + 351)$
23	$(327i + 55, 230i + 238)$
24	$(326i + 56, 334i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

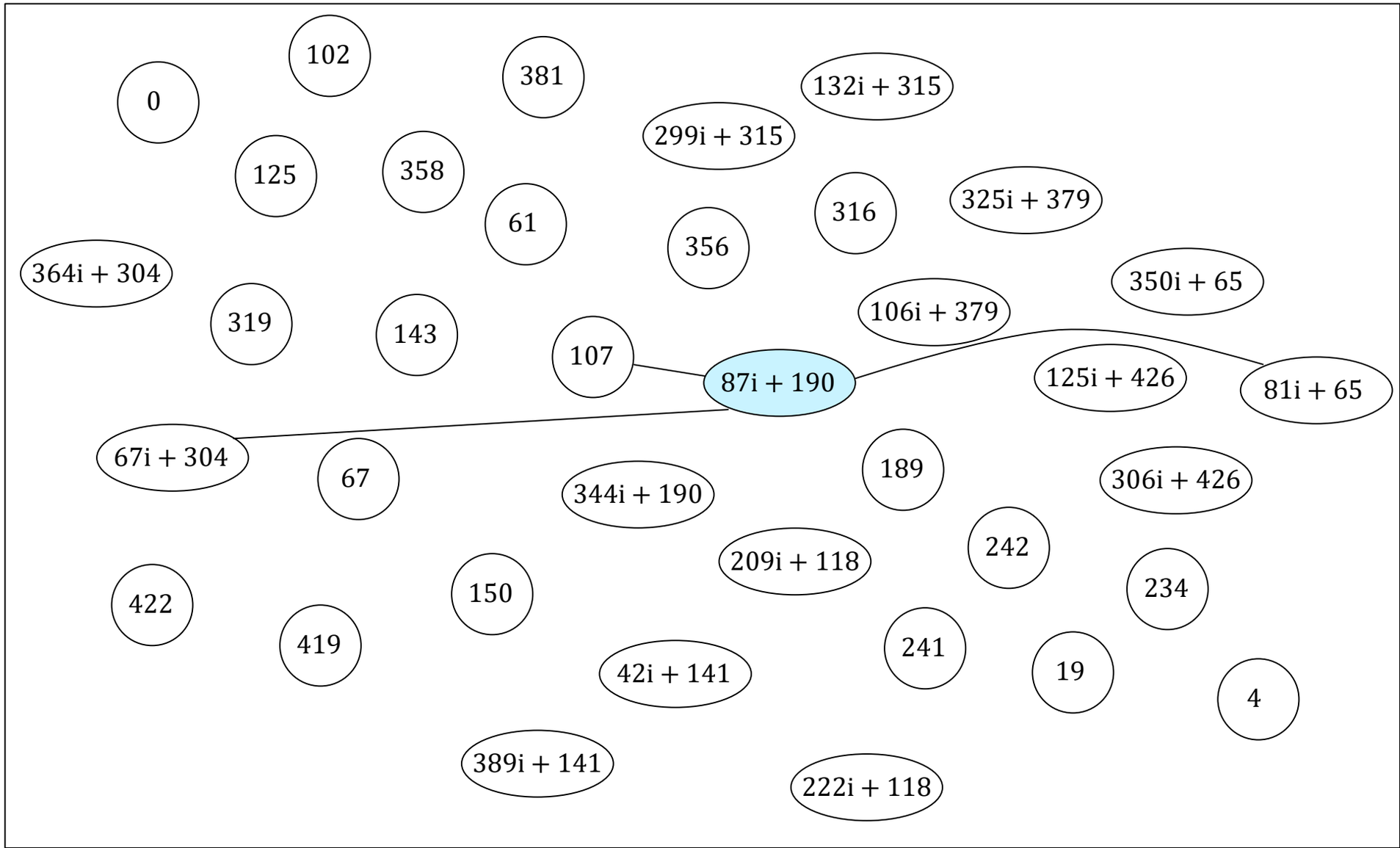
$S = (271i + 79\ ,\ 153i + 430)$

[2]

[2]

[2]

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



Alice's key generation

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

[2]

[2]

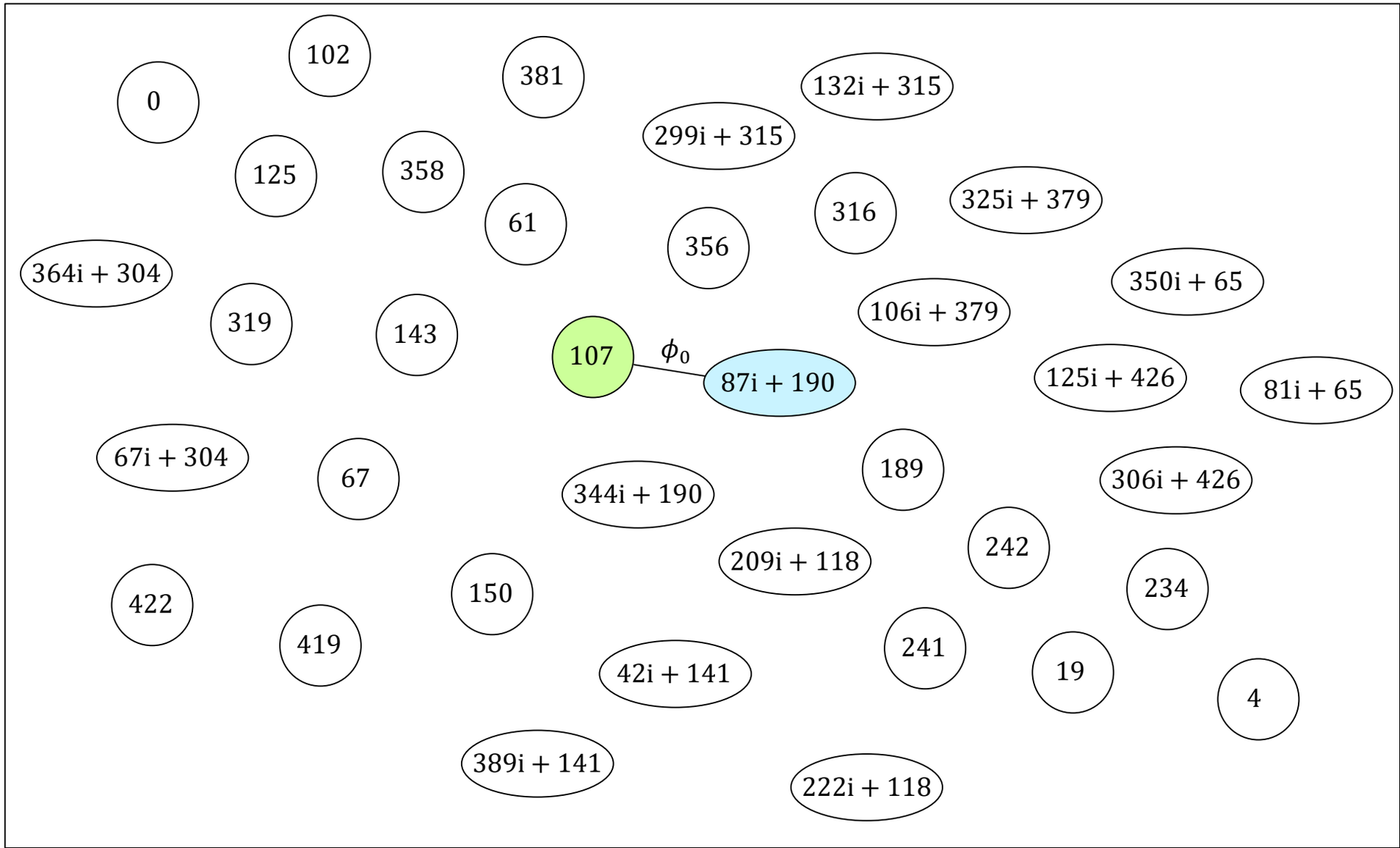
[2]

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

$$\phi_0 : E_0 \to E_1$$

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

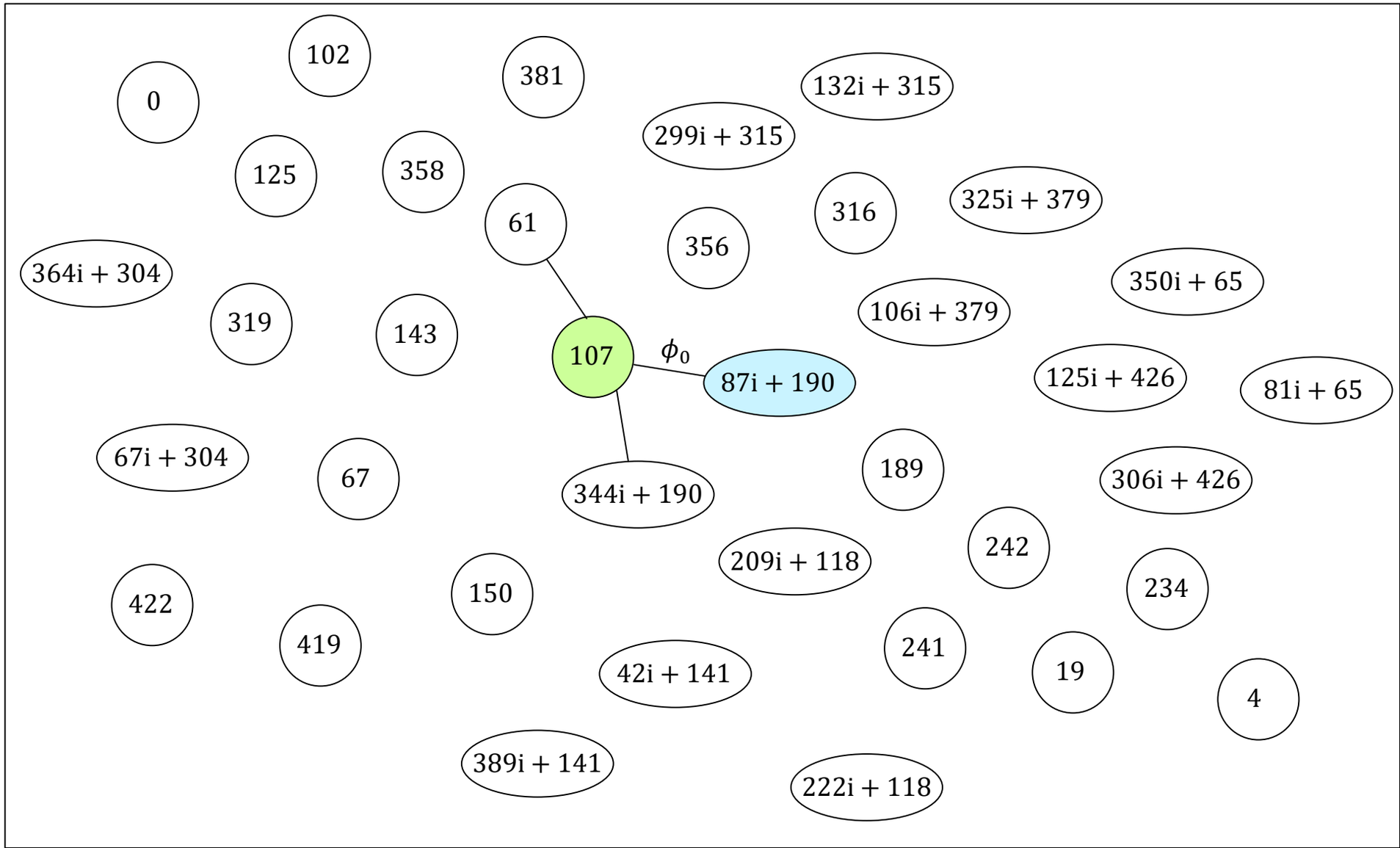
$$j(E_1) = 107$$



Alice's key generation

ϕ_0

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



Alice's key generation

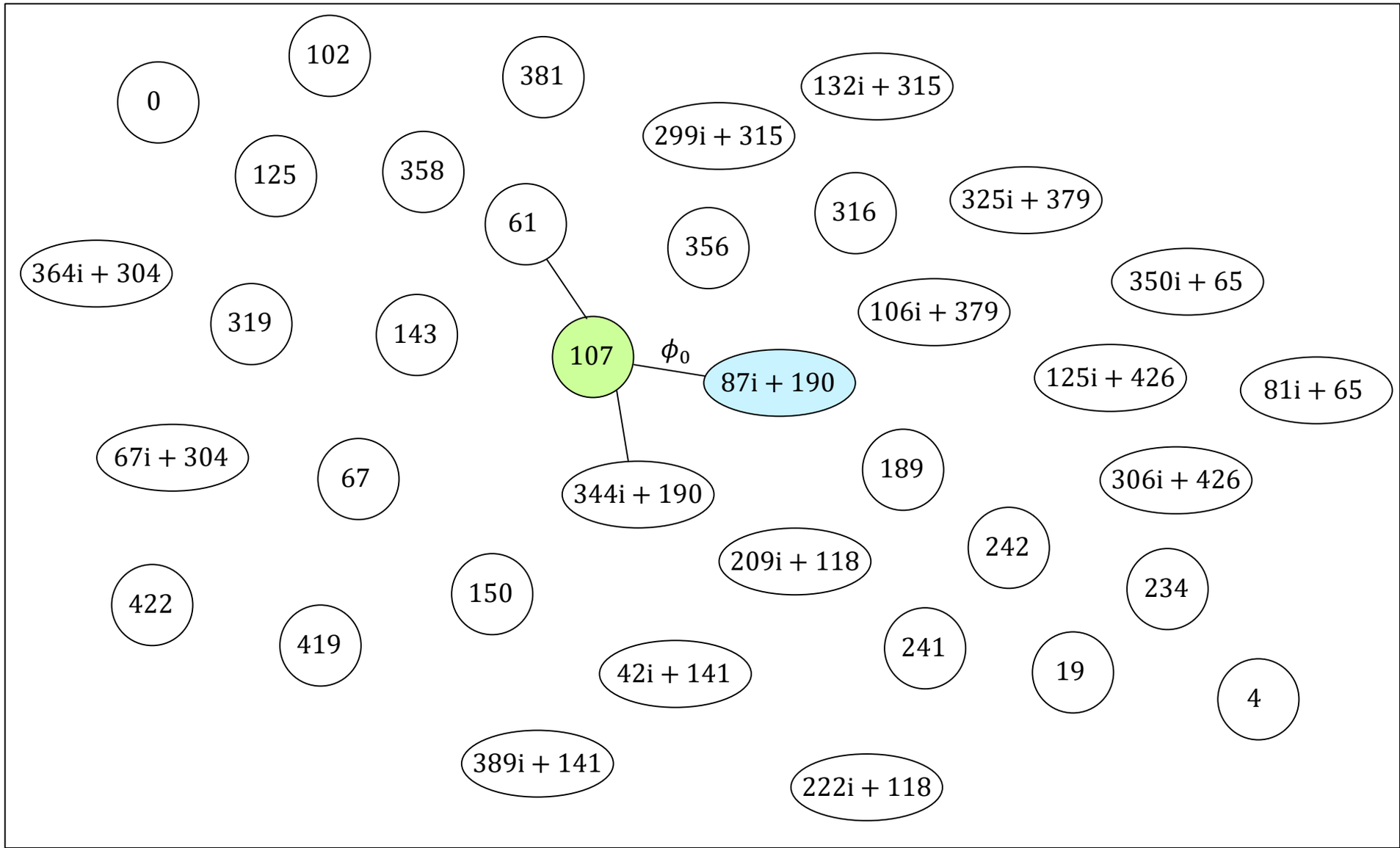
ϕ_0

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

[2]

[2]

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



Alice's key generation

ϕ_0

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

[2]

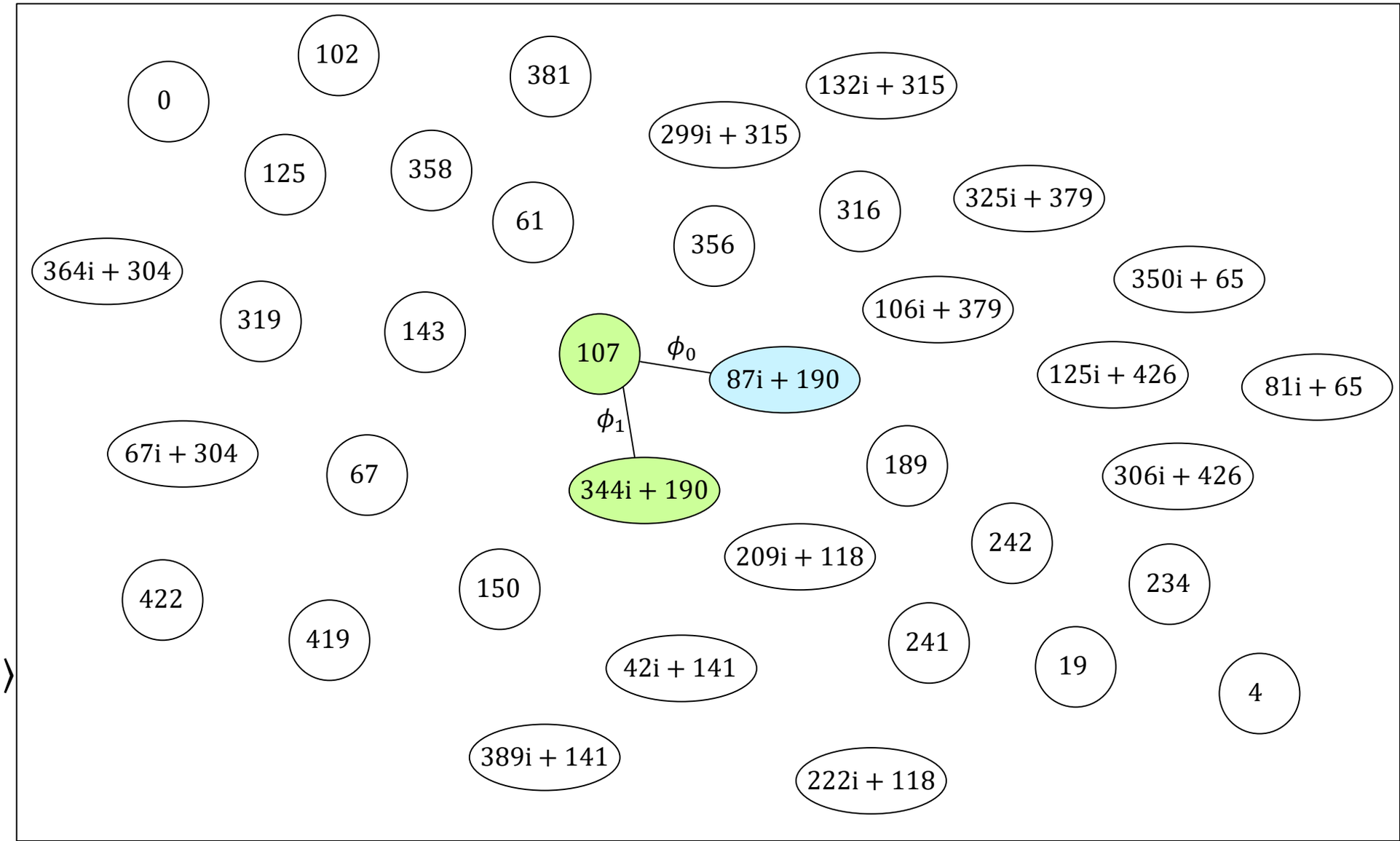
[2]

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

$$\phi_1 : E_1 \to E_2$$

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

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

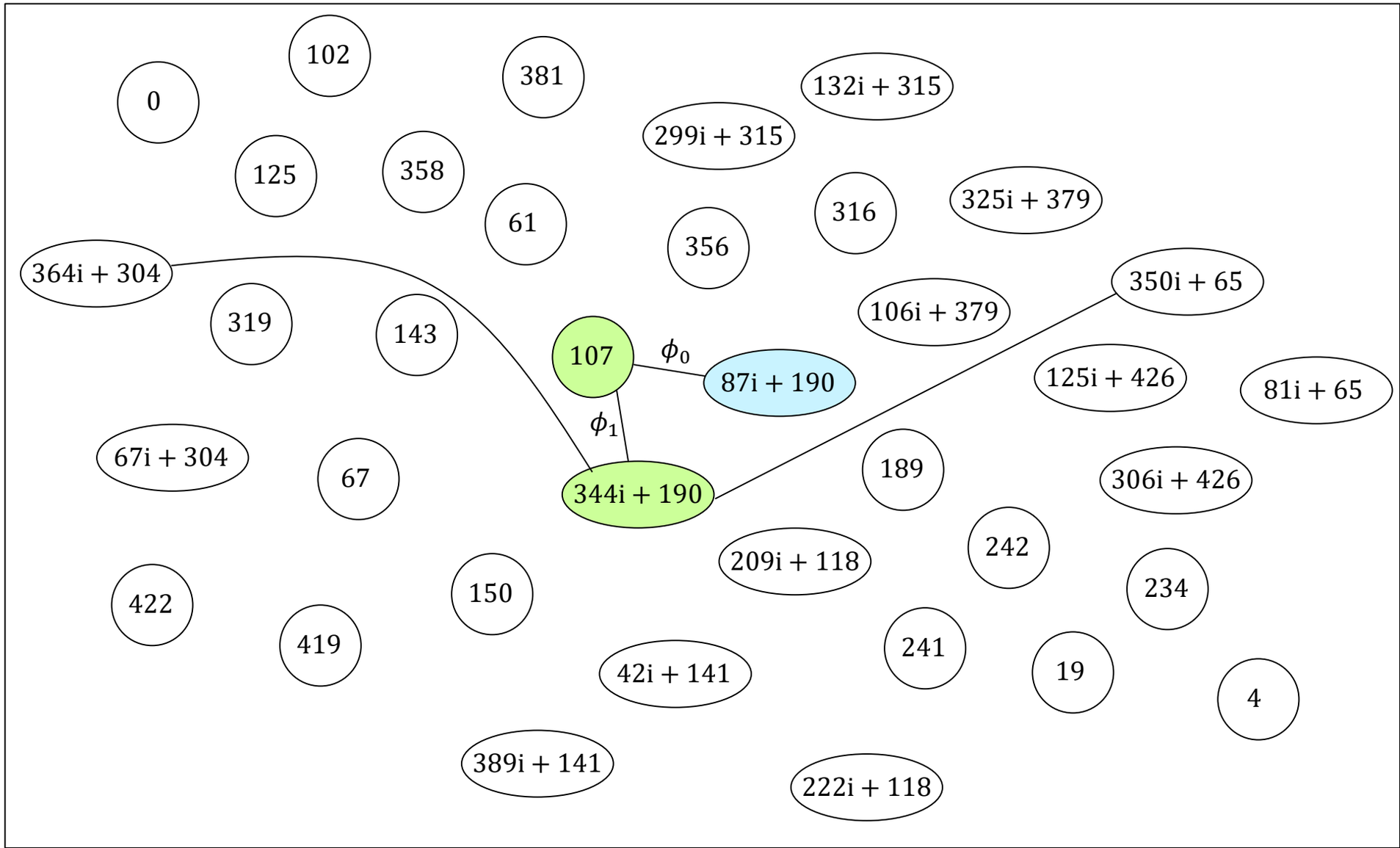


Alice's key generation

ϕ_0

ϕ_1

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



Alice's key generation

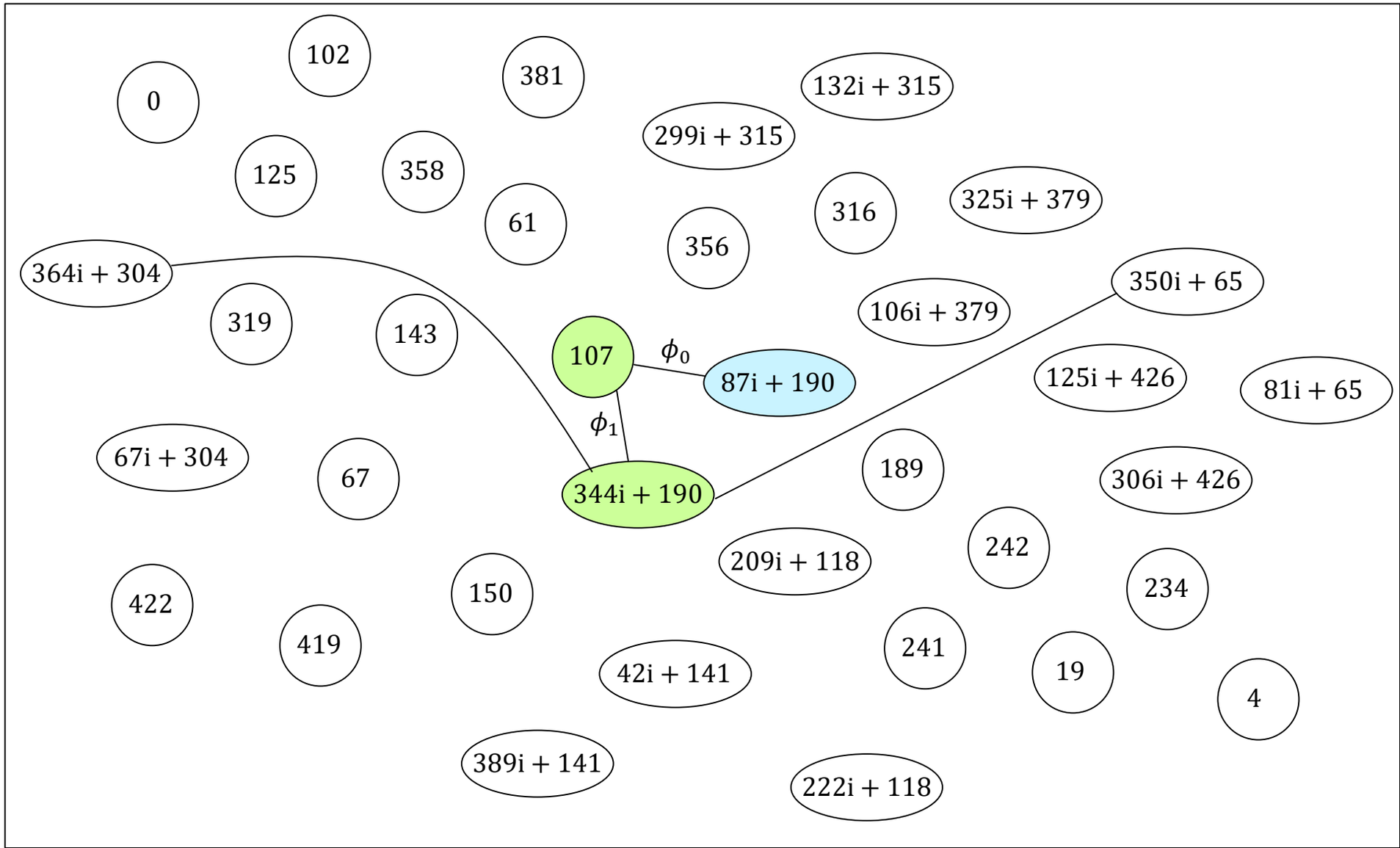
ϕ_0

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

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

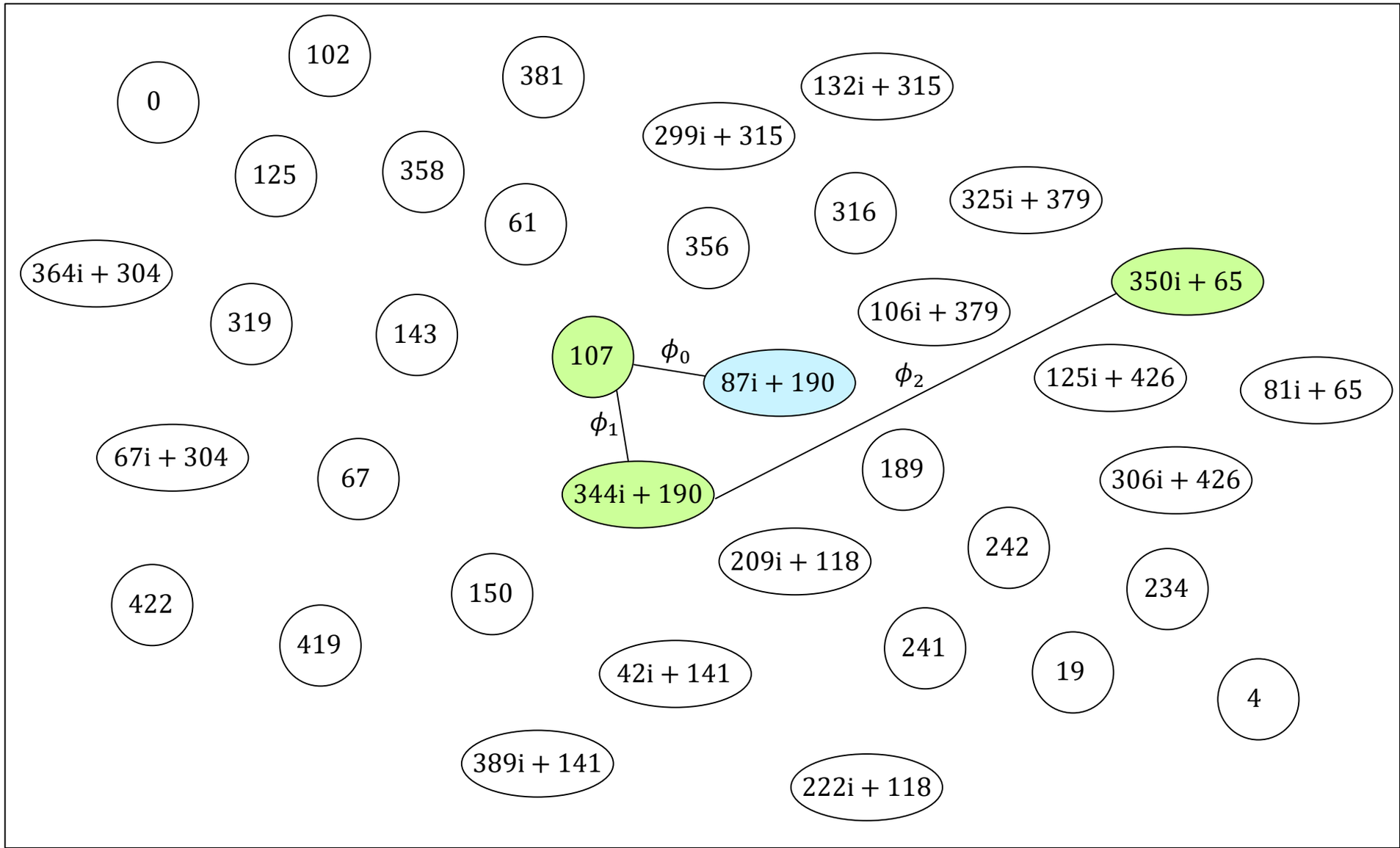
[2]

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

$$\phi_2 : E_2 \to E_3$$

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

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



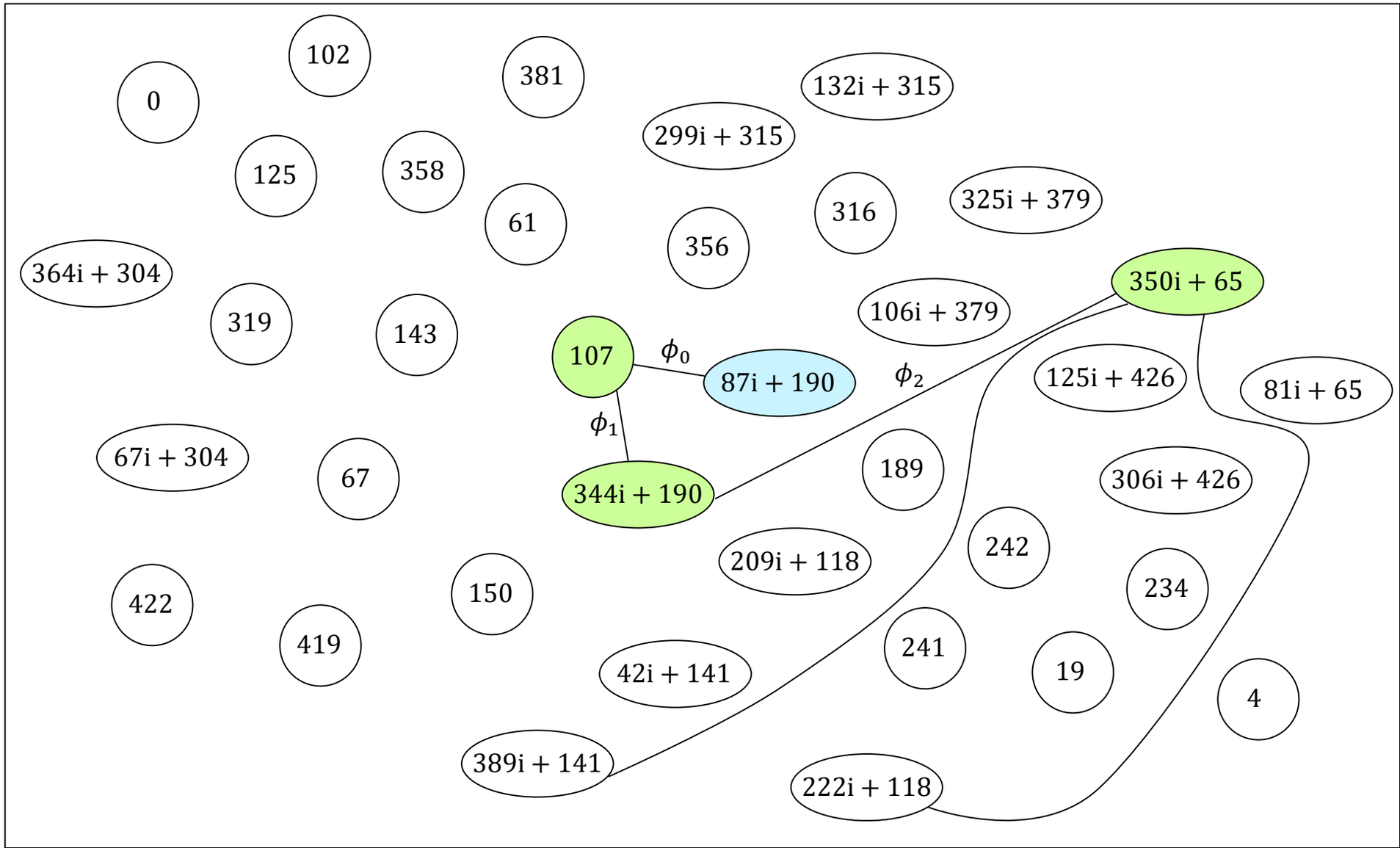
Alice's key generation

ϕ_0

ϕ_1

ϕ_2

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



Alice's key generation

ϕ_0

ϕ_1

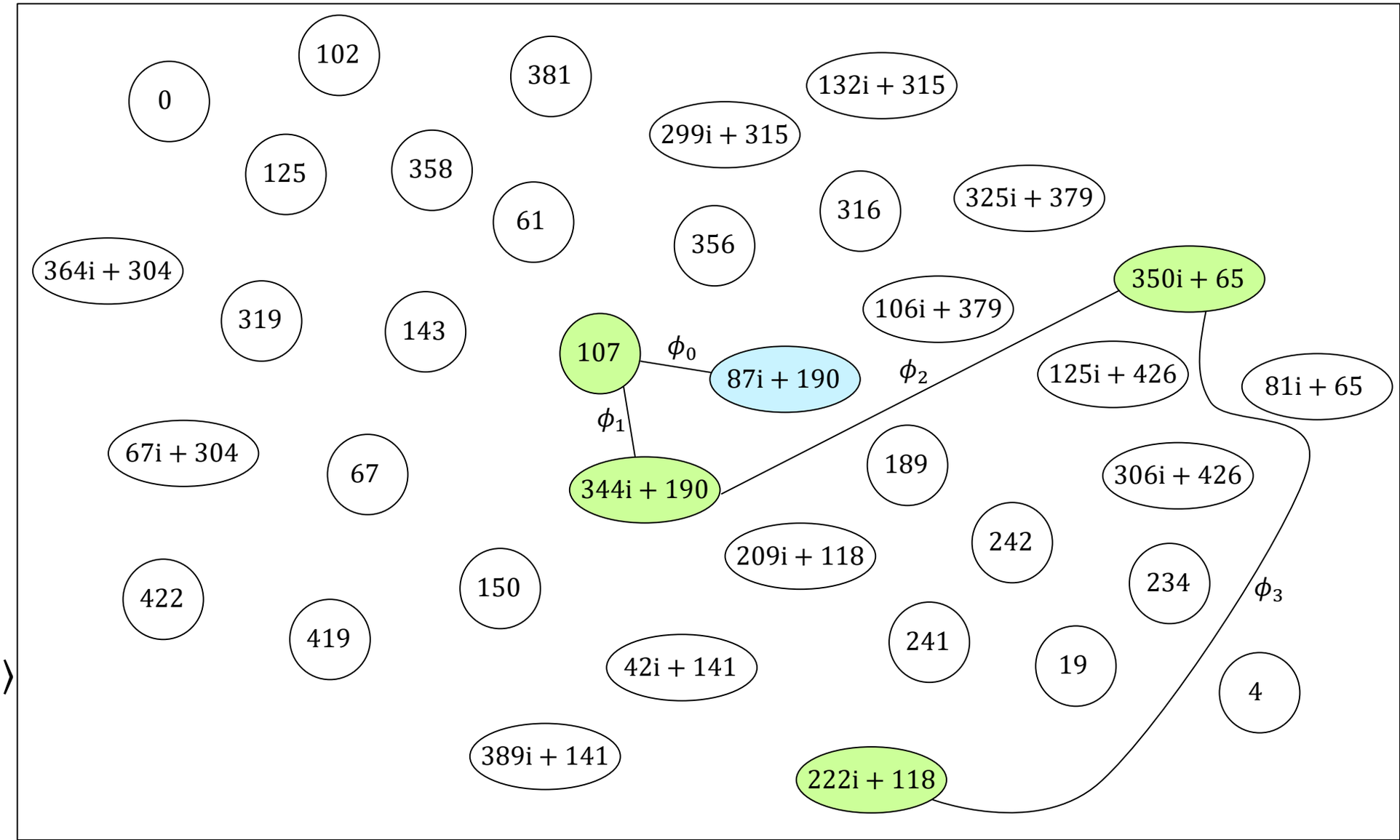
ϕ_2

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

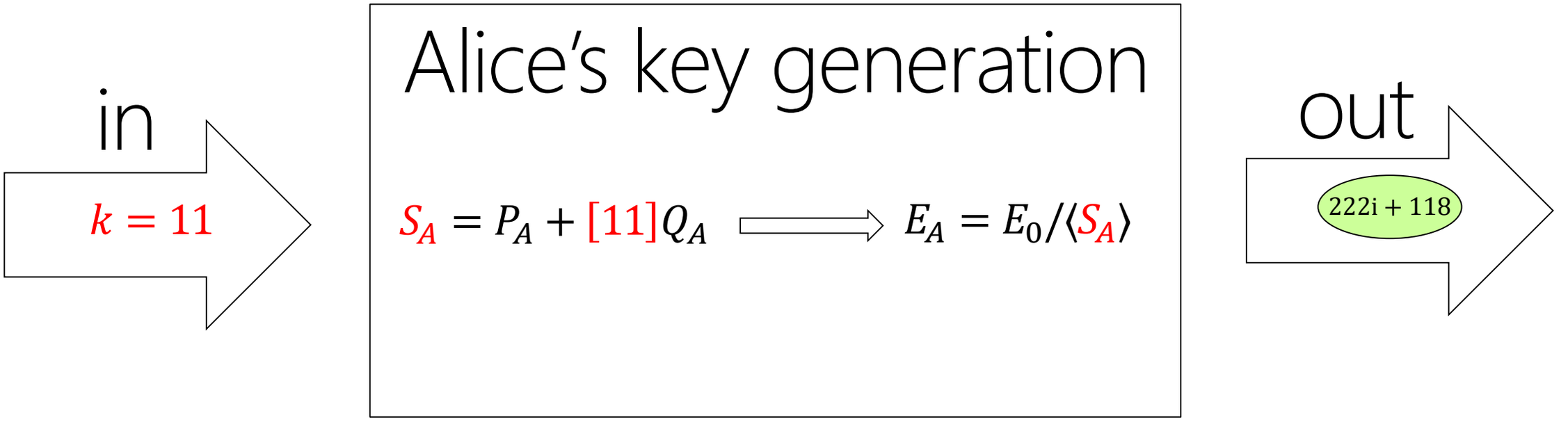
$\phi_3 : E_3 \to E_4$

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

$j(E_4) = 222i + 118$

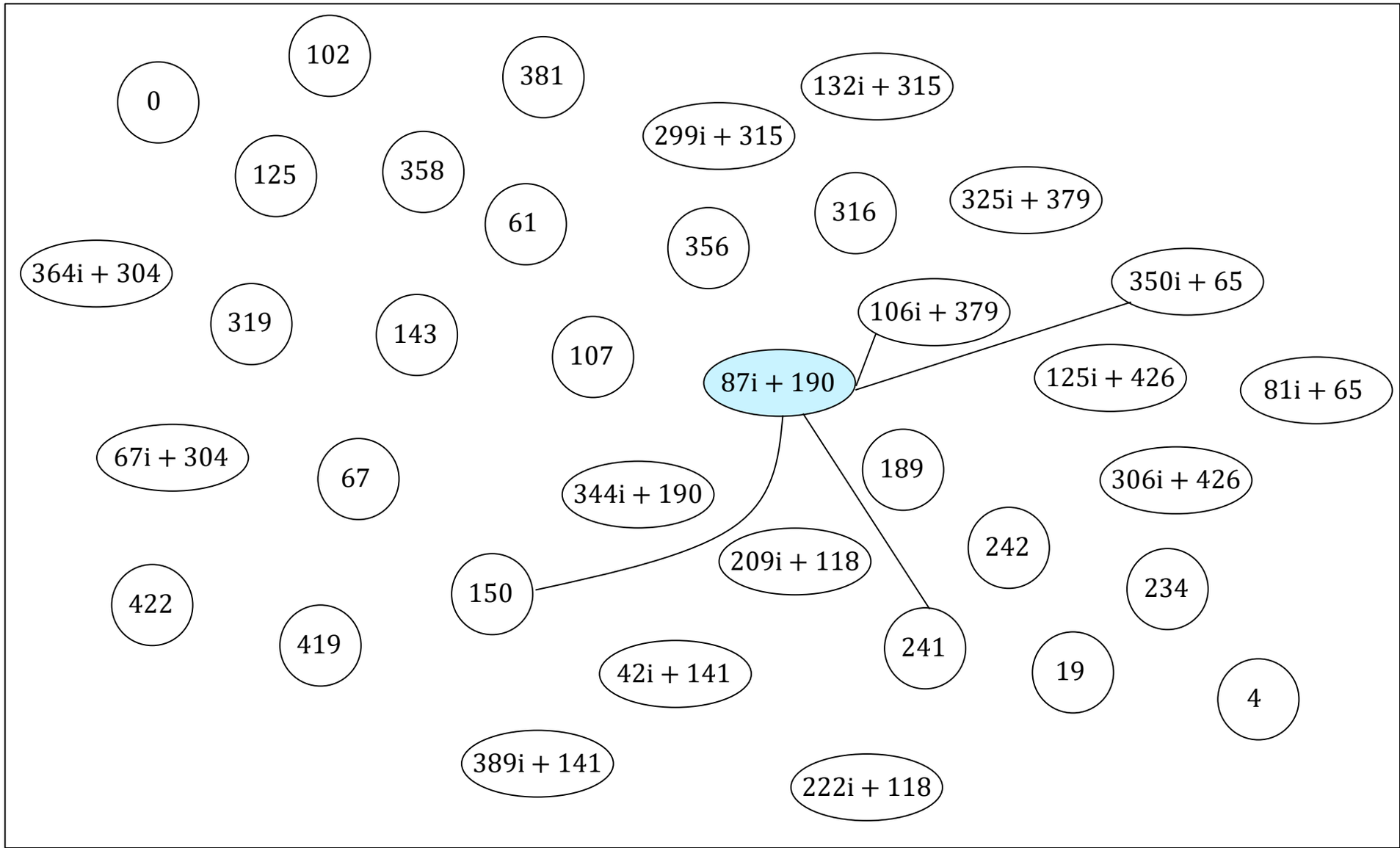


Summary


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

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



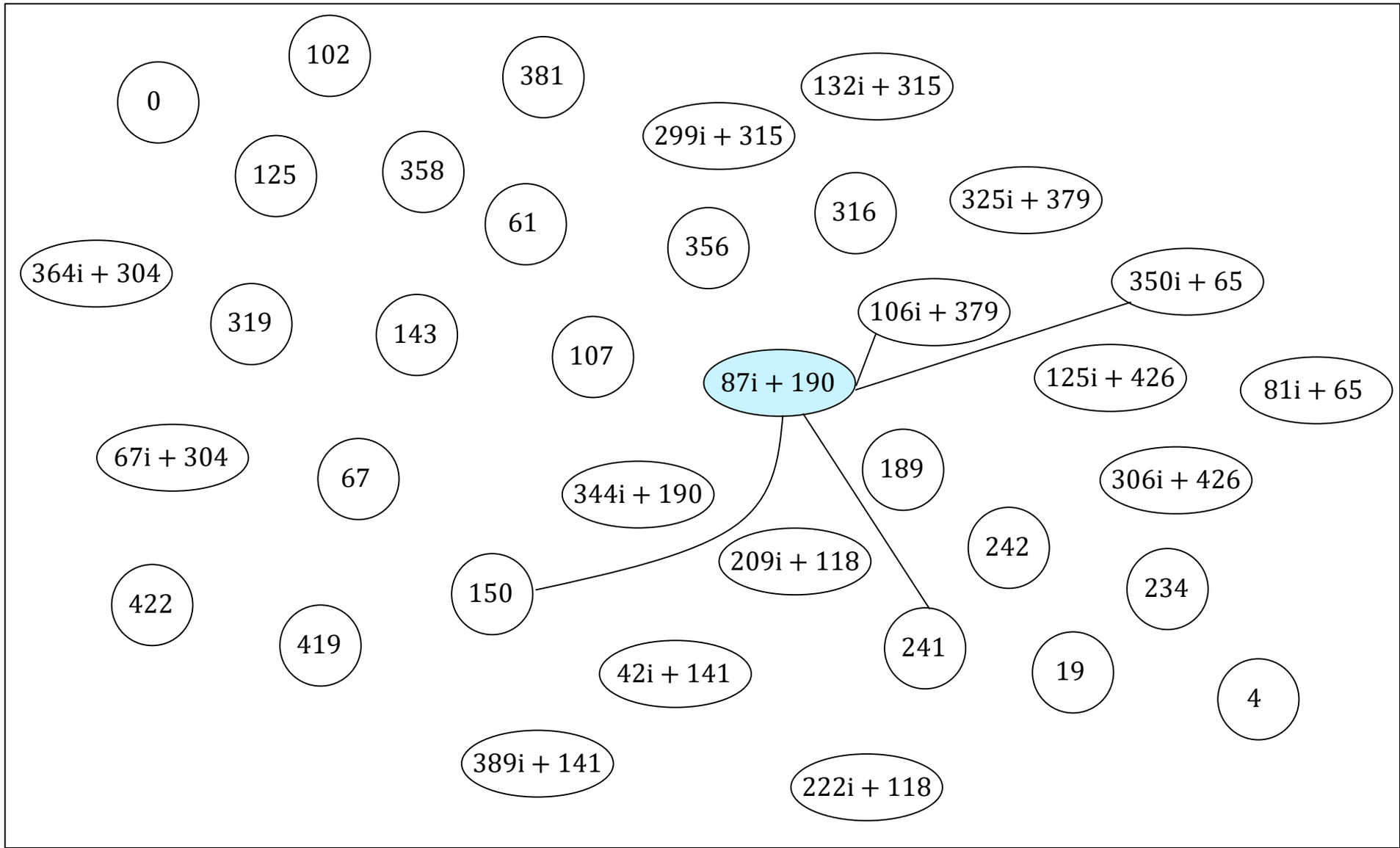
Bob's key generation

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

[3]

[3]

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



Bob's key generation

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

[3]

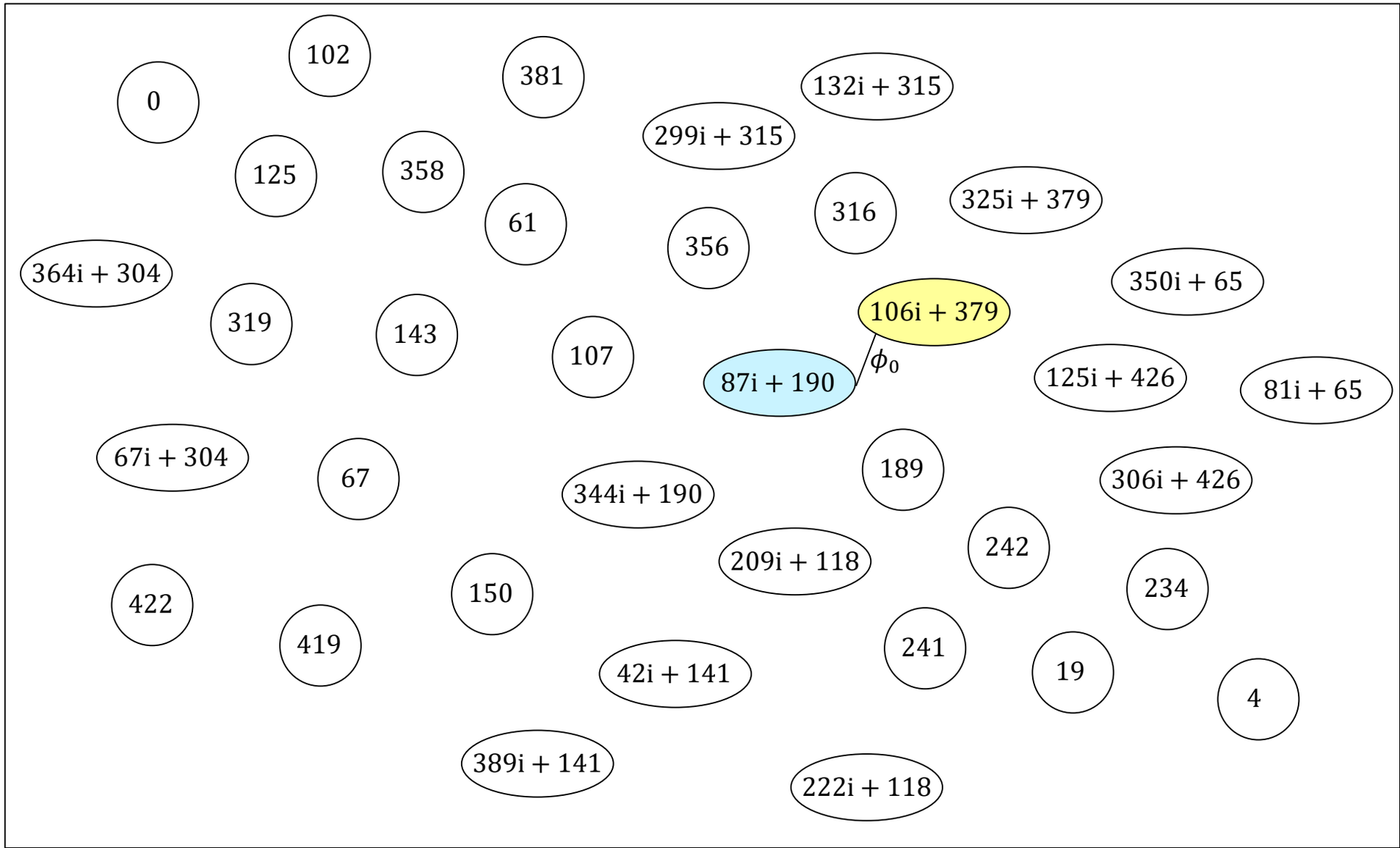
[3]

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

$\phi_0 : E_0 \to E_1$

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

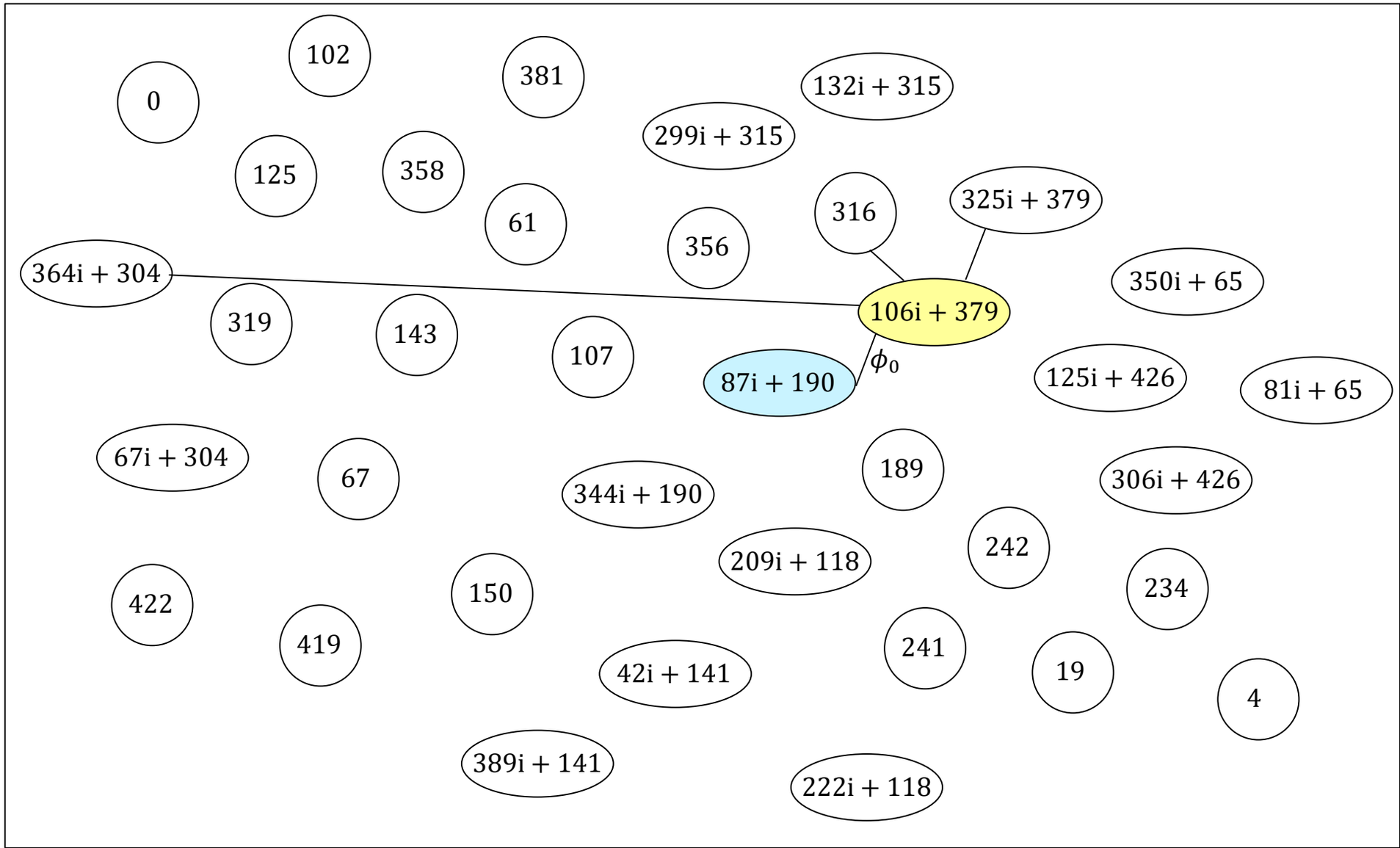
$j(E_1) = 106i + 379$



Bob's key generation

ϕ_0

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



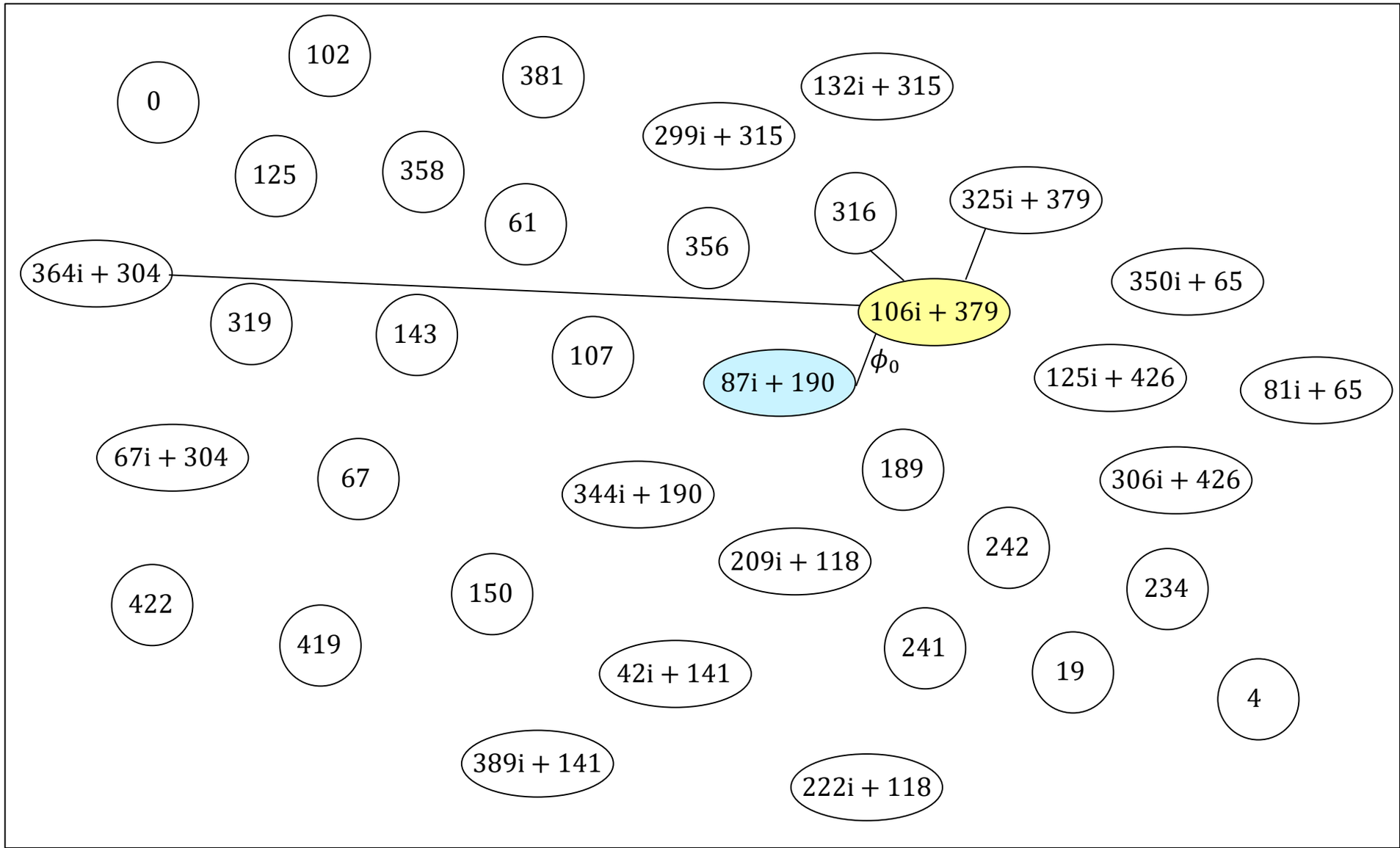
Bob's key generation

ϕ_0

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

[3]

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



Bob's key generation

ϕ_0

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

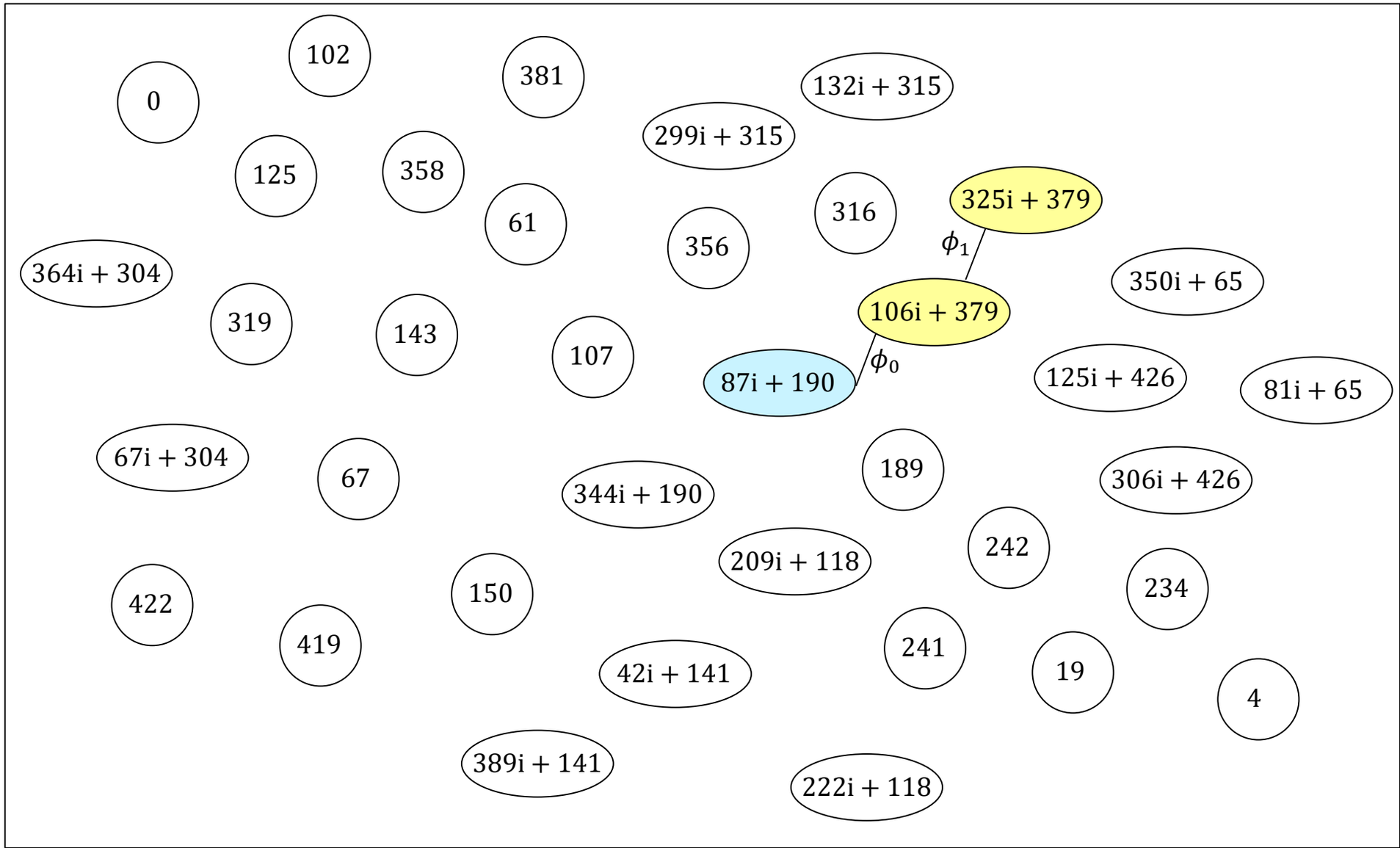
[3]

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

$\phi_1 : E_1 \to E_2$

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

$j(E_2) = 325i + 379$



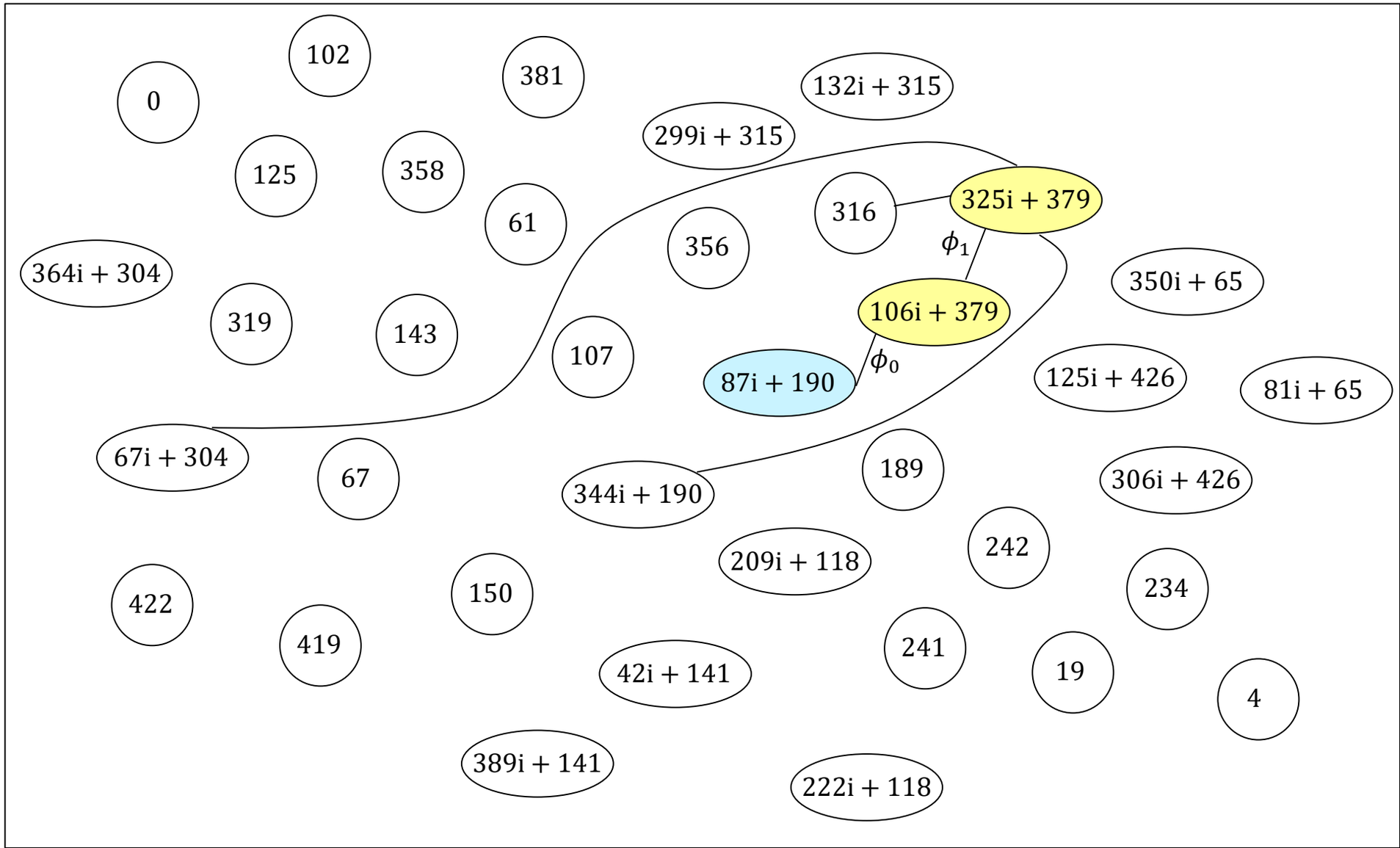
Bob's key generation

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

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

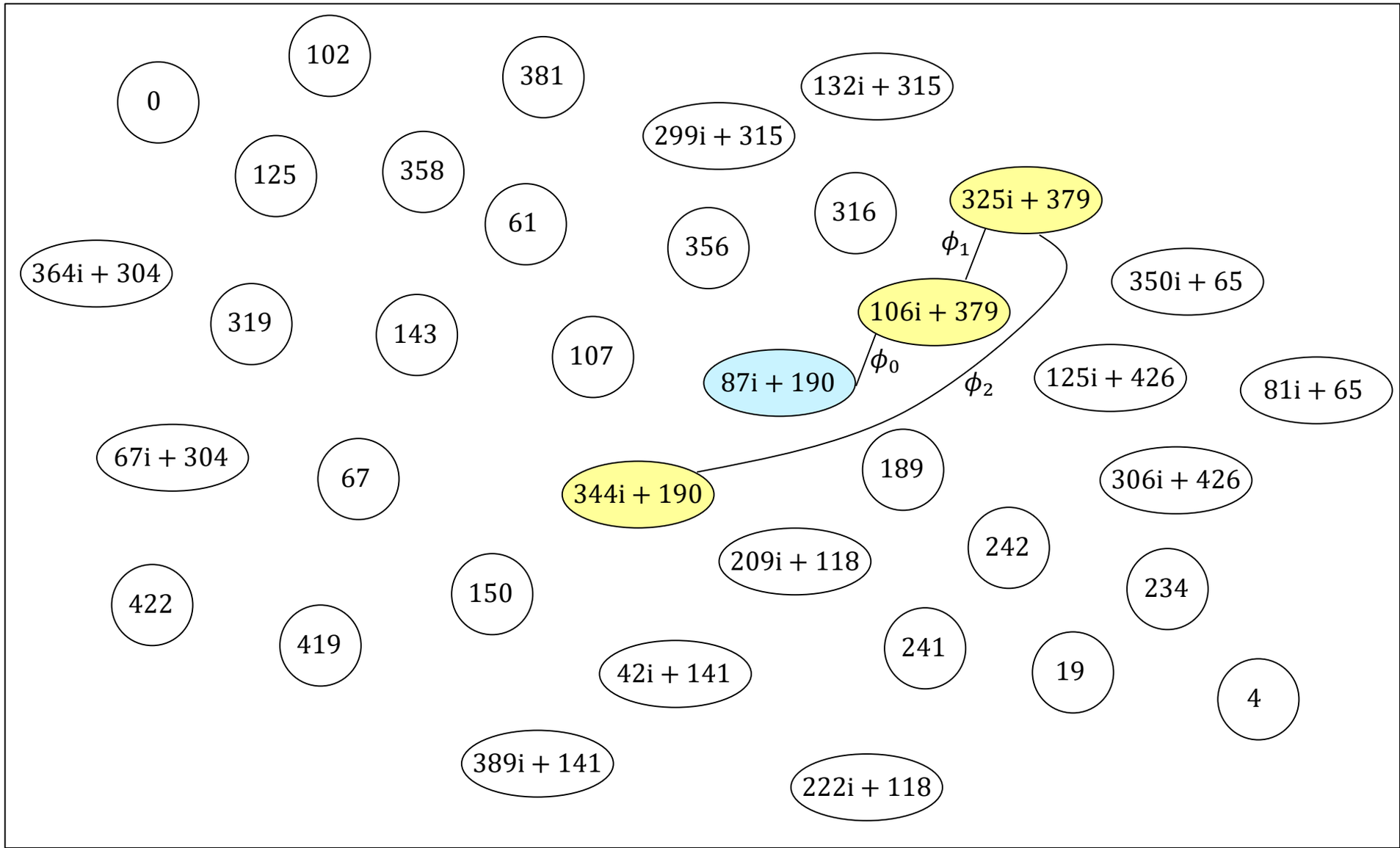
ϕ_1

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

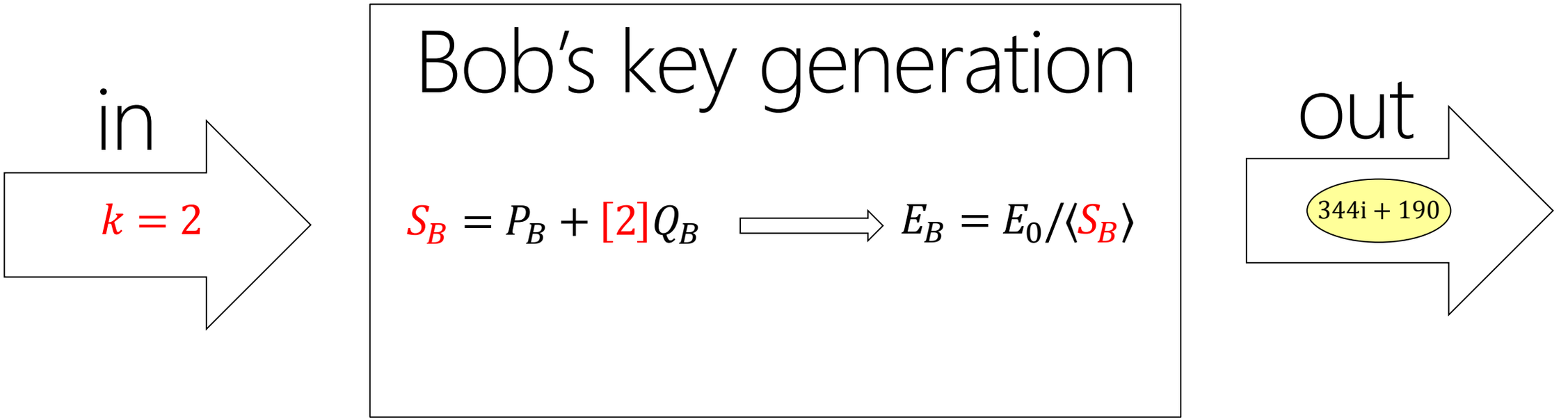
$\phi_2 : E_2 \to E_3$

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

$j(E_3) = 344i + 190$



Summary

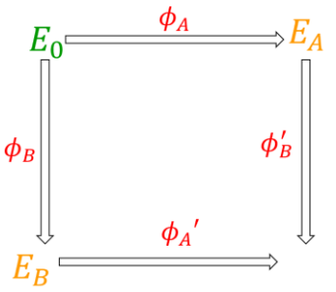

in
$k = 2$
Bob's key generation
$S_B = P_B + [2]Q_B \longrightarrow E_B = E_0/\langle S_B \rangle$
out
344i + 190

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:

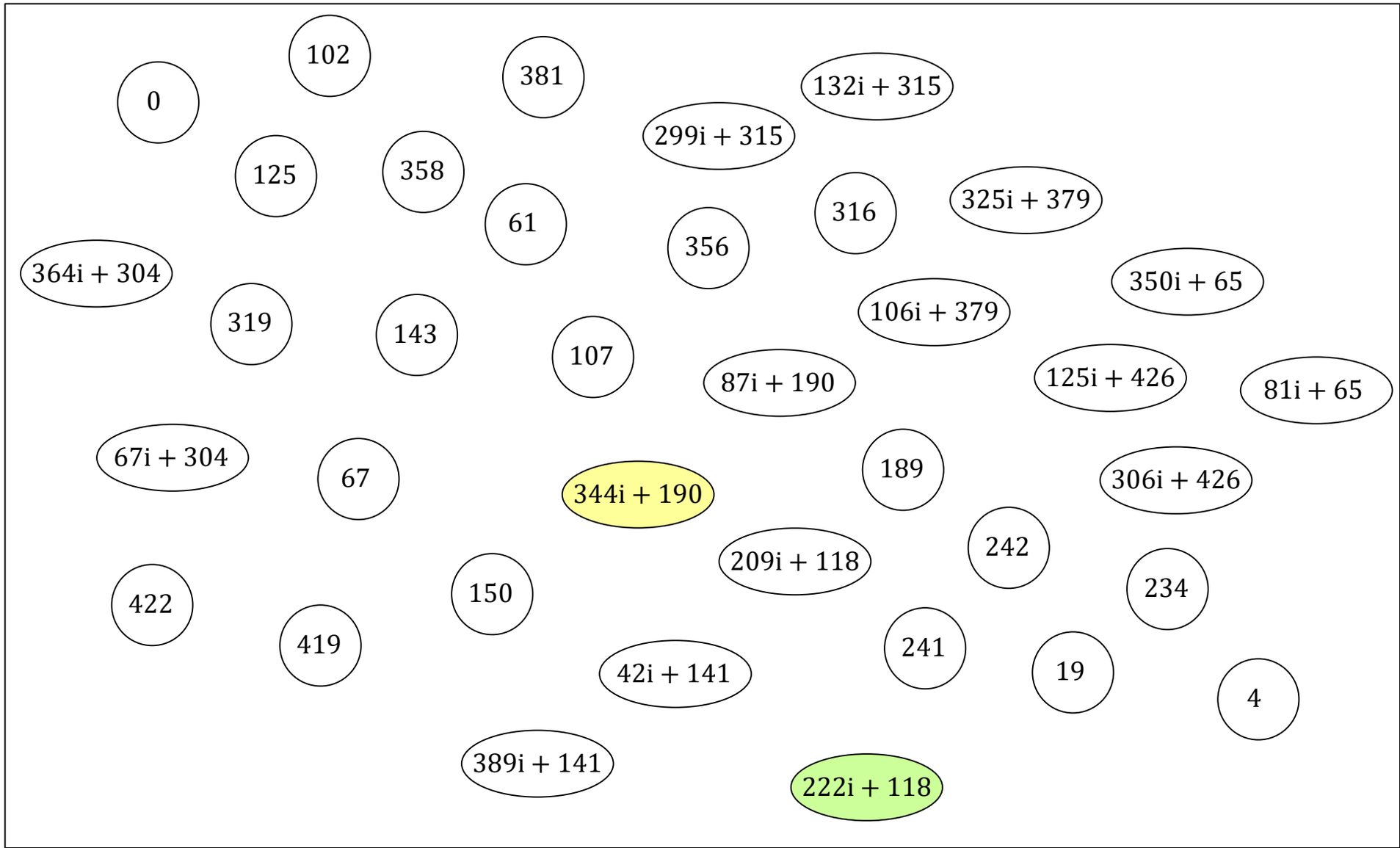
$$E_A = \phi_A(E_0) \qquad P_{AB} = \phi_A(P_B) \qquad Q_{AB} = \phi_A(Q_B)$$

Bob's public key:

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

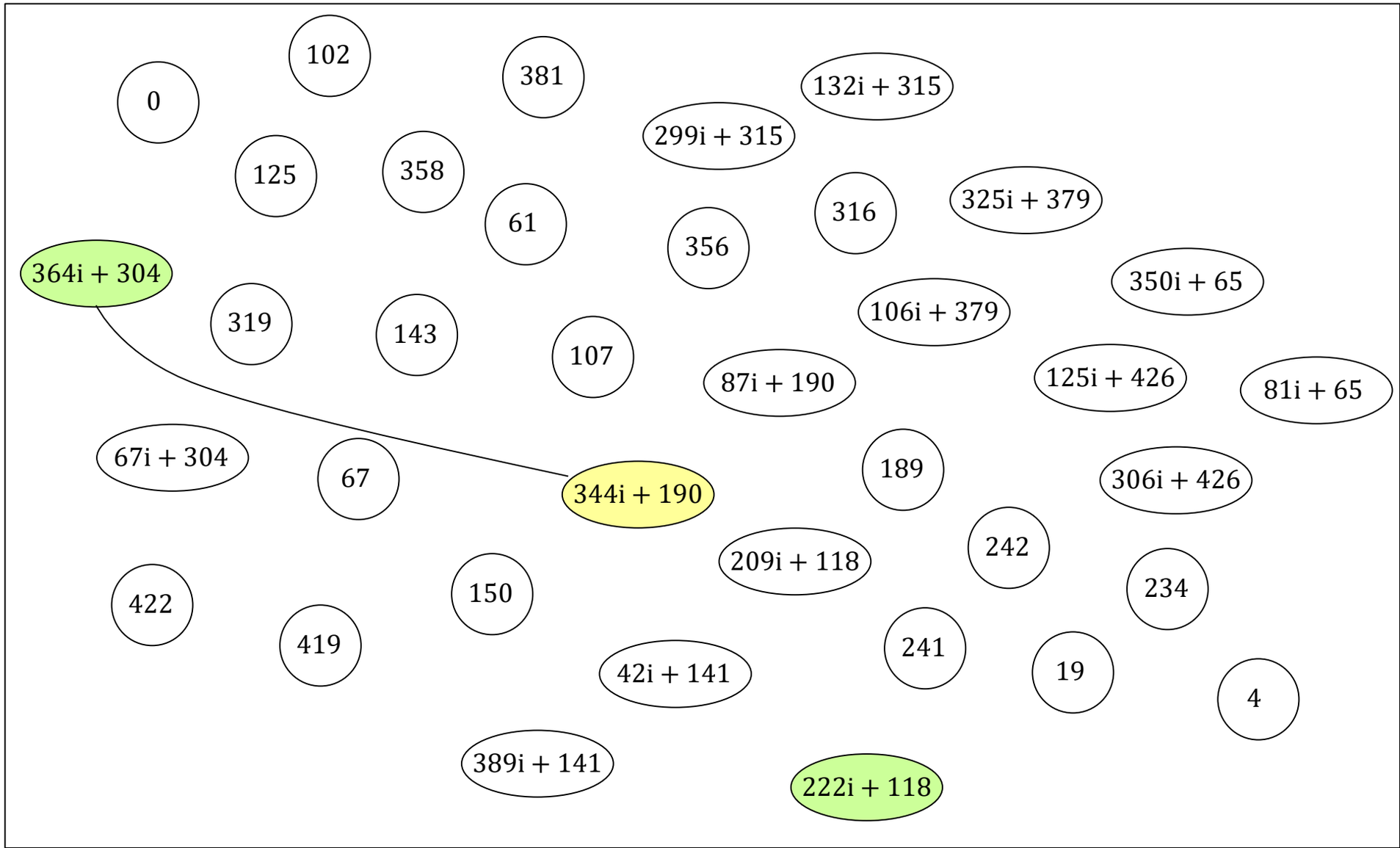
Alice's shared secret

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



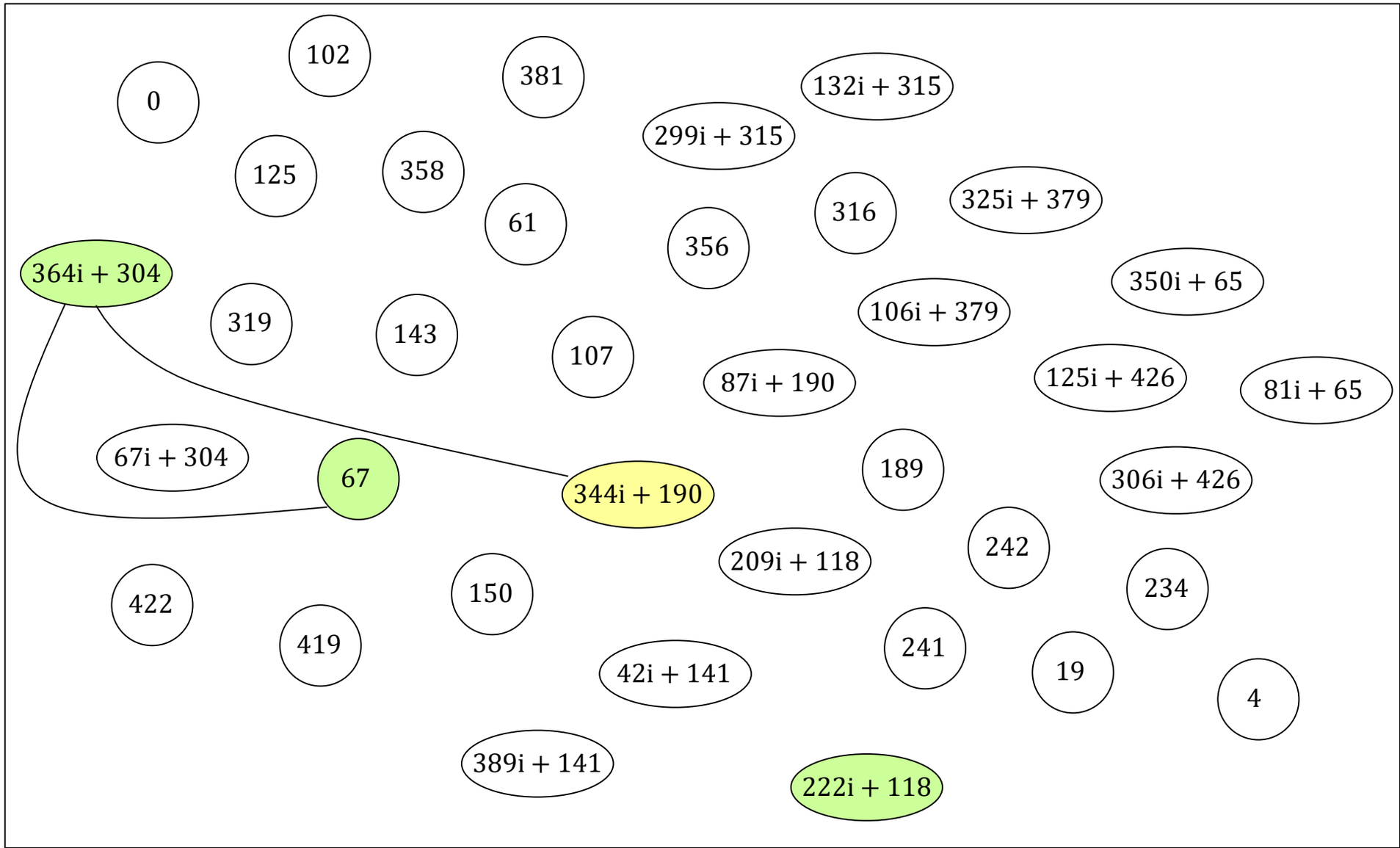
Alice's shared secret

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



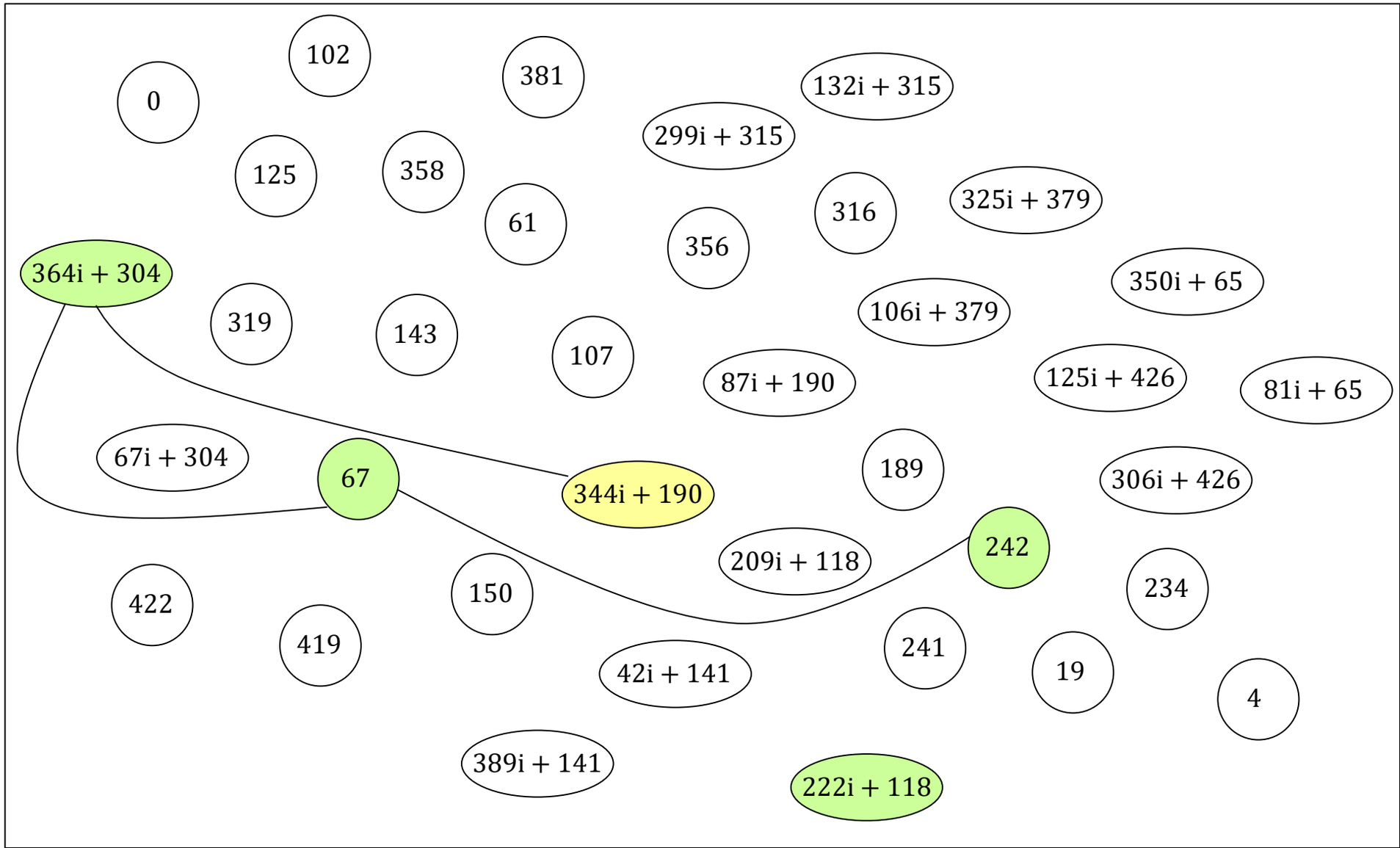
Alice's shared secret

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



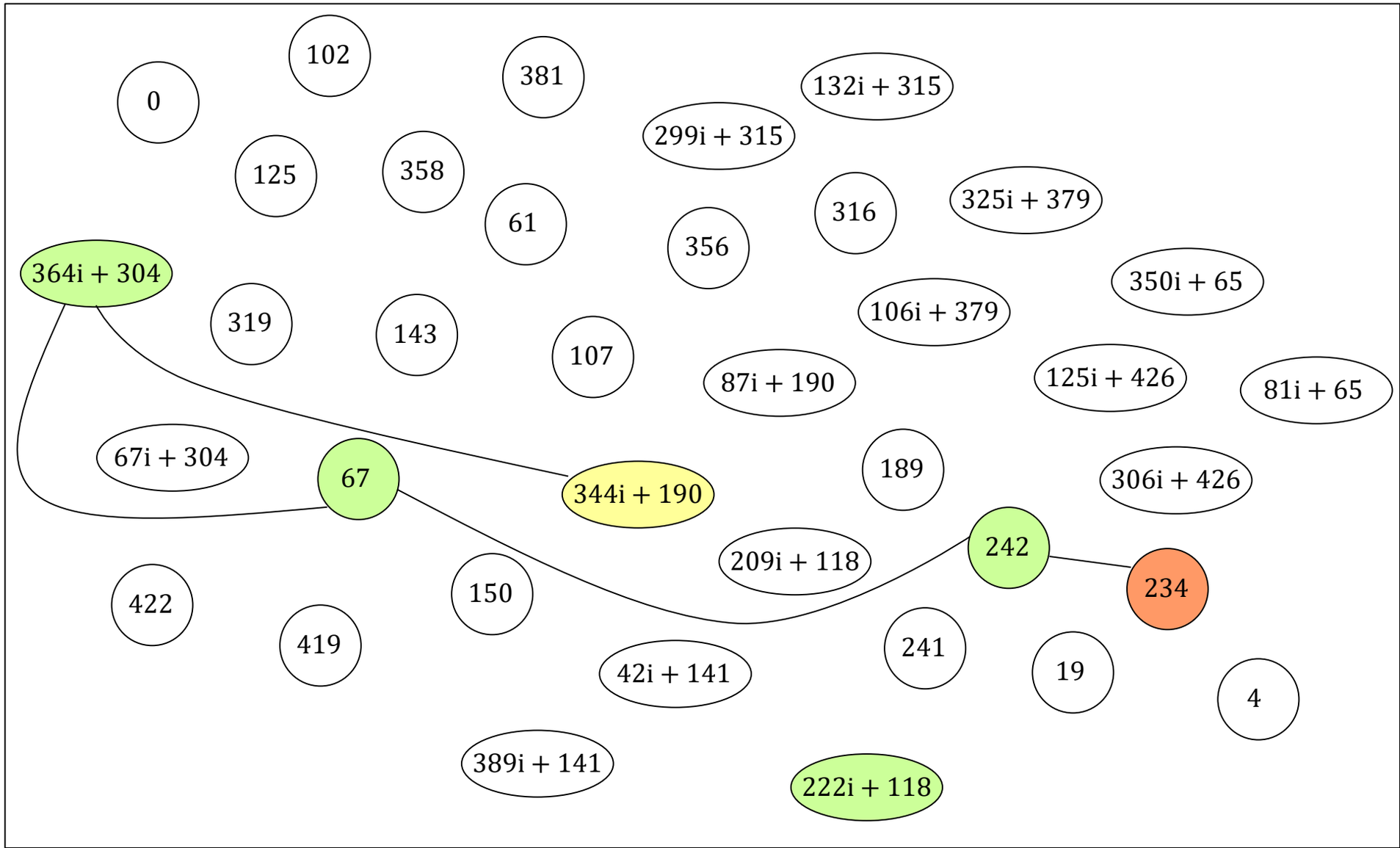
Alice's shared secret

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



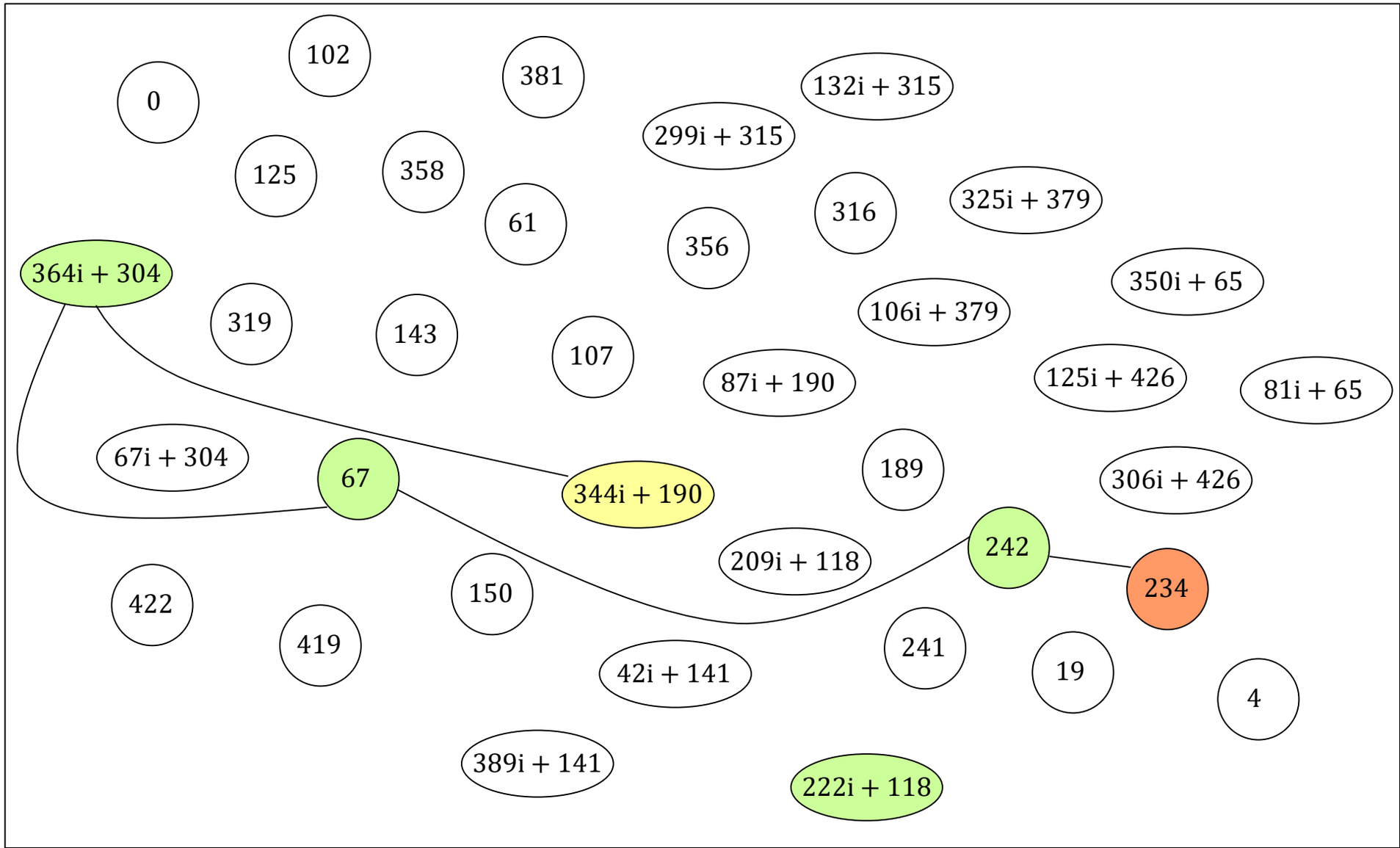
Alice's shared secret

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



Bob's shared secret

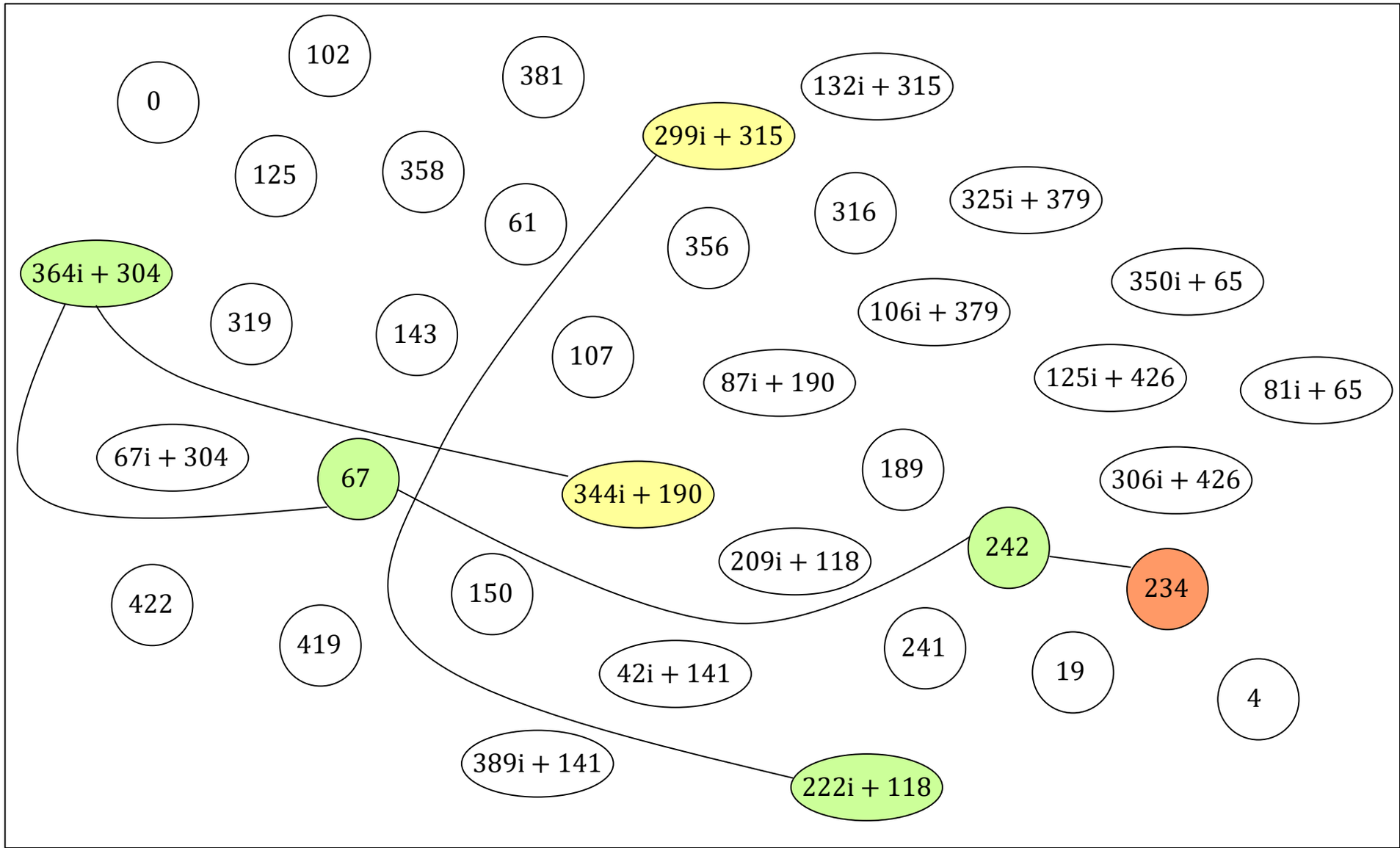
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

Bob's shared secret

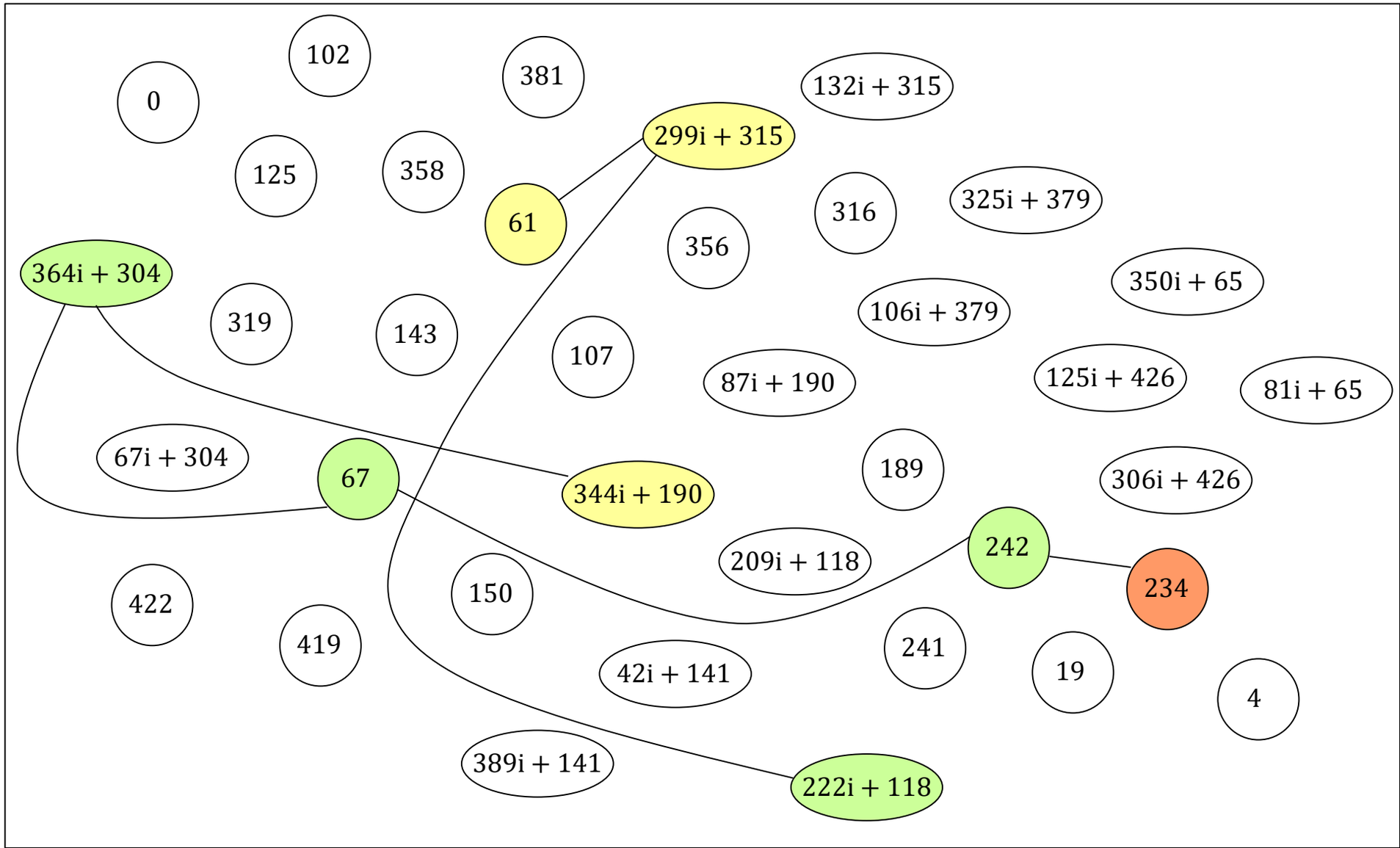
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

Bob's shared secret

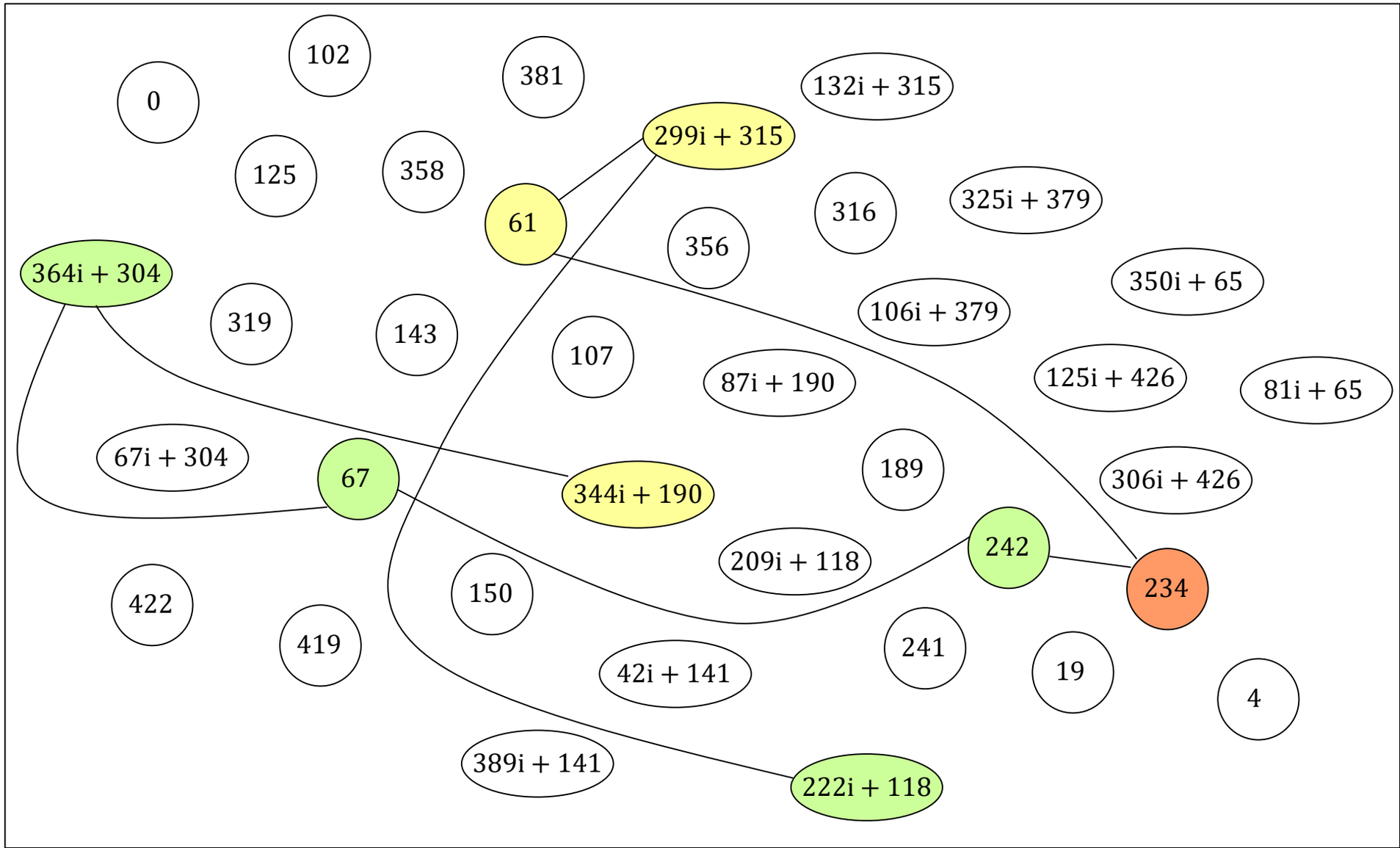
$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$



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

Bob's shared secret

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



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

Bob's shared secret

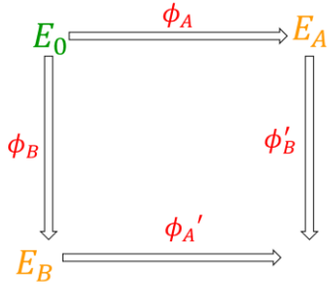
$$S'_A = \phi_B(P_A) + [k_A]\phi_B(Q_A)$$

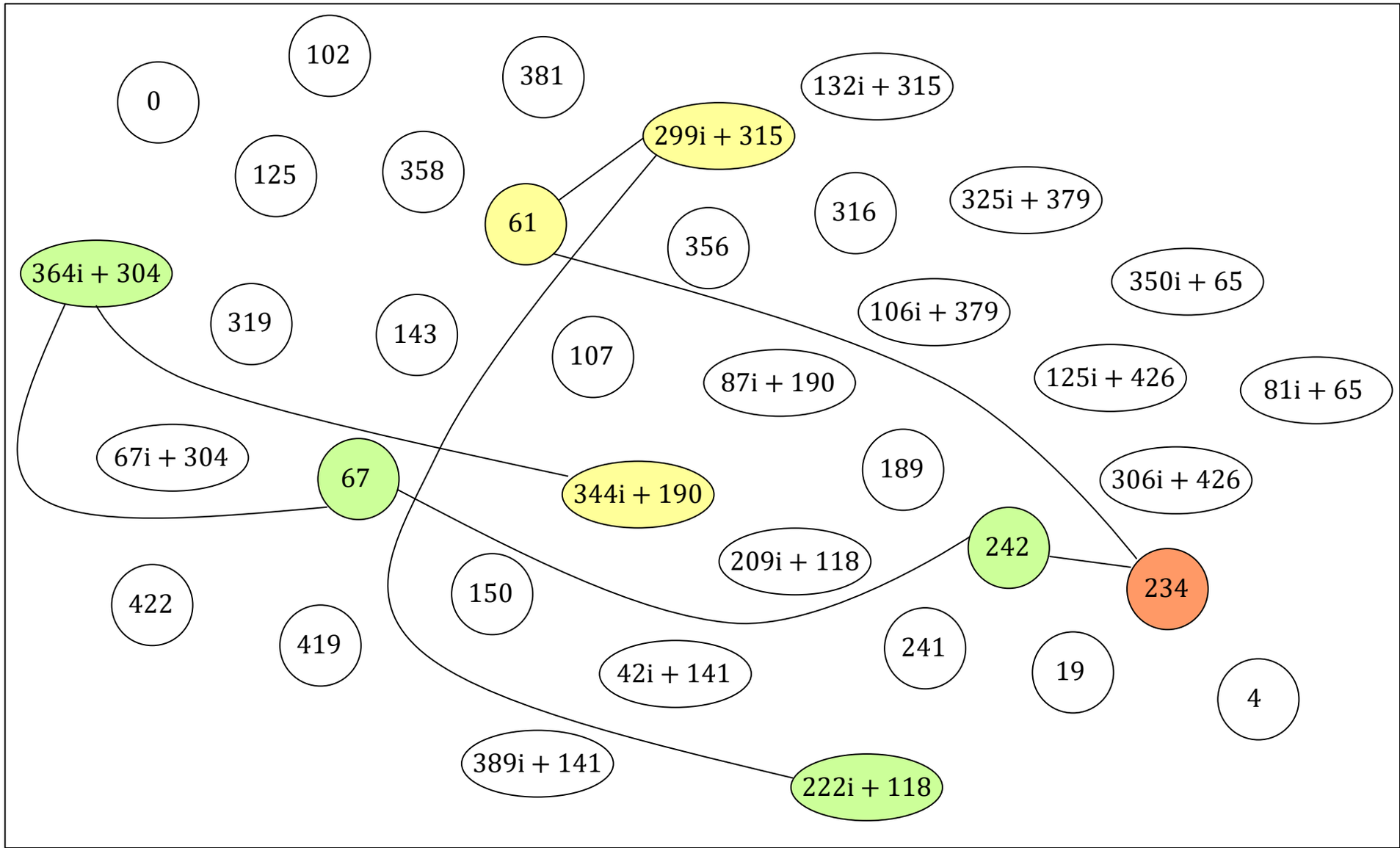
$$S'_A = \phi_B(P_A) + \phi_B([k_A]Q_A)$$

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

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

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





its ^ cryptanalysis

classical

CSSI problem: given E, E', find path (of known length)…

Assumption in SIDH: the auxiliary points don't help solve CSSI

Galbraith-Petit-Shani-Ti: they do if you're an active adversary!

SIDH (passive security) → SIKE (active security, FO transform)

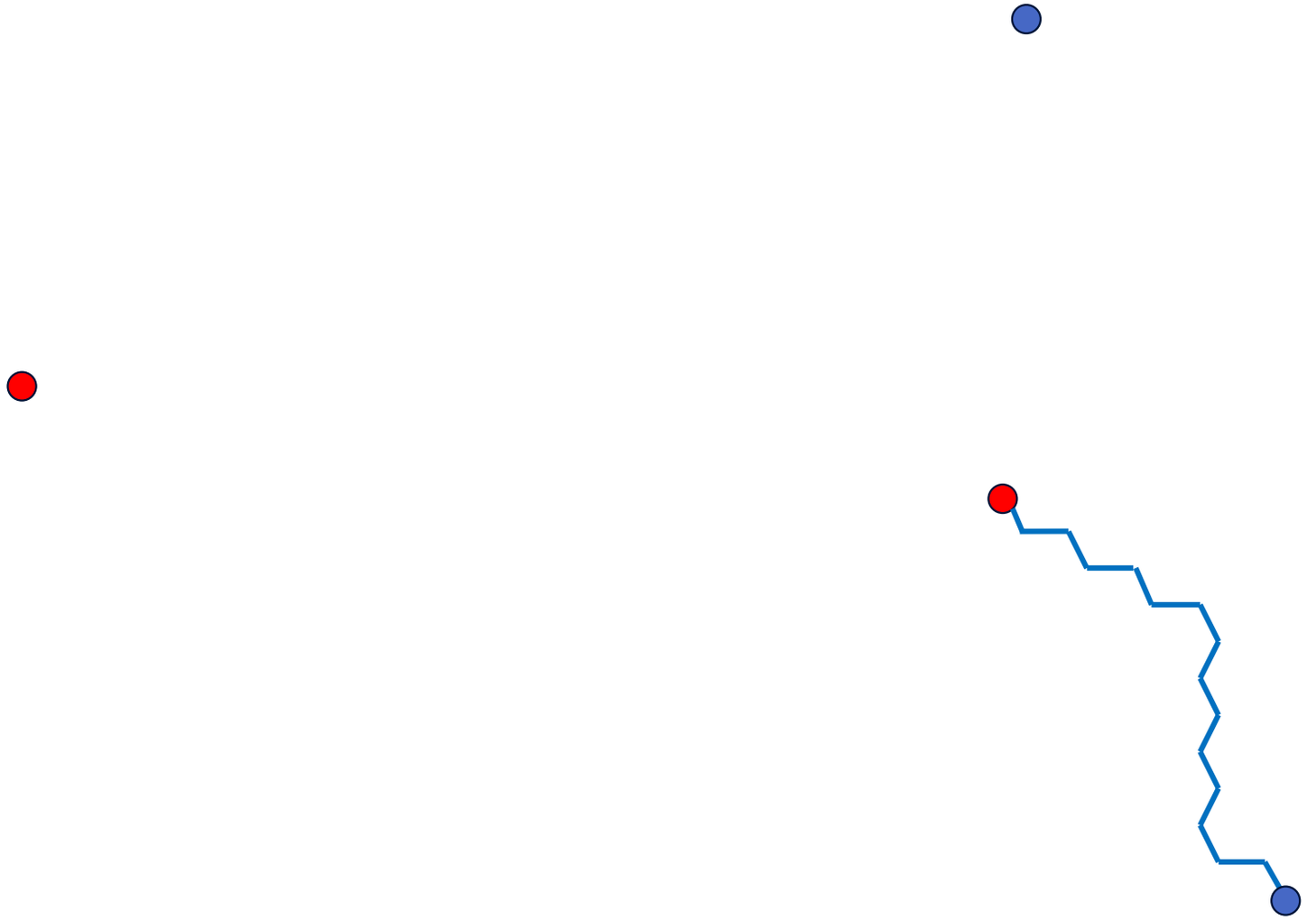
Claw finding: meet-in-the-middle

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

Claw finding: meet-in-the-middle

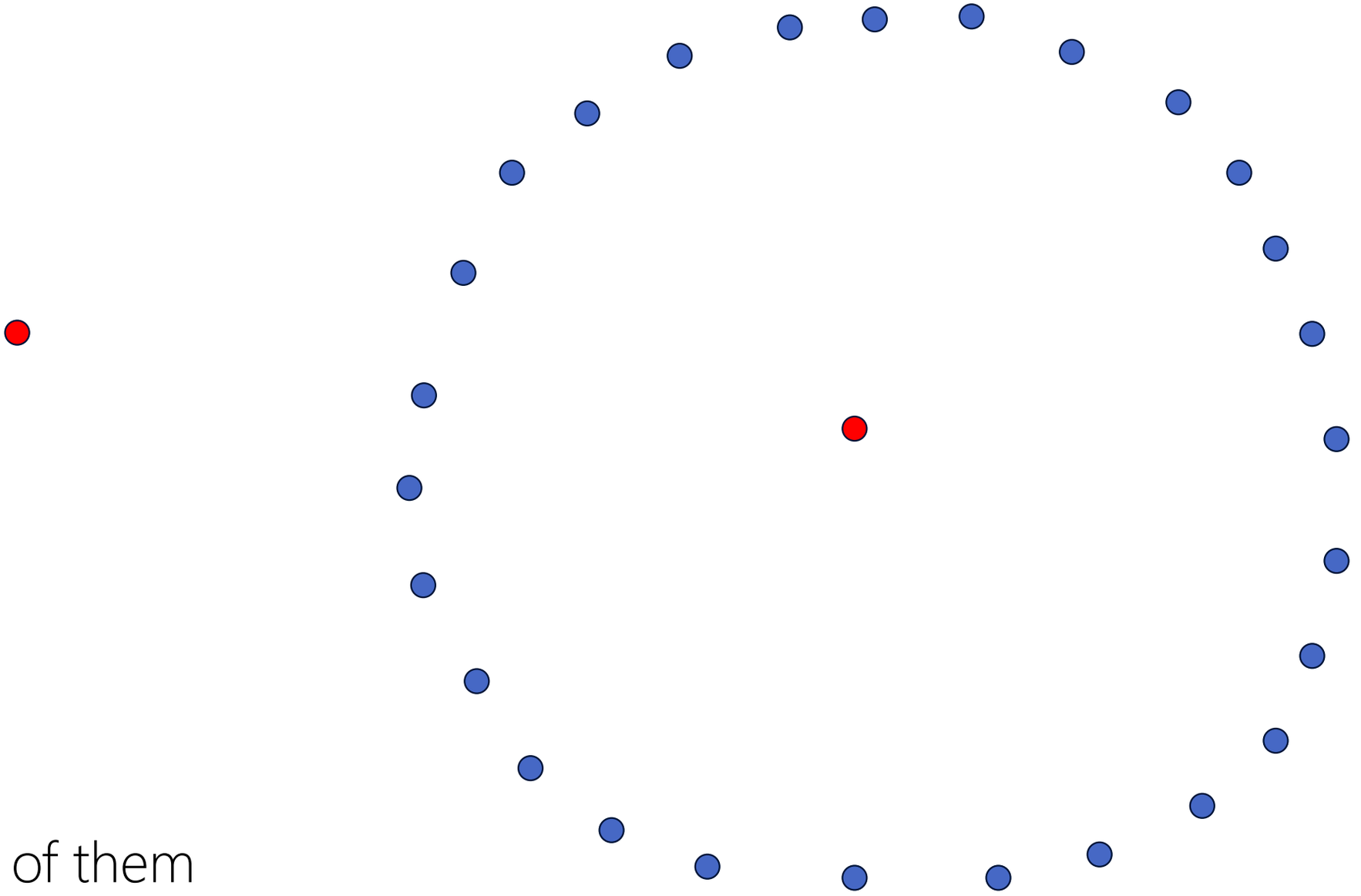
Compute and store $\ell^{e/2}$-isogenies on one side

Claw finding: meet-in-the-middle



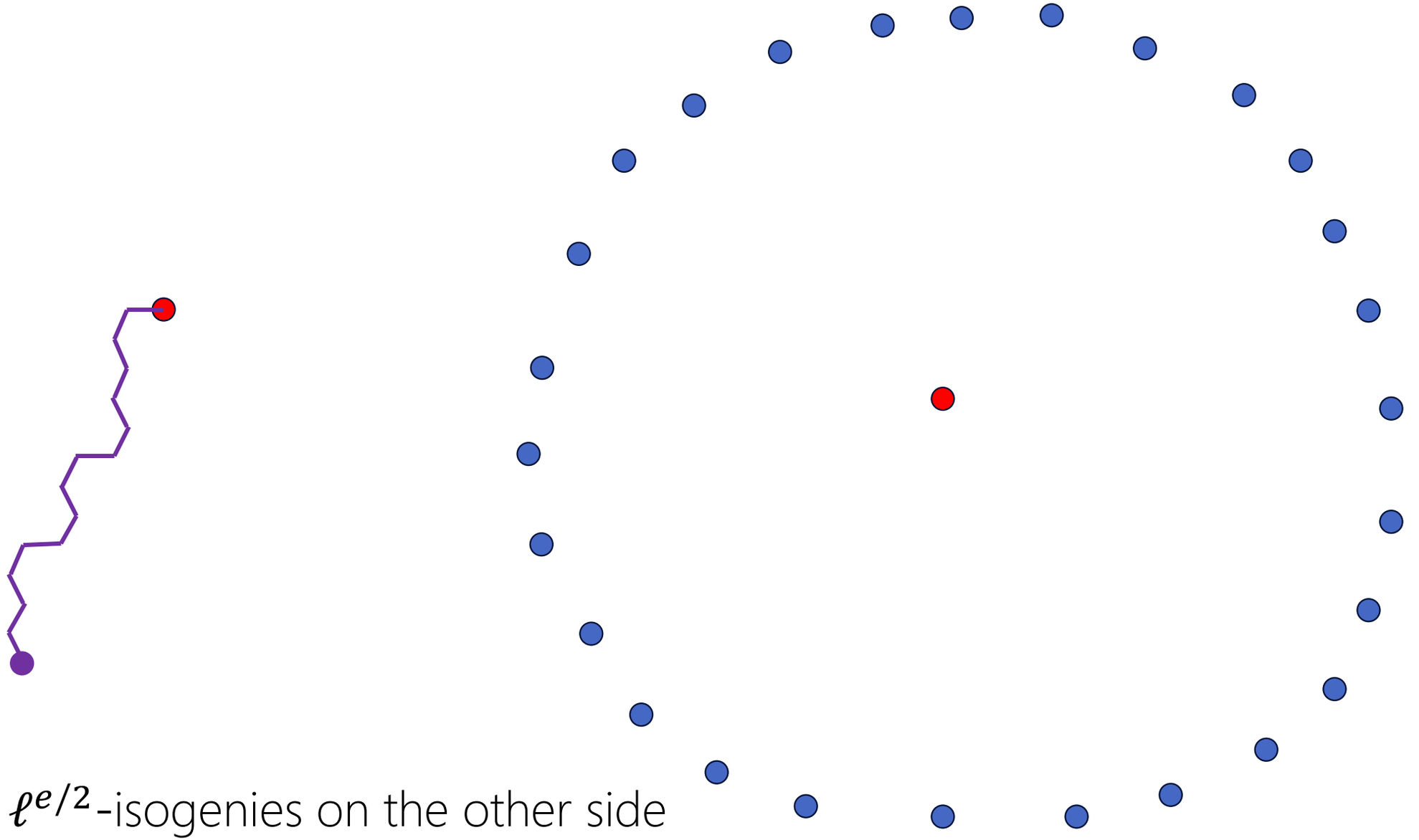
Compute and store $\ell^{e/2}$-isogenies on one side

Claw finding: meet-in-the-middle



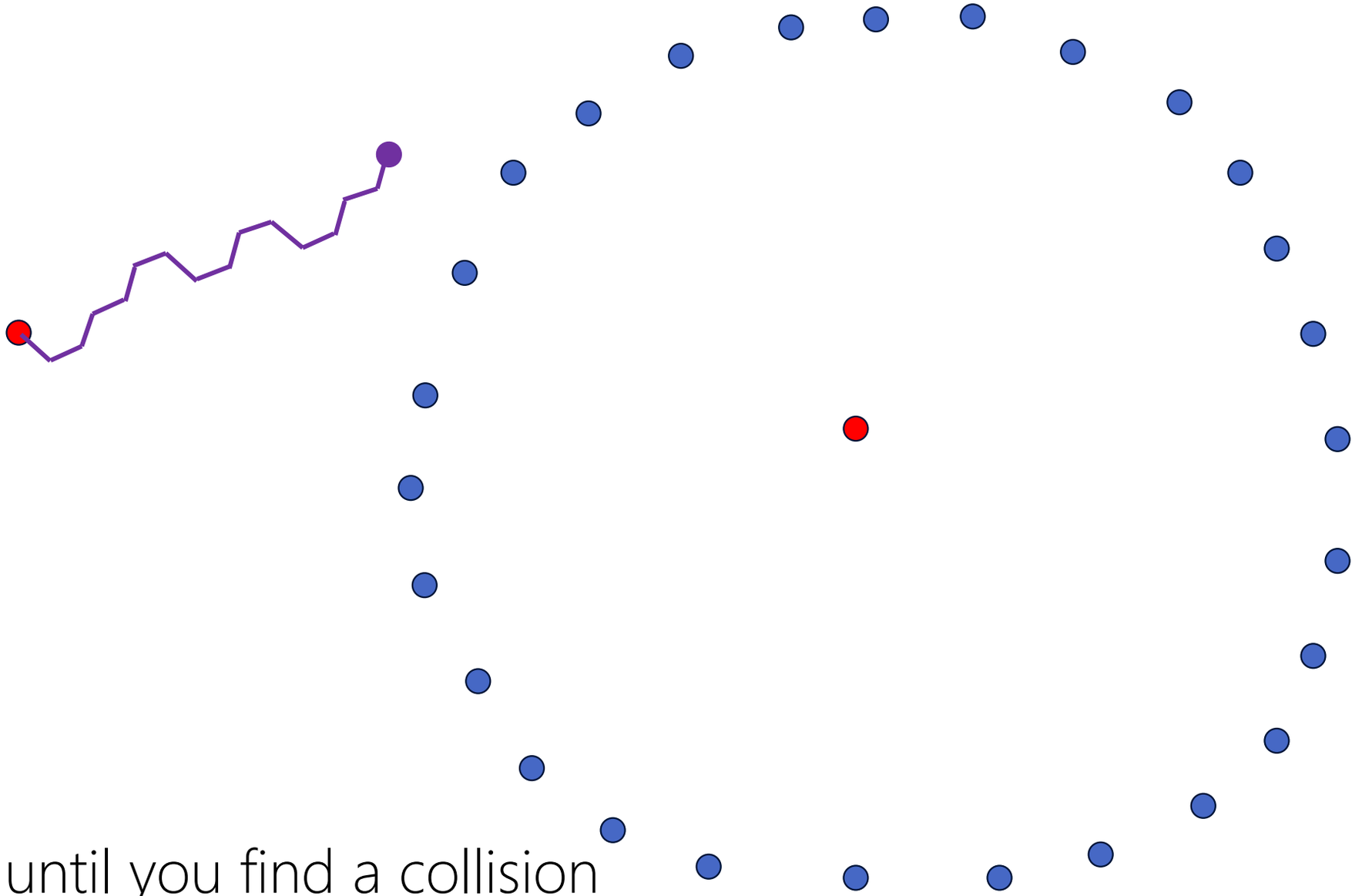
… until you have all of them

Claw finding: meet-in-the-middle



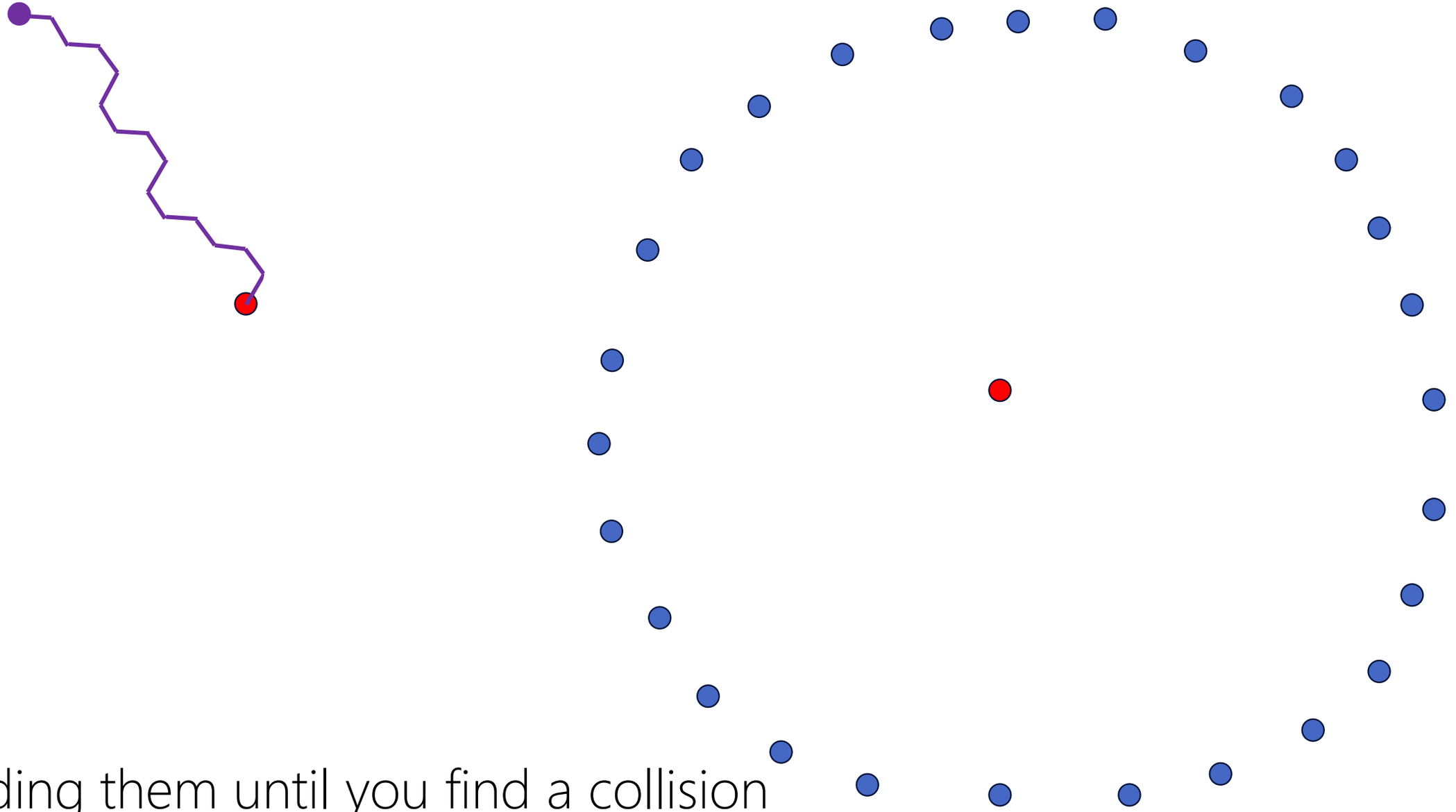
Now compute $\ell^{e/2}$-isogenies on the other side

Claw finding: meet-in-the-middle



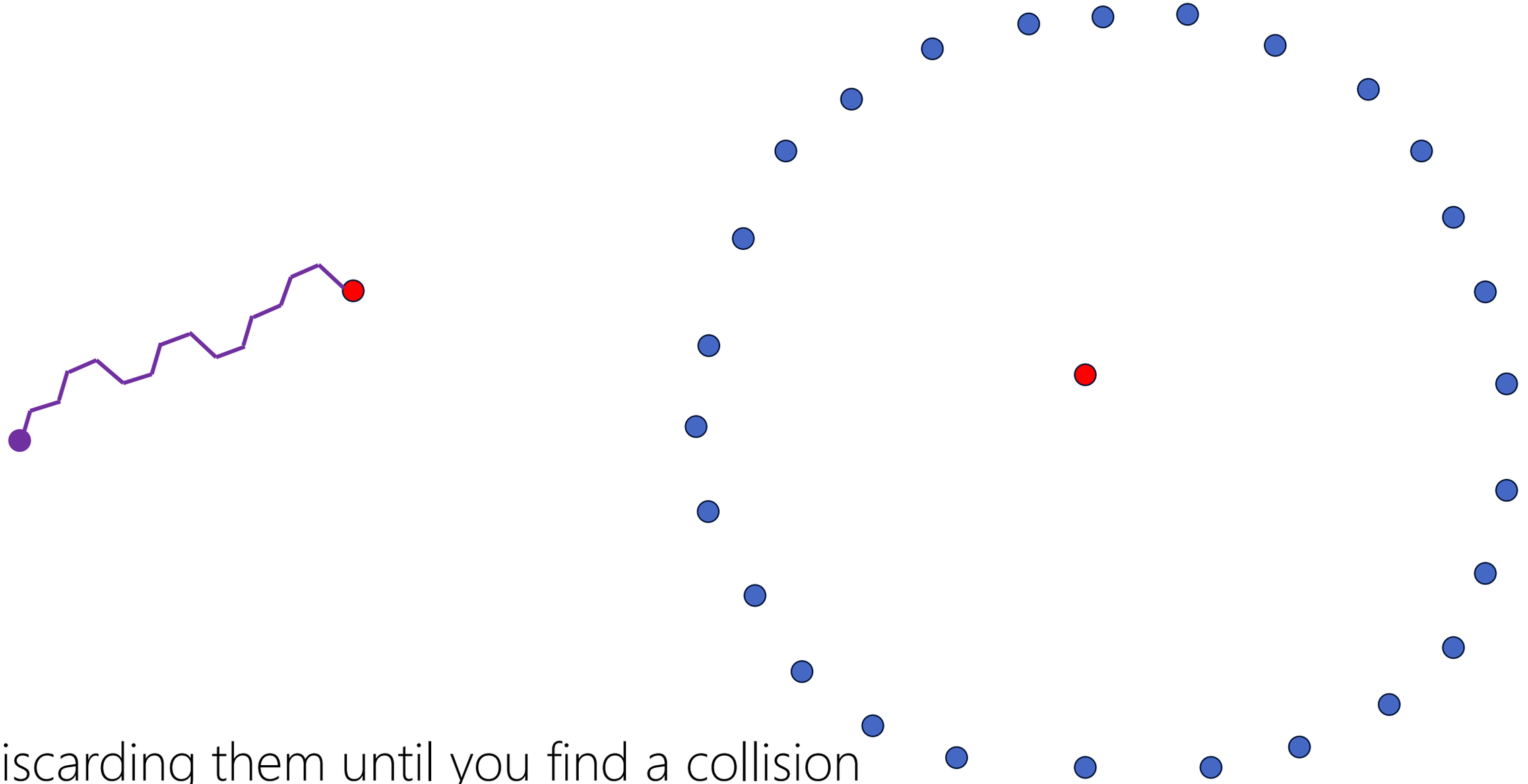
… discarding them until you find a collision

Claw finding: meet-in-the-middle



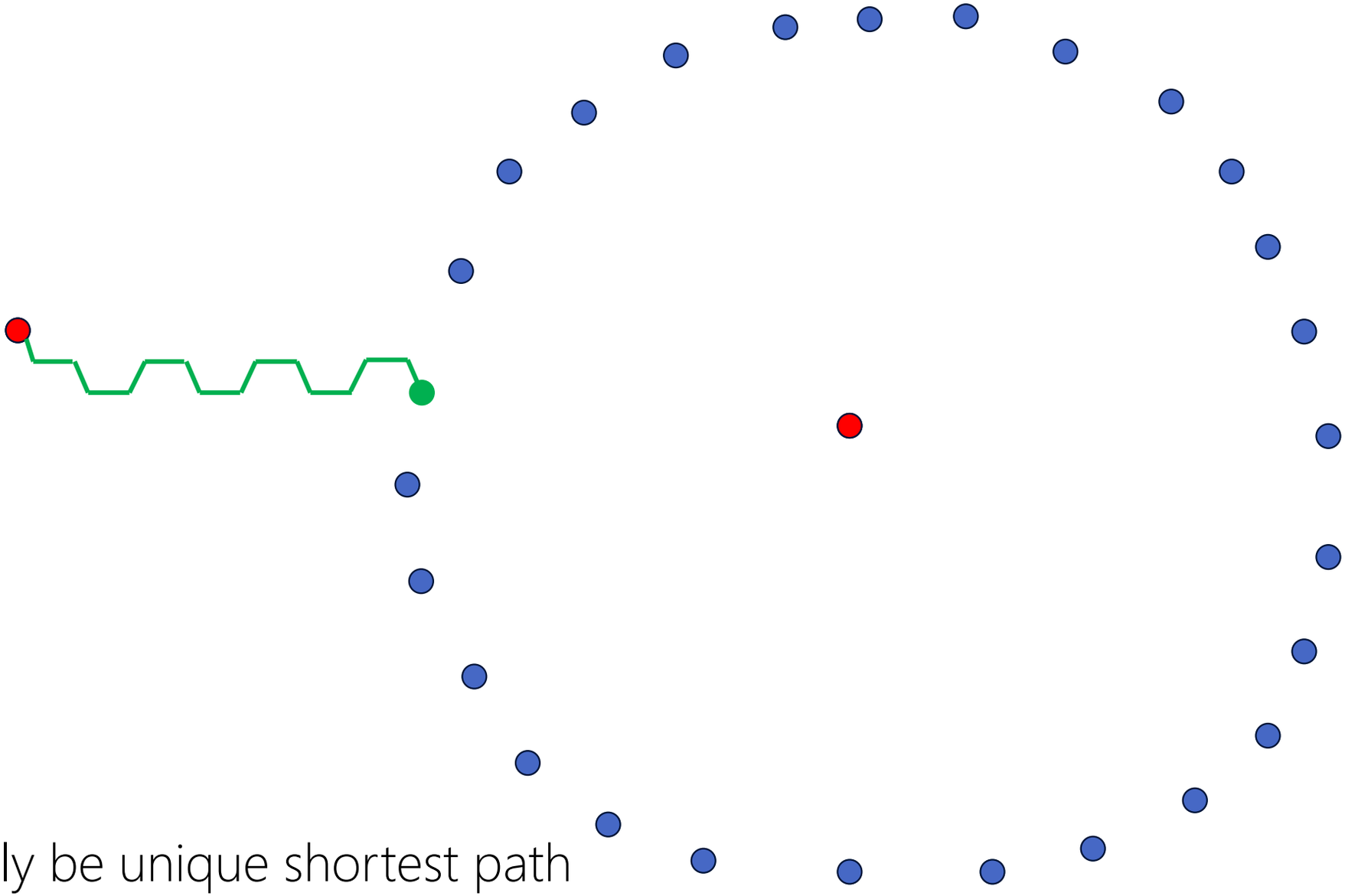
… discarding them until you find a collision

Claw finding: meet-in-the-middle



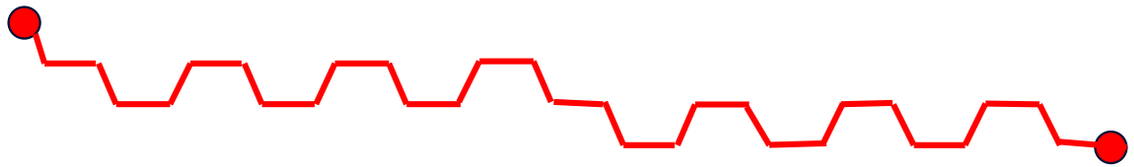
… discarding them until you find a collision

Claw finding: meet-in-the-middle



Collision will most likely be unique shortest path

Claw finding: meet-in-the-middle



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

Meet-in-the-middle: classical 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

OLD SLIDE

- **Best (known) attacks:** classical $O(p^{1/4})$ and Tani's quantum $O(p^{1/6})$
- **Confidence:** both complexities are optimal for a black-box claw attack

SIKE Round 1 parameters

$$p = 2^{e_A}3^{e_B} - 1$$

Target Security Level	**Name** (SIKEp+ $\lceil \log_2 p \rceil$)	(e_A, e_B)	k	2^{k-1}	**min** $(\sqrt{2^{e_A}}, \sqrt{3^{e_3}})$	$\sqrt{2^k}$	**min** $(\sqrt[3]{2^{e_2}}, \sqrt[3]{3^{e_3}})$
NIST 1	SIKEp503	(250,159)	128	2^{127}	2^{125}	2^{64}	2^{83}
NIST 3	SIKEp761	(372,239)	192	2^{191}	2^{186}	2^{96}	2^{124}
NIST 5	SIKEp964	(486,301)	256	2^{255}	2^{238}	2^{128}	2^{159}

classical quantum

OLD SIDE

Not long after NIST submission deadline…

Adj, Cervantes-Vazquez, Chi-Dominguez, Menezes, Rodriguez-Henriquez (SAC 2018).

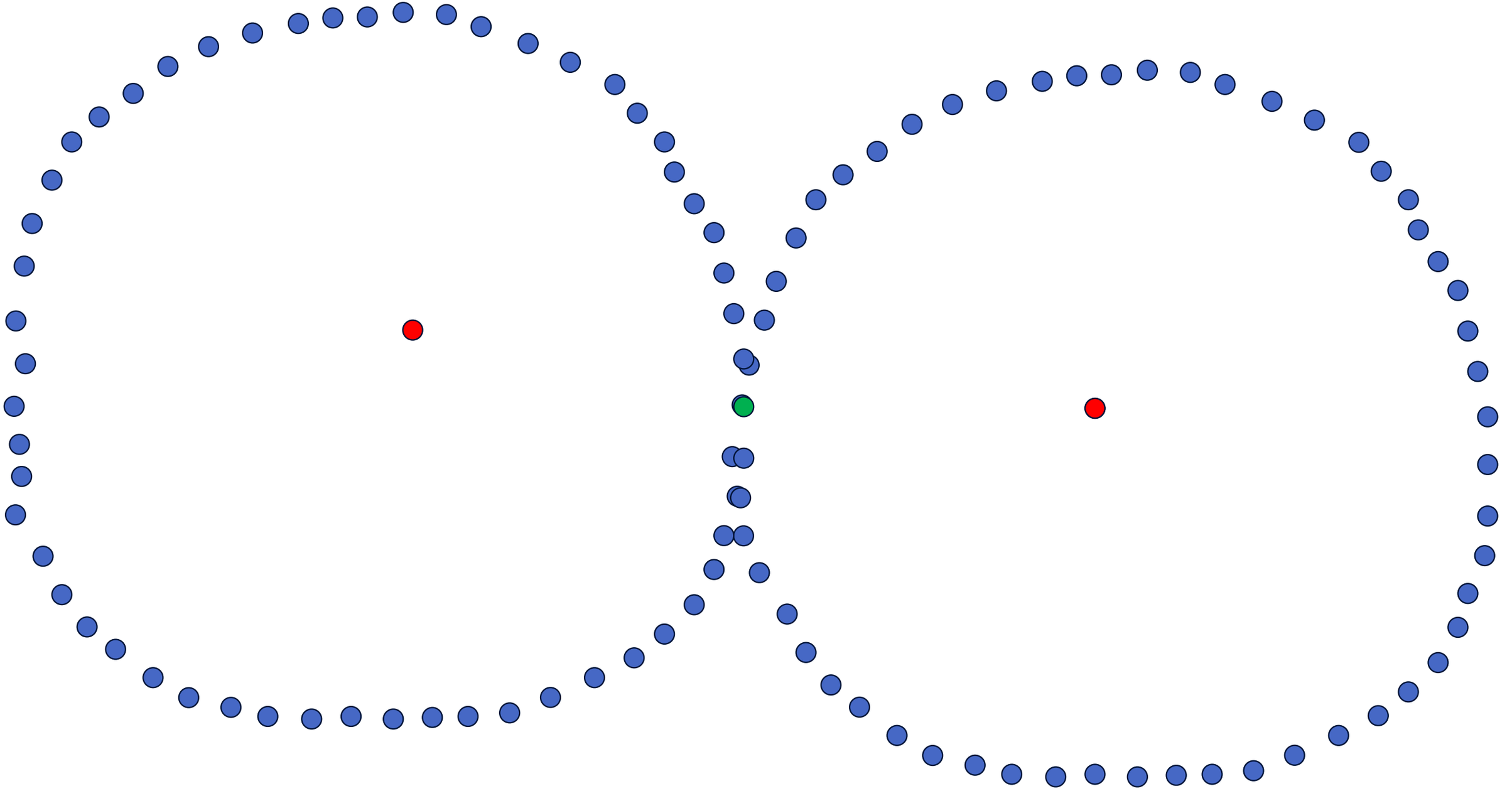
"van Oorschot-Wiener golden collision has a lower cost (but higher running time) for solving CSSI, and thus should be used instead of MitM to assess the security of SIDH"

Jaques-Schanck. CRYPTO 2019.

"Our conclusion is that an adversary with enough quantum memory to run Tani's algorithm with the query-optimal parameters could break SIKE faster by using the classical control hardware to run van Oorschot-Wiener."

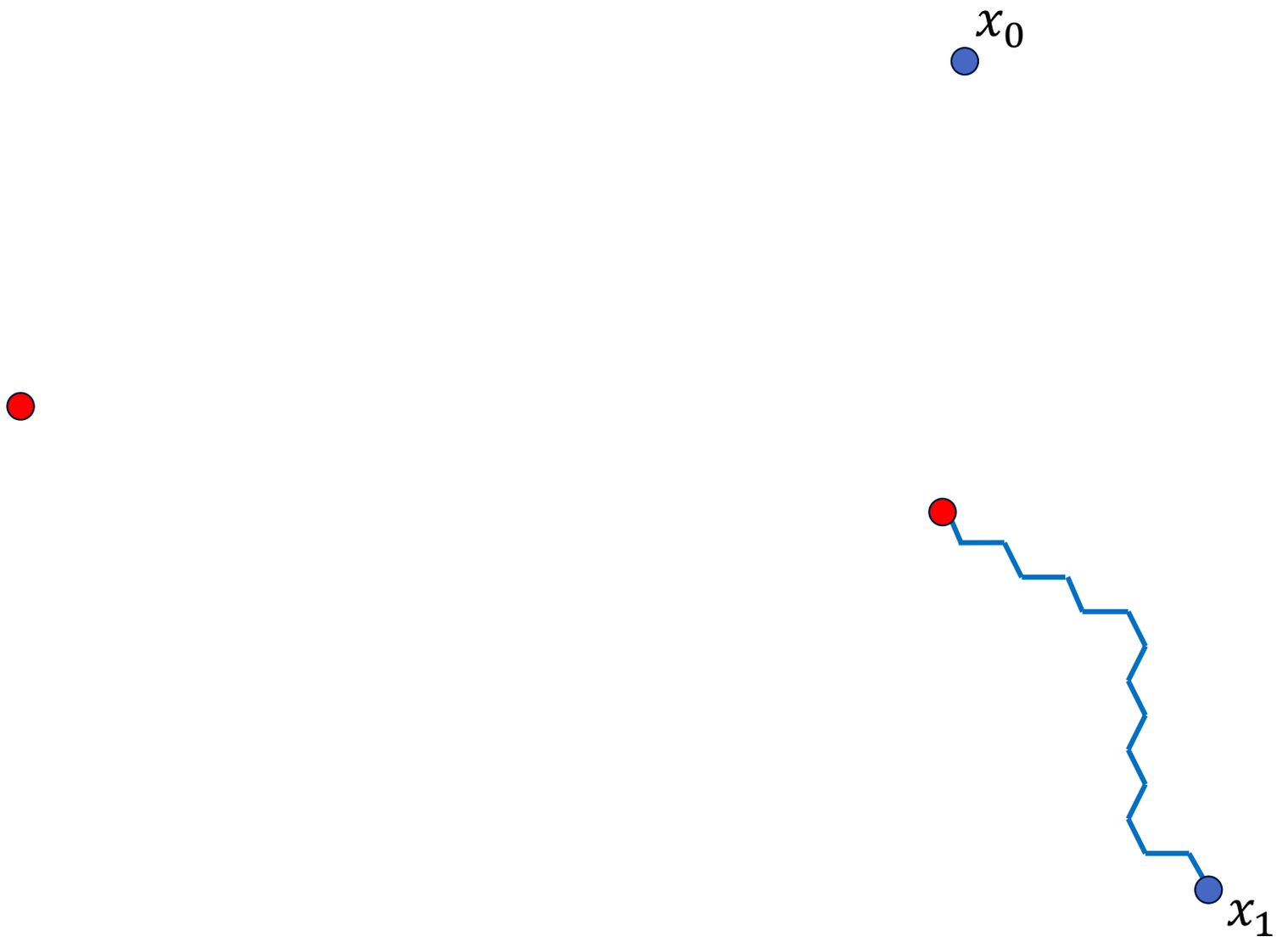
Assumption: fair analysis will fix upper bound on feasible storage, then analyse runtime

vOW: define $S = \{$●$\}$ and a pseudo-random deterministic function $f : S \to S$

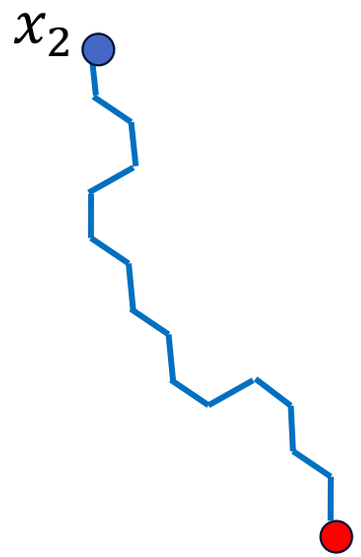


$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$

$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



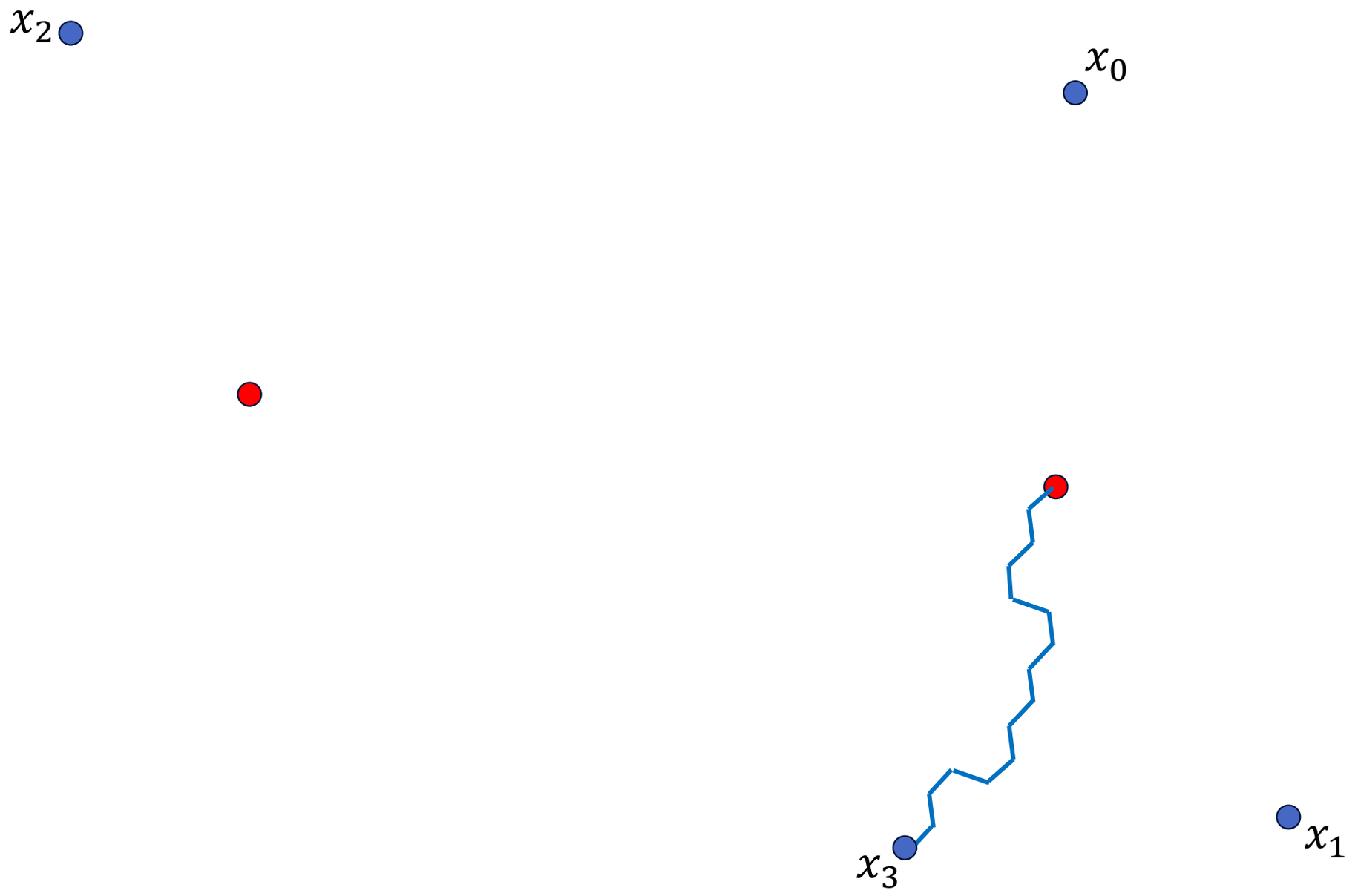
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



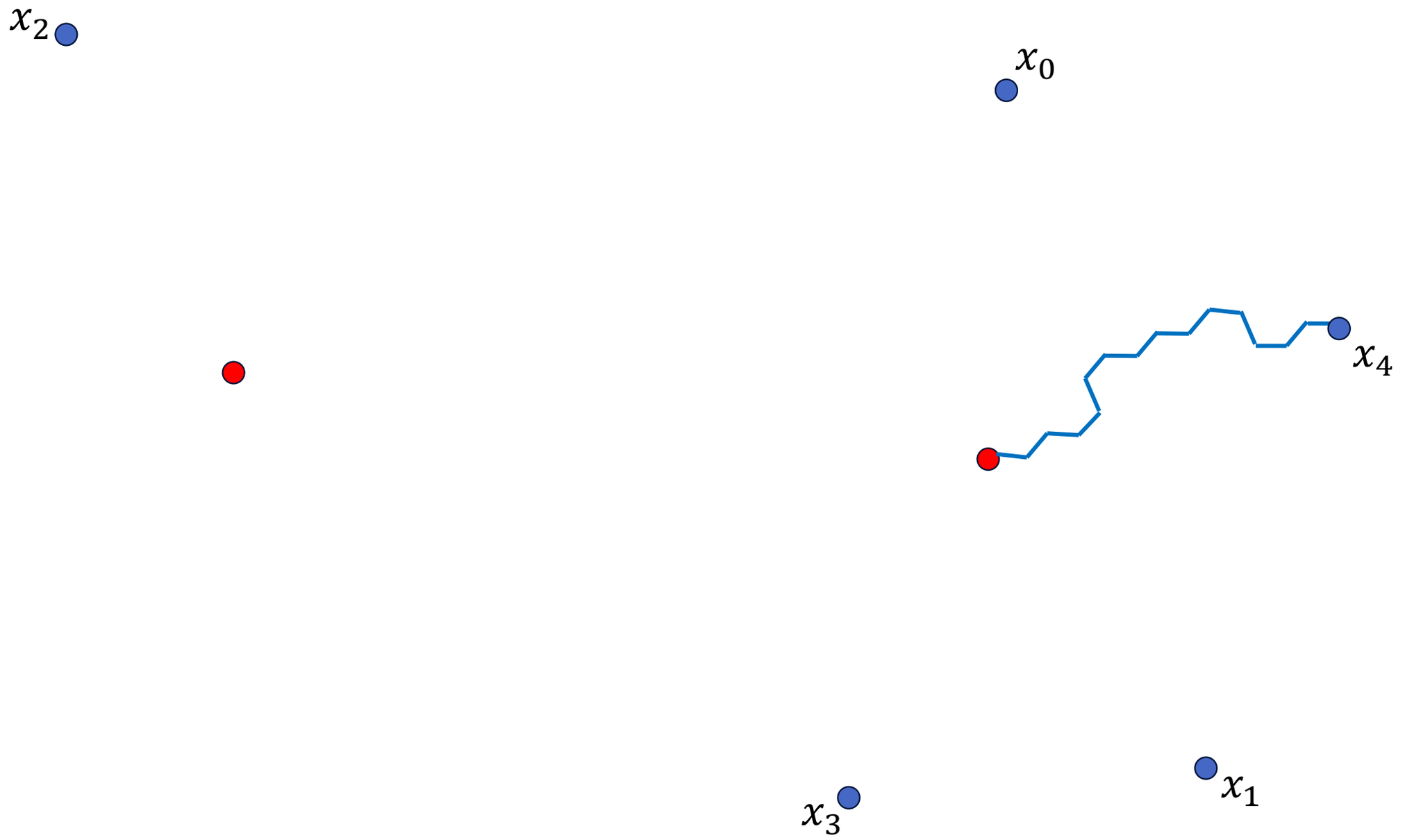
x_0

x_1

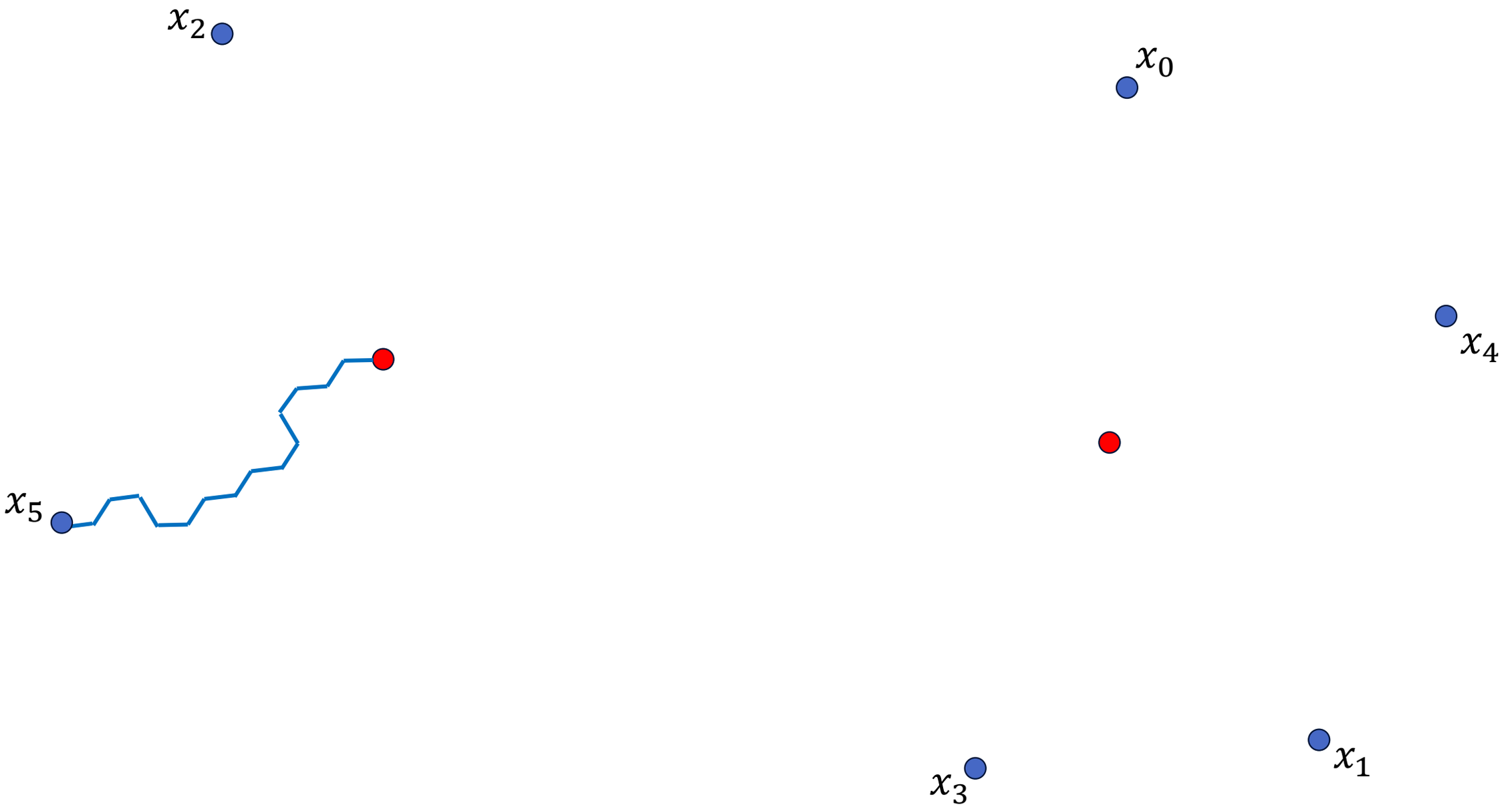
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



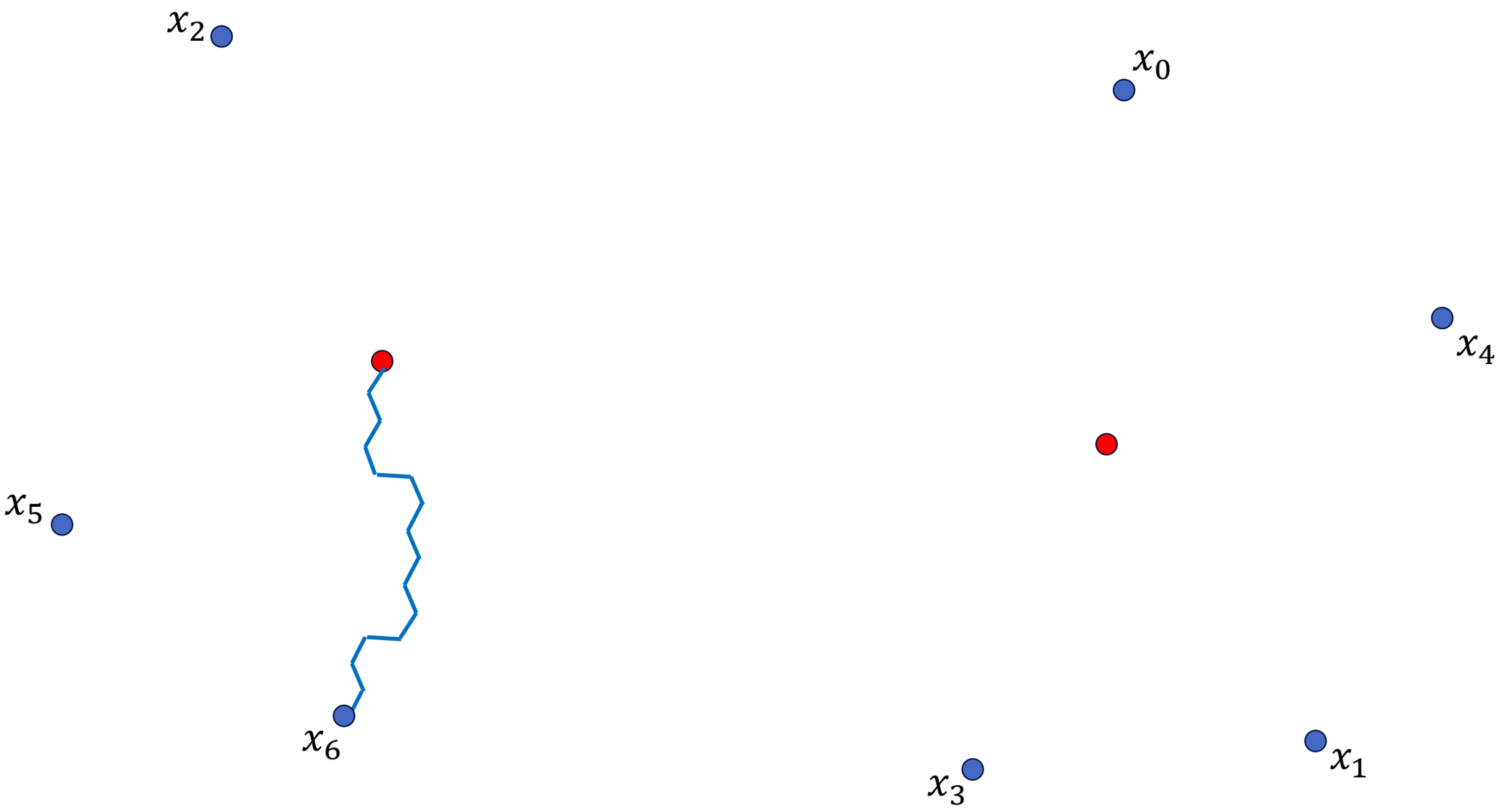
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



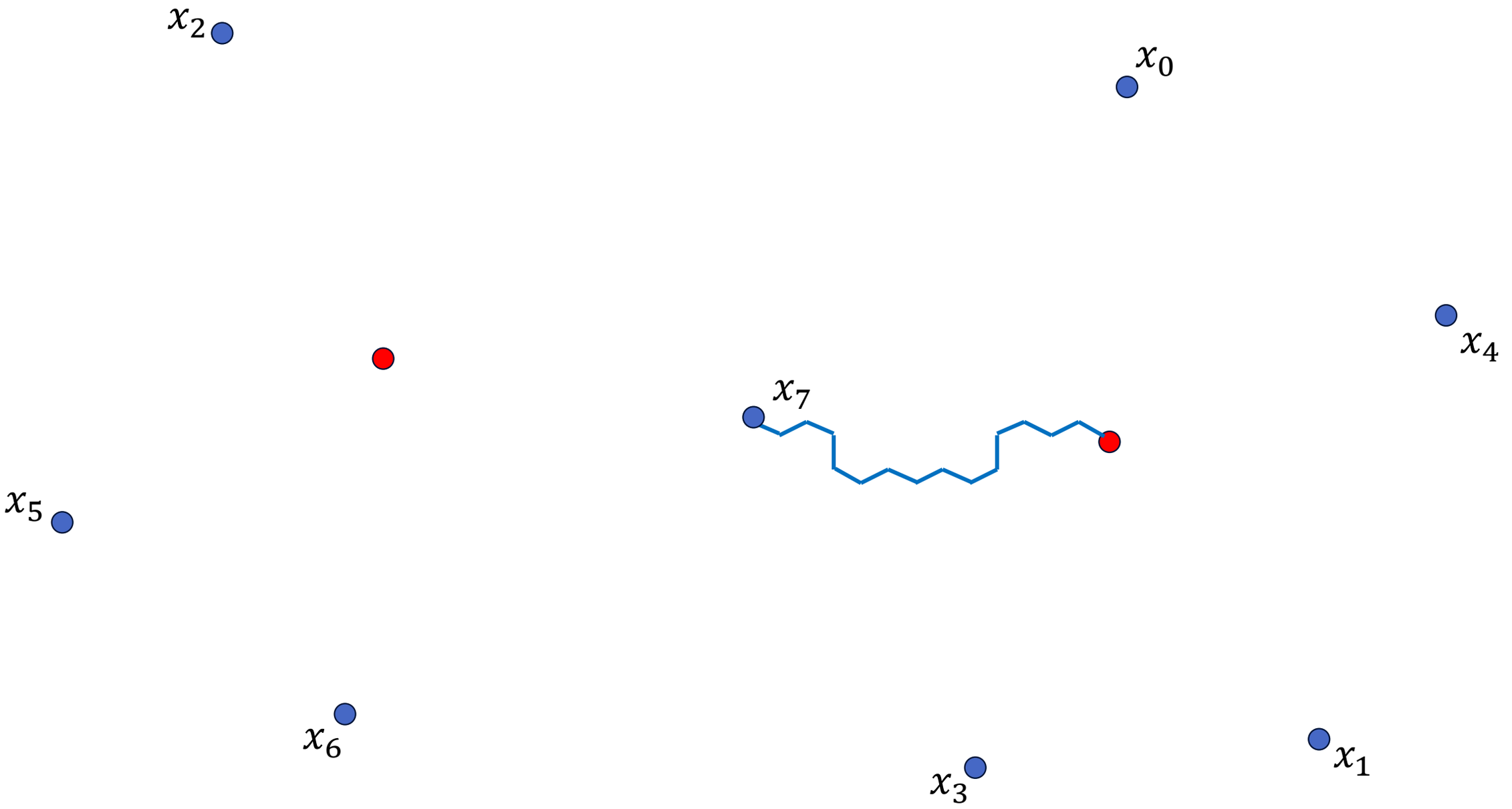
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



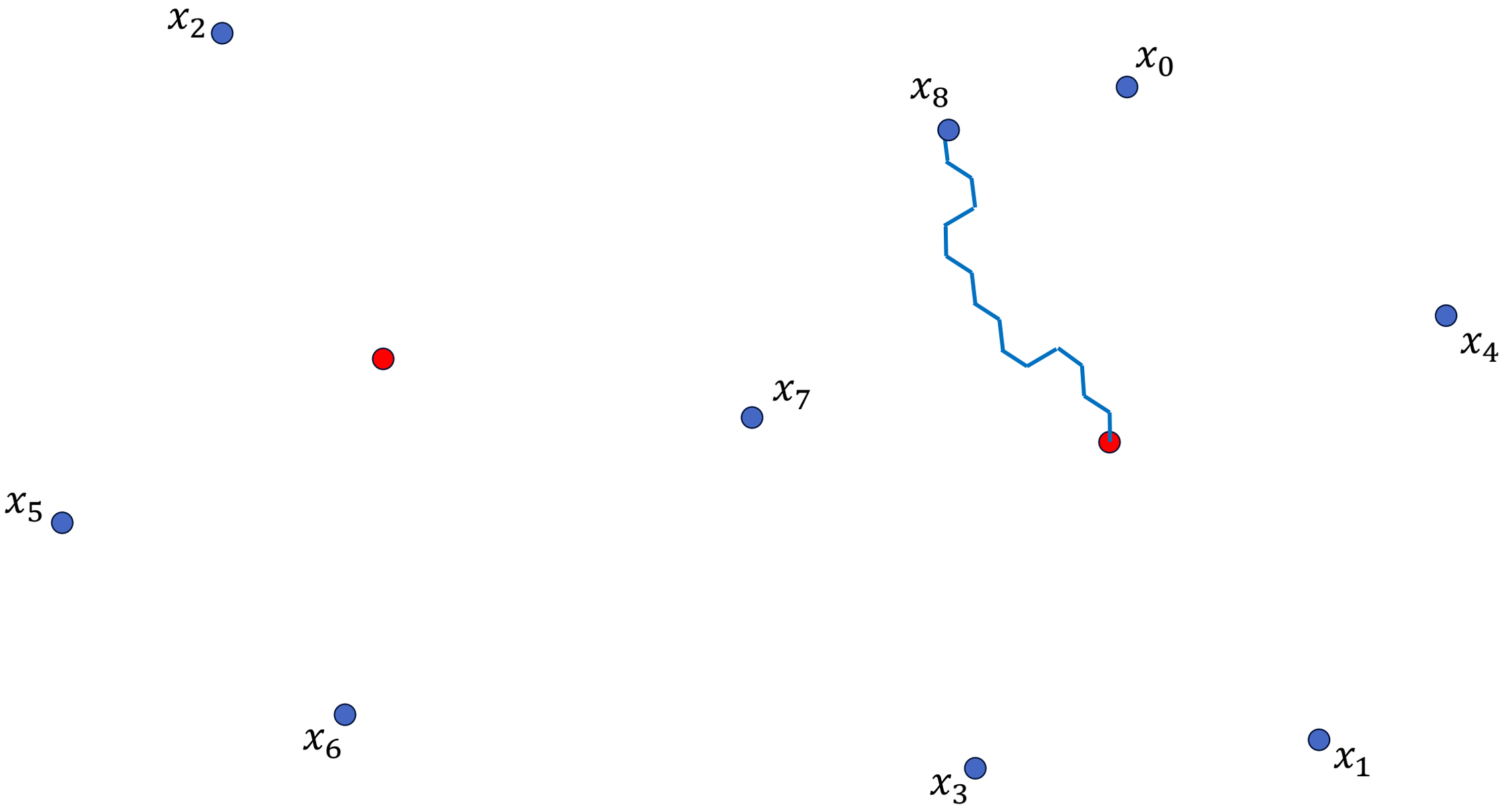
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



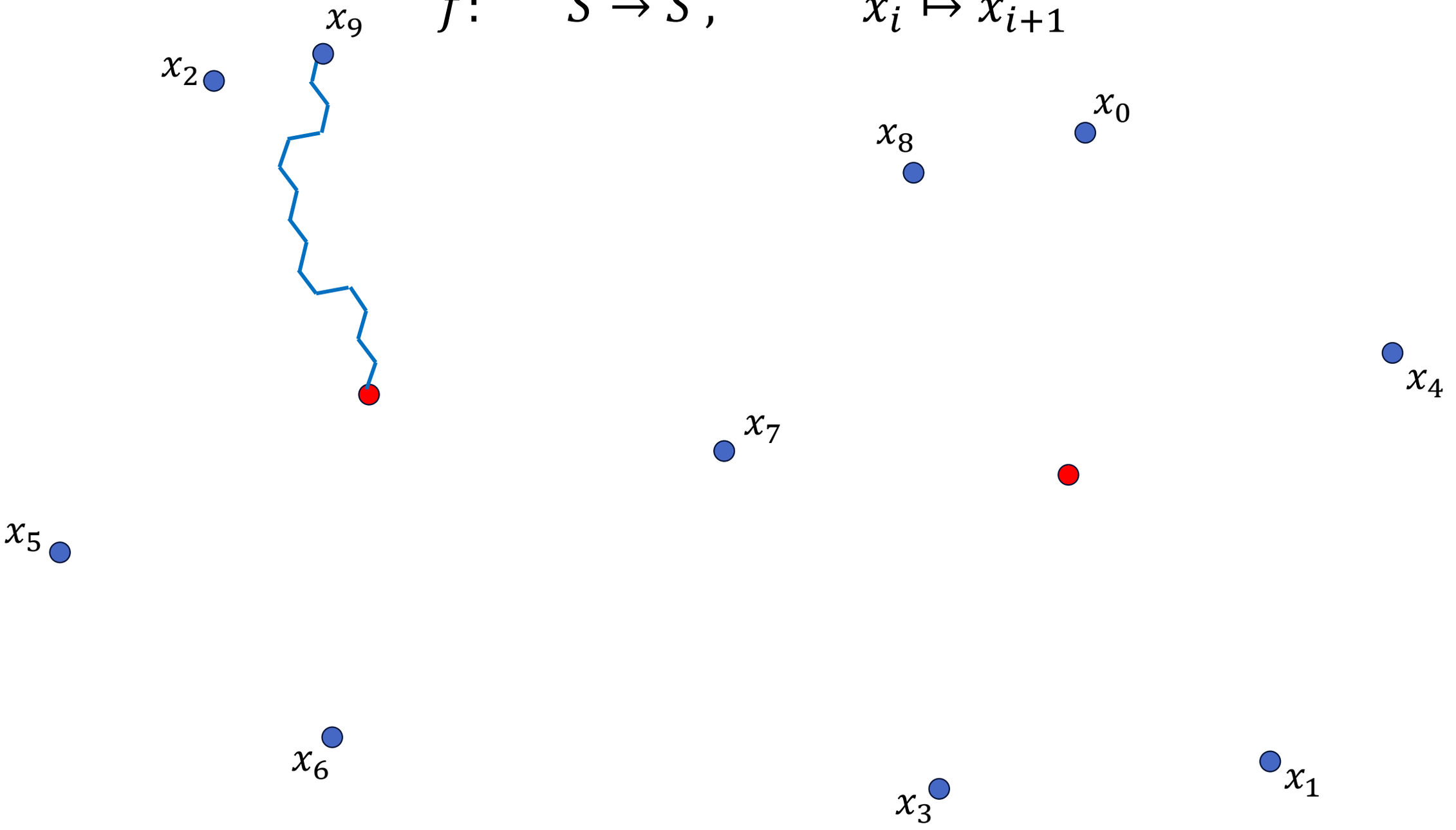
$$f: \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$$



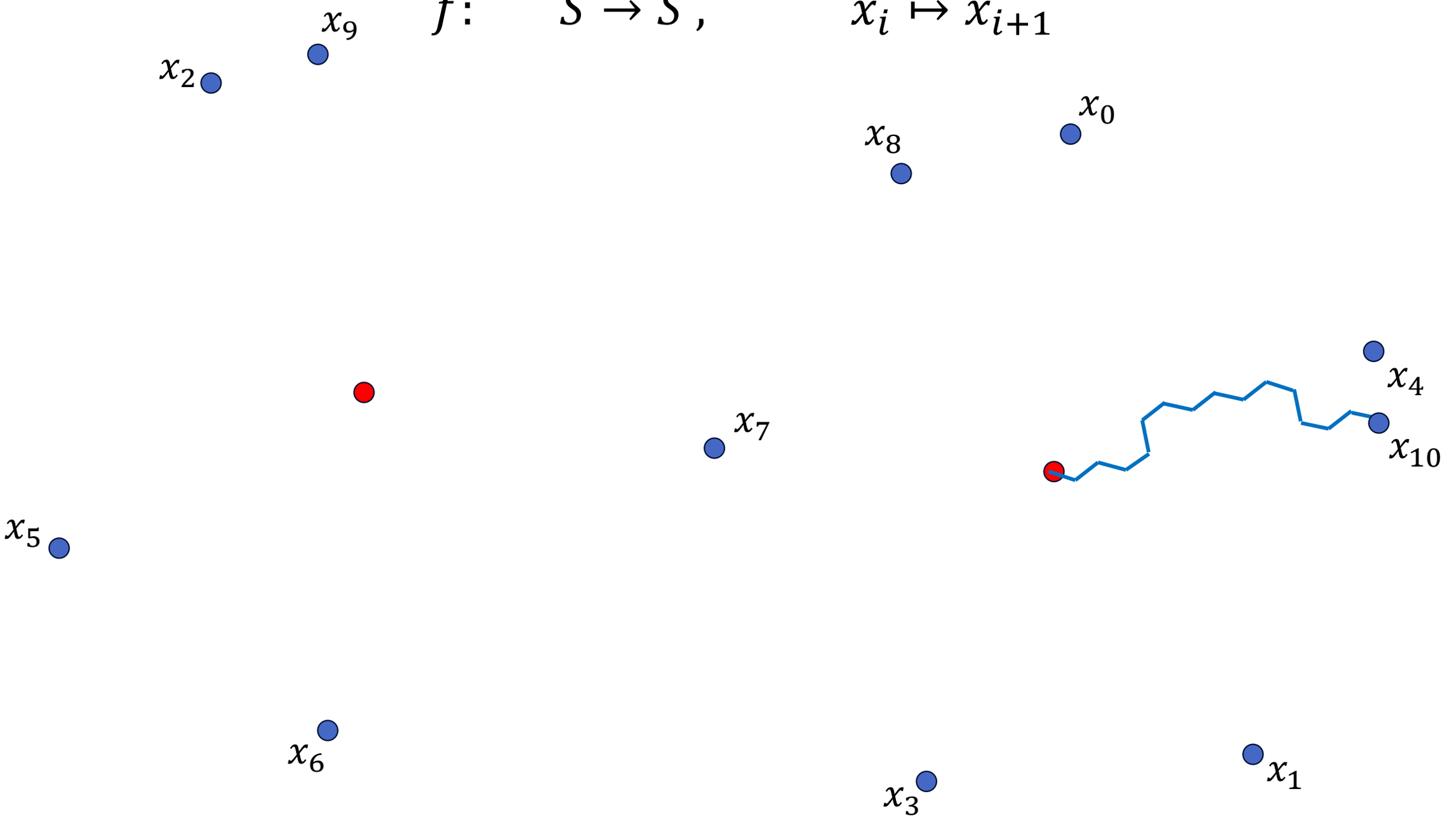
$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



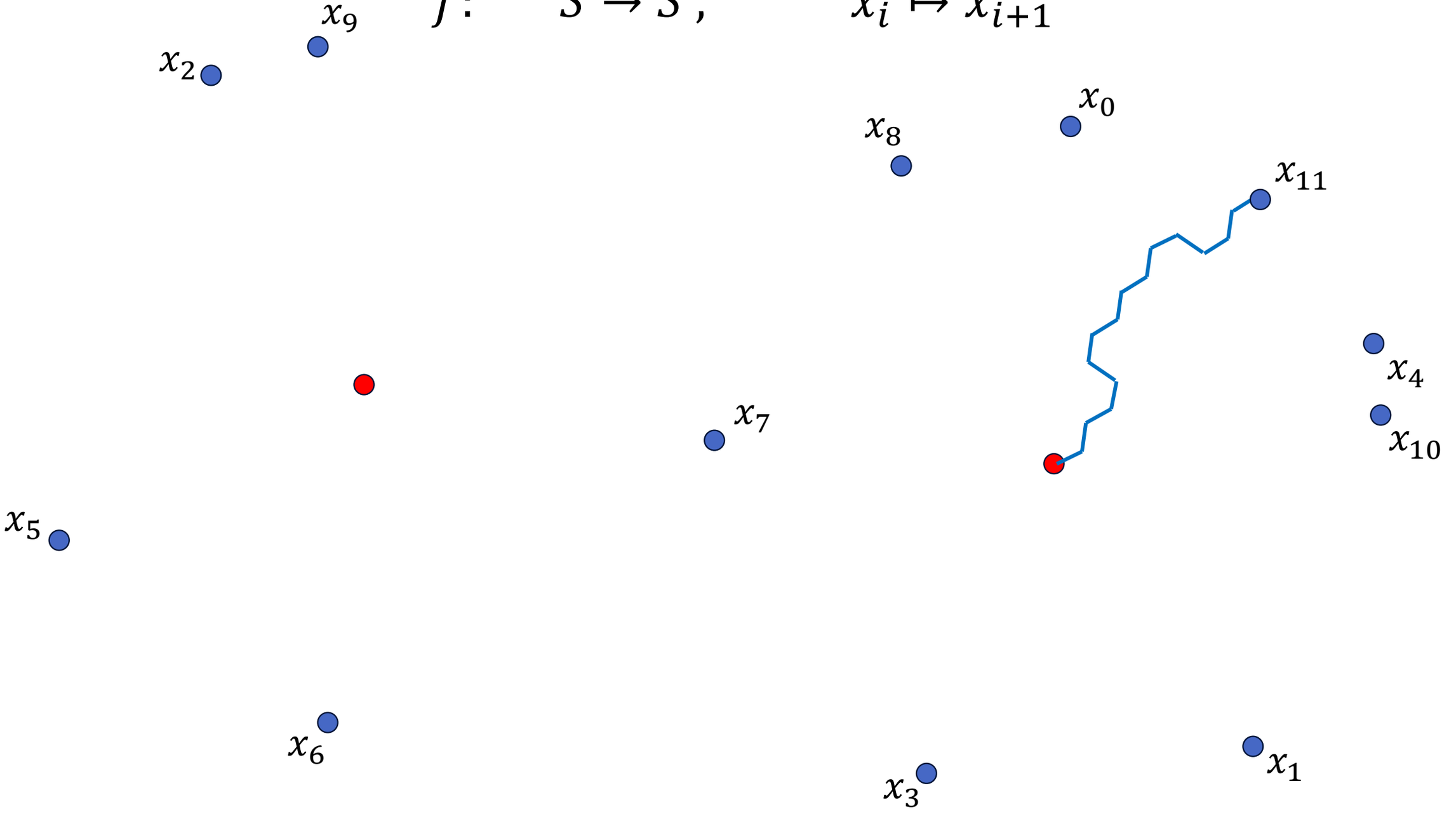
$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



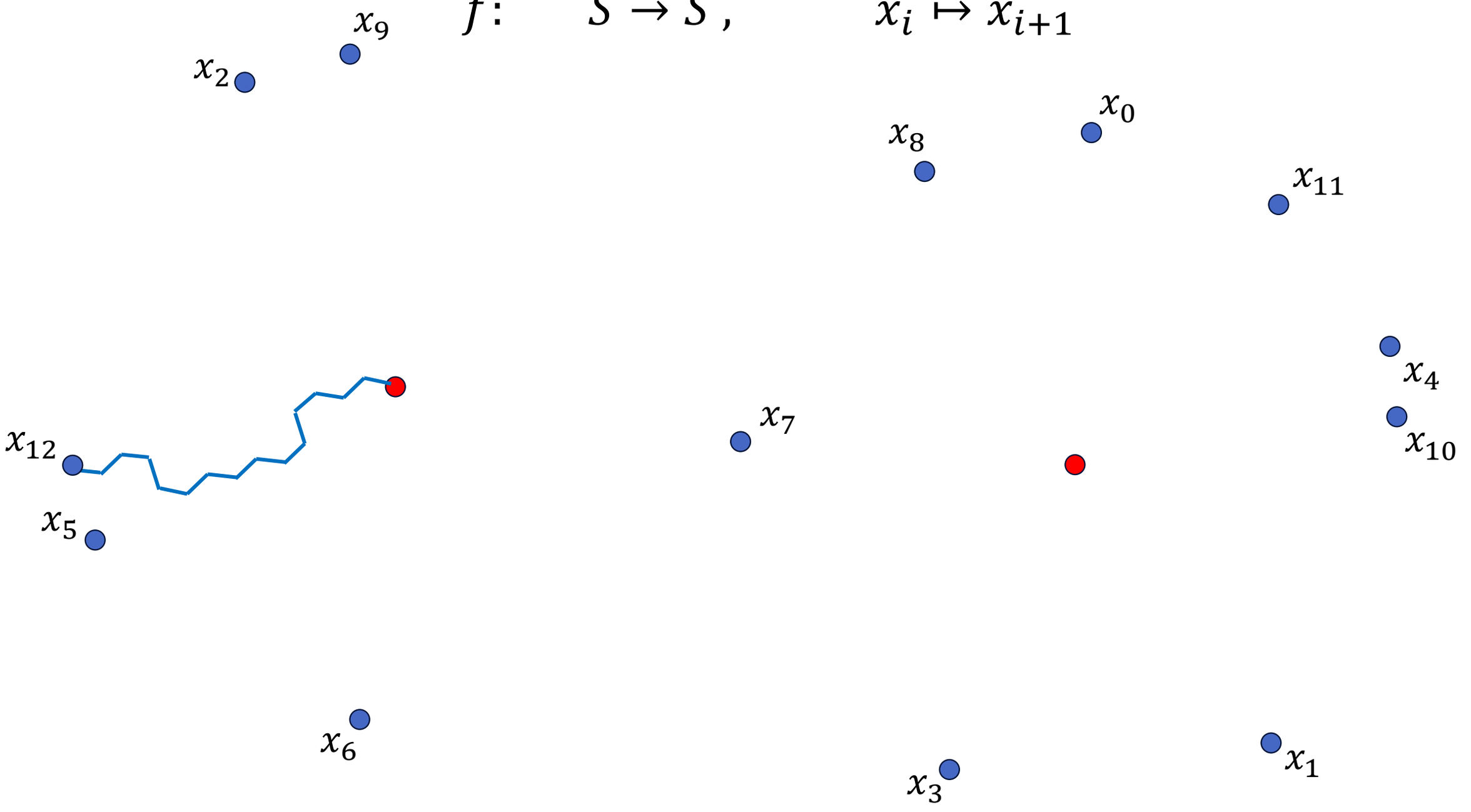
$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



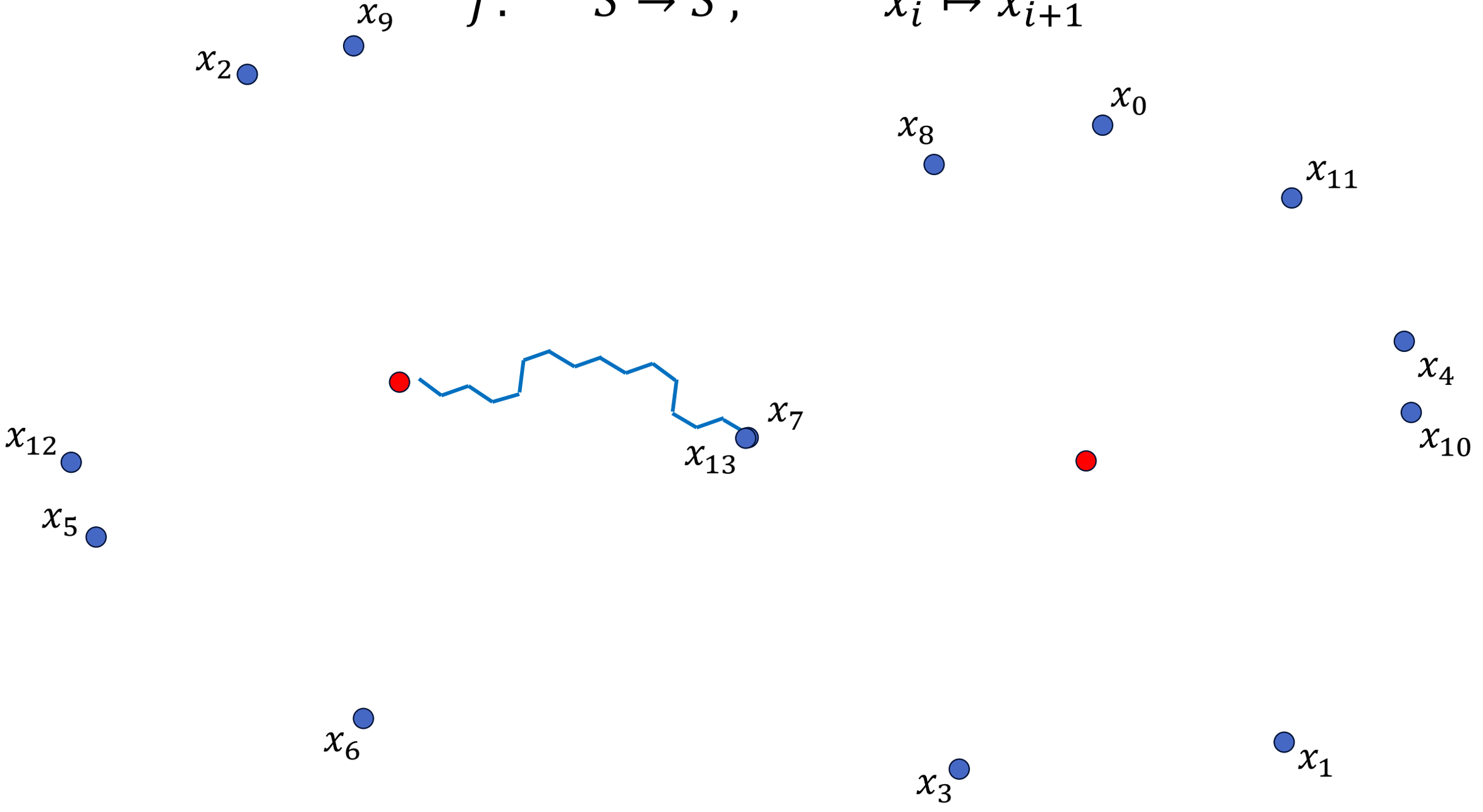
$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



$f\colon \quad S \to S\,, \qquad x_i \mapsto x_{i+1}$



$$f: \quad S \to S, \qquad x_i \mapsto x_{i+1}$$

x_9

x_2

x_0

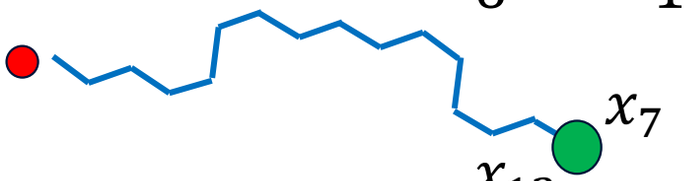
x_8

x_{11}

FOUND!!!

$$f(x_6) = f(x_{12})$$

$$x_6 \neq x_{12}$$



x_7

x_{13}

x_4

x_{10}

x_{12}

x_5

x_6

x_3

x_1

Two problems…

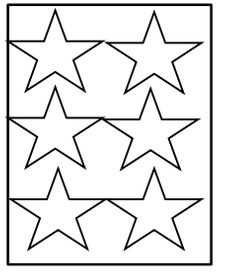
- We can't store all the x_i (otherwise MitM fastest)
- A random function $f : S \to S$ has many more collisions…

Two problems…

- We can't store all the x_i (otherwise MitM fastest)
- A random function $f : S \to S$ has many more collisions… $O(|S|)$ more!!!

There's only one we want: the "golden collision"

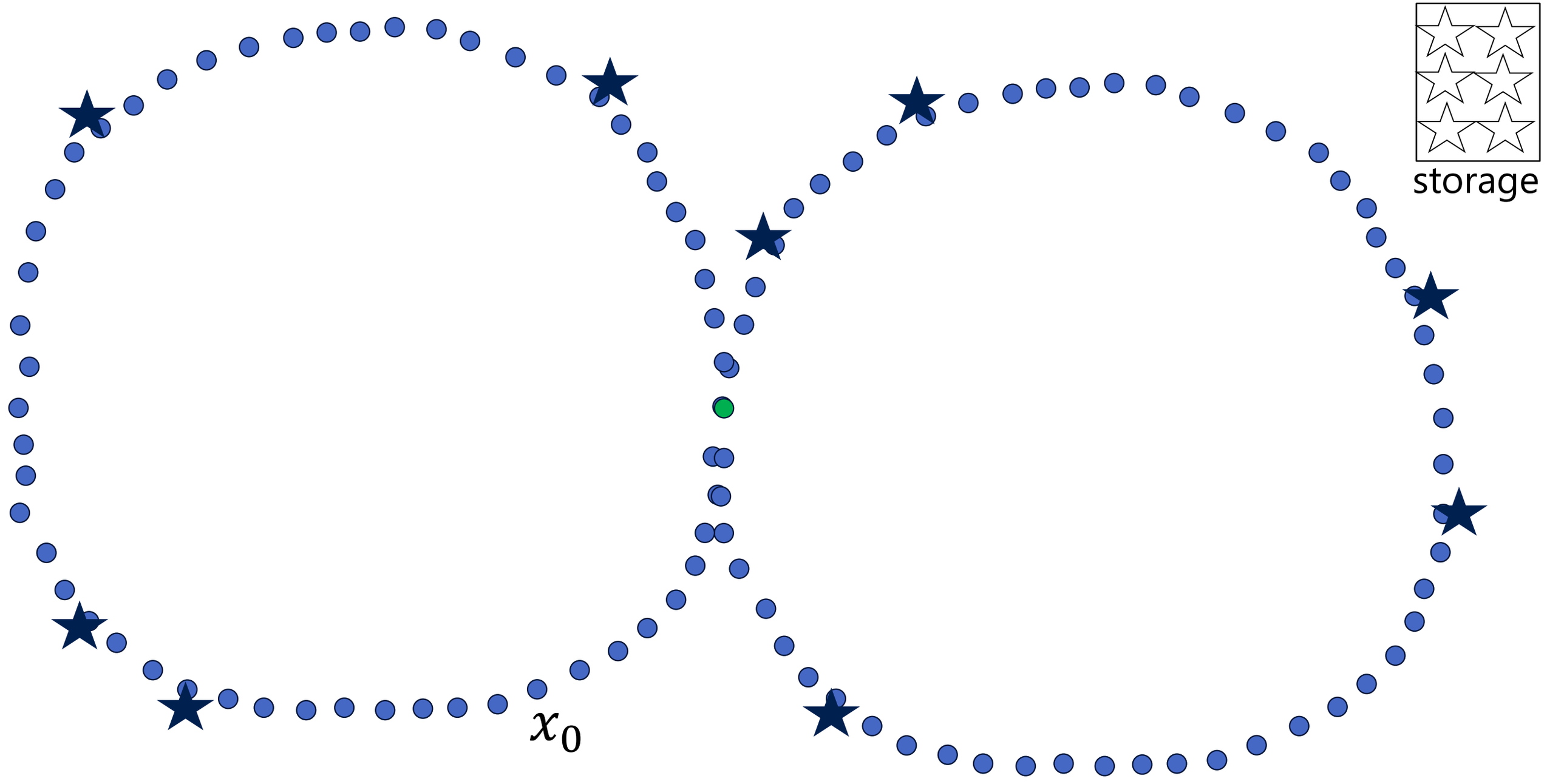
can’t possibly store all these: fix $\boldsymbol{w}$ as upper bound on $\#x_i$ storage (e.g. $\boldsymbol{w = 2^{80}}$)



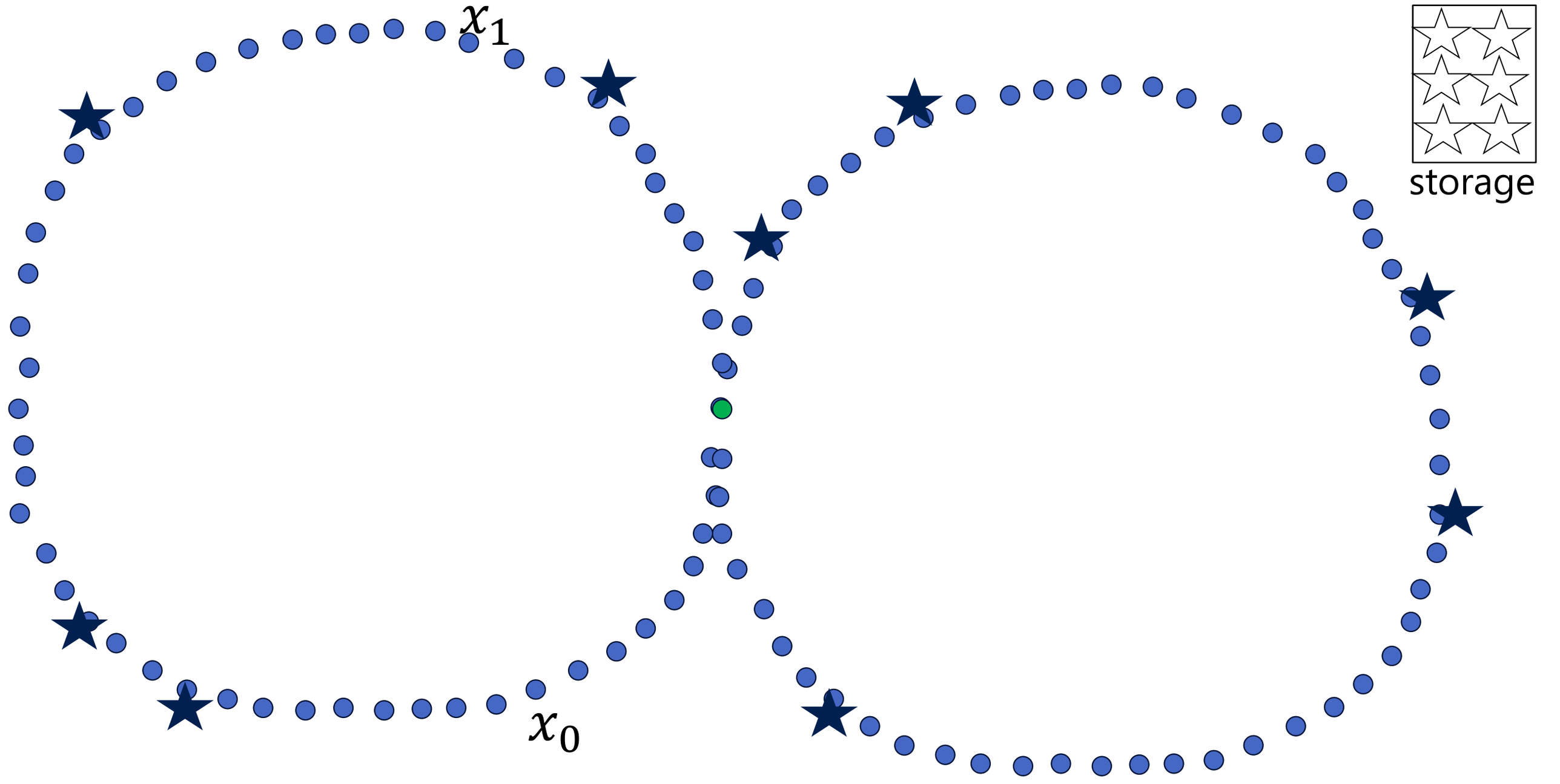
storage

store fraction $0 < \theta \ll 1$ (e.g. $\boldsymbol{\theta = 2^{-30}}$)

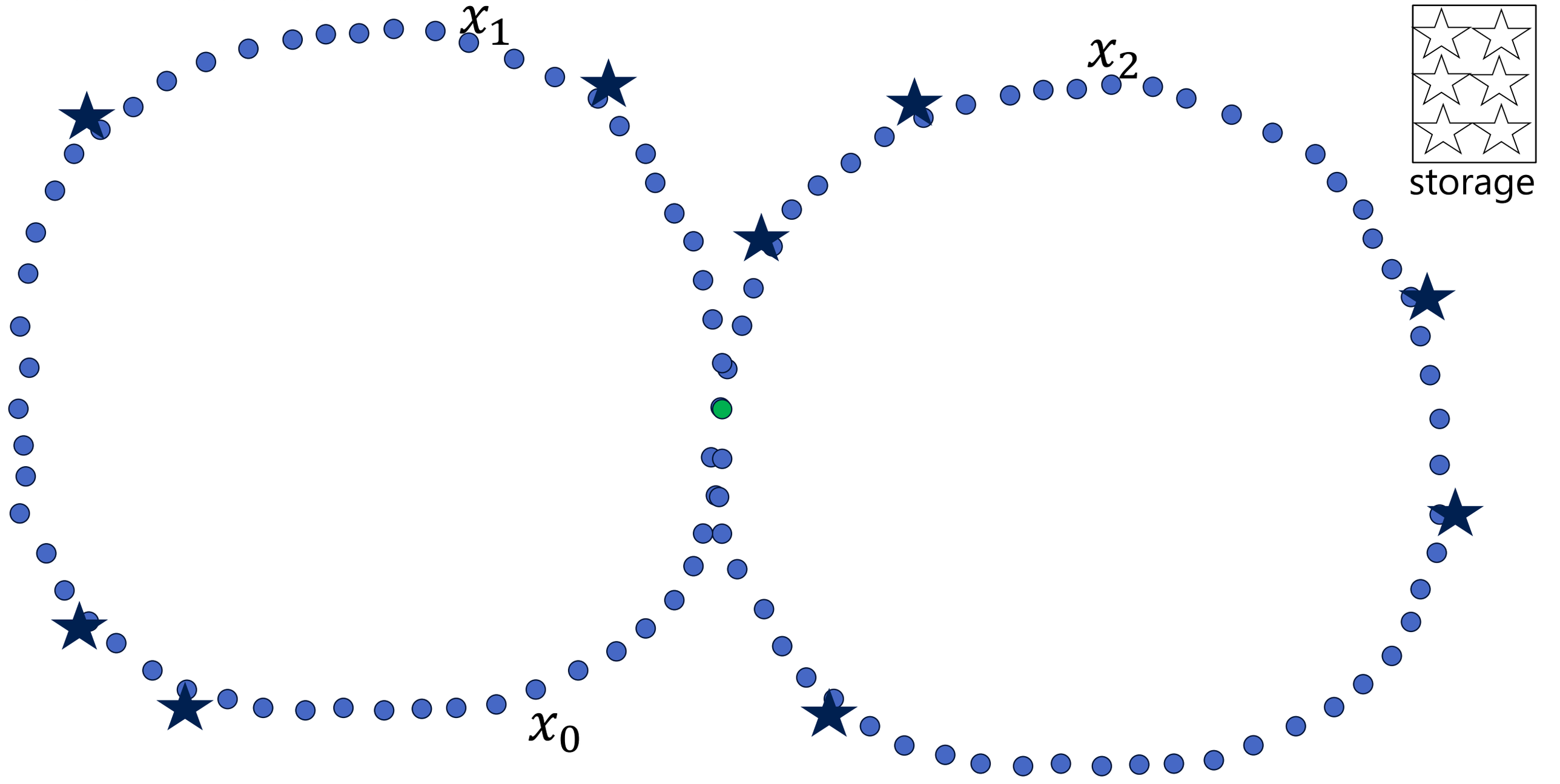
vOW cont…



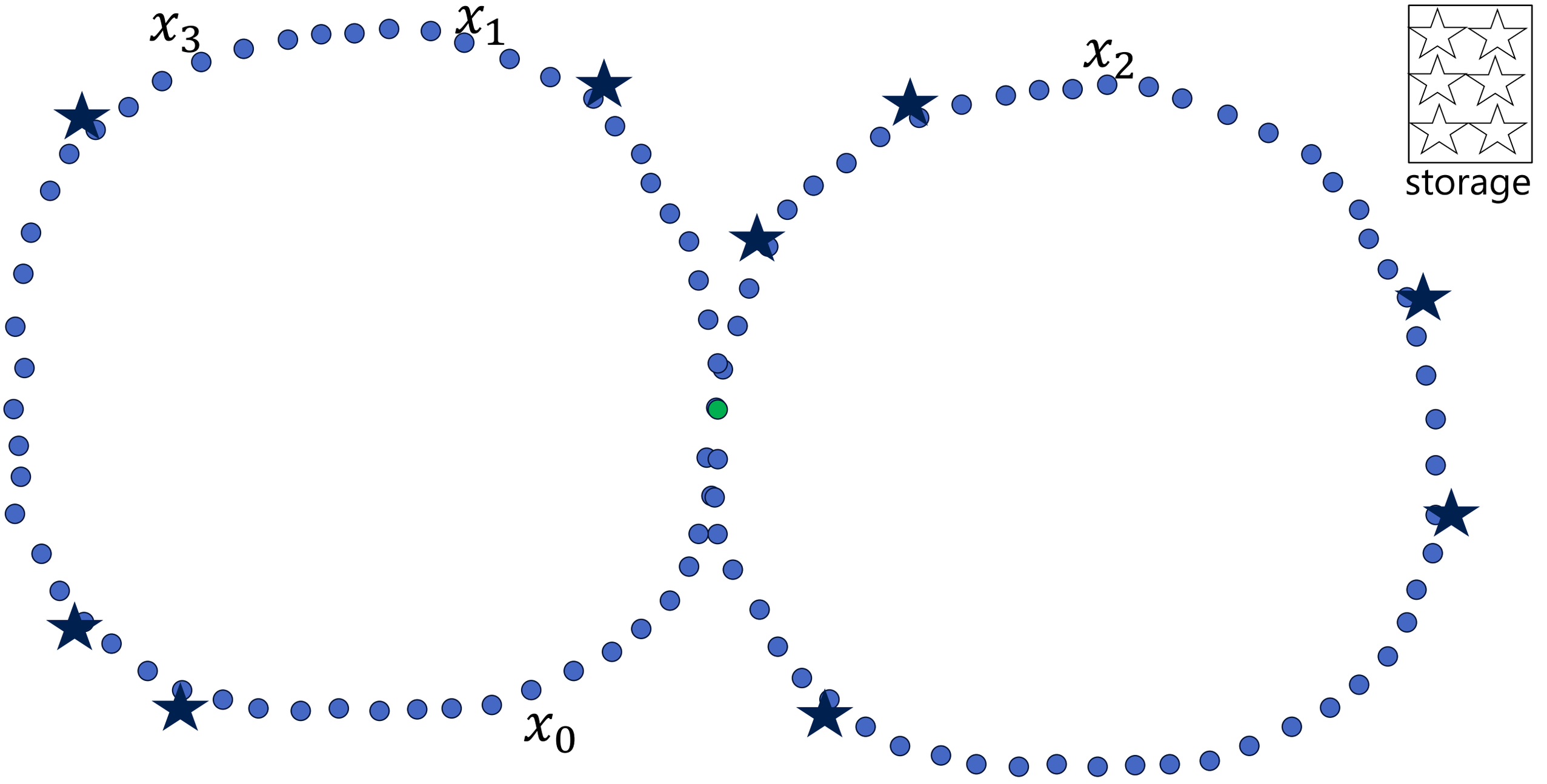
vOW cont…



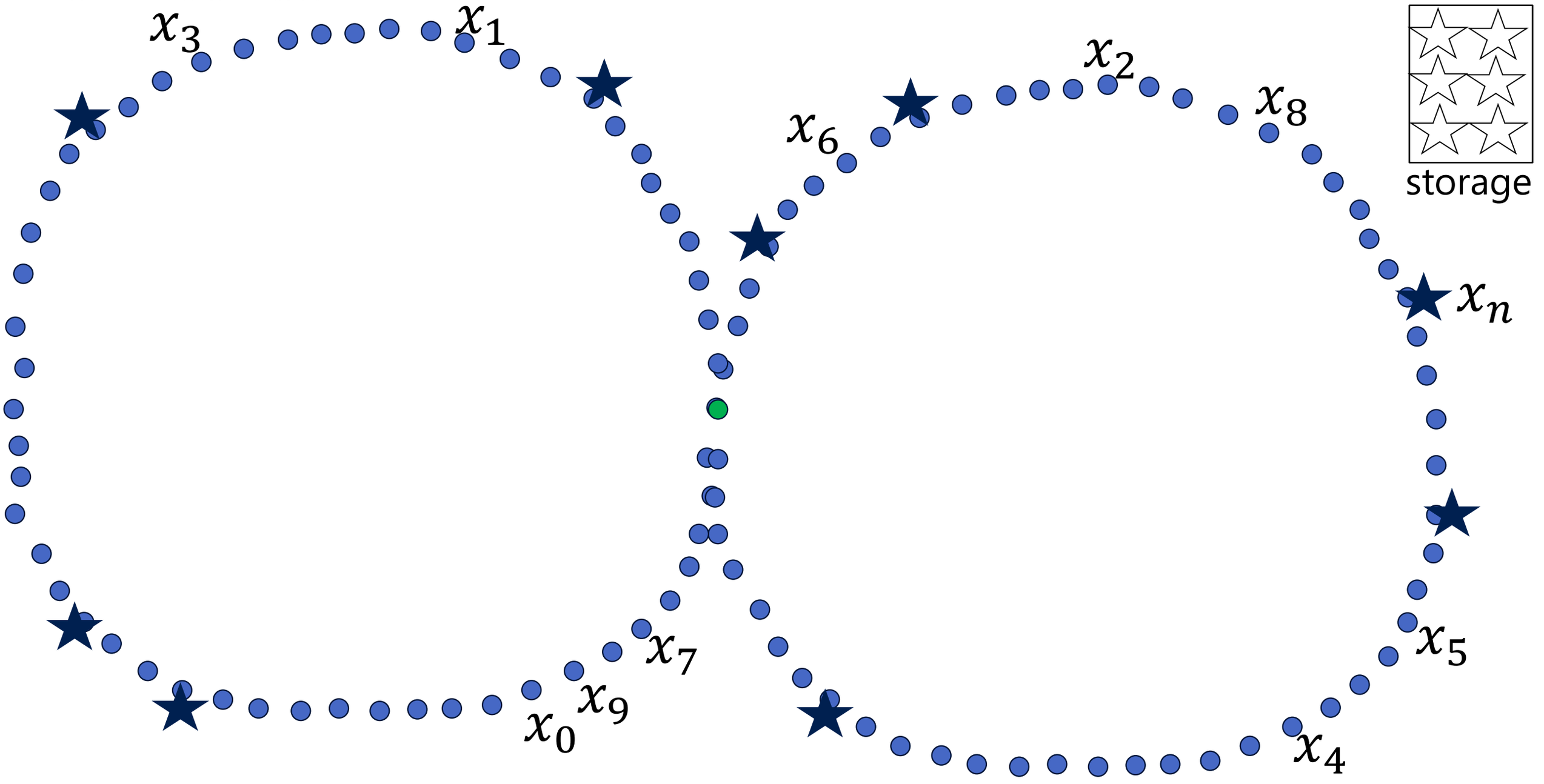
vOW cont…



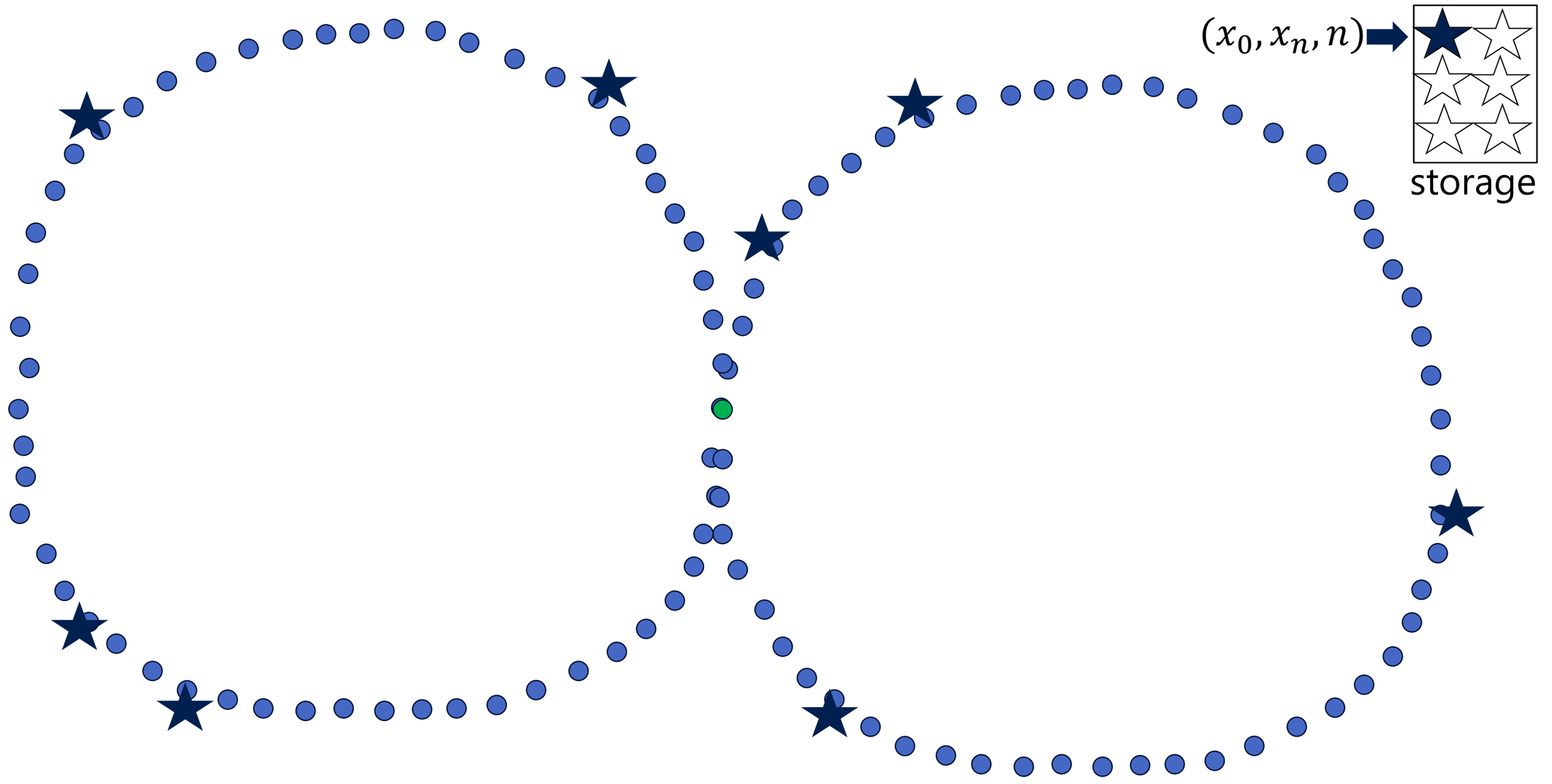
vOW cont…



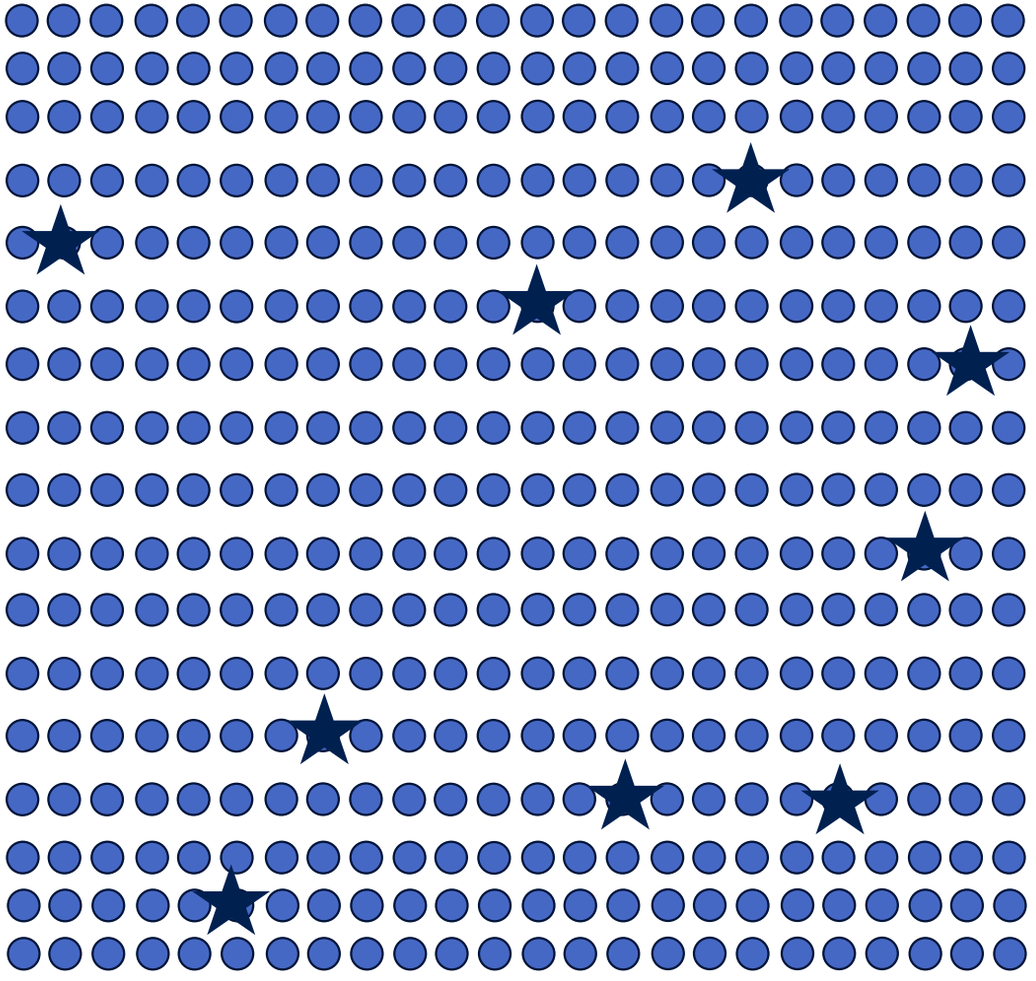
vOW cont…

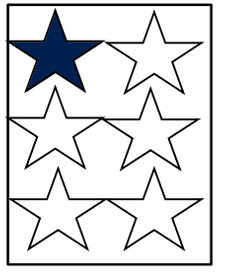


vOW cont…



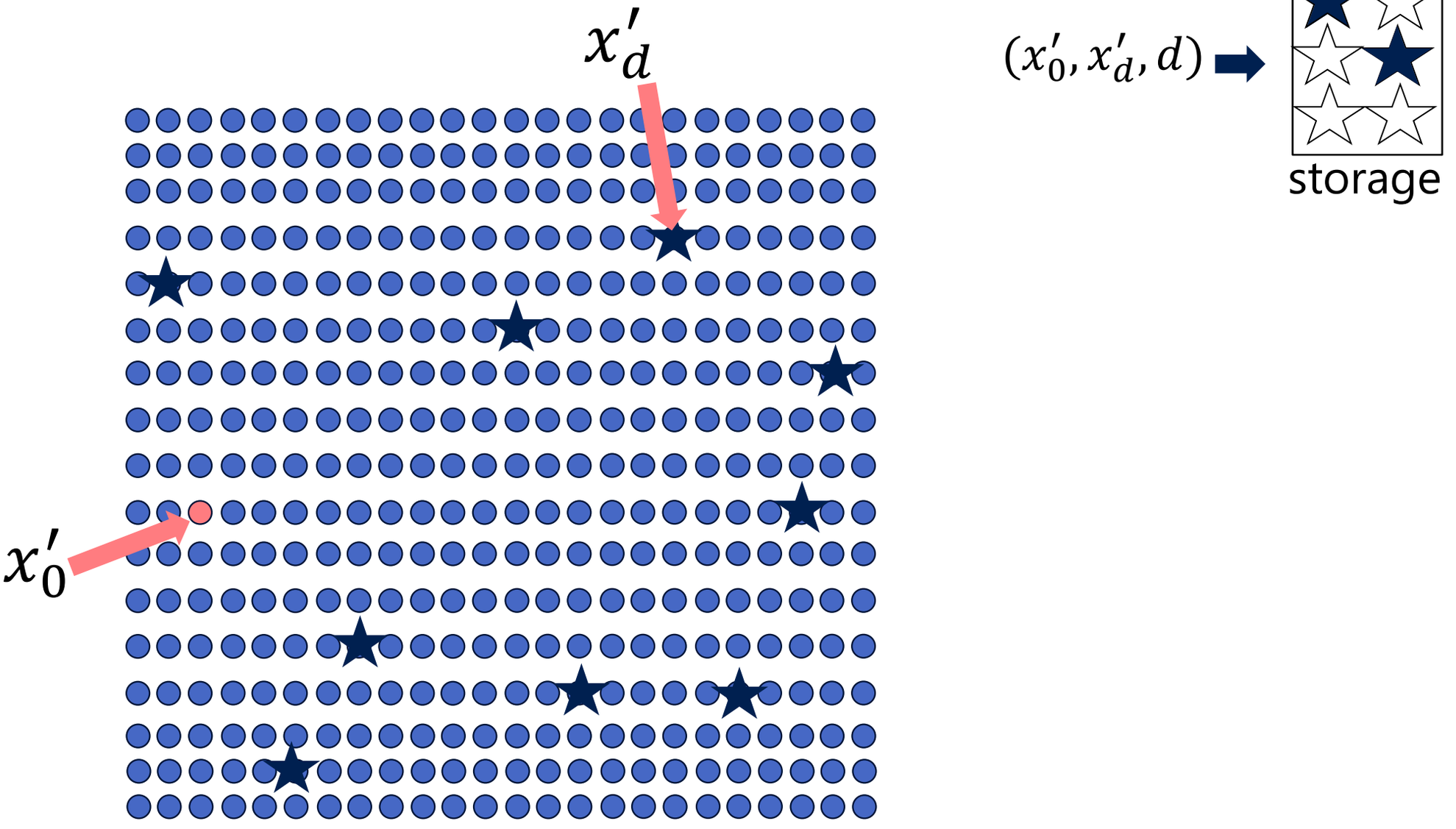
vOW cont…



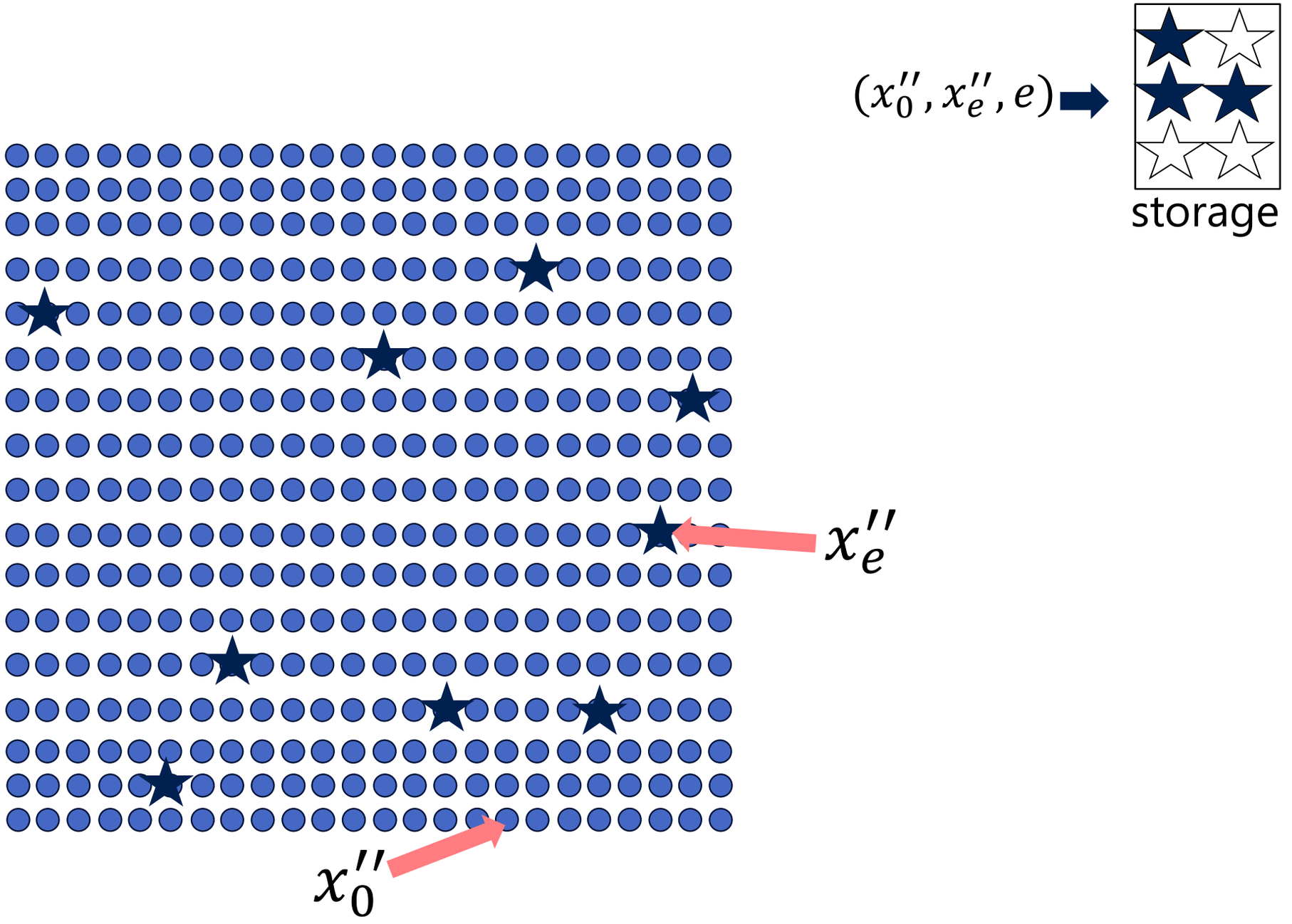


storage

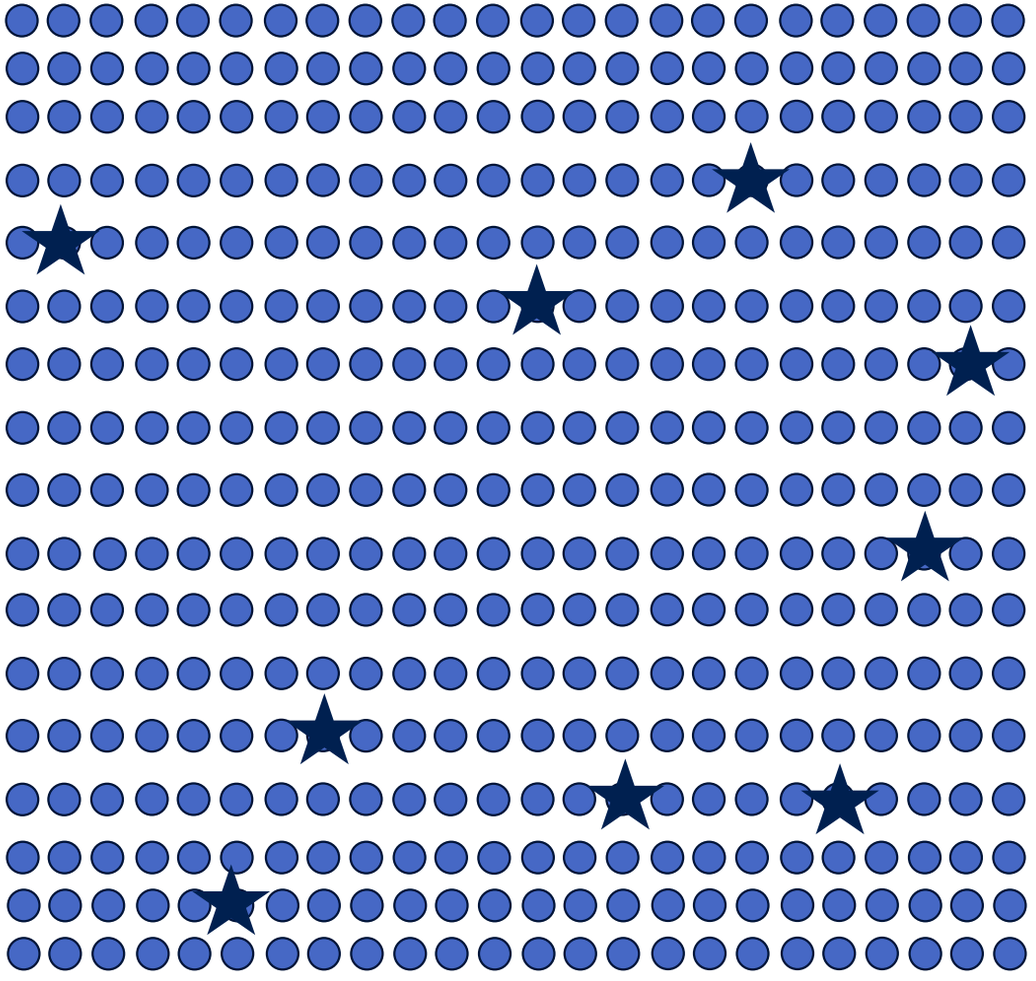
vOW cont…

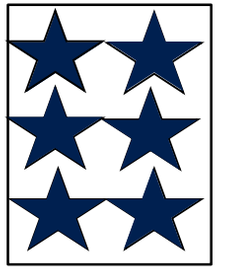


vOW cont…

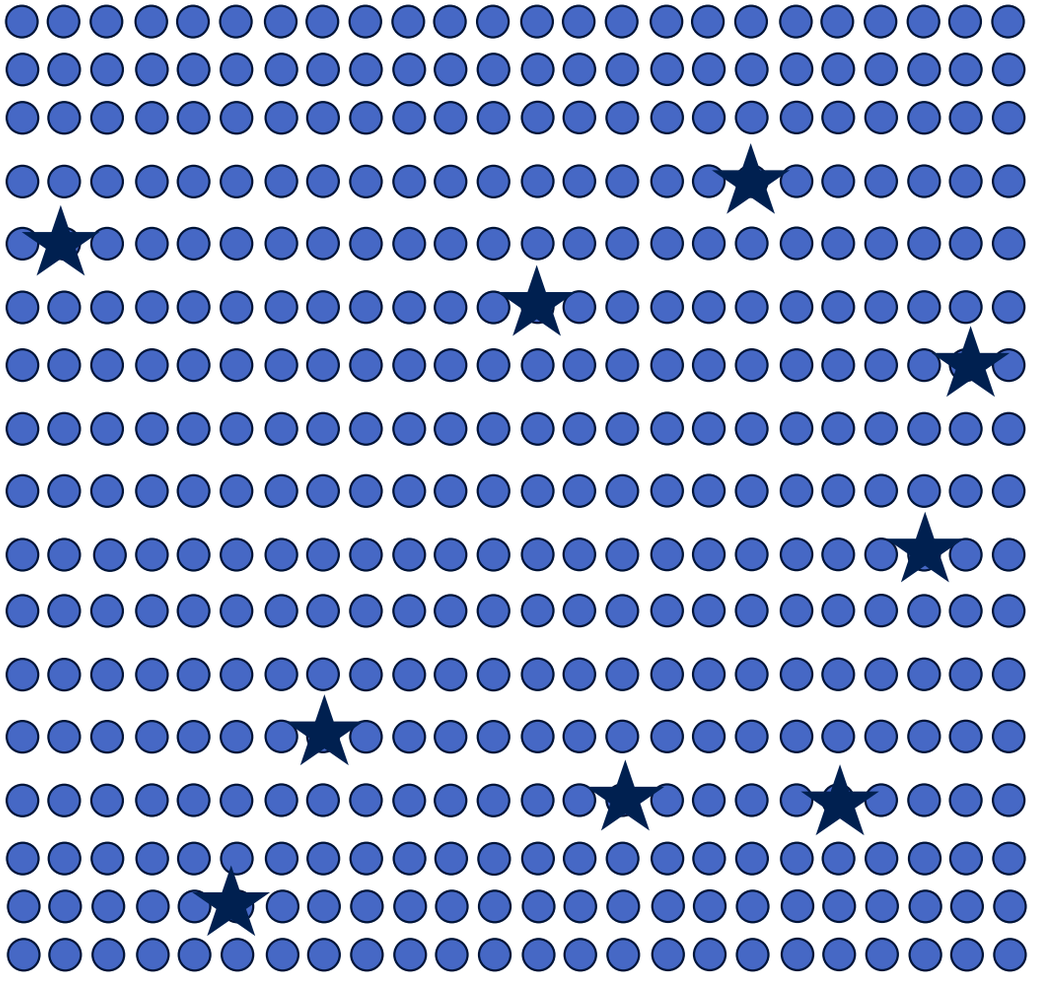


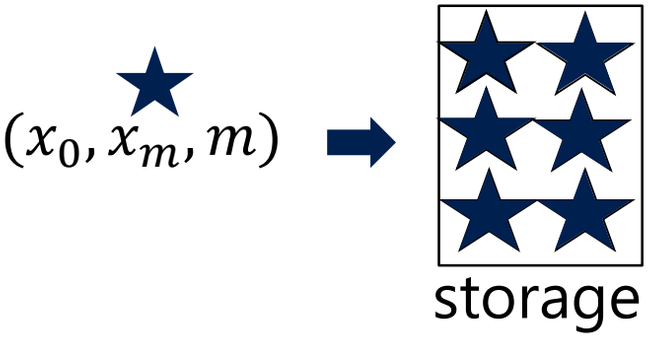
vOW cont…



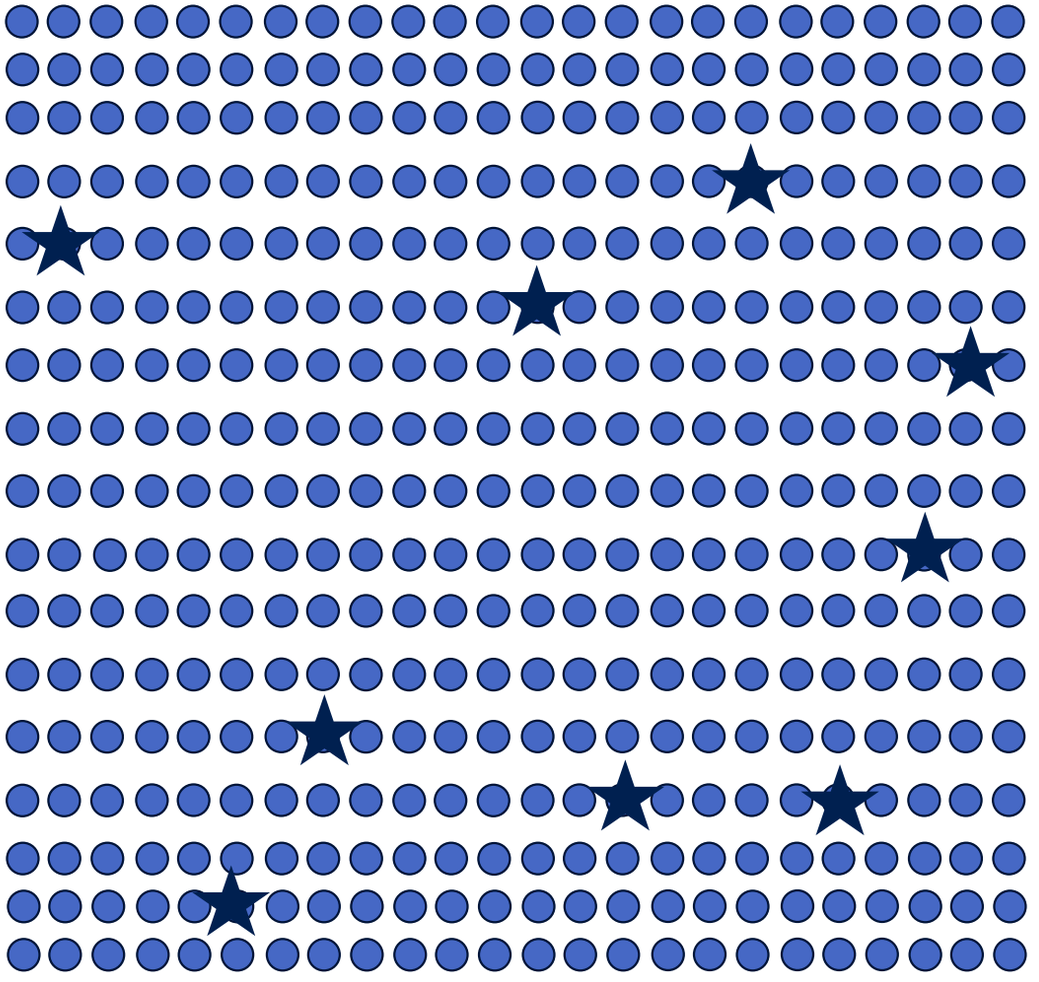


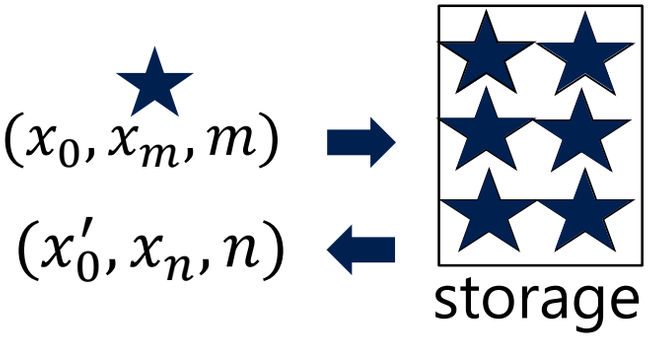
vOW cont…





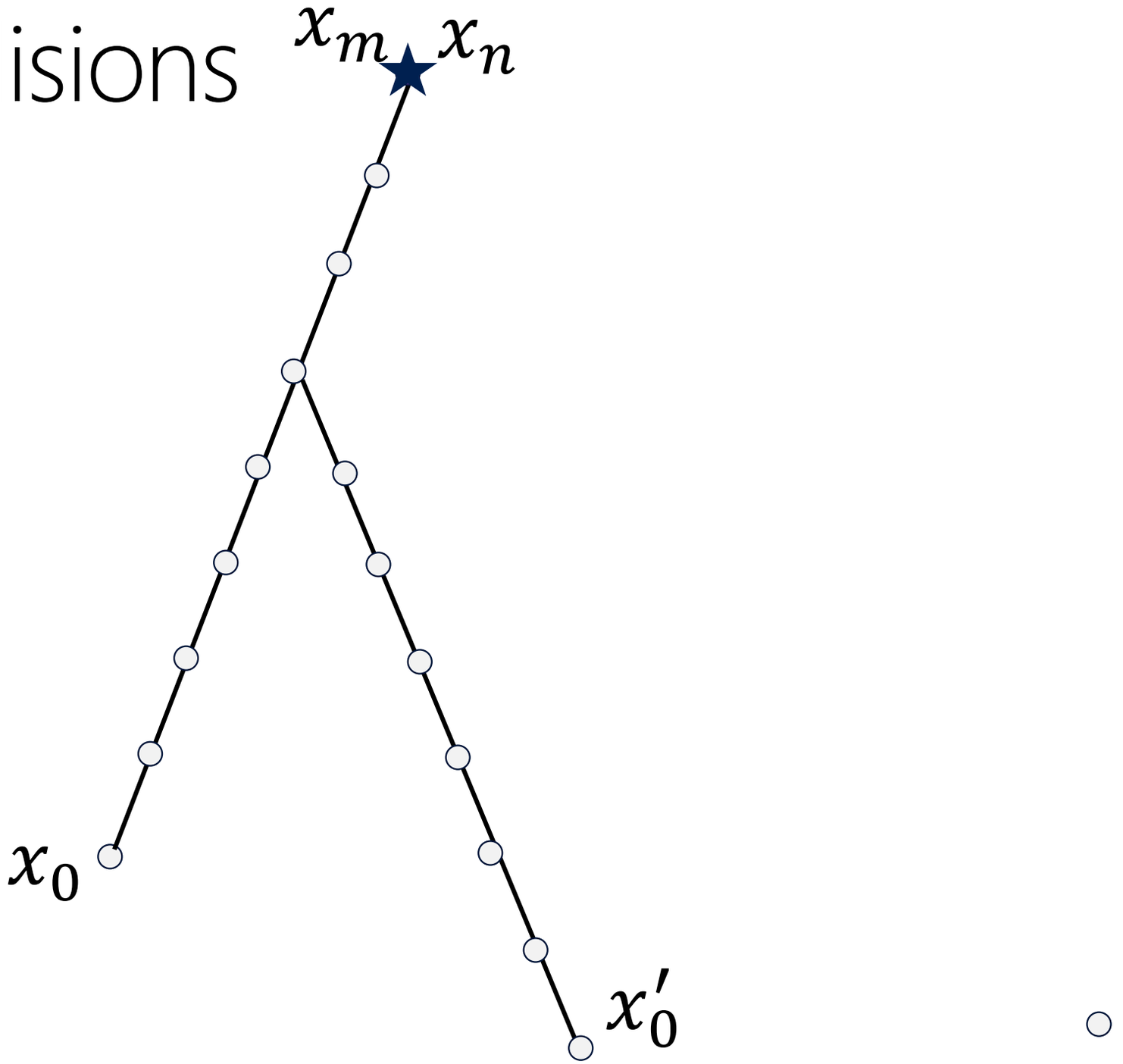
vOW cont…





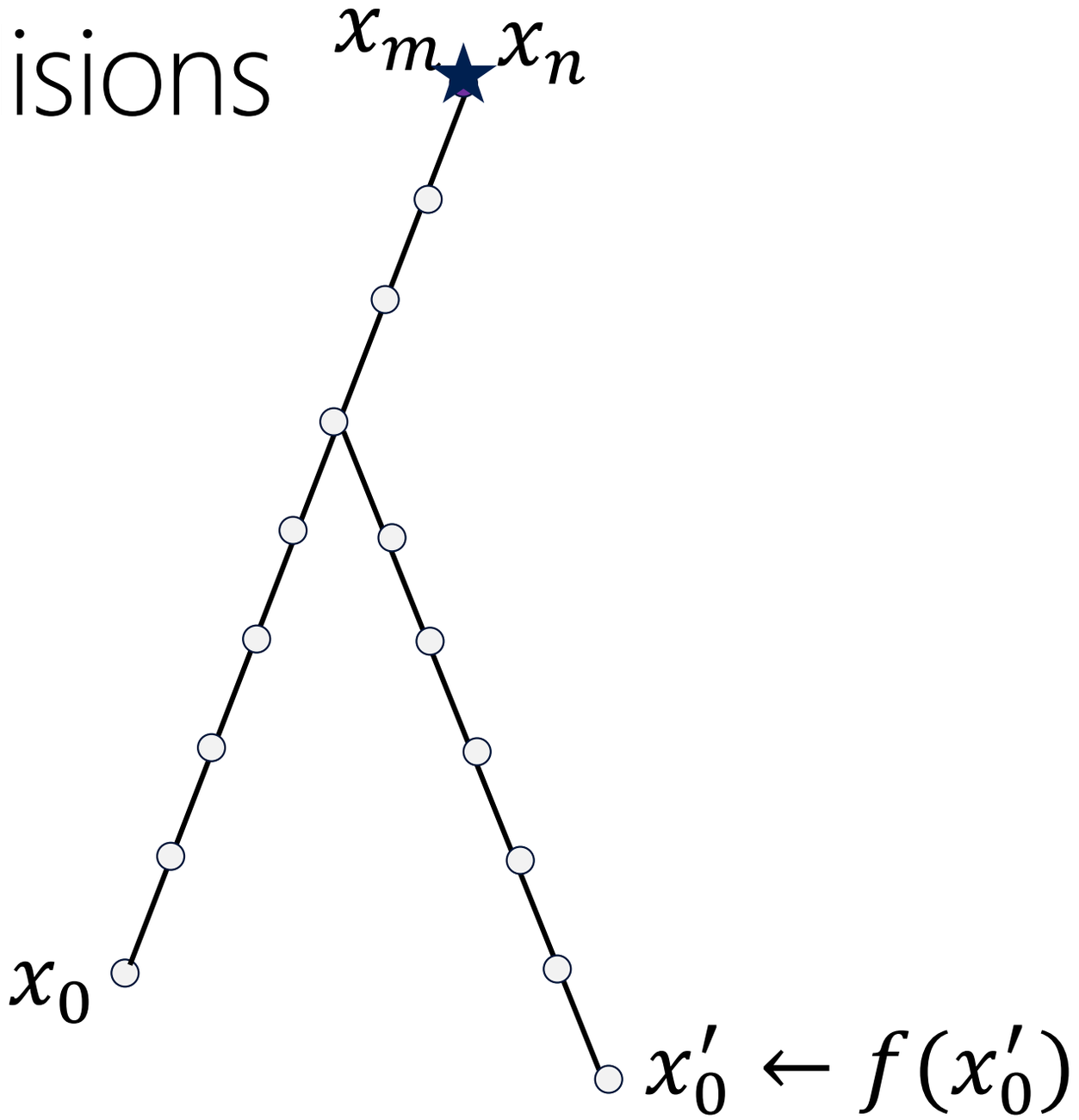
Checking collisions

memory
(x_0, x_m, m)
(x_0', x_n, n)



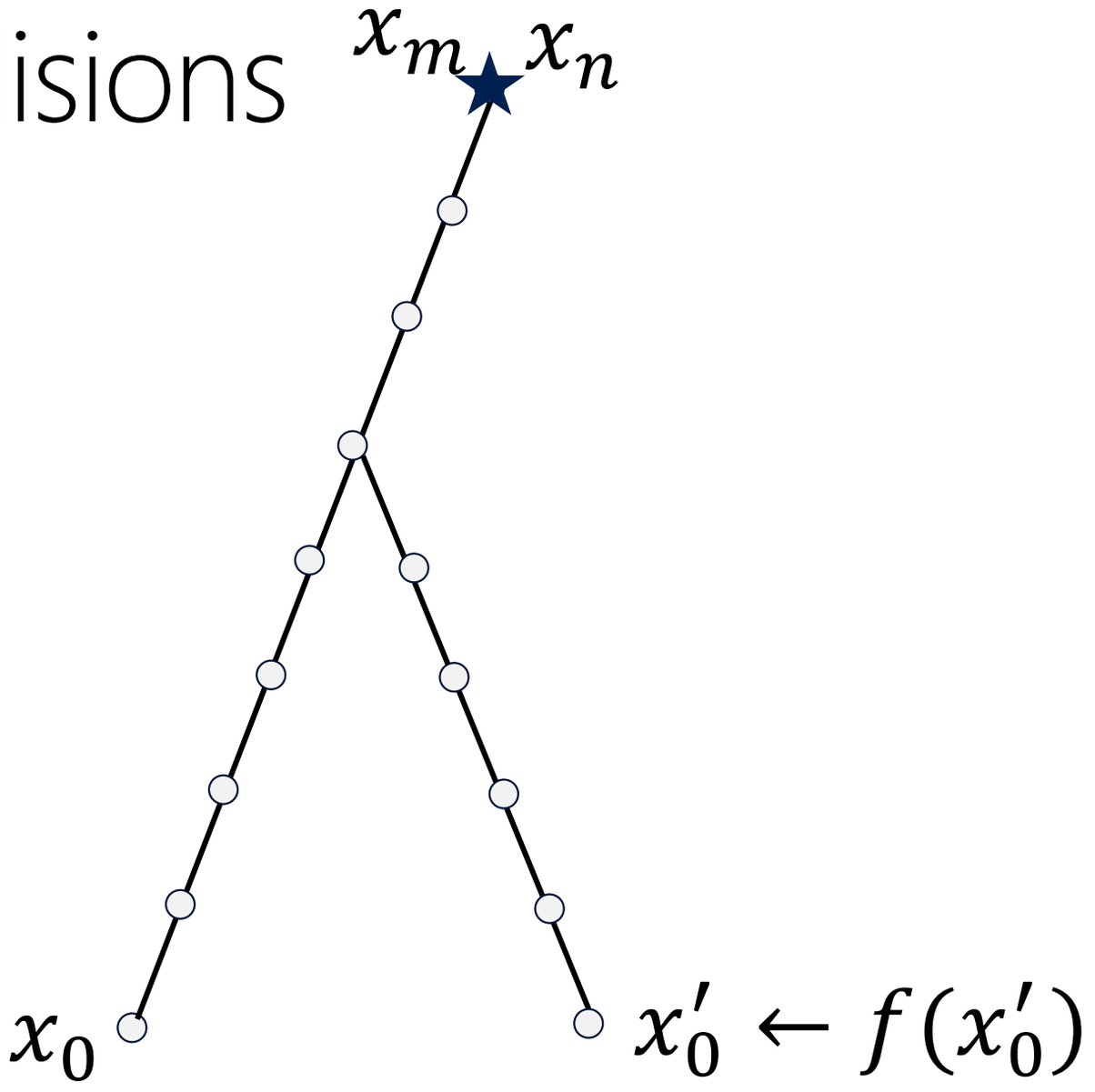
Checking collisions

memory
(x_0, x_m, m)
(x'_0, x_n, n)



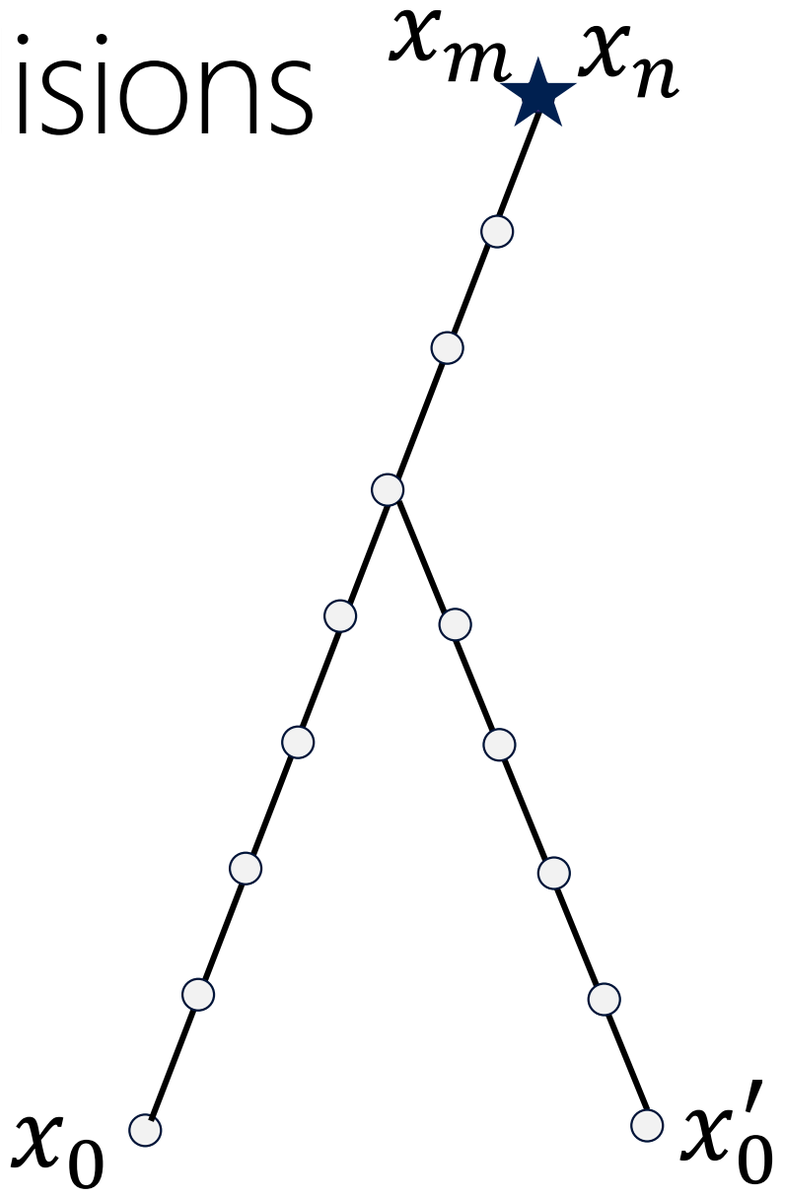
Checking collisions

memory
(x_0, x_m, m)
(x_0', x_n, n)



Checking collisions

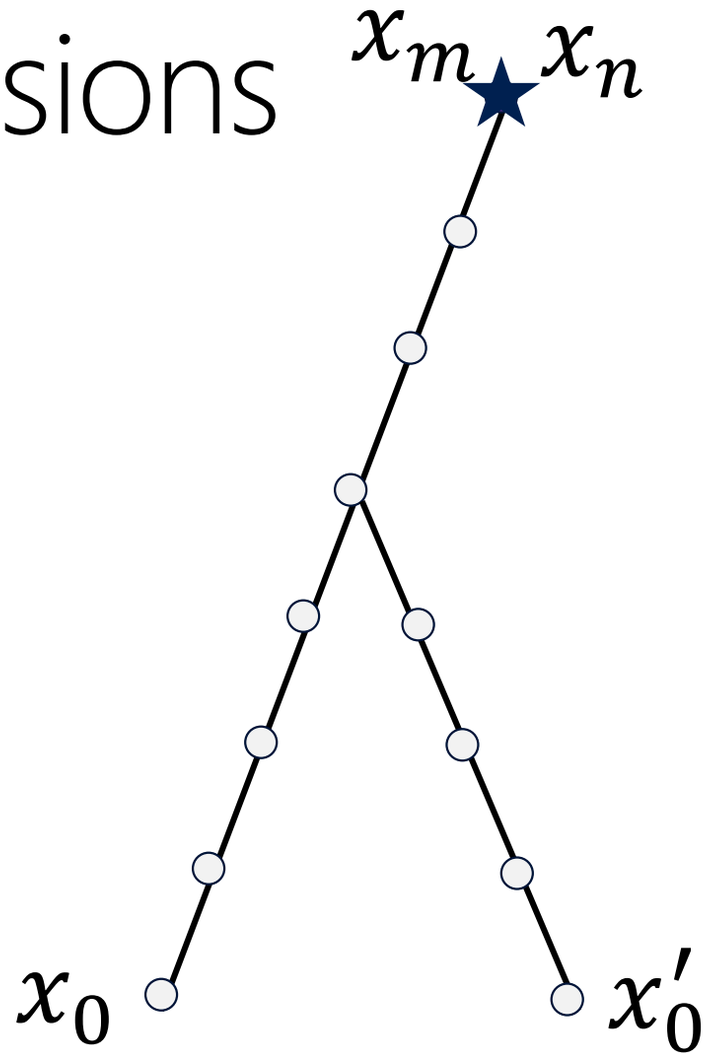
memory
(x_0, x_m, m)
(x'_0, x_n, n)



$f_n(x_0) \neq f_n(x'_0)$

Checking collisions

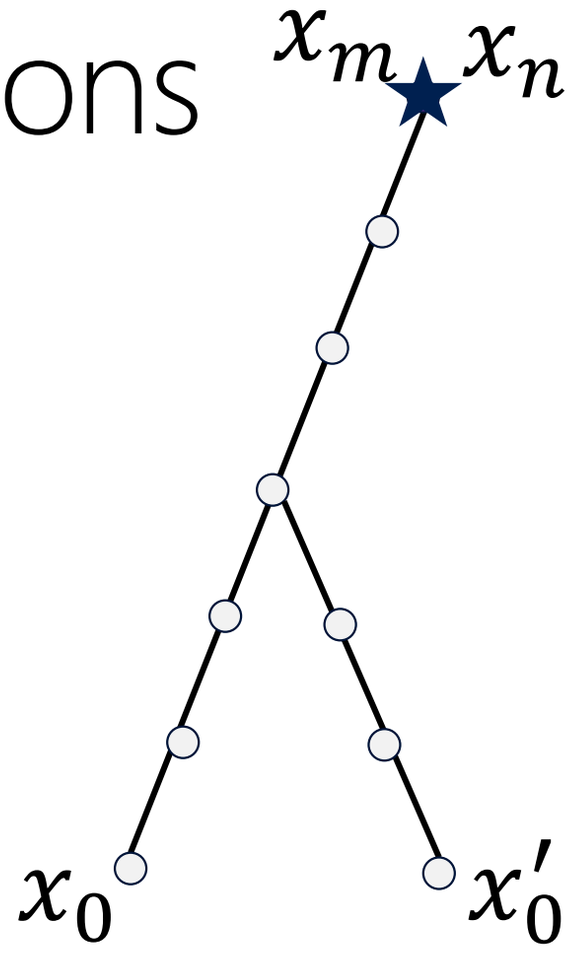
memory
(x_0, x_m, m)
(x'_0, x_n, n)



$f_n(x_0) \neq f_n(x'_0)$

Checking collisions

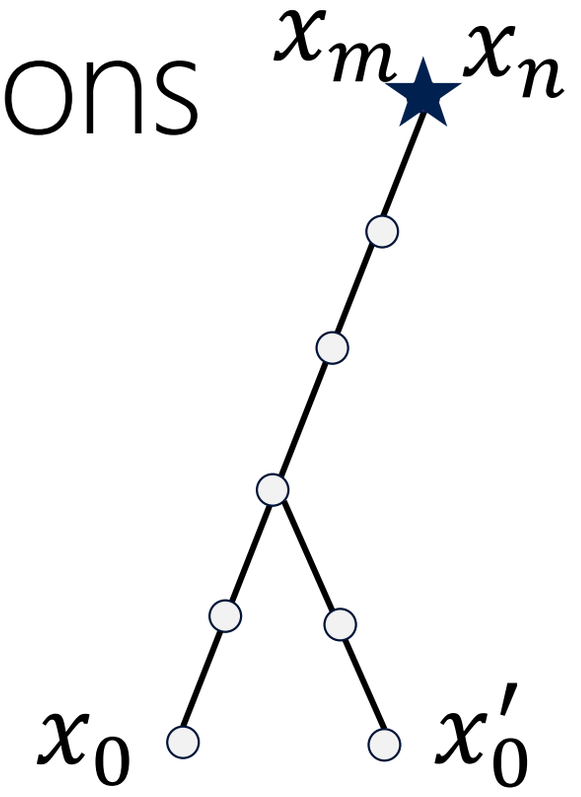
memory
(x_0, x_m, m)
(x'_0, x_n, n)



$f_n(x_0) \neq f_n(x'_0)$

Checking collisions

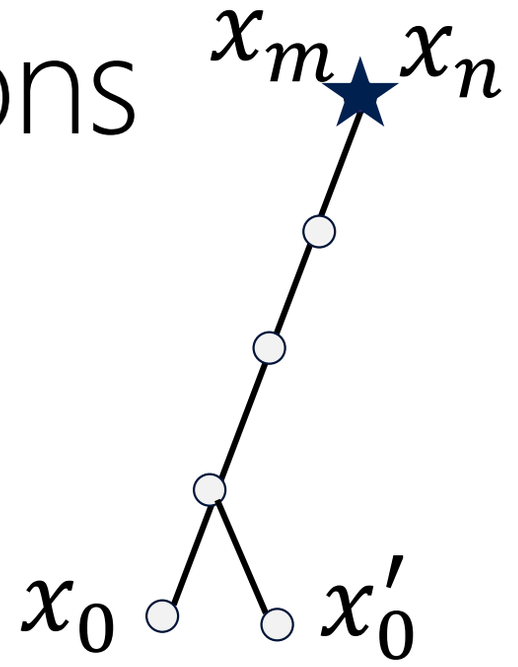
memory
(x_0, x_m, m)
(x'_0, x_n, n)



$f_n(x_0) \neq f_n(x'_0)$

Checking collisions

memory
(x_0, x_m, m)
(x_0', x_n, n)

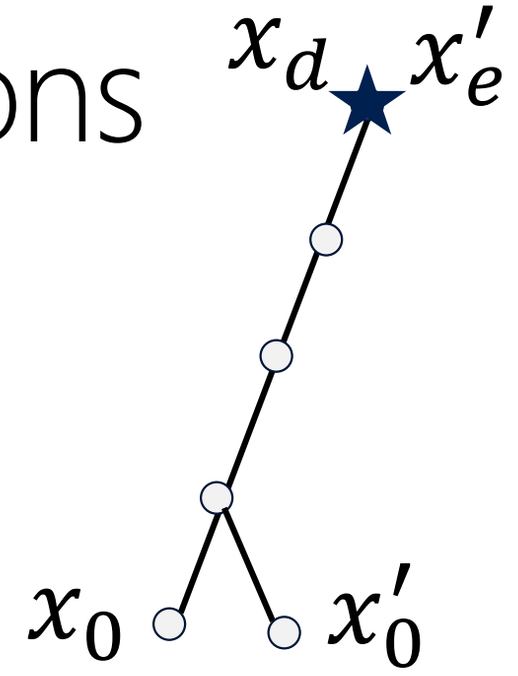


$f_n(x_0) = f_n(x_0')$
$x_0 \neq x_0'$

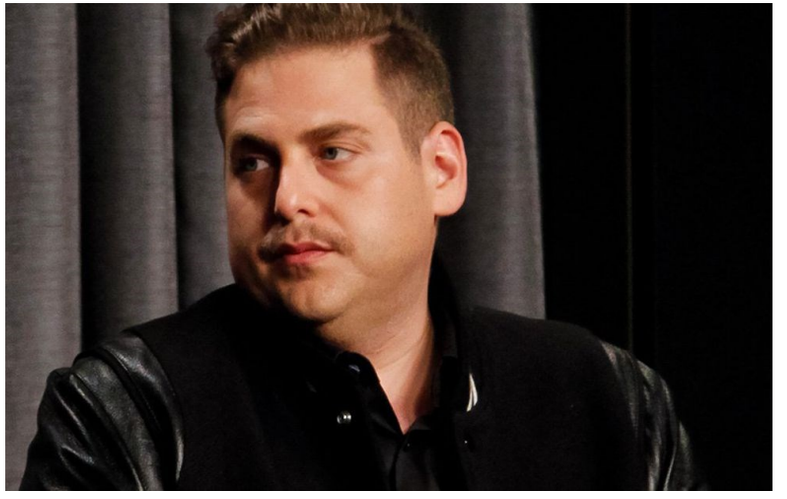
DONE?

Checking collisions

memory
(x_0, x_d, d)
(x'_0, x'_e, e)



Nope! False alarm



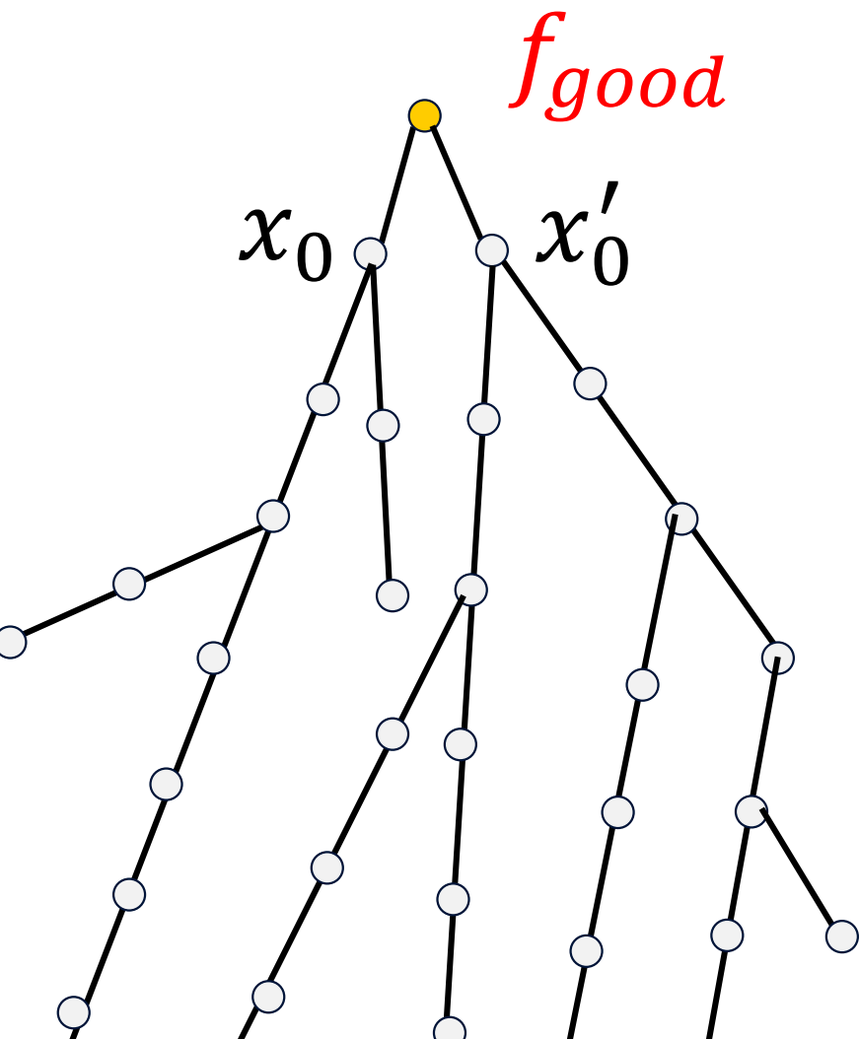
Upshot: we have to check many, many useless collisions before we find the golden collision

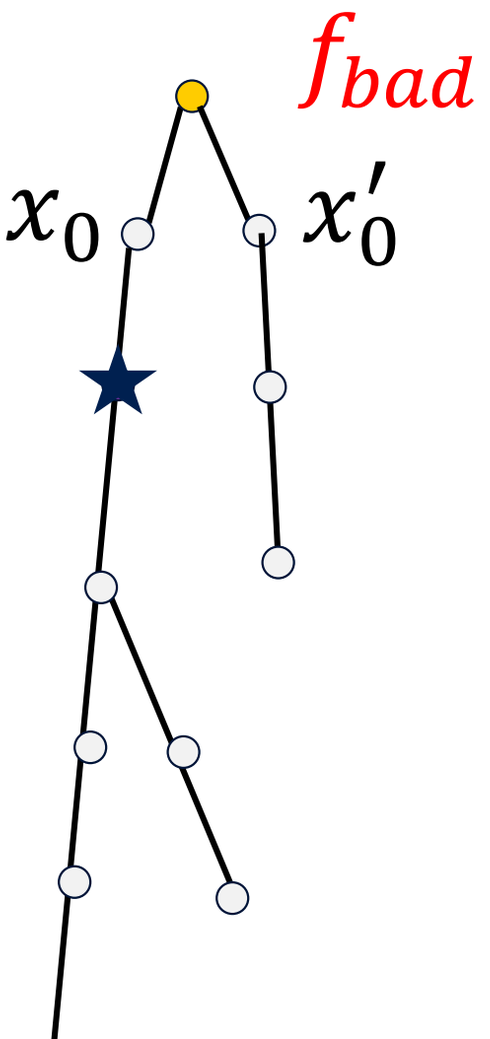
… and it gets worse…

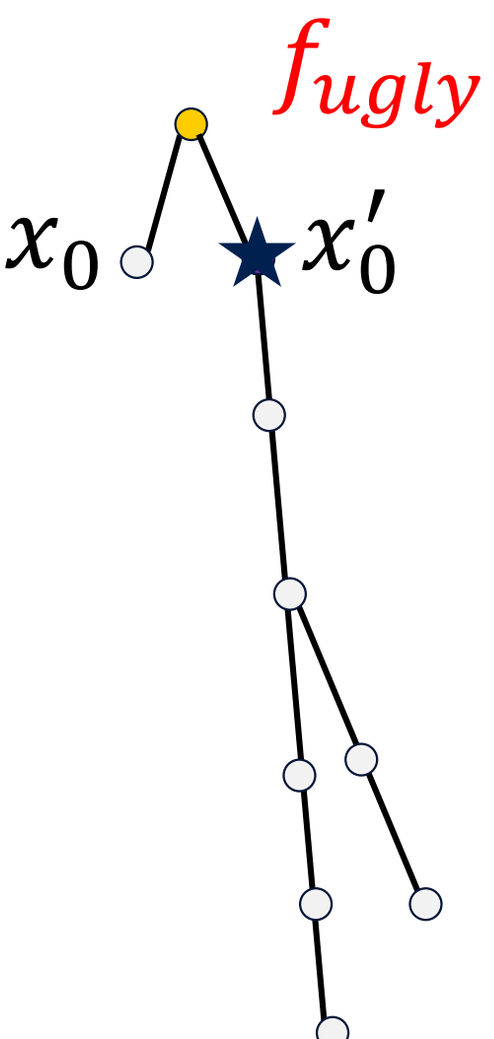
1. Can't store all distinguished points! May have found golden collision and thrown it away

2. But, even worse than that…

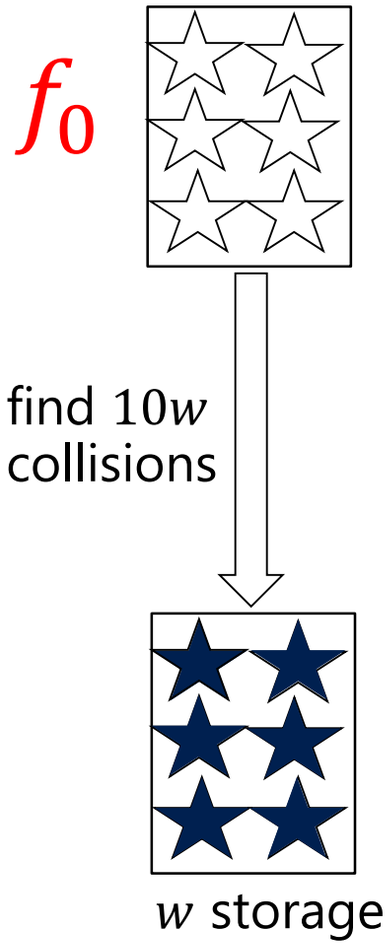
Random f: the good, the bad and the ugly…



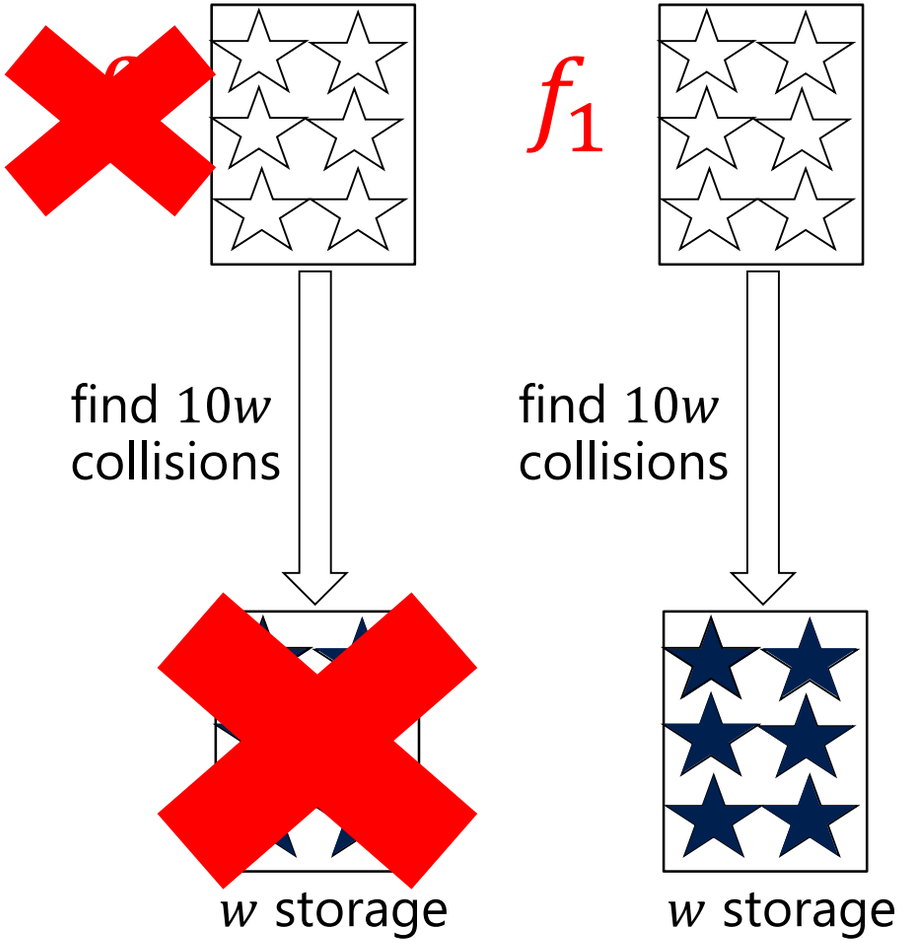




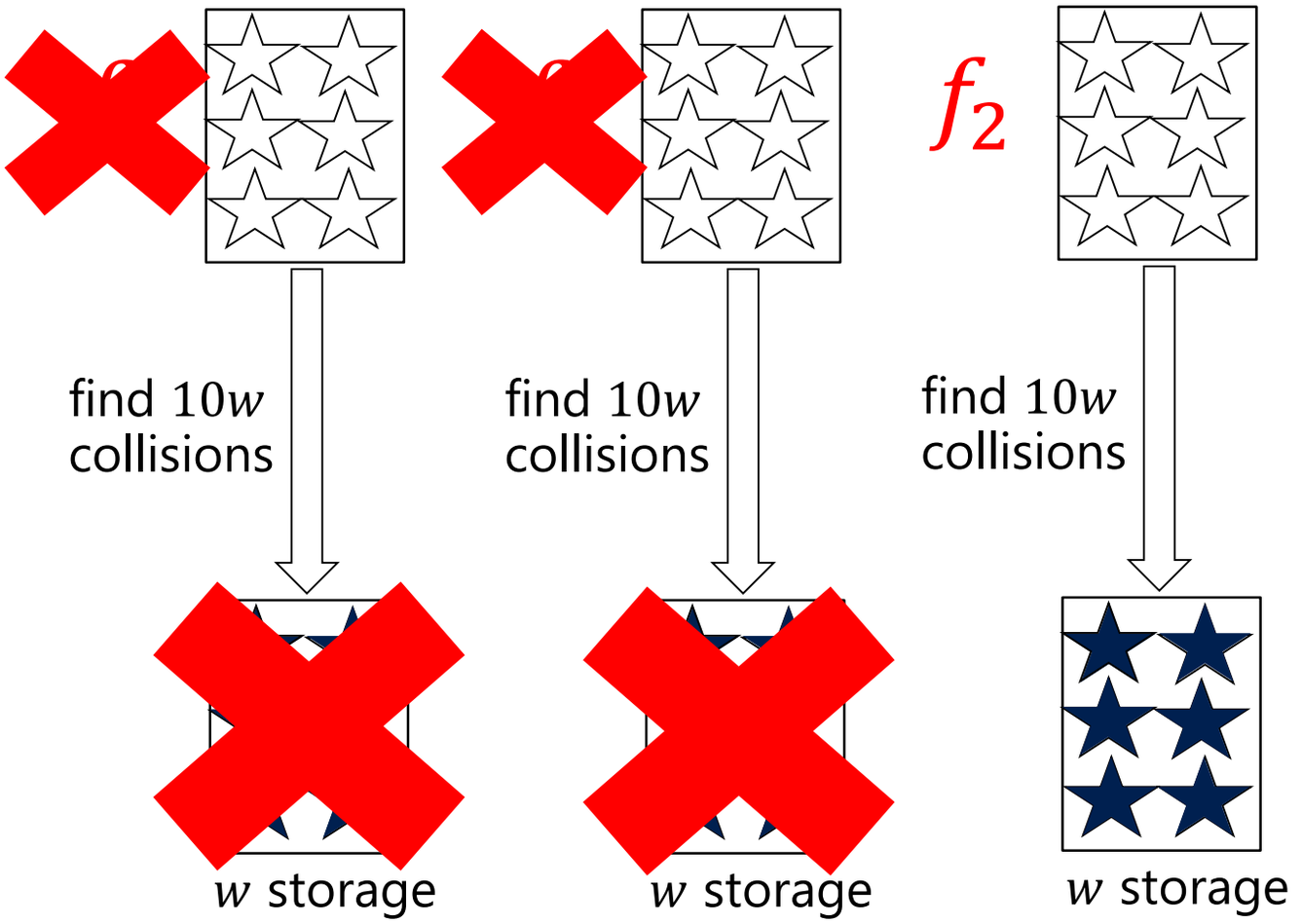
Restarting the algorithm… again, and again, and again…



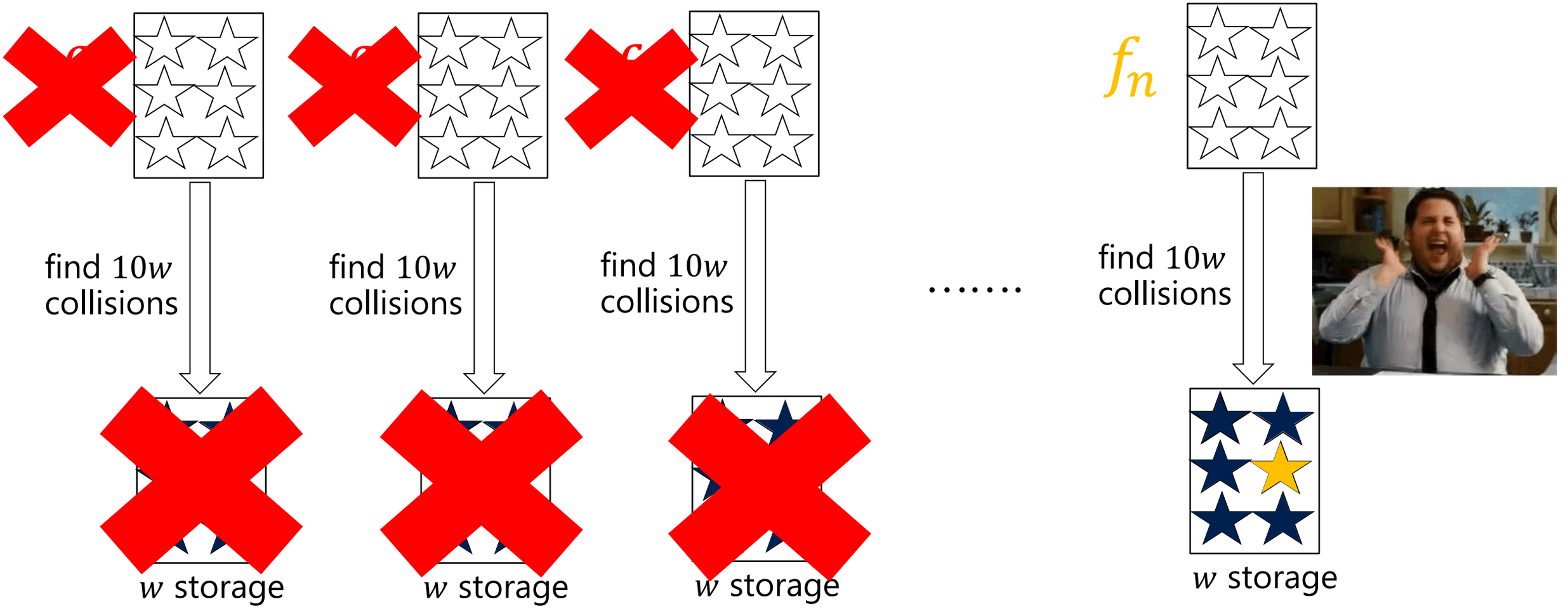
Restarting … again, and again, and again…



Restarting … again, and again, and again…



Restarting … again, and again, and again…



Analysis

SIKE: $|S| \approx p^{1/4}$

Adj et al: $w \approx 2^{80}$

$$o\left(\frac{|S|^2}{w}\right)$$

MitM

$$o\left(\frac{|S|^{\frac{3}{2}}}{\sqrt{w}}\right)$$

vOW

https://eprint.iacr.org/2019/298 C-Longa-Naehrig-Renes-Virdia

- Fast(er) collision checking
- SIKE-specific optimisations: conjugates, fixed-bits, …
- Precomputation
- Compressed distinguished points
- Optimised isogeny computations
- Multi-target attacks
- Larger experiments closely matching theoretical analysis of vOW: $O\left(|S|^{\frac{3}{2}}/\sqrt{w}\right)$
- …

Implications

Adj+18
& JS19
& CLNRV19

Target Security Level	**SIKE Round 1** $\log_2(p)$	**SIKE Round 2** $\log_2(p)$
NIST 1 (AES128)	503	434
NIST 2 (SHA256)	-	503
NIST 3 (AES192)	751	610
NIST 4 (SHA384)	-	-
NIST 5 (AES256)	964	751

SIKE Round 2 summary

Scheme	PK size (bytes)	Skylake Cycles ($\times \mathbf{10^3}$) (Enc+Dec)	PK size (bytes)	Skylake Cycles ($\times \mathbf{10^3}$) (Enc+Dec)
SIKEp434	330	21,320	196	38,975
SIKEp503	378	30,542	224	53,077
SIKEp610	462	57,061	273	92,548
SIKEp751	564	87,572	331	151,522

Questions?

Alice

Bob