Disorientation faults in CSIDH

Gustavo Banegas
INRIA

Juliane Krämer
University of Regensburg

Tanja Lange
TU/e & Academia Sinica

Michael Meyer
University of Regensburg

Lorenz Panny
Academia Sinica

Krijn Reijnders
Radboud University

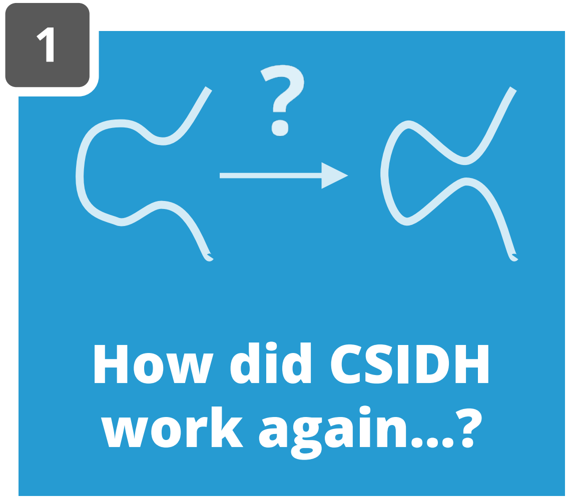
Jana Sotáková
UvA & QuSoft

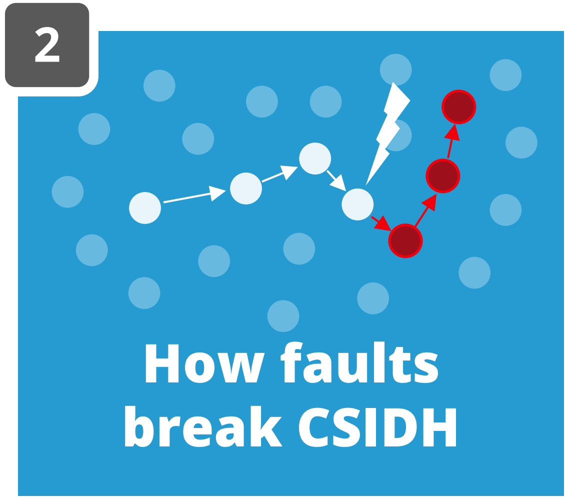
Monika Trimoska
Radboud University

Radboud University

26 April 2023
Eurocrypt '23

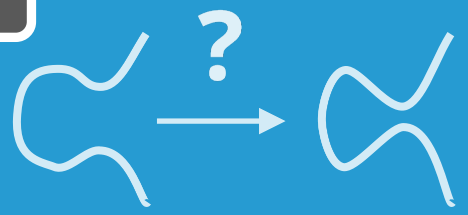
From disorientation attacks to key recovery





CSIDH FOR BEGINNERS

1



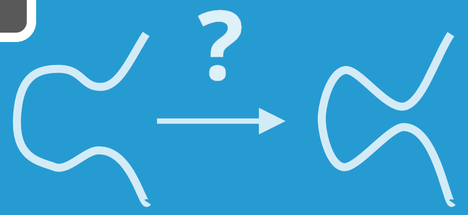
How did CSIDH work again...?

CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

1



How did CSIDH work again...?

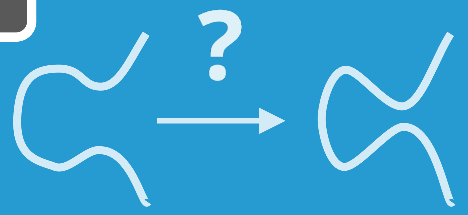
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

1



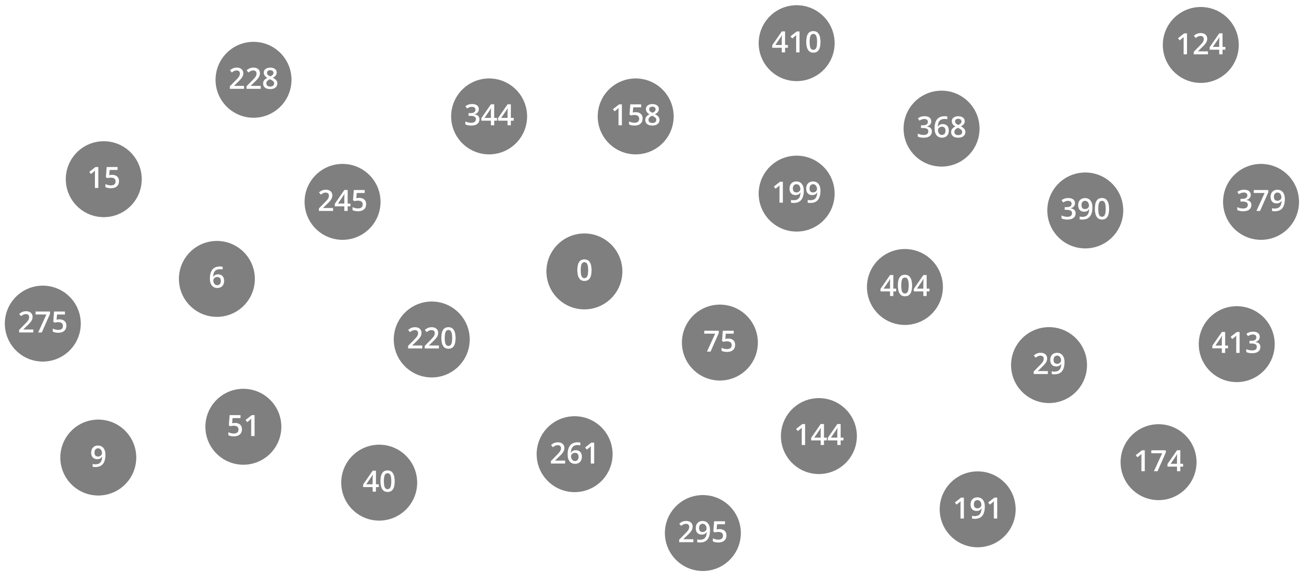
How did CSIDH work again...?

CSIDH for beginners

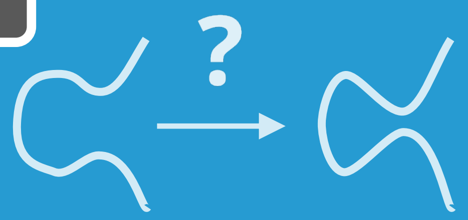
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$



1



How did CSIDH work again...?

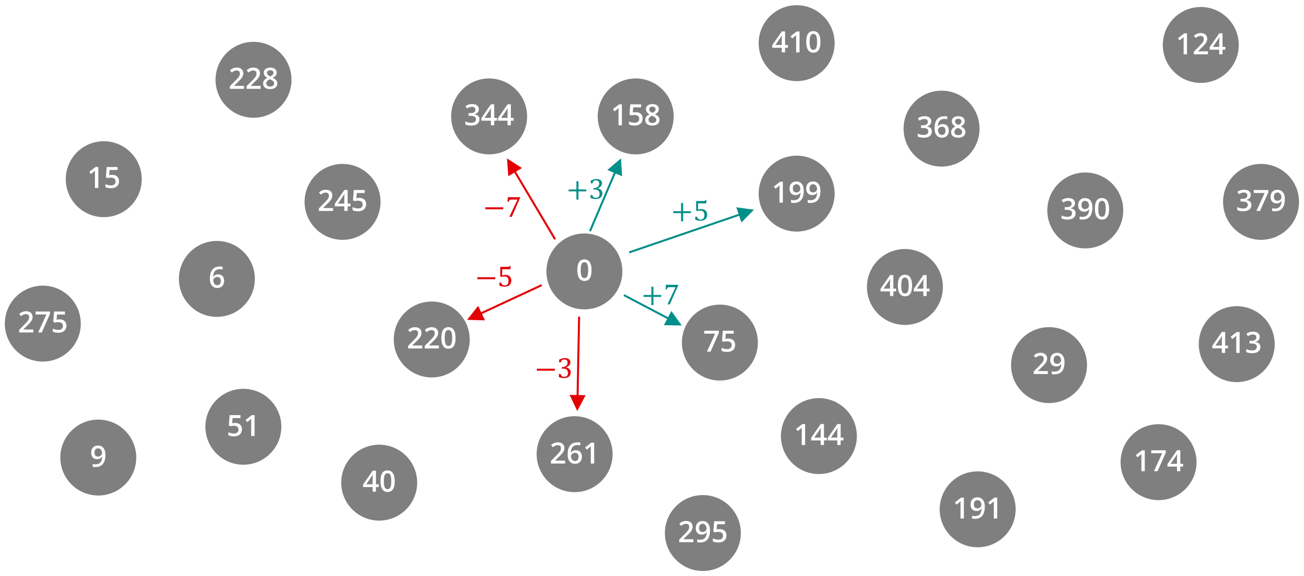
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

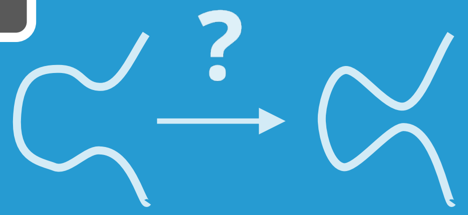
$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$



1



How did CSIDH work again...?

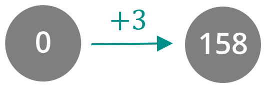
CSIDH for beginners

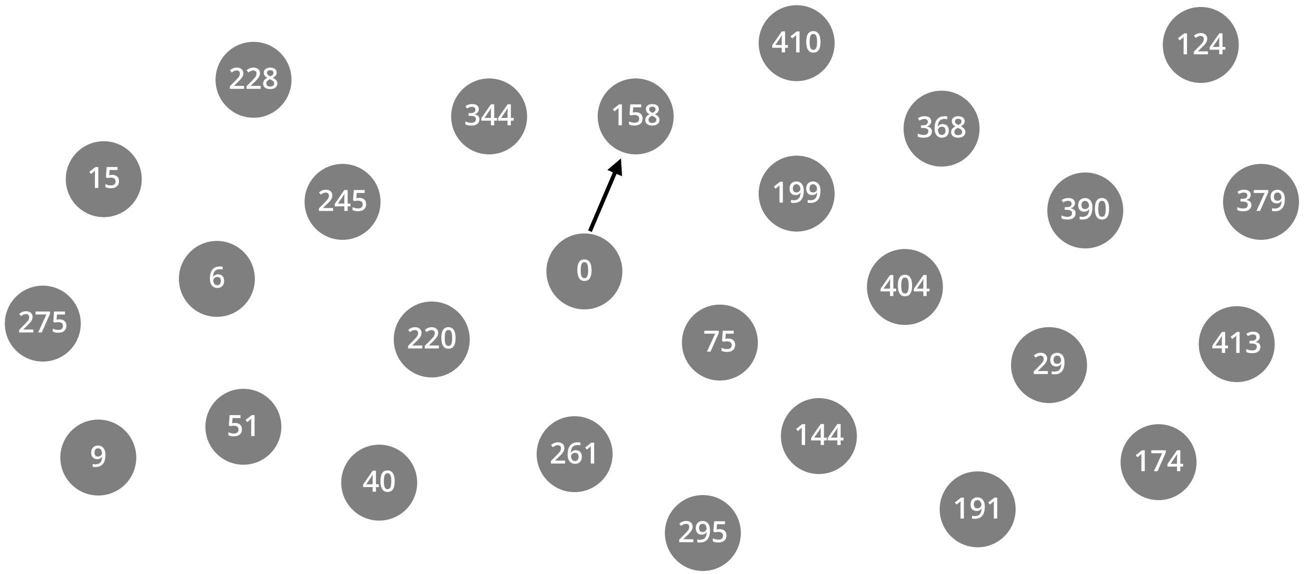
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

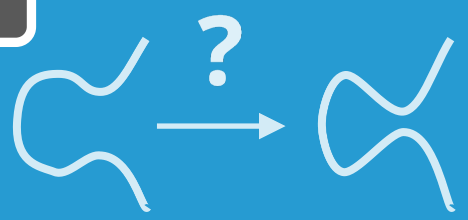
gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





1



How did CSIDH work again...?

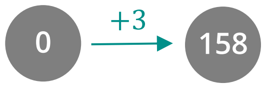
CSIDH for beginners

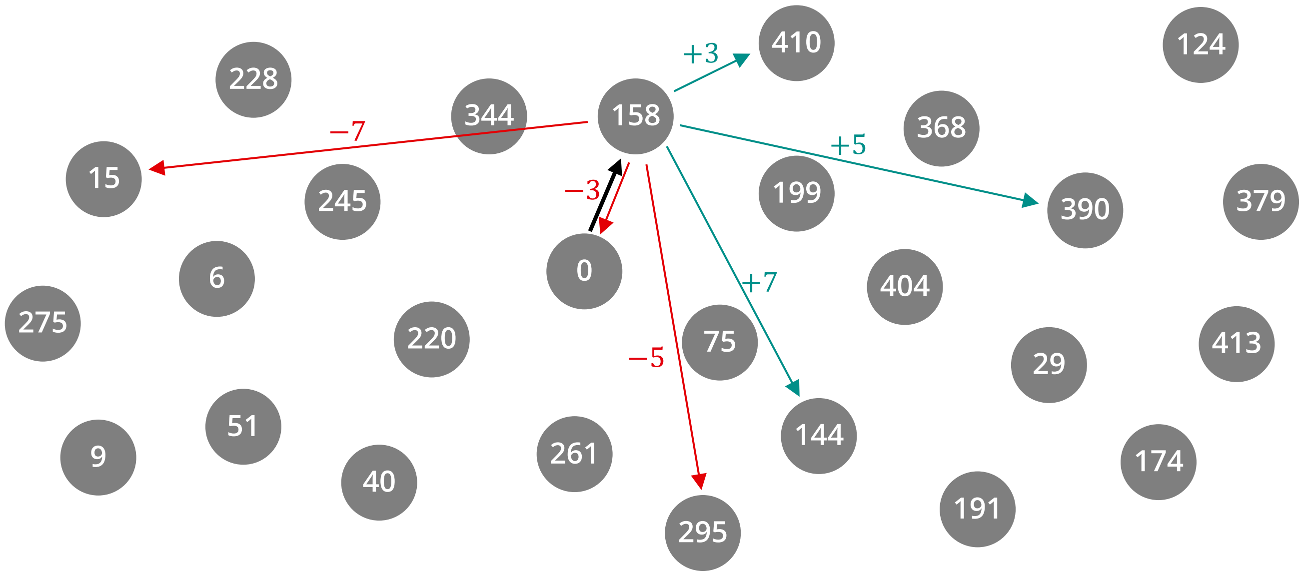
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

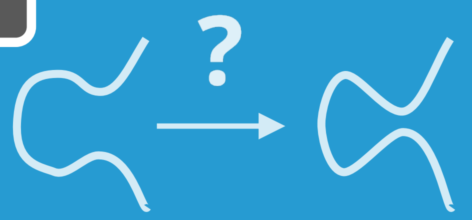
gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





1



How did CSIDH work again...?

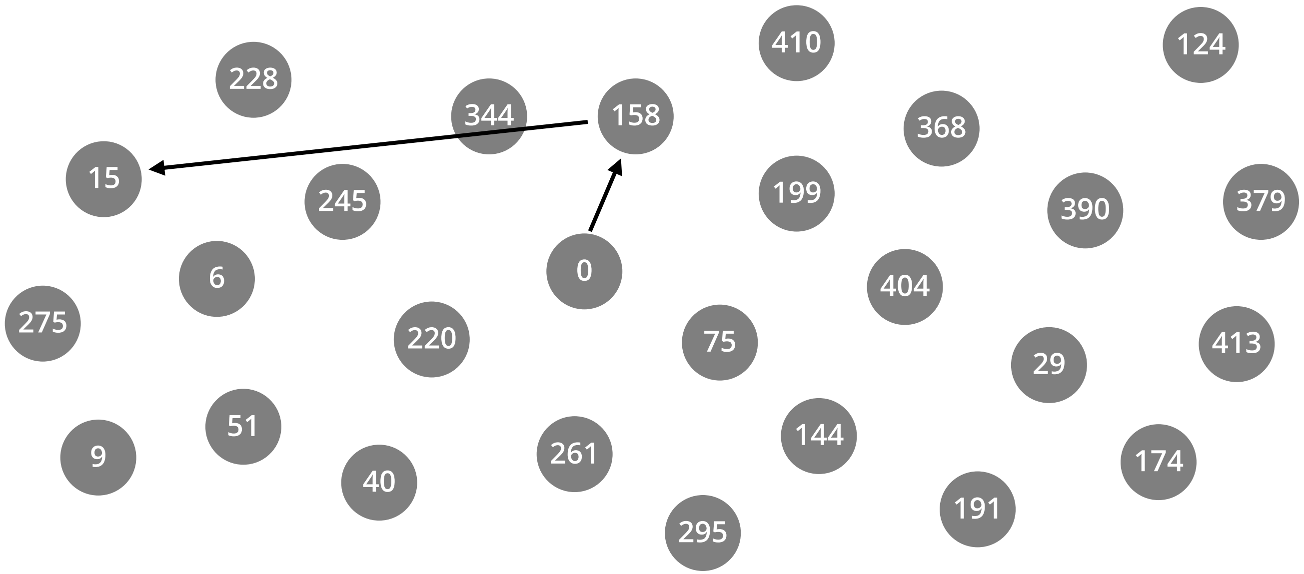
CSIDH for beginners

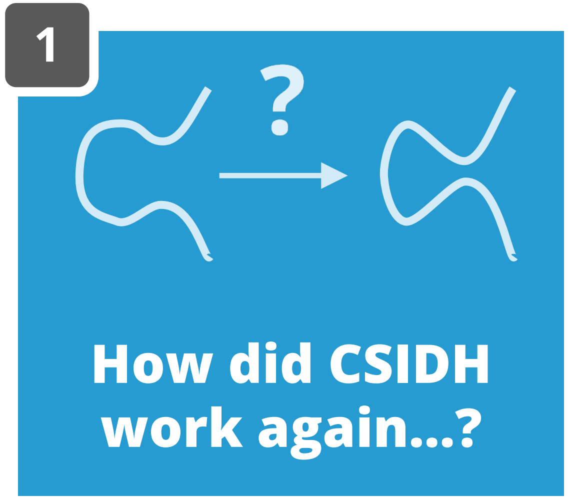
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are “special” $A \in \mathbb{F}_p$ that give us “supersingular” curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

gives 27 “special” $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





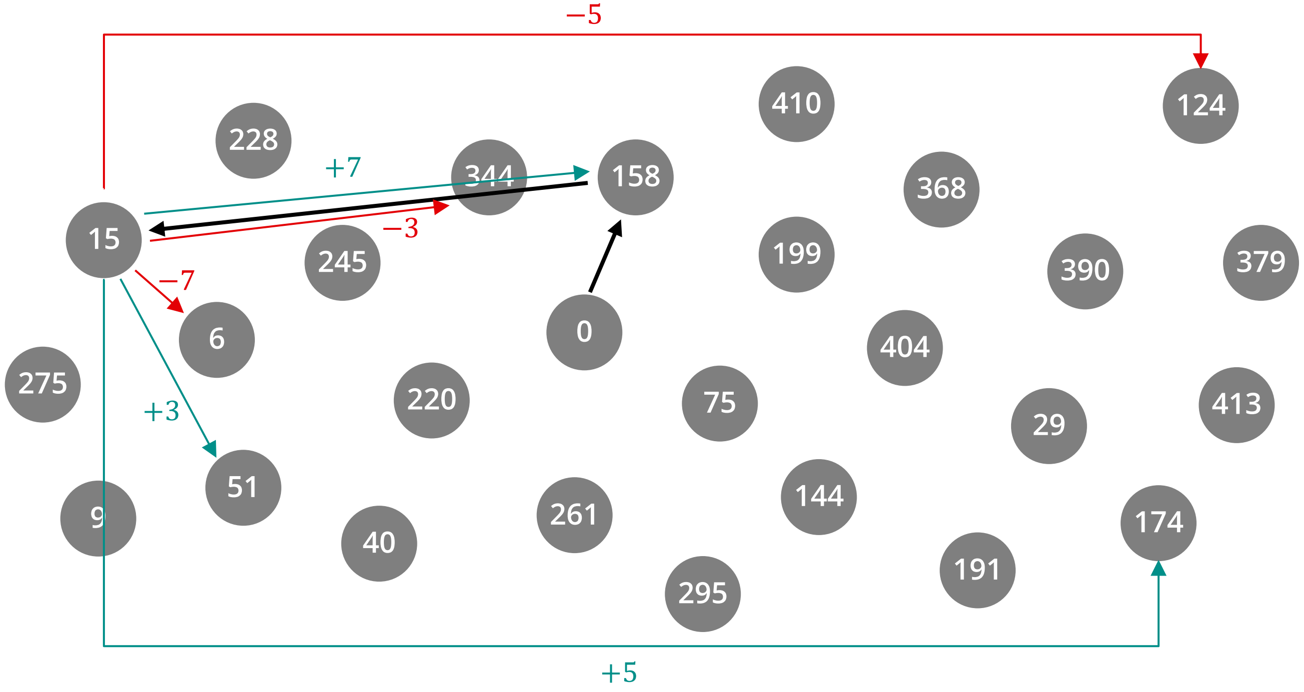
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

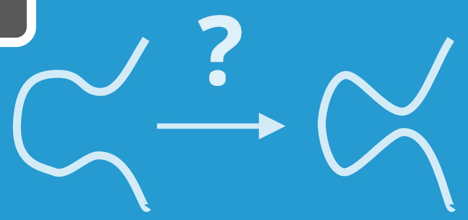
$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$



1



How did CSIDH work again...?

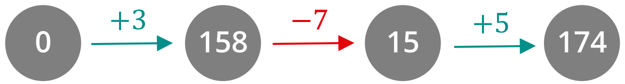
CSIDH for beginners

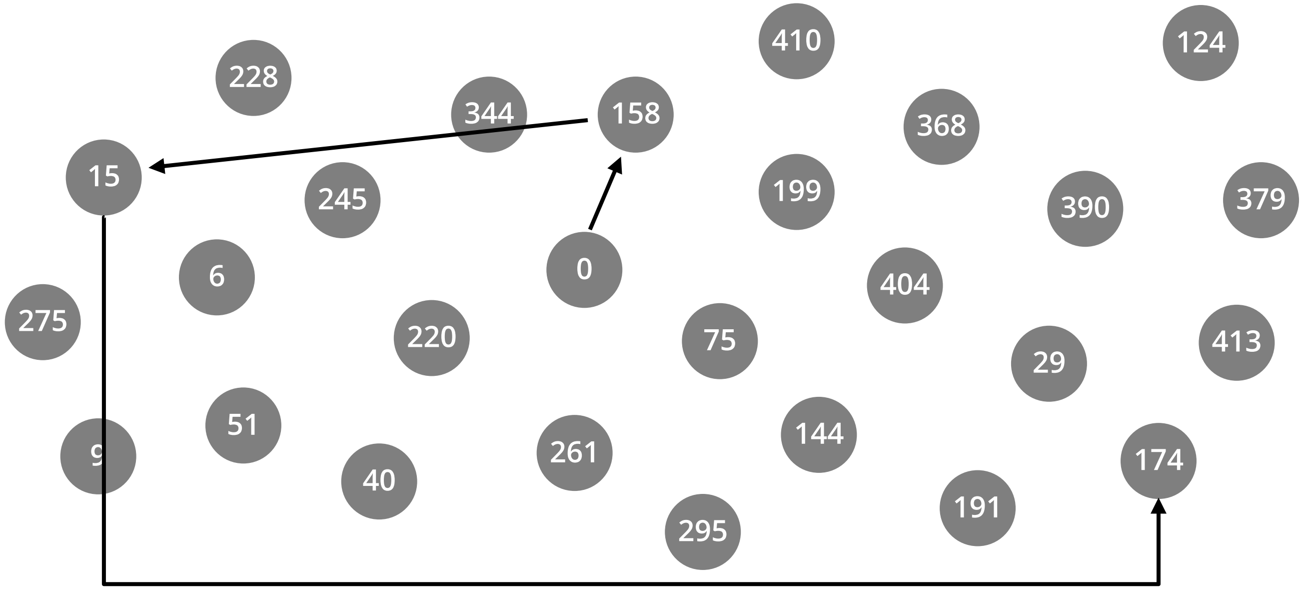
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are “special” $A \in \mathbb{F}_p$ that give us “supersingular” curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

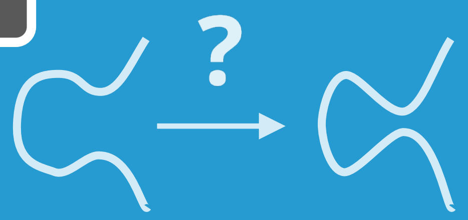
gives 27 “special” $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





1



How did CSIDH work again…?

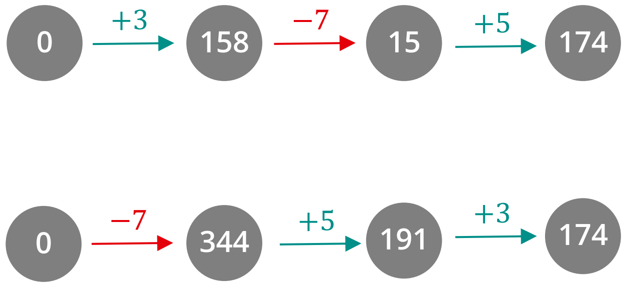
CSIDH for beginners

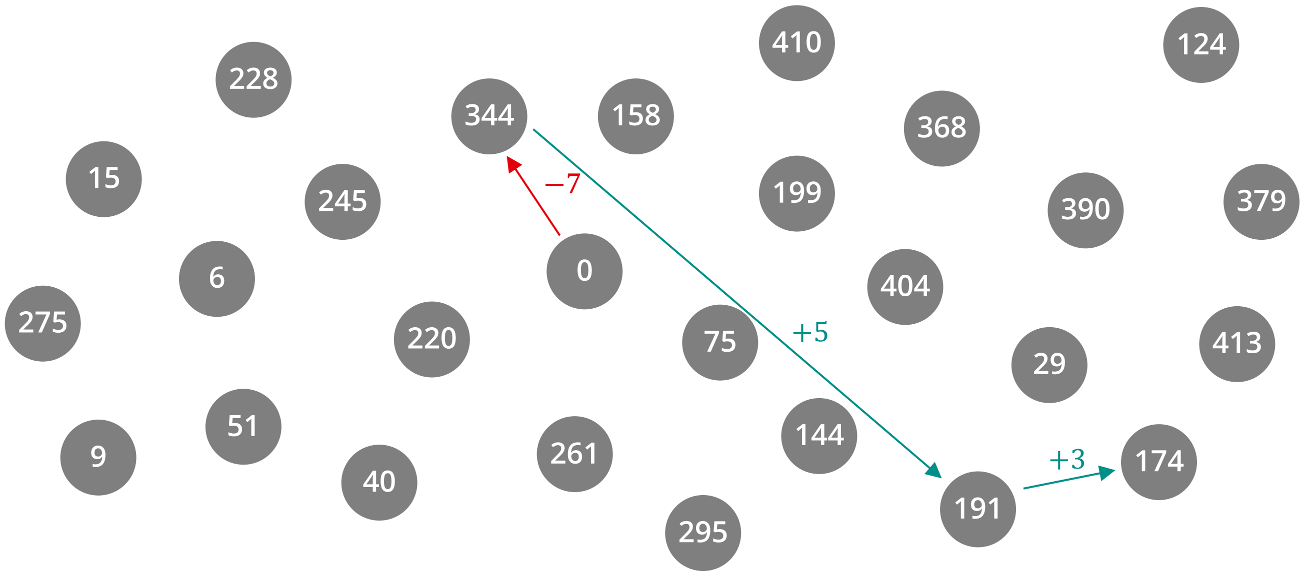
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. per ℓ we can take either a positive or a negative step

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

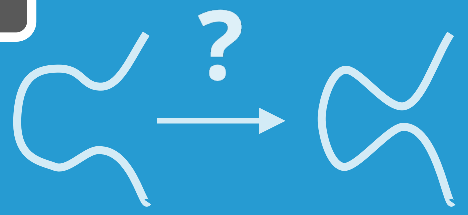
gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





1



How did CSIDH work again...?

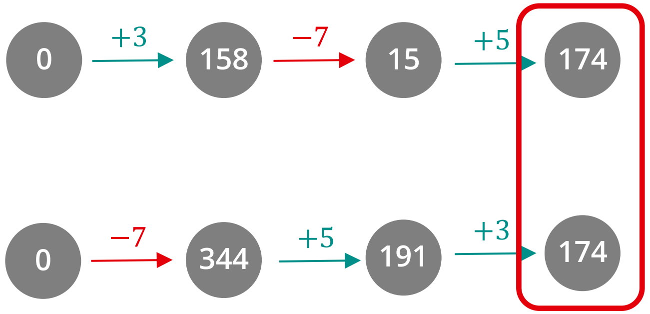
CSIDH for beginners

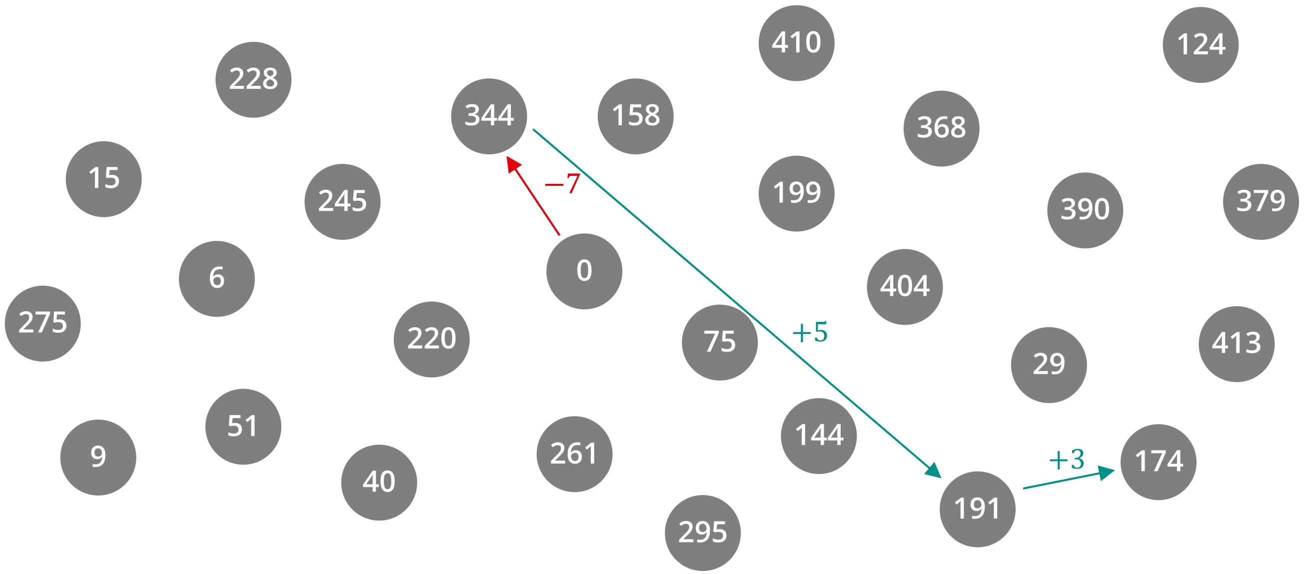
1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p+1$
3. Per ℓ we can take either a positive or a negative step
4. Magic!

$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

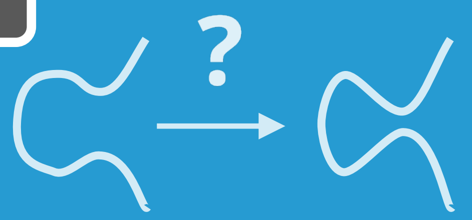
gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p+1$

steps by $\ell \in \{3, 5, 7\}$





1



How did CSIDH work again...?

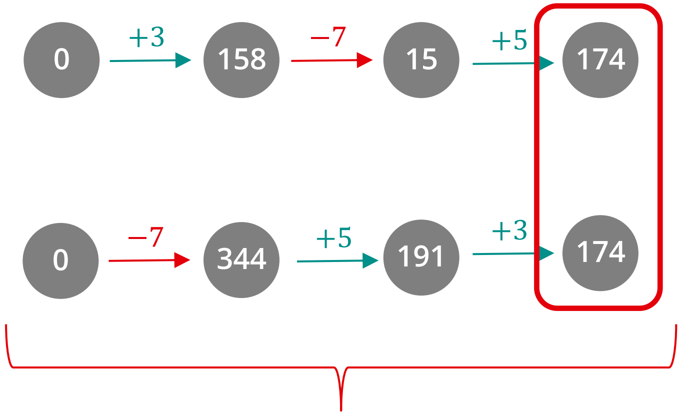
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes ℓ dividing $p+1$
2. There are "special" $A \in \mathbb{F}_p$ that give us "supersingular" curves $E_A : y^2 = x^3 + Ax^2 + x$ with $\#E_A(\mathbb{F}_p) = p + 1$
3. Per ℓ we can take either a positive or a negative step
4. Magic!

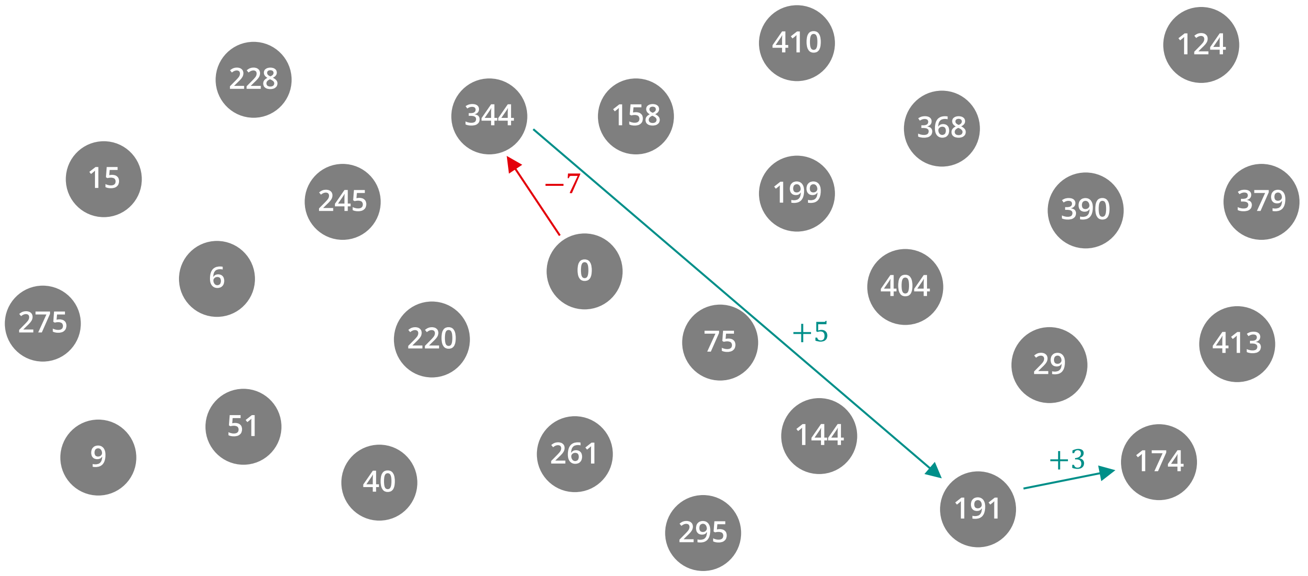
$p = 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1$

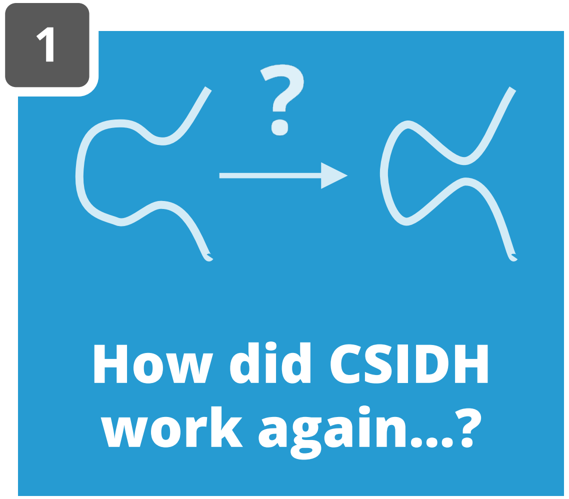
gives 27 "special" $A \in \mathbb{F}_p$ with $\#E_A(\mathbb{F}_p) = p + 1$

steps by $\ell \in \{3, 5, 7\}$



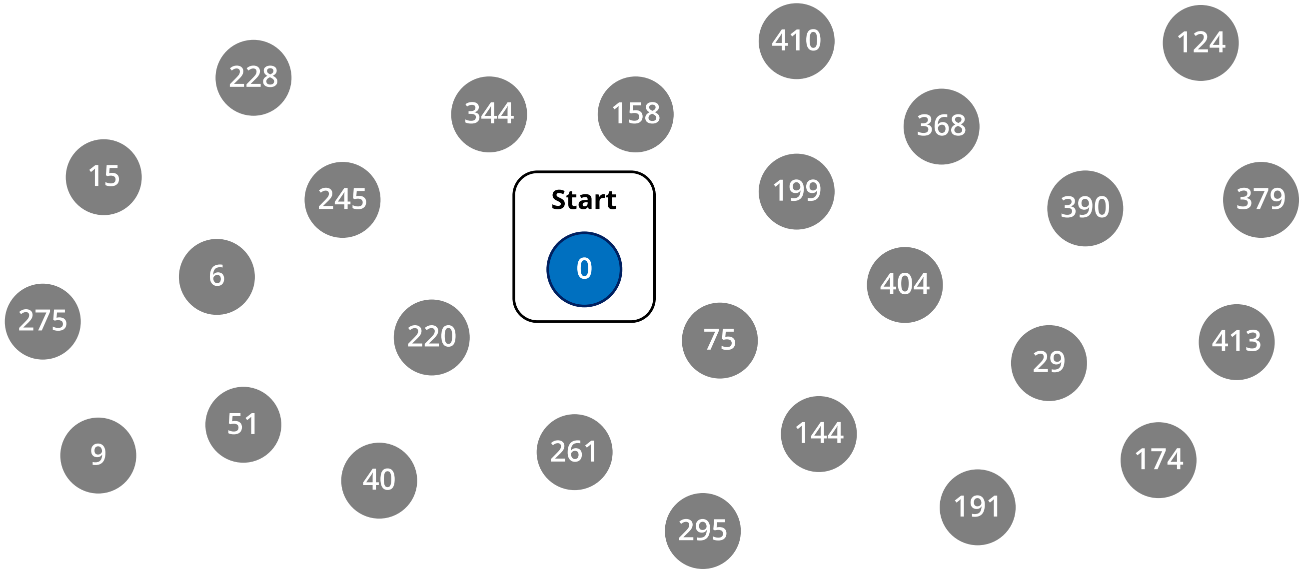
path is $(+1, +1, -1)$

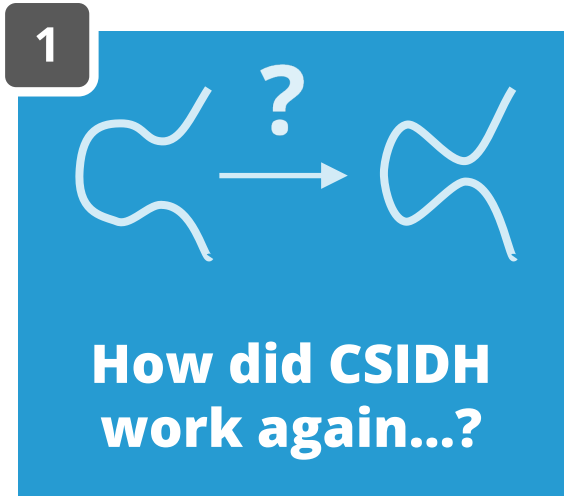




CSIDH key exchange

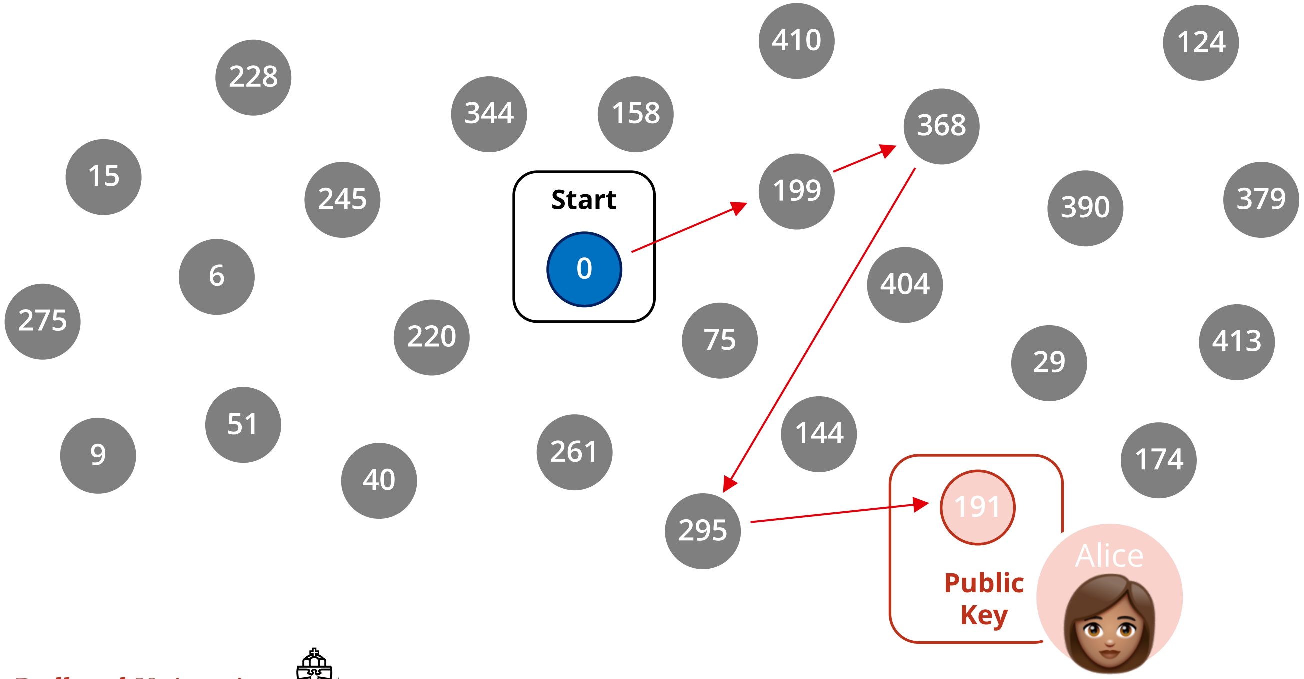
1. Pick somewhere to start

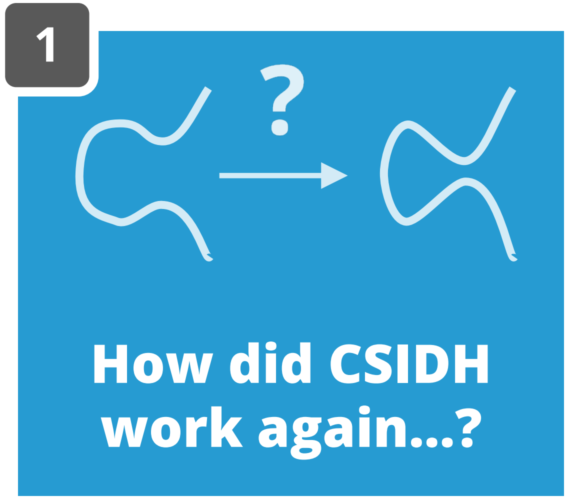




CSIDH key exchange

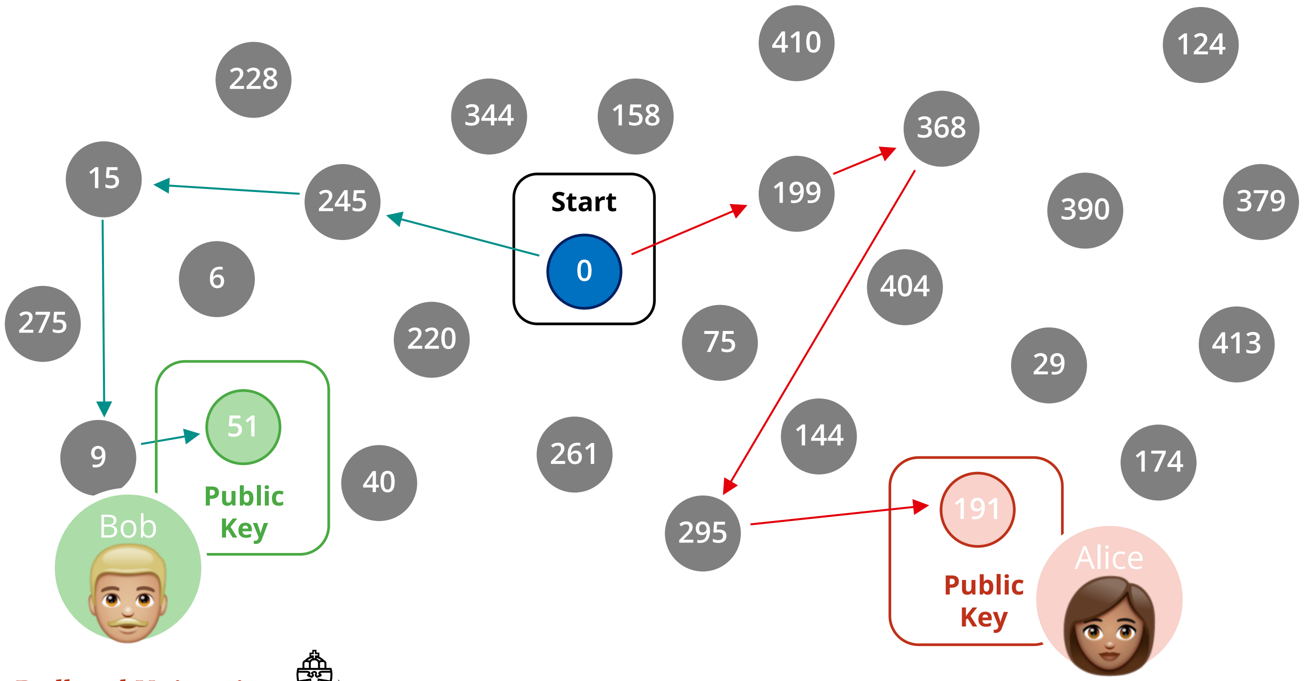
1. Pick somewhere to start
2. Alice picks **secret path** $\mathfrak{a} = (e_1, e_2, e_3)$

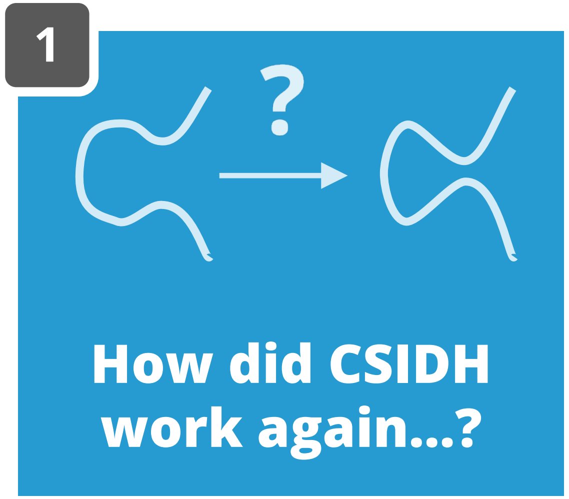




CSIDH key exchange

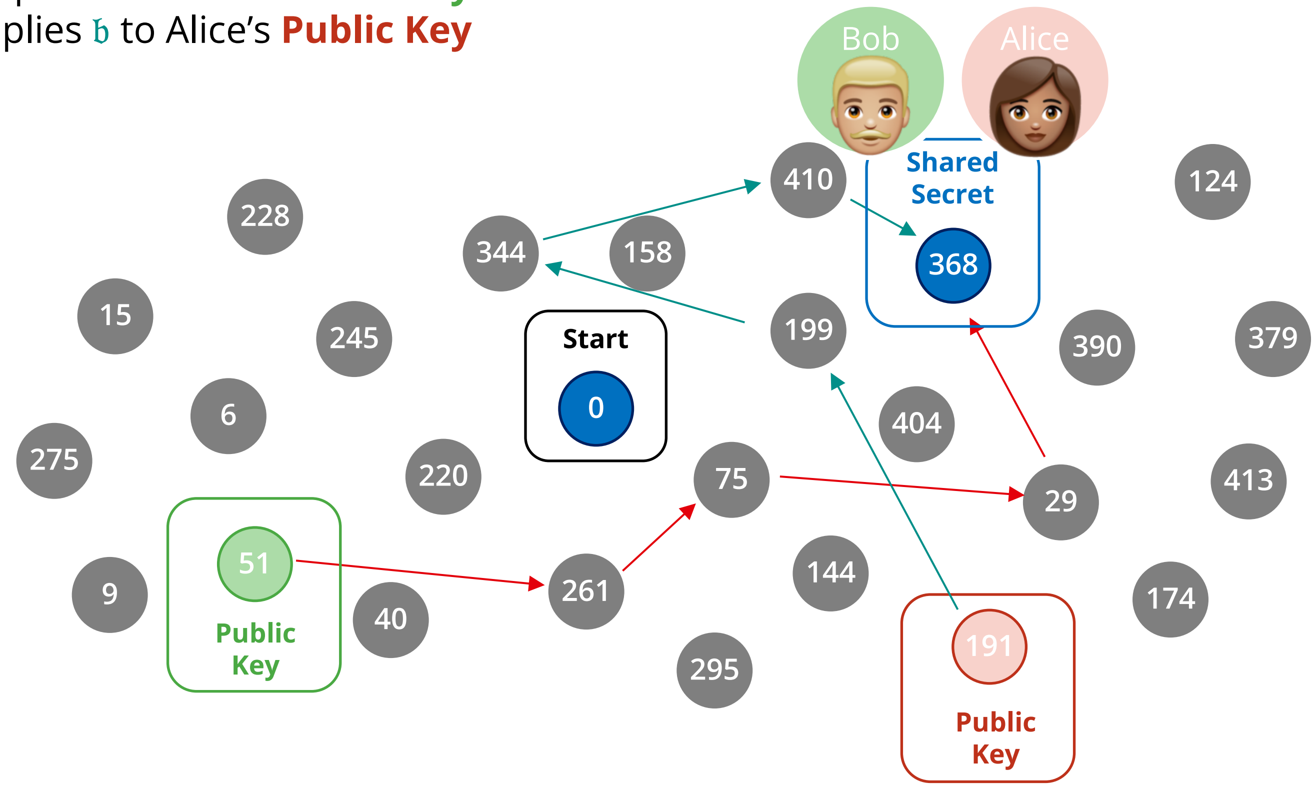
1. Pick somewhere to start
2. Alice picks **secret path** $\mathfrak{a} = (e_1, e_2, e_3)$
3. Bob picks **secret path** $\mathfrak{b} = (e_1, e_2, e_3)$

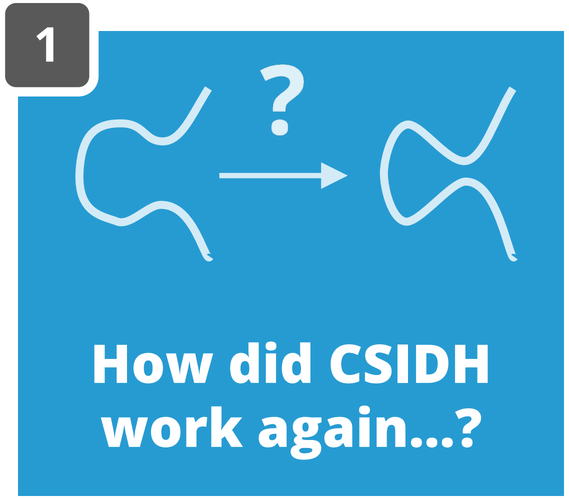




CSIDH key exchange

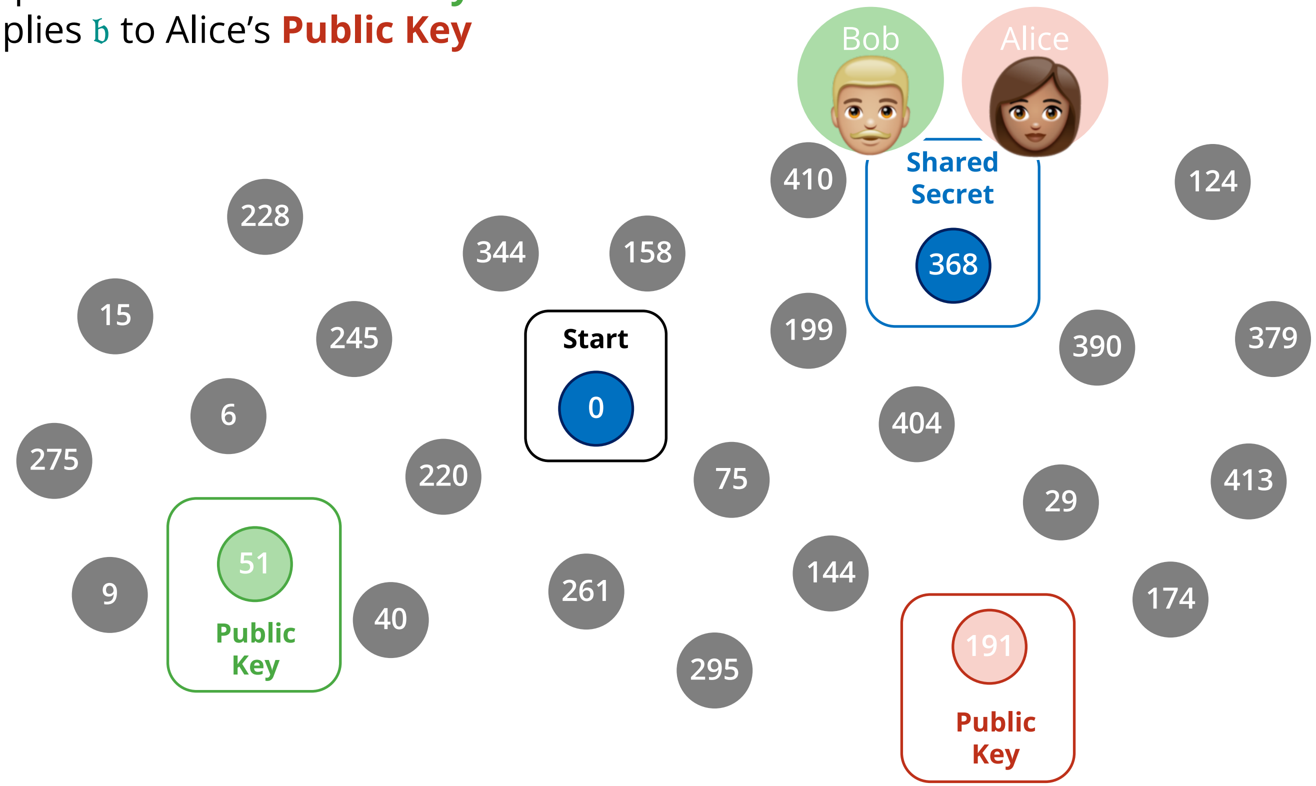
1. Pick somewhere to start
2. Alice picks **secret path** $\mathfrak{a} = (e_1, e_2, e_3)$
3. Bob picks **secret path** $\mathfrak{b} = (e_1, e_2, e_3)$
4. Alice applies $\mathfrak{a}$ to Bob's **Public Key**
   Bob applies $\mathfrak{b}$ to Alice's **Public Key**

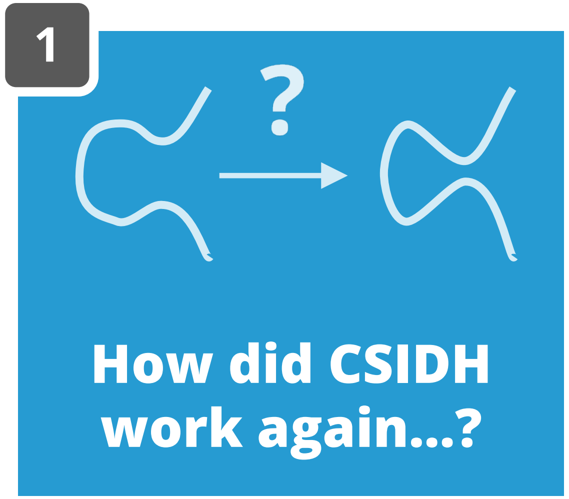




CSIDH key exchange

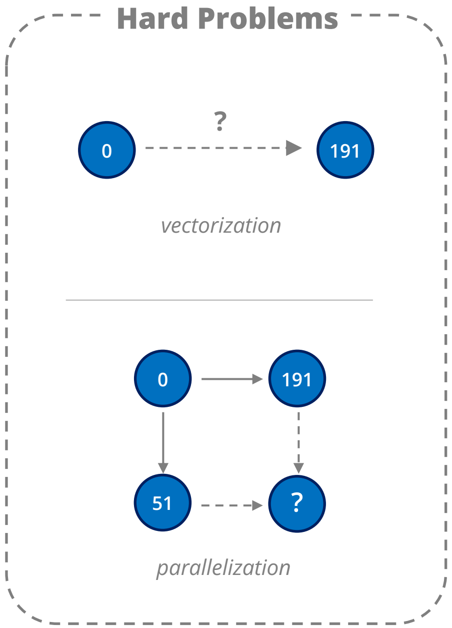
1. Pick somewhere to start
2. Alice picks **secret path** $\mathfrak{a} = (e_1, e_2, e_3)$
3. Bob picks **secret path** $\mathfrak{b} = (e_1, e_2, e_3)$
4. Alice applies $\mathfrak{a}$ to Bob's **Public Key**
   Bob applies $\mathfrak{b}$ to Alice's **Public Key**

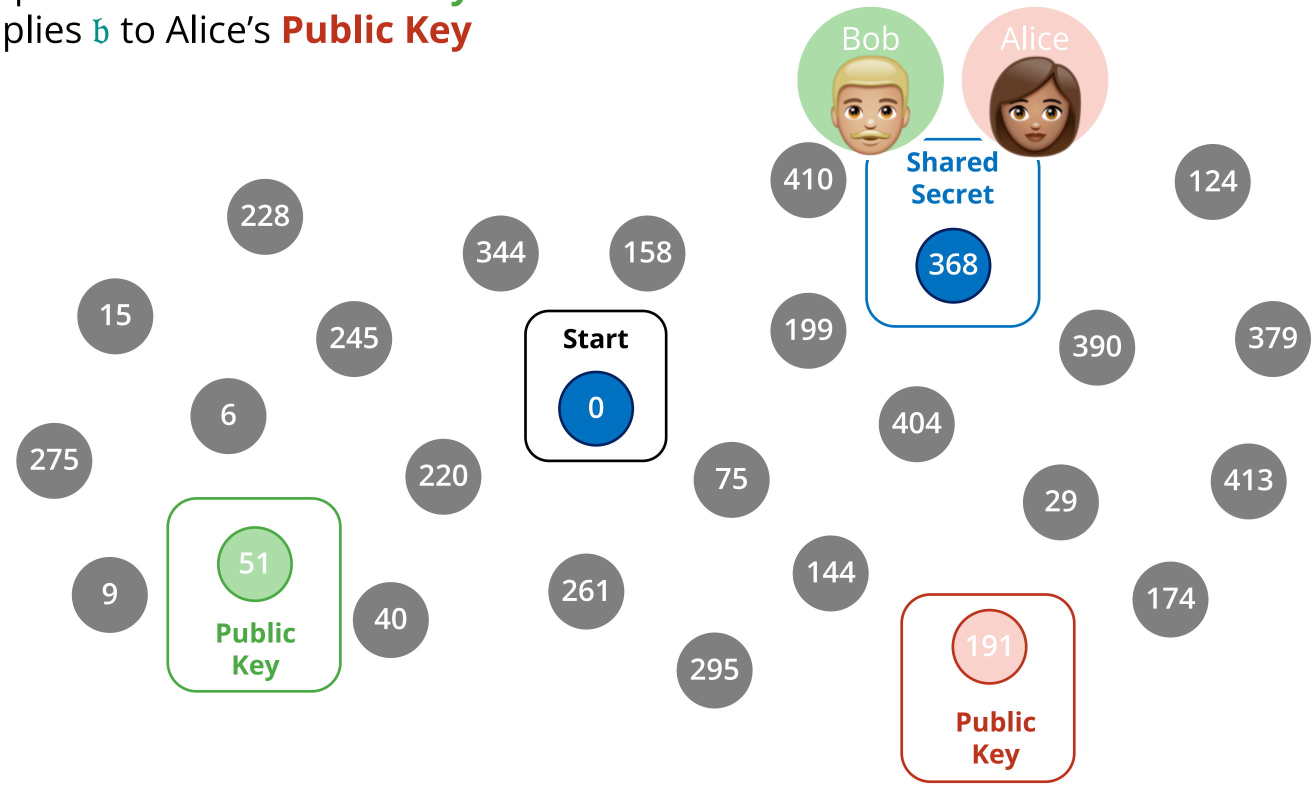




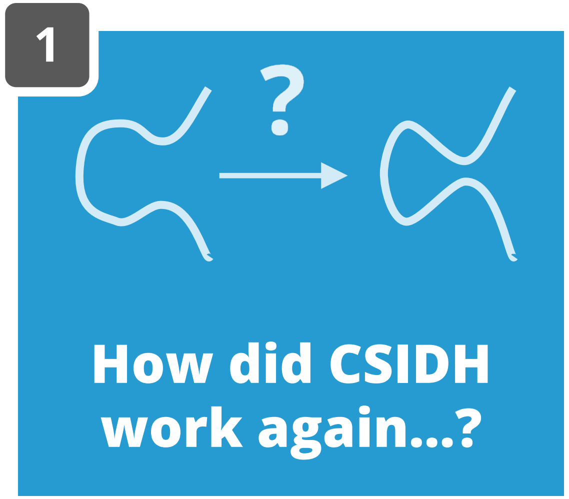
CSIDH key exchange

1. Pick somewhere to start
2. Alice picks **secret path** $\mathfrak{a} = (e_1, e_2, e_3)$
3. Bob picks **secret path** $\mathfrak{b} = (e_1, e_2, e_3)$
4. Alice applies $\mathfrak{a}$ to Bob's **Public Key**
   Bob applies $\mathfrak{b}$ to Alice's **Public Key**

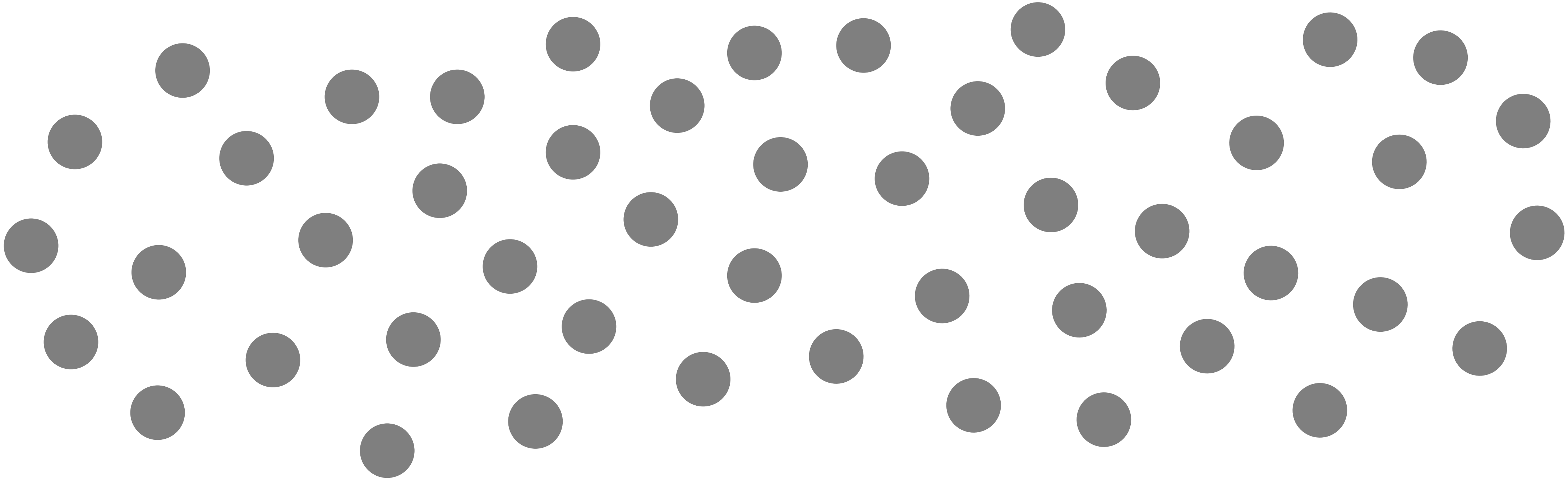


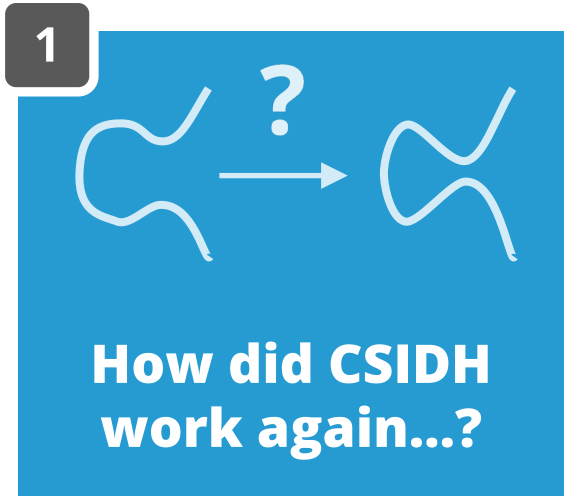


HOW TO WALK



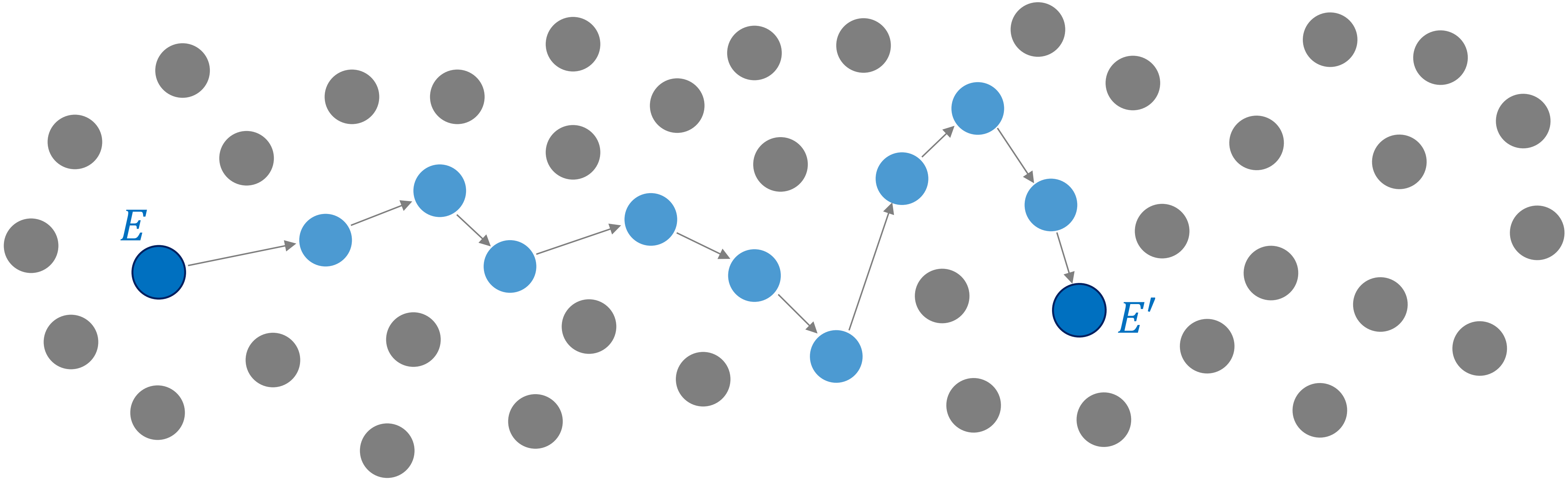
How to compute walk

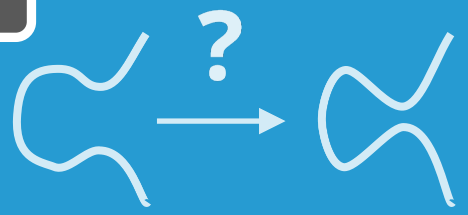




How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$





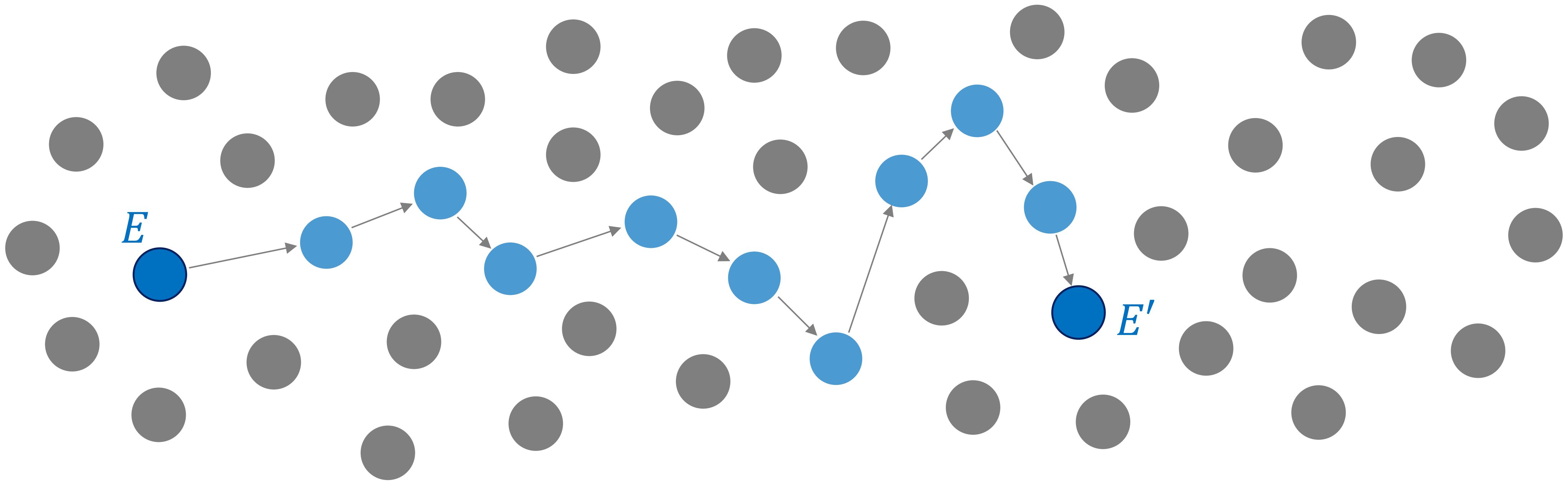
1

How did CSIDH work again...?

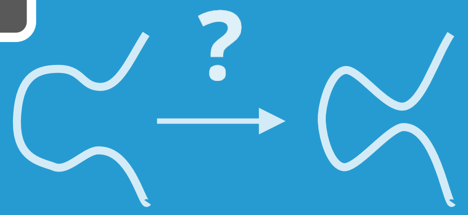
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

e.g. take two negative steps for third ℓ that divides $p + 1$



1

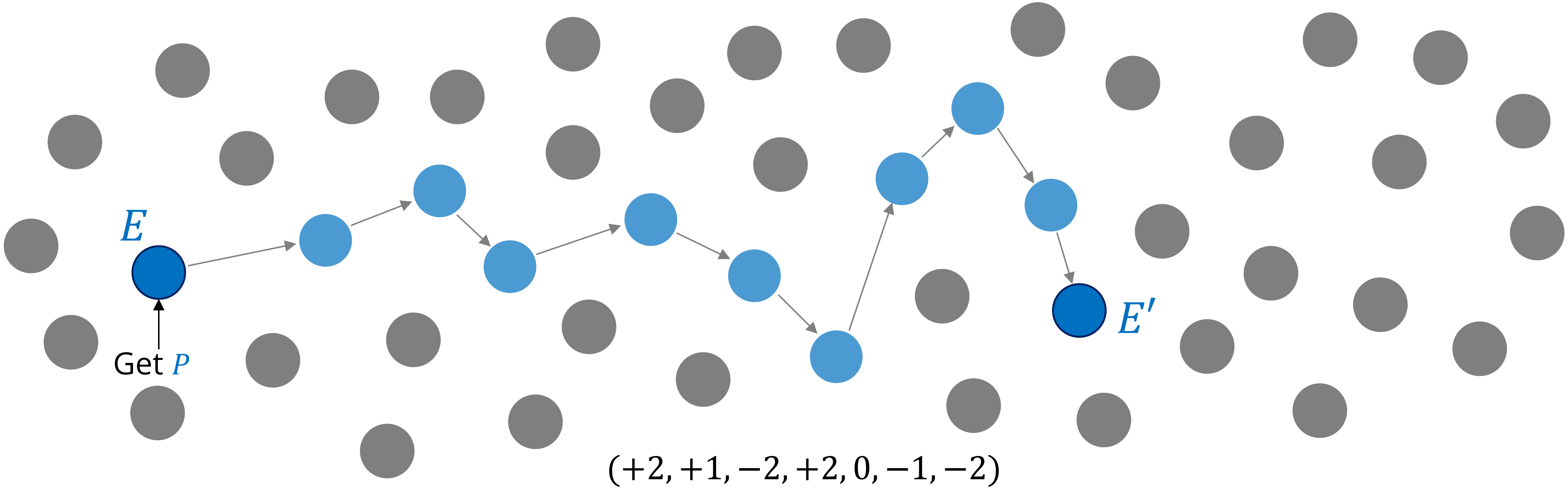


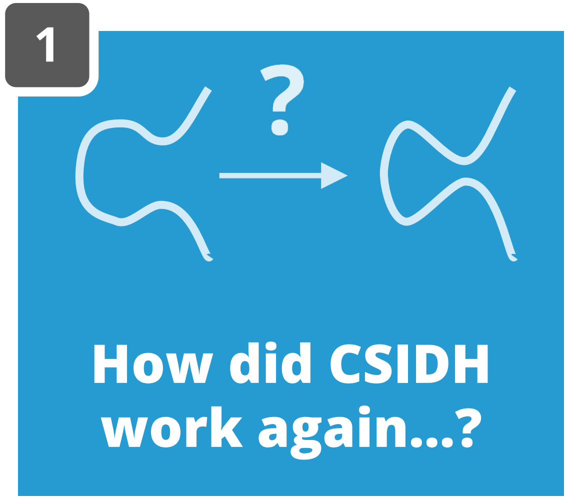
How did CSIDH work again...?

How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed

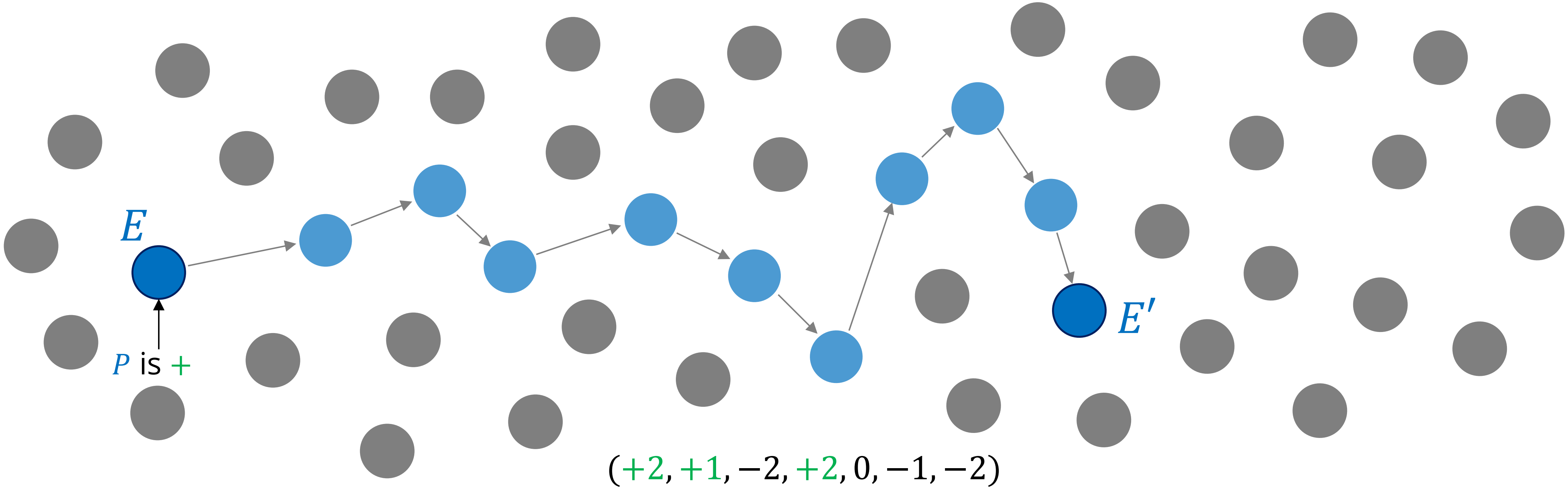




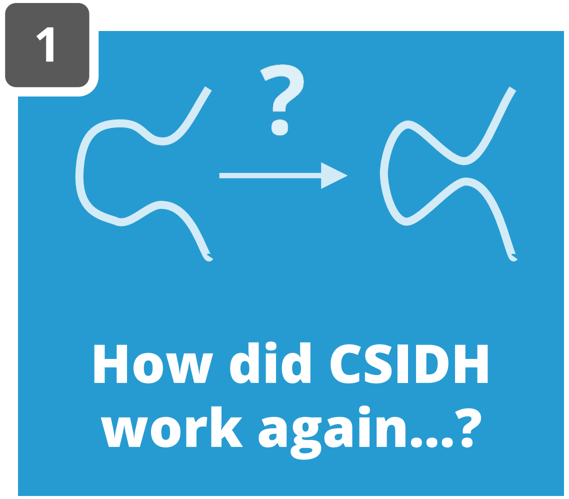
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



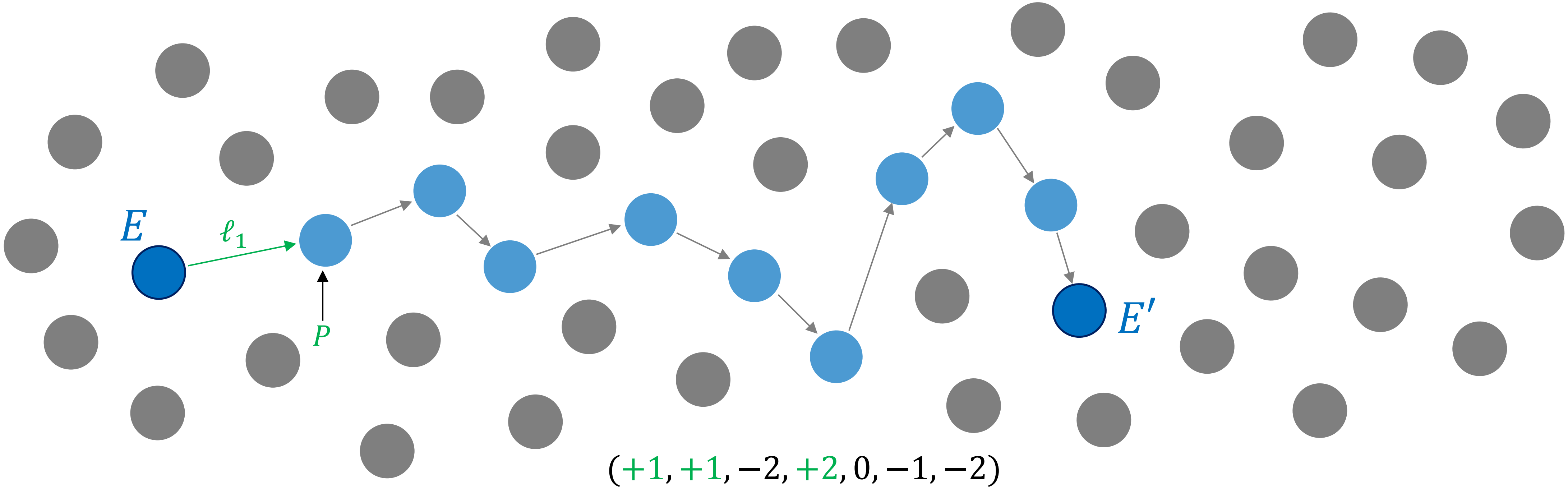
$(+2, +1, -2, +2, 0, -1, -2)$



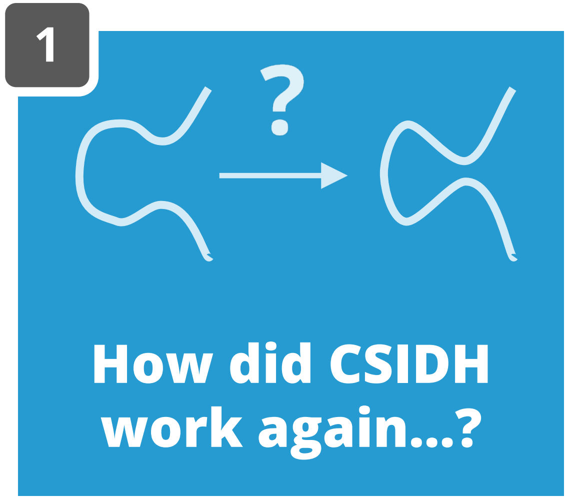
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



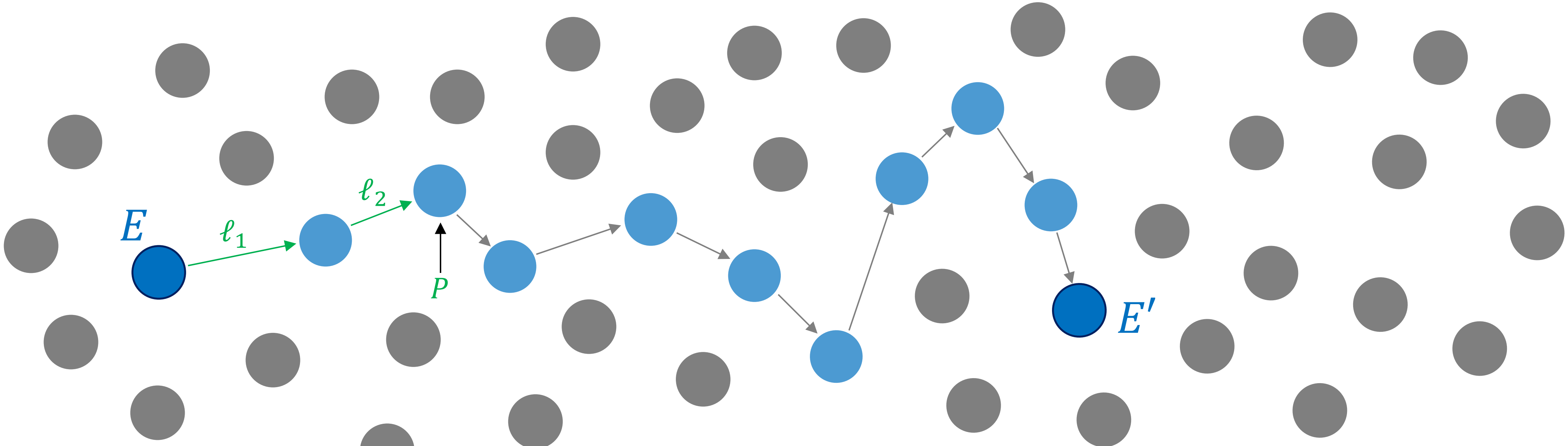
$(+1, +1, -2, +2, 0, -1, -2)$



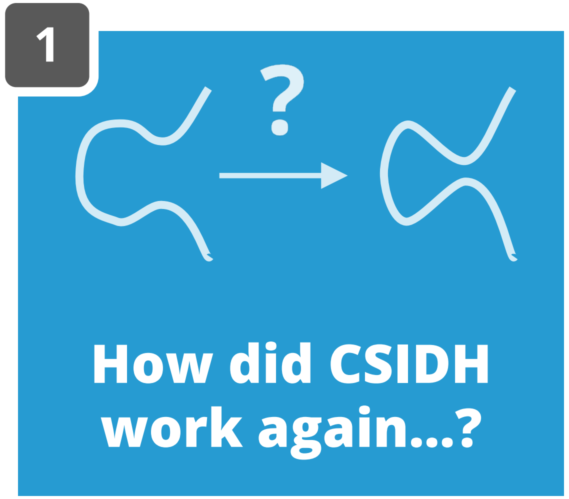
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



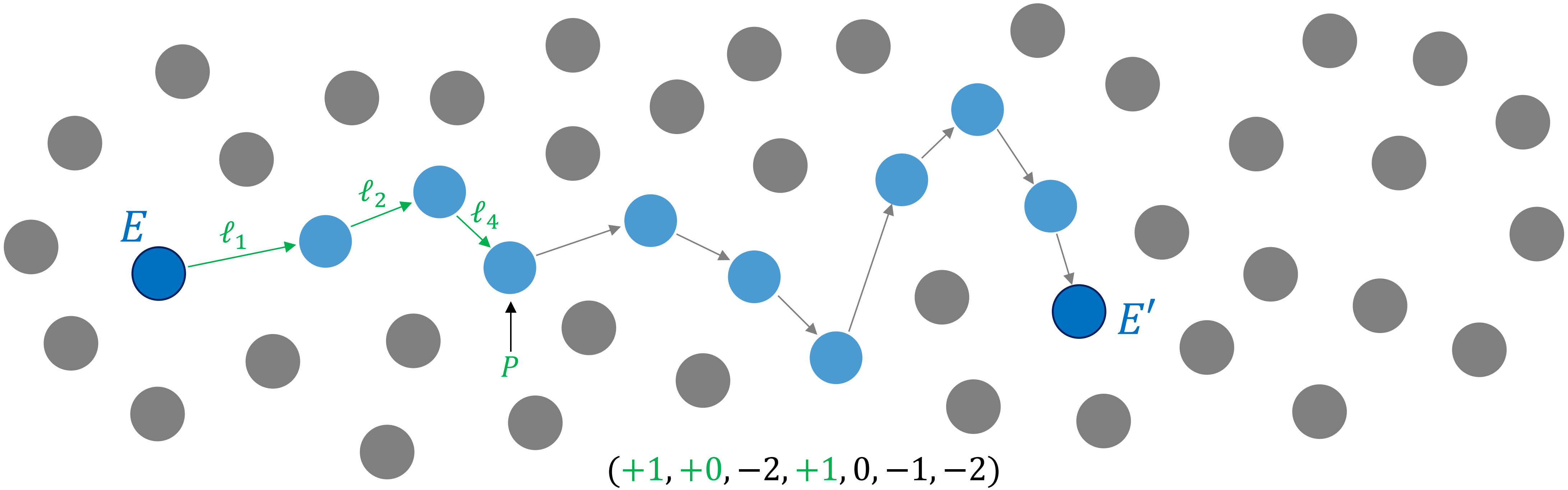
$(+1, +0, -2, +2, 0, -1, -2)$



How to compute walk

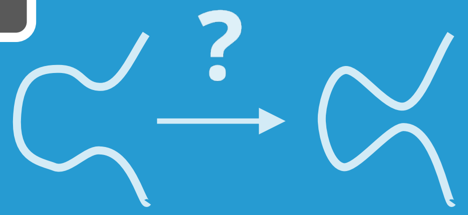
Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



$(+1, +0, -2, +1, 0, -1, -2)$

1

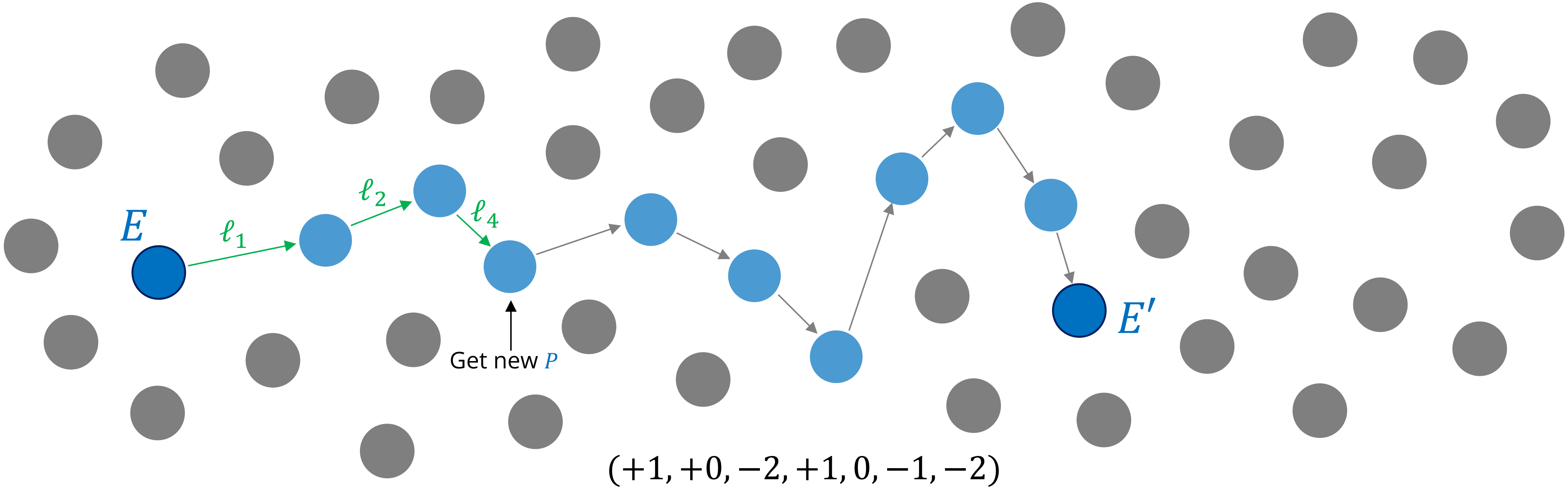


How did CSIDH work again...?

How to compute walk

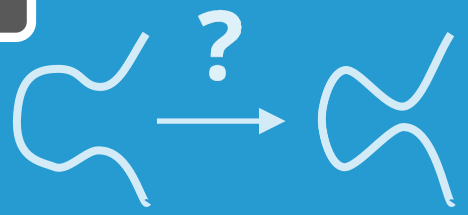
Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



$(+1, +0, -2, +1, 0, -1, -2)$

1

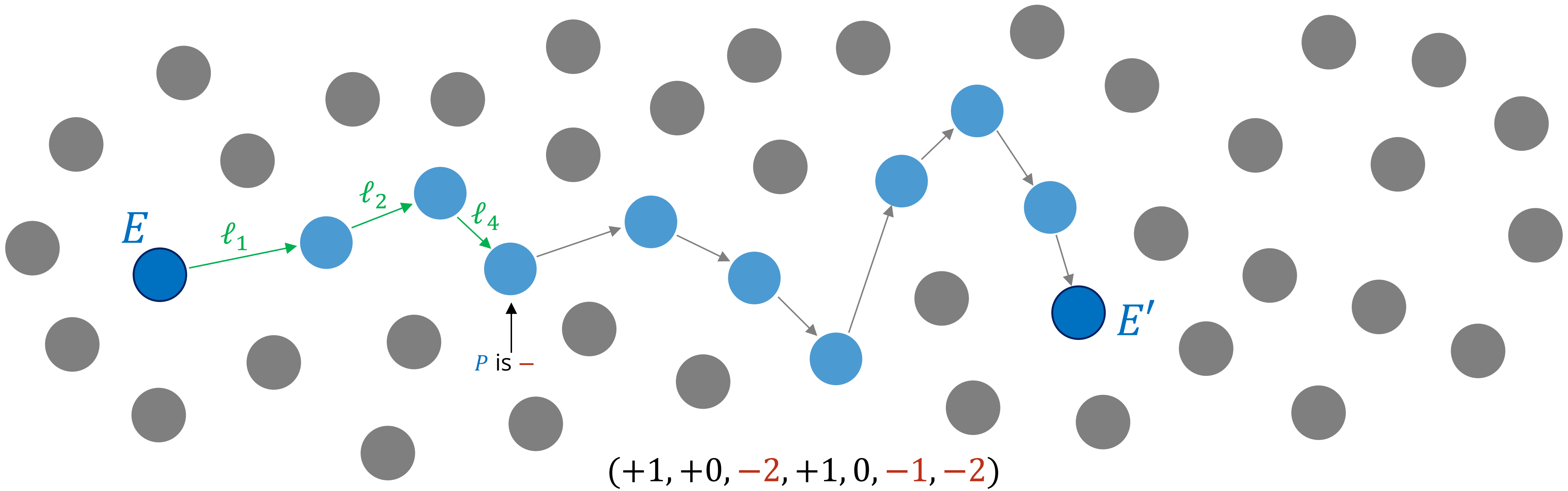


How did CSIDH work again...?

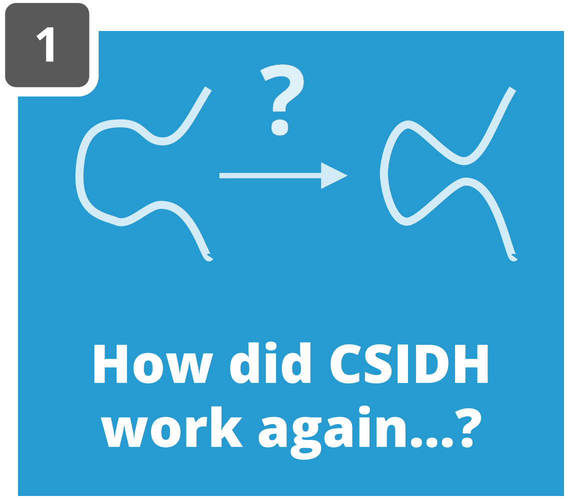
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



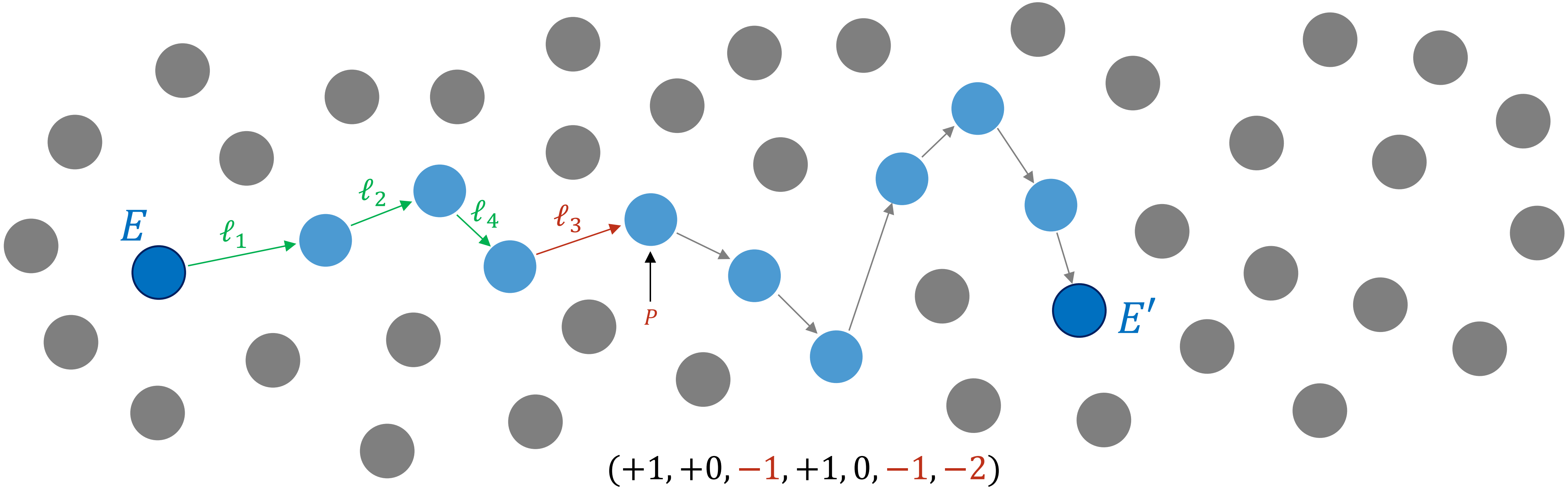
$$(+1, +0, -2, +1, 0, -1, -2)$$

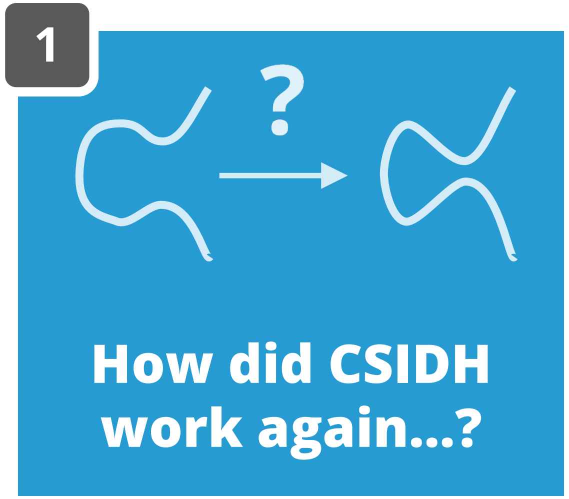


How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed

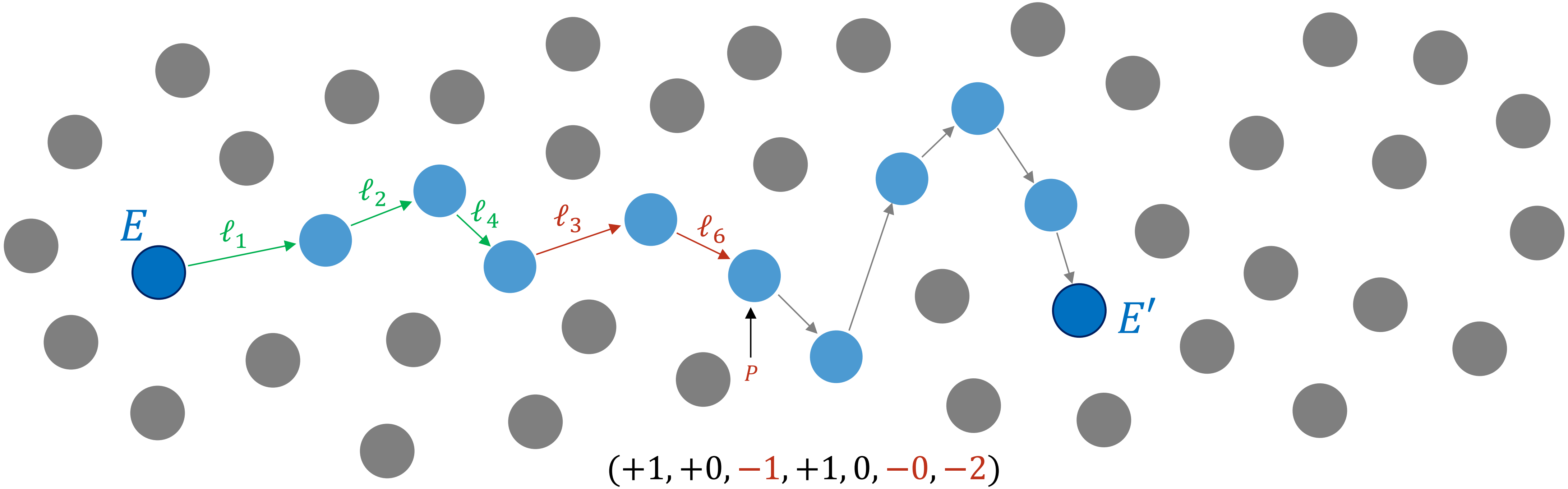




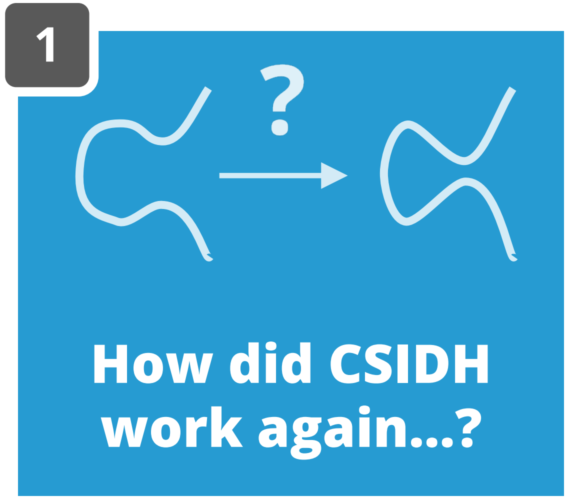
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



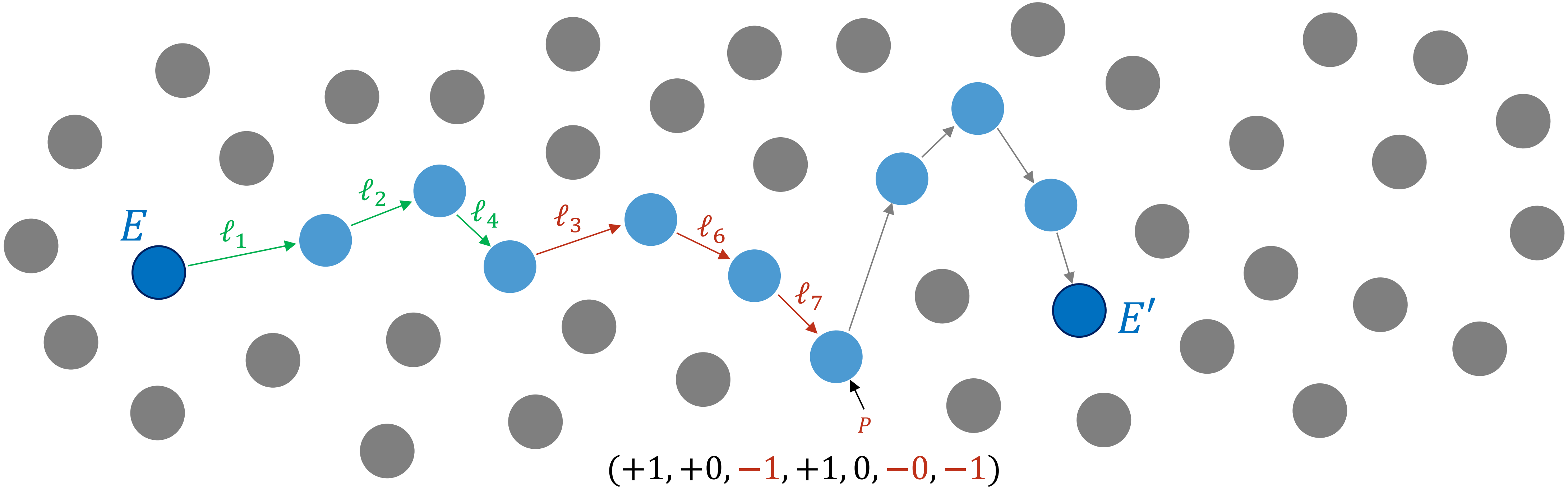
$(+1, +0, -1, +1, 0, -0, -2)$



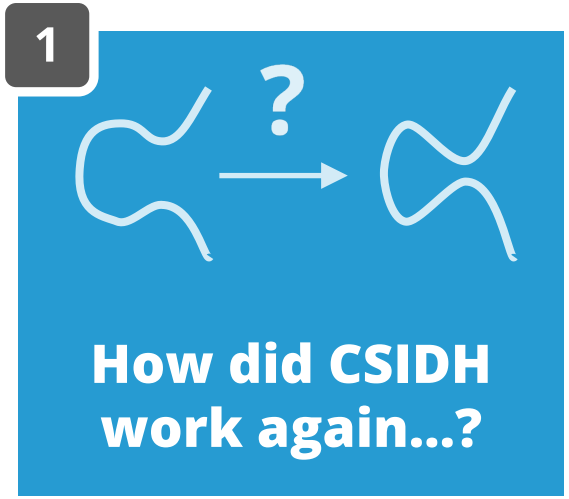
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



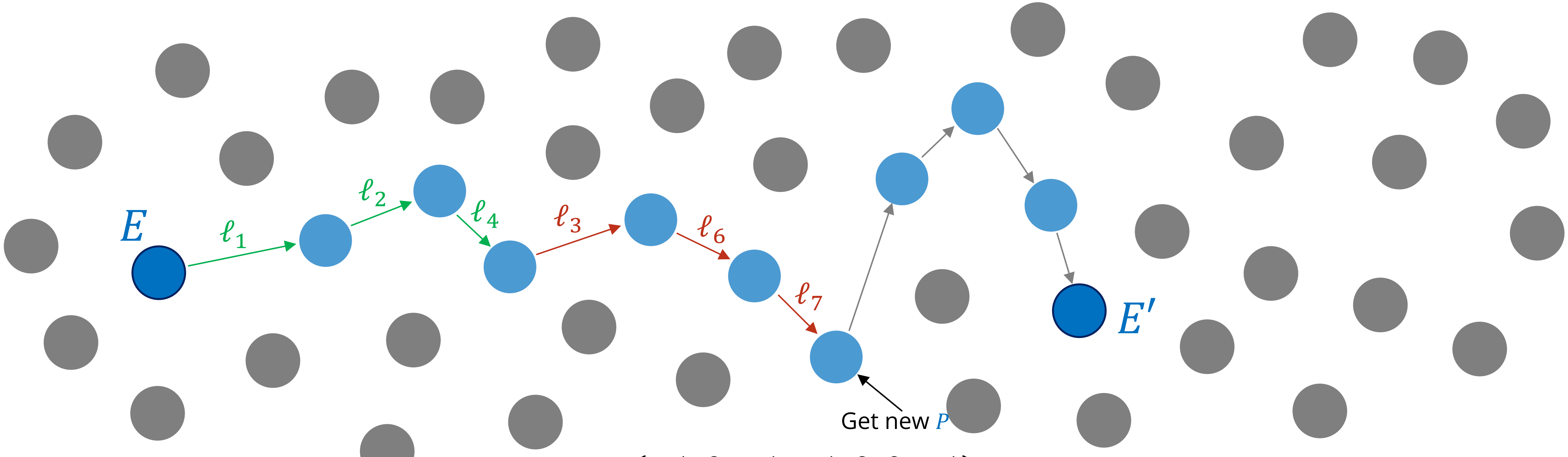
$(+1, +0, -1, +1, 0, -0, -1)$



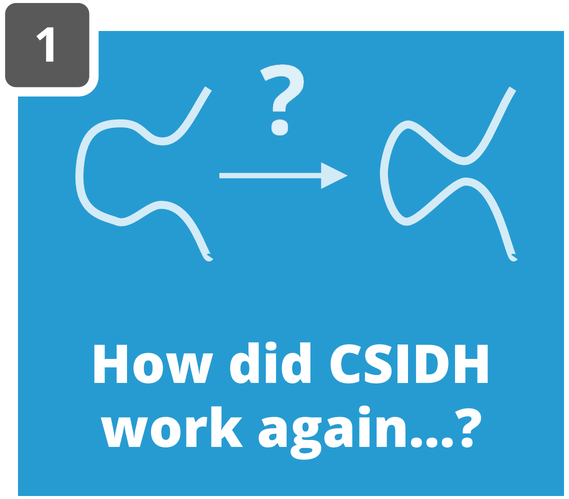
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



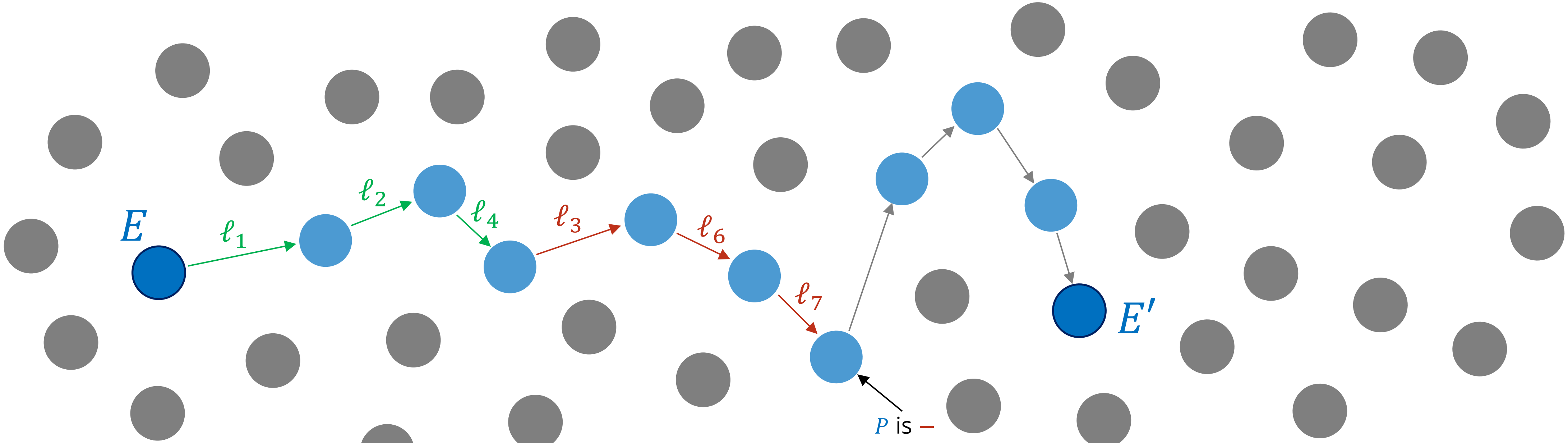
$(+1, 0, -1, +1, 0, 0, -1)$



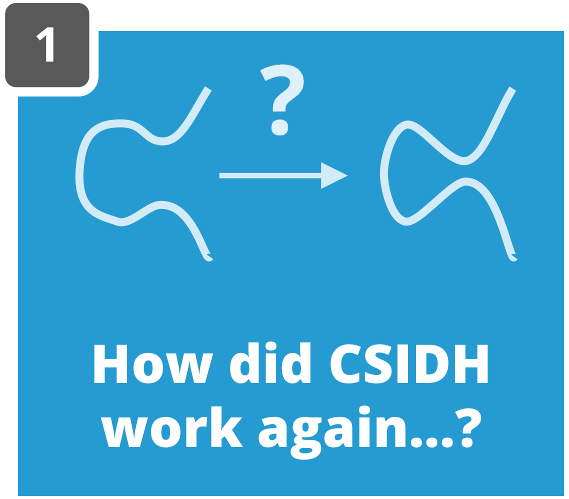
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



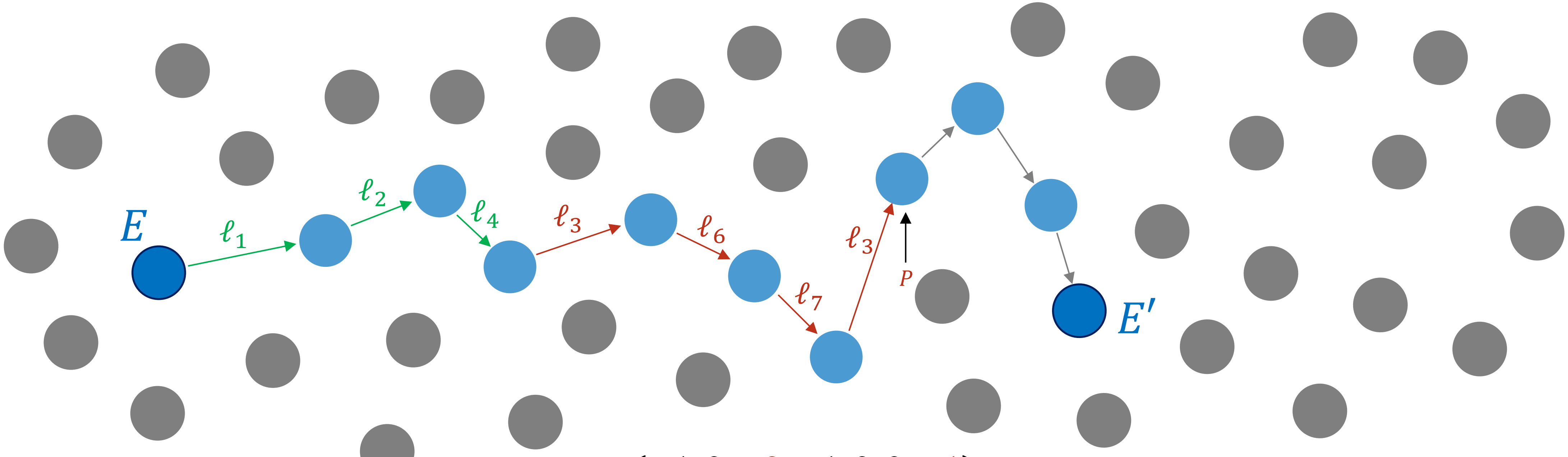
$(+1, 0, -1, +1, 0, 0, -1)$



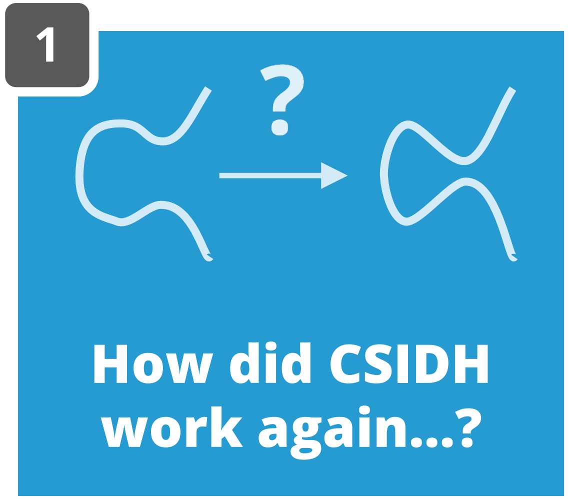
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



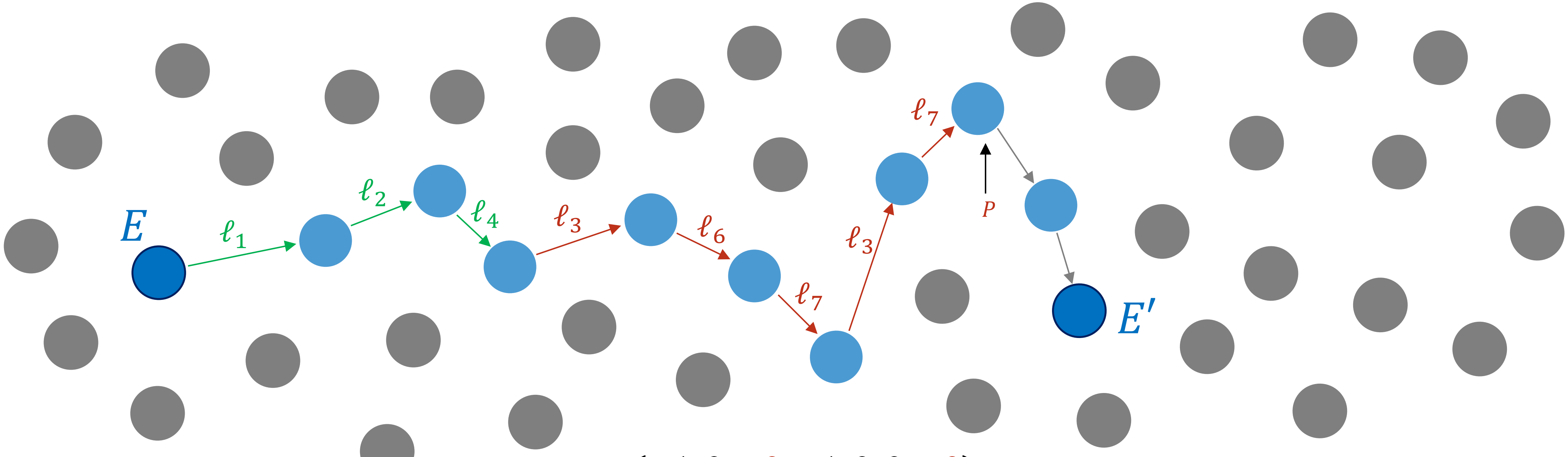
$(+1, 0, -0, +1, 0, 0, -1)$



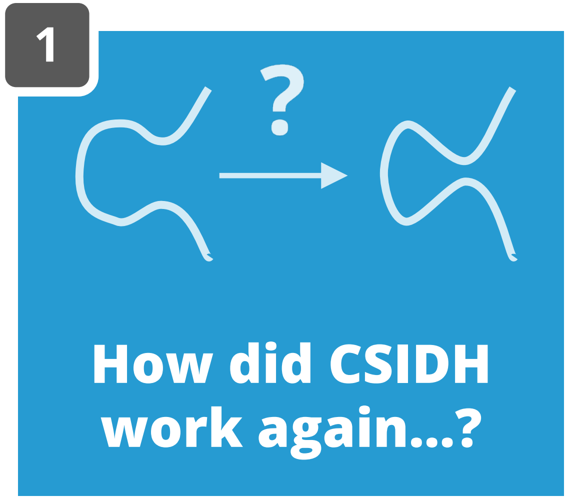
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



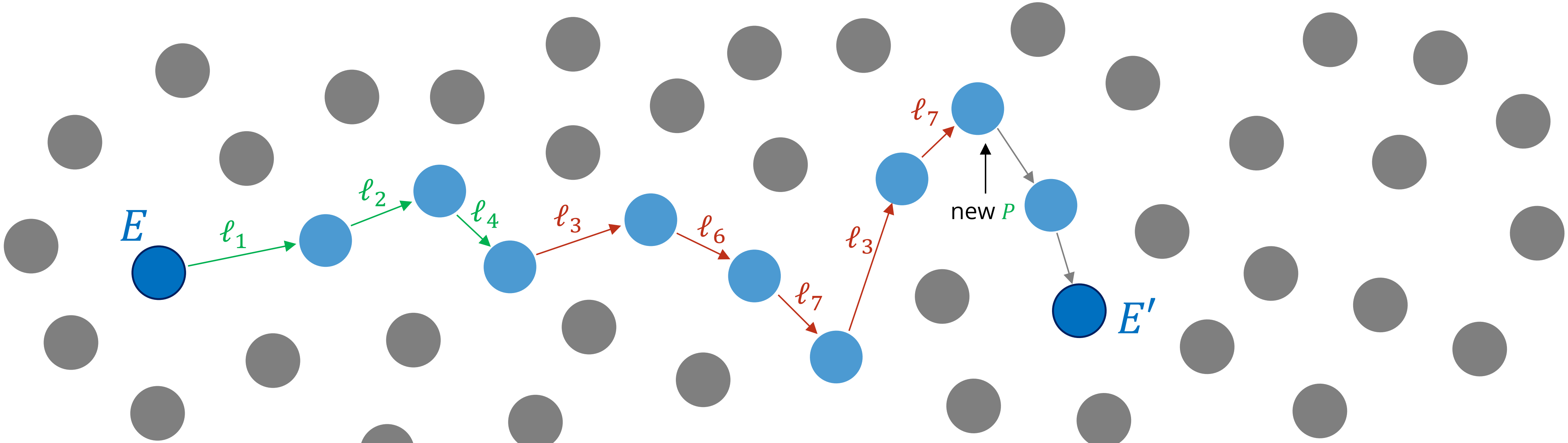
$(+1, 0, -0, +1, 0, 0, -0)$



How to compute walk

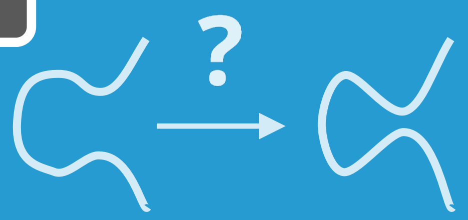
Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



$(+1, 0, 0, +1, 0, 0, 0)$

1

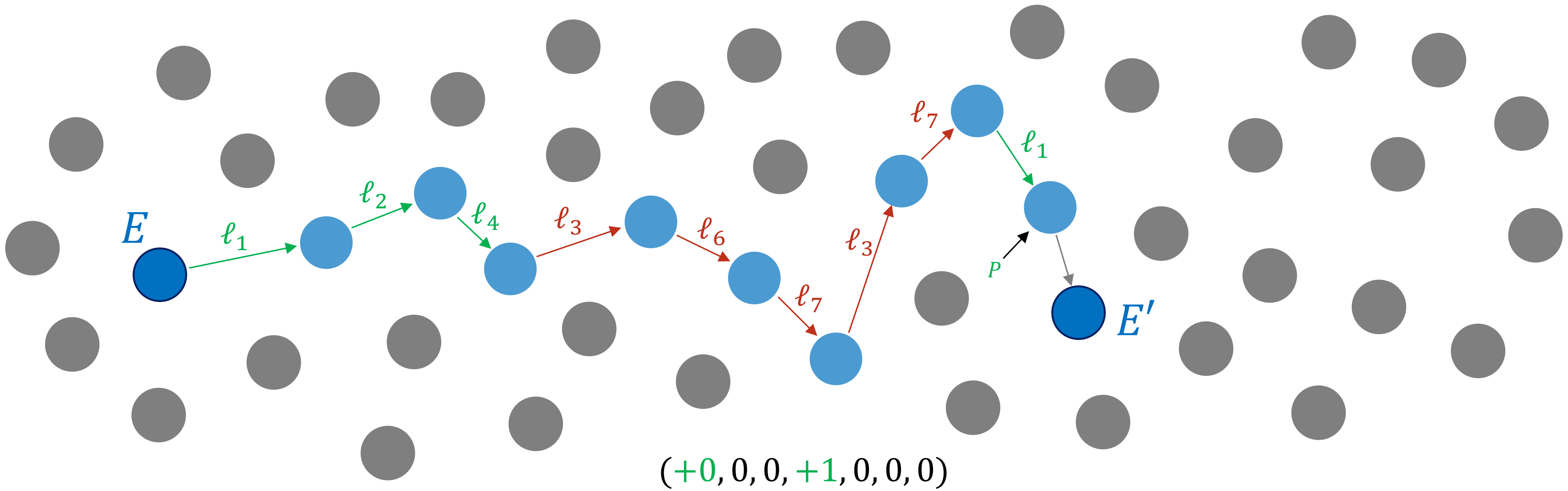


How did CSIDH work again...?

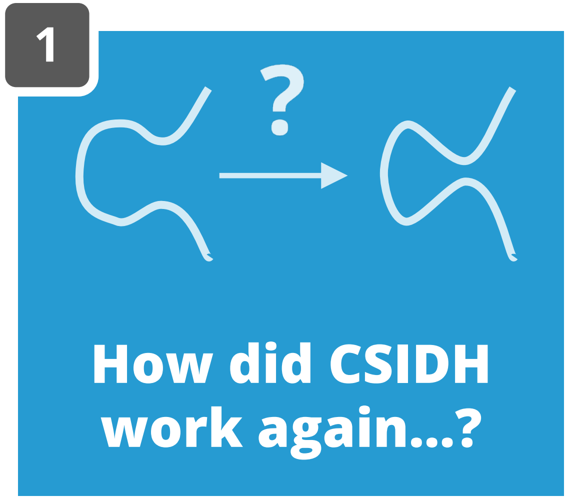
How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



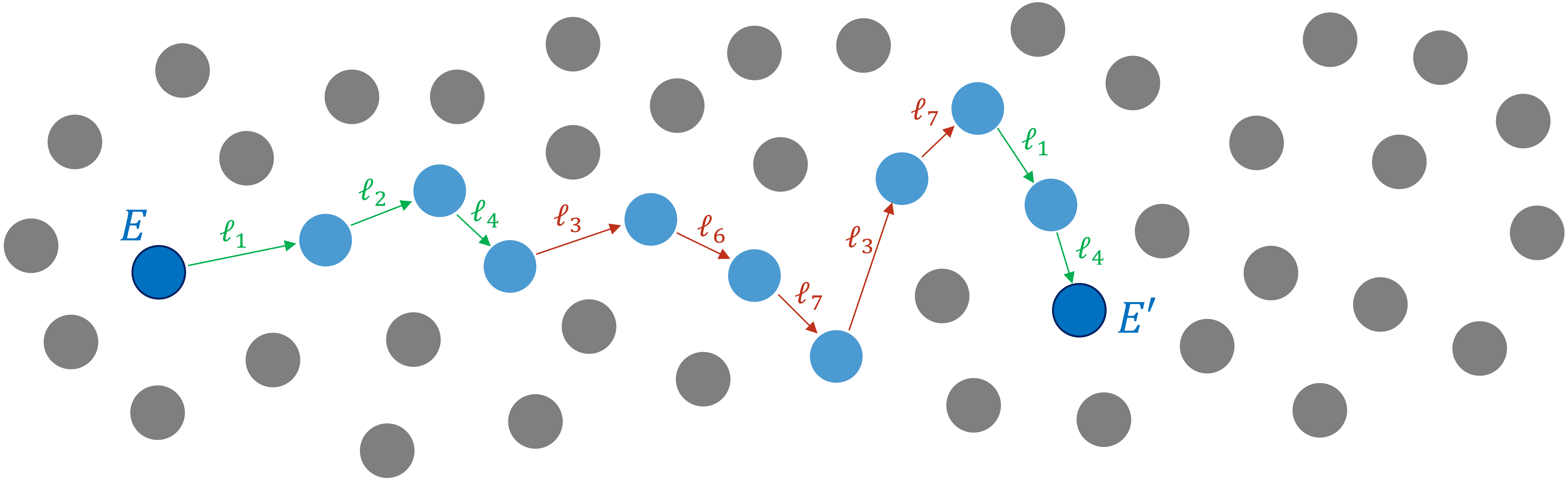
$(+0, 0, 0, +1, 0, 0, 0)$

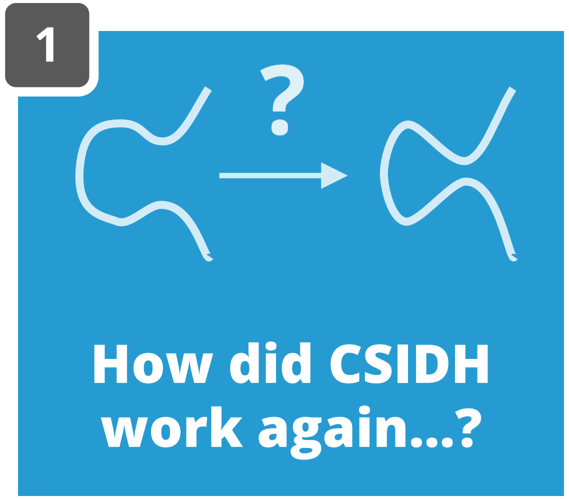


How to compute walk

Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed

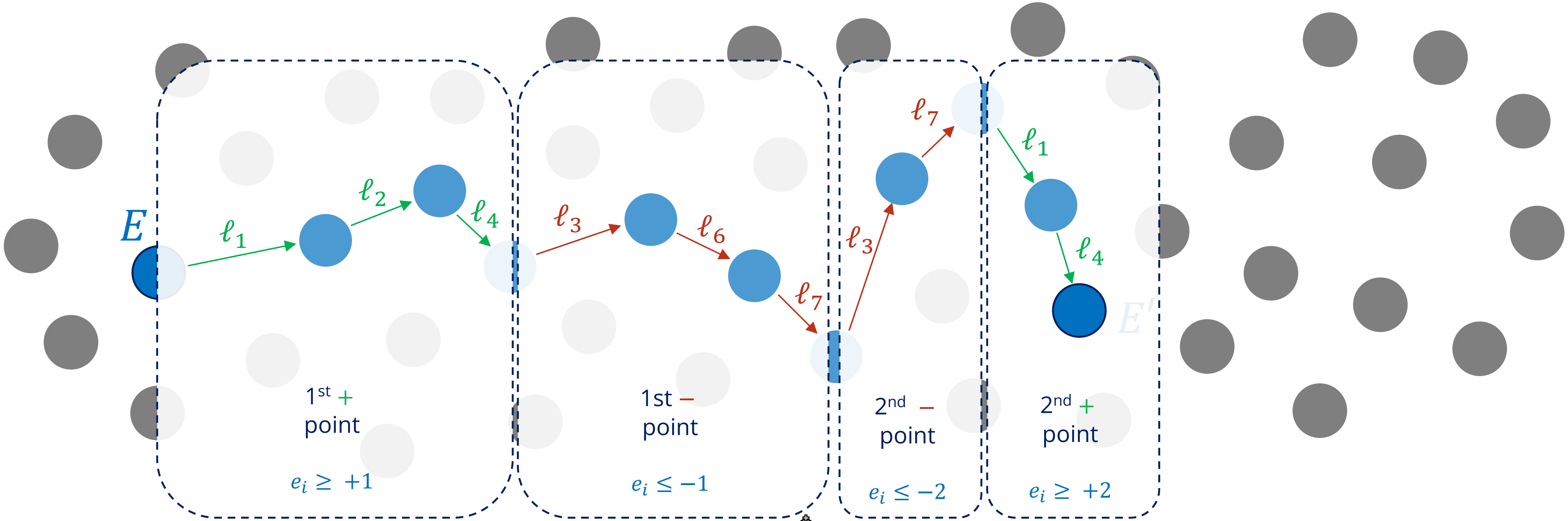




How to compute walk

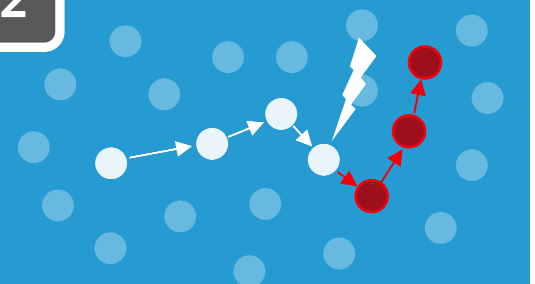
Let's say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$

1. Sample point P, check if $+$ or $-$
2. Can use P to perform one step of each ℓ_i
3. Repeat until path is performed



FAULT INJECTIONS

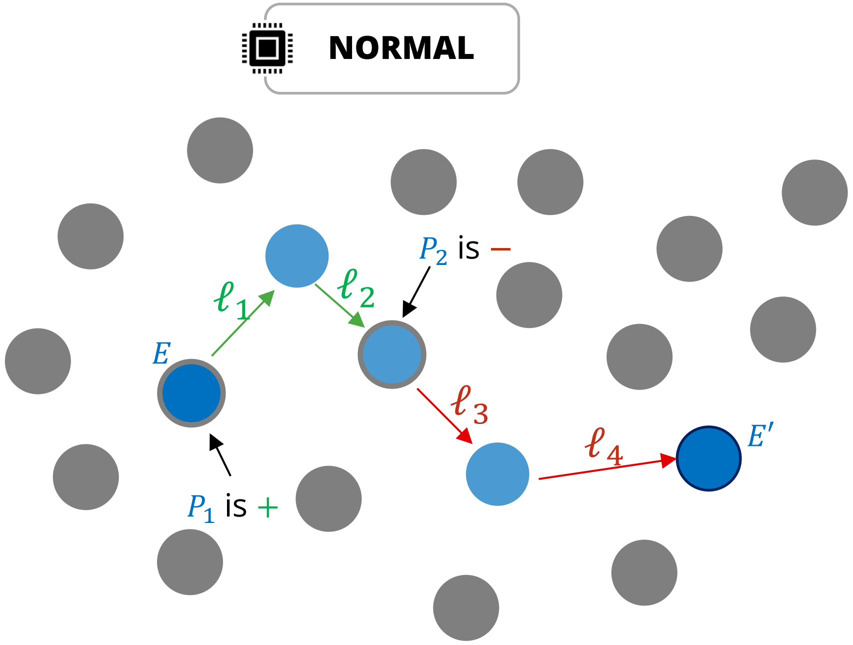
Or: How I Learned to Stop Worrying and Love the Laser

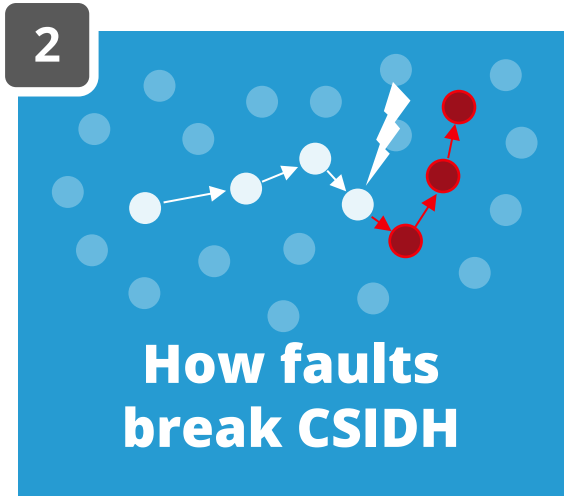


How faults break CSIDH

Toy example

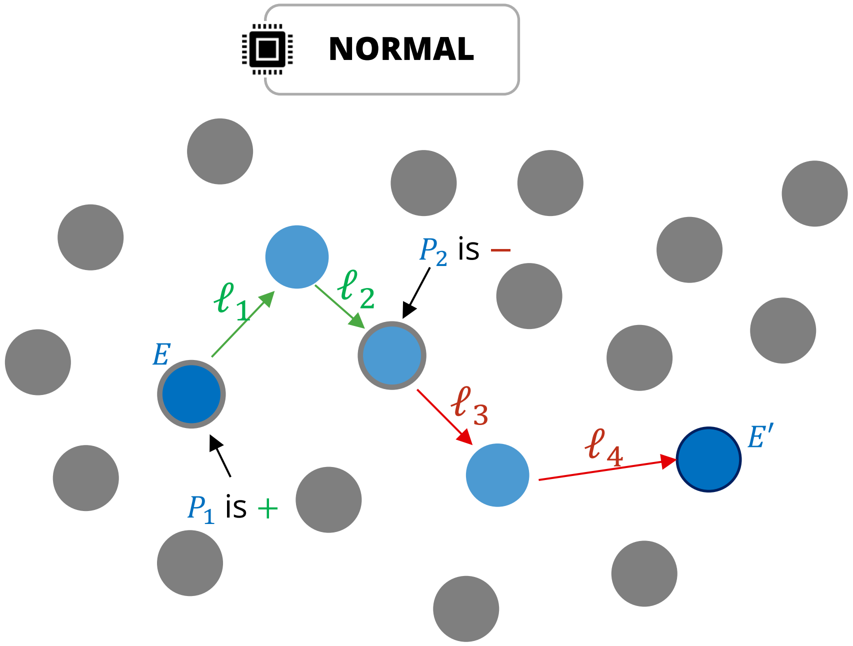
- Let's say $E \rightarrow E'$ is path $(+1, +1, -1, -1, 0, 0, 0)$

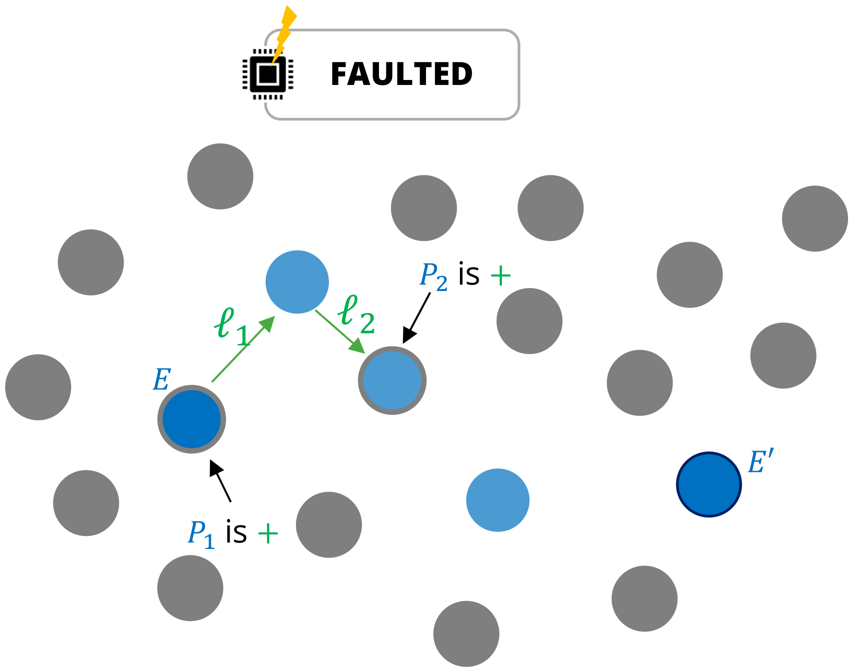




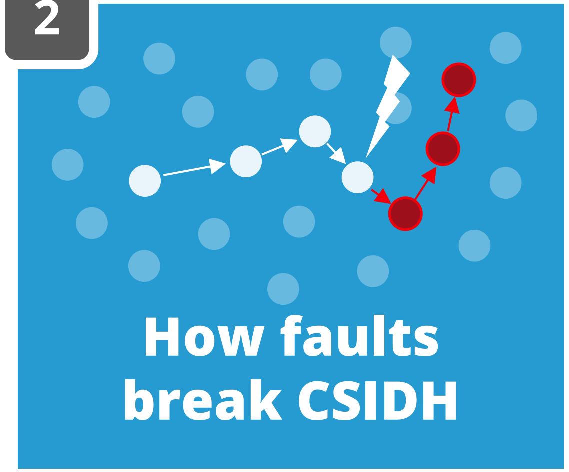
Toy example

- Let's say $E \rightarrow E'$ is path $(+1, +1, -1, -1, 0, 0, 0)$
- we sample a second positive point
- but fault inject so device thinks its negative



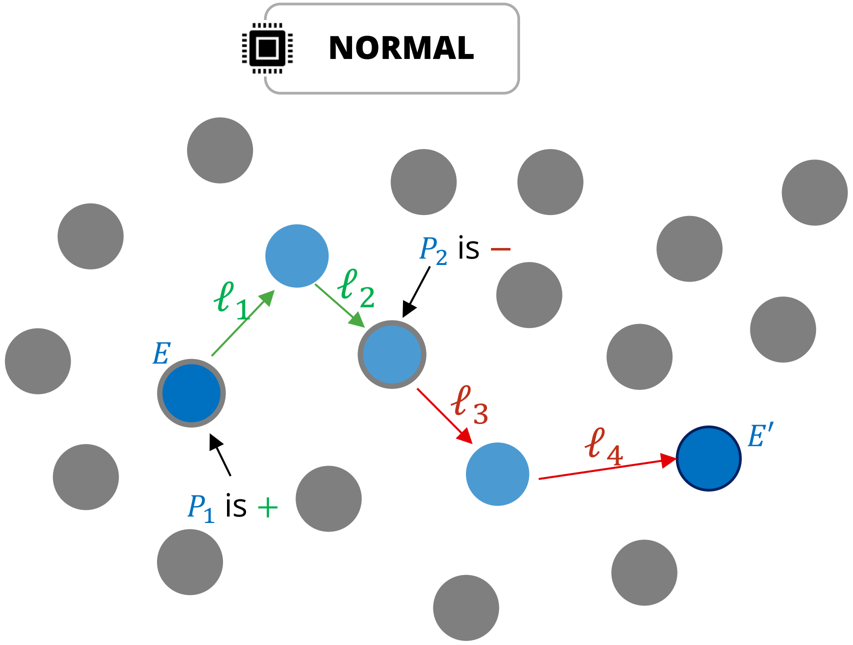


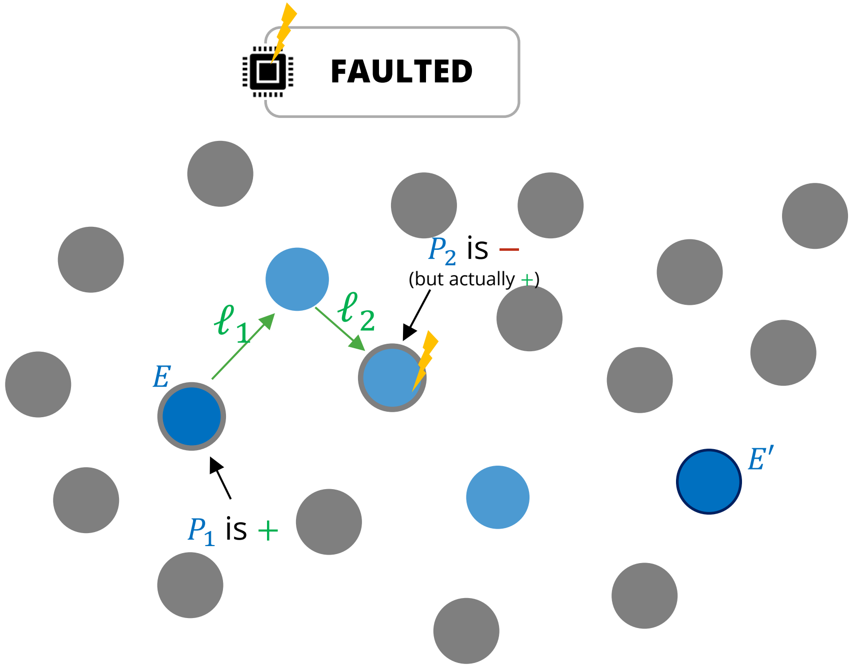
2



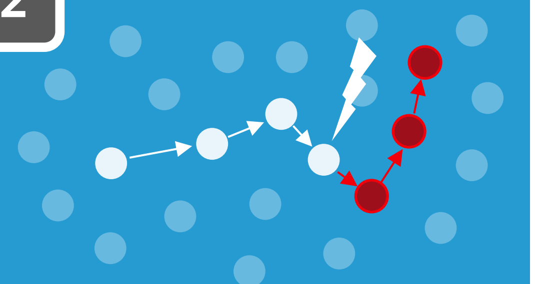
Toy example

- Let's say $E \rightarrow E'$ is path $(+1, +1, -1, -1, 0, 0, 0)$
- we sample a second positive point
- but fault inject so device thinks its negative





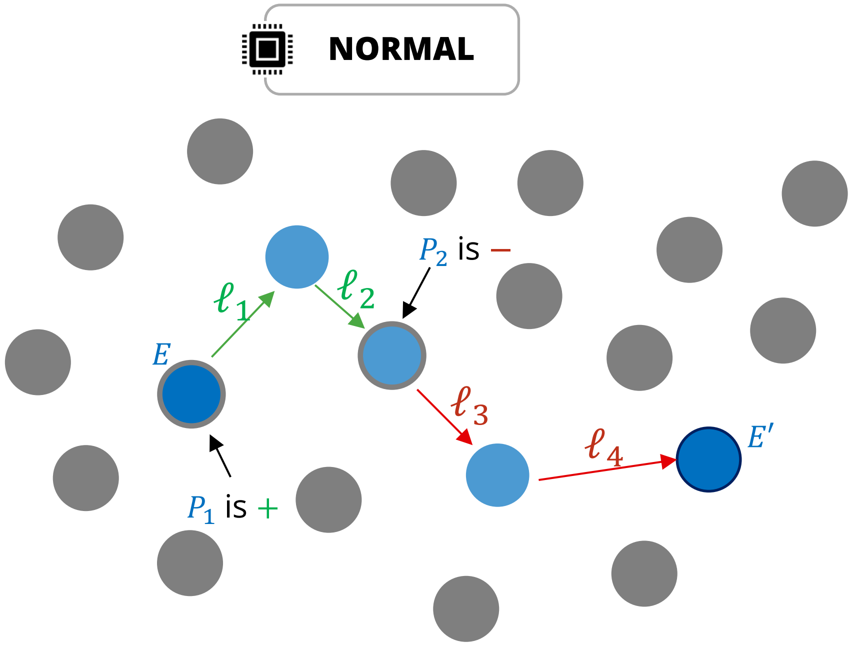
2

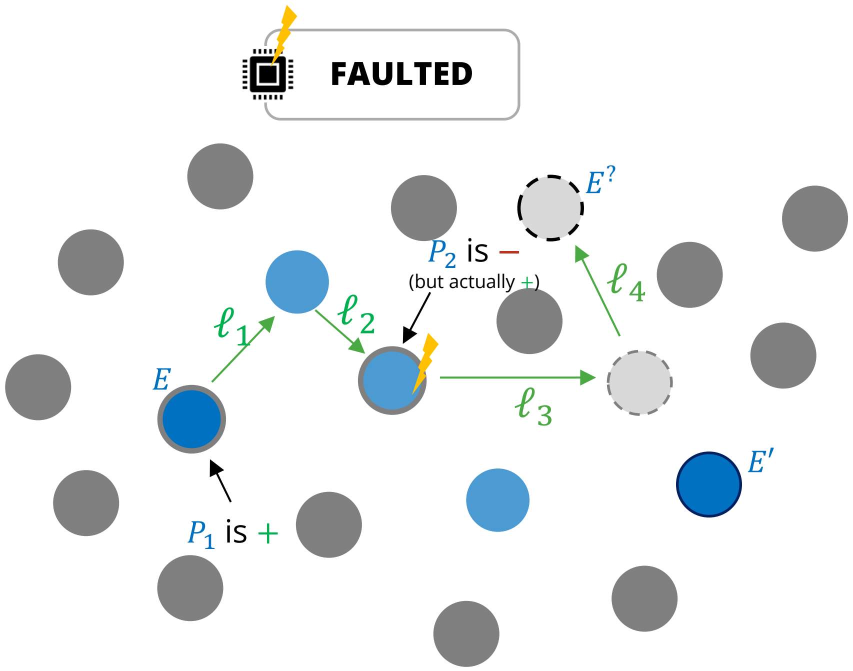


How faults break CSIDH

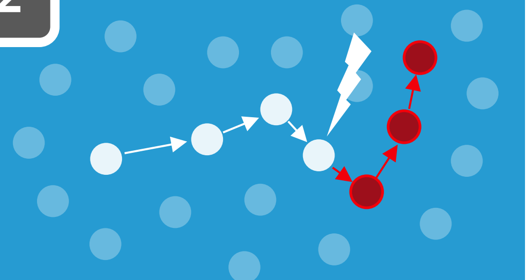
Toy example

- Let's say $E \rightarrow E'$ is path $(+1, +1, -1, -1, 0, 0, 0)$
- we sample a second positive point
- but fault inject so device thinks its negative





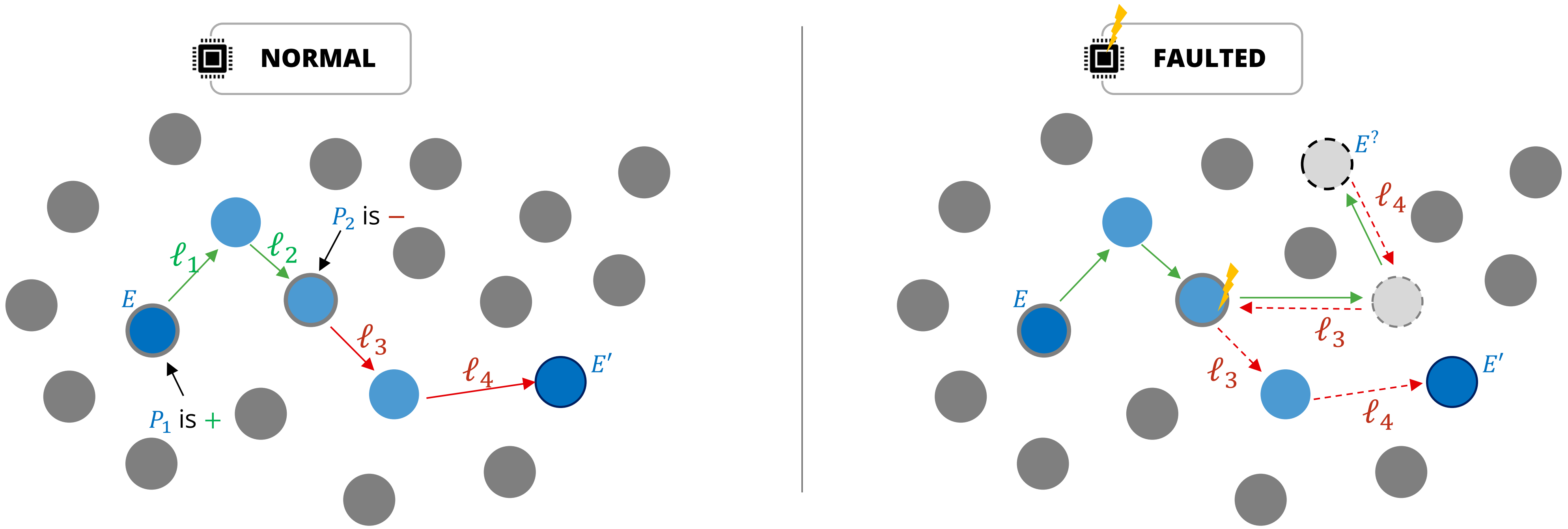
2



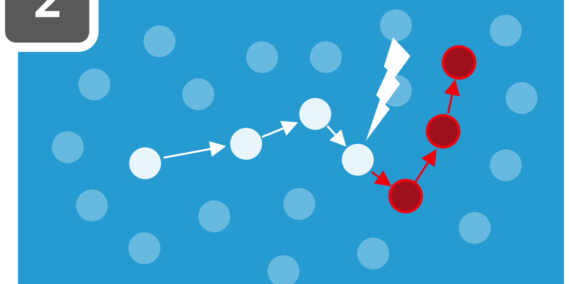
How faults break CSIDH

Toy example

- Let's say $E \rightarrow E'$ is path $(+1, +1, -1, -1, 0, 0, 0)$
- we sample a second positive point
- but fault inject so device thinks its negative



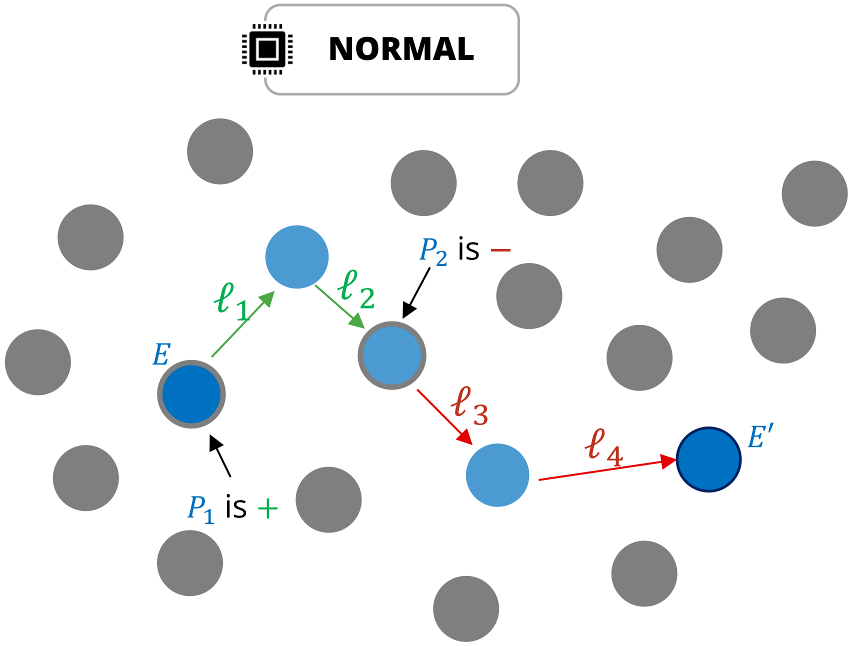
2

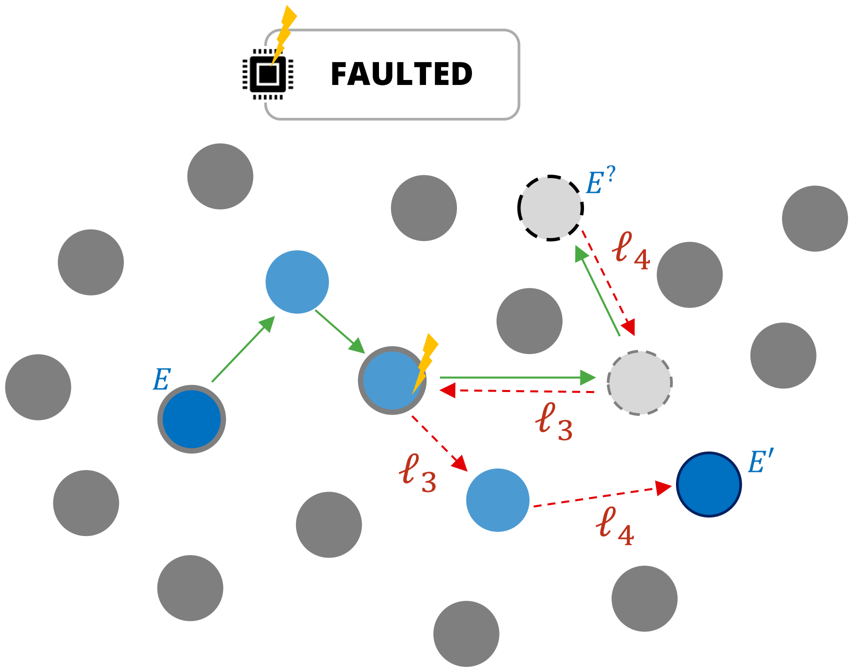


How faults break CSIDH

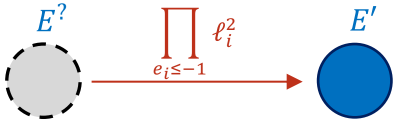
Toy example

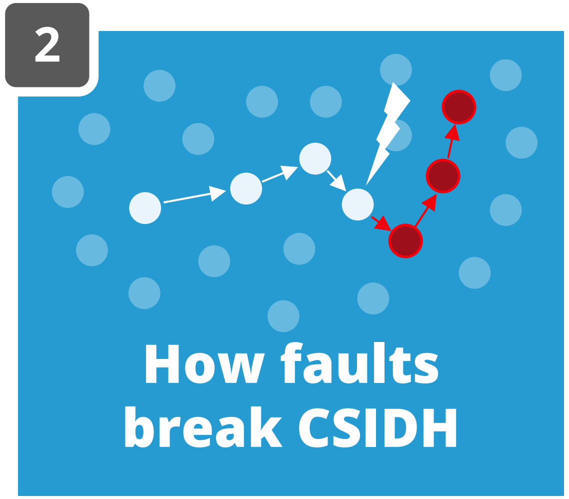
- Let's say $E \rightarrow E'$ is path $(+1,+1,-1,-1,0,0,0)$
- we sample a second positive point
- but fault inject so device thinks its negative





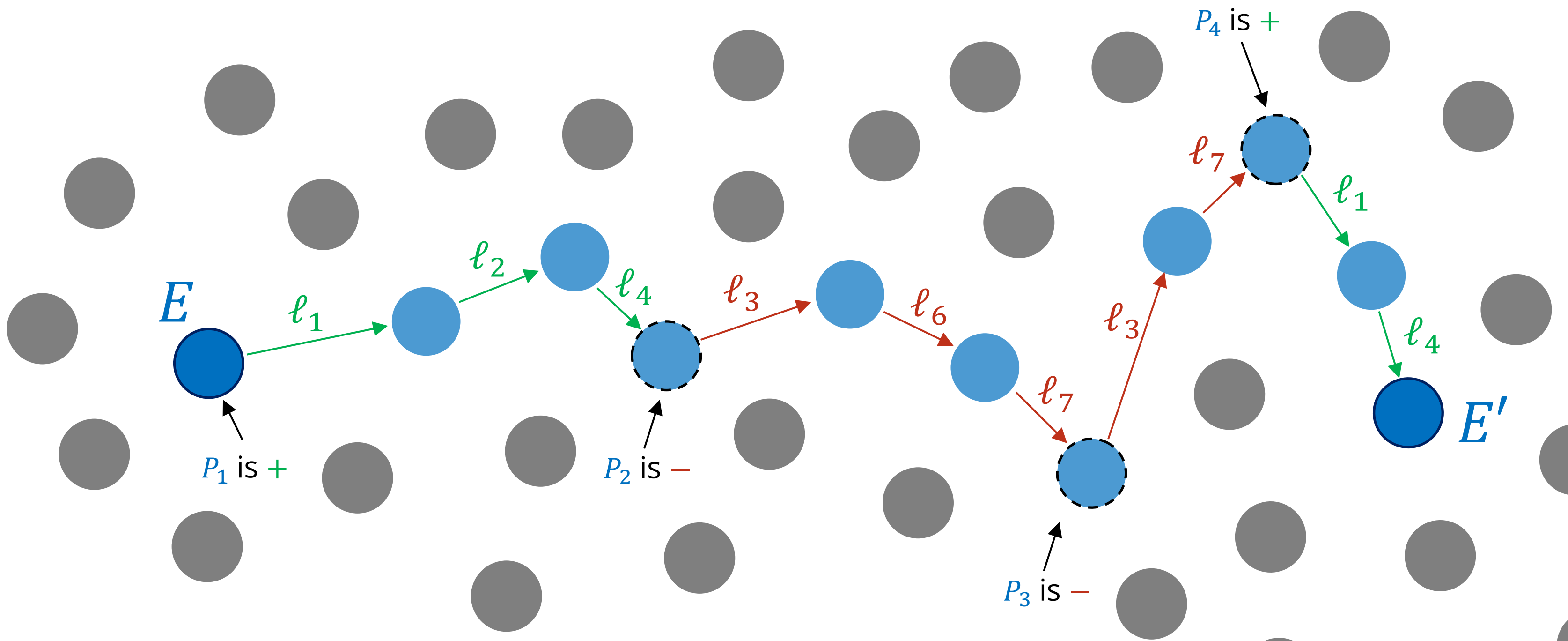
off by



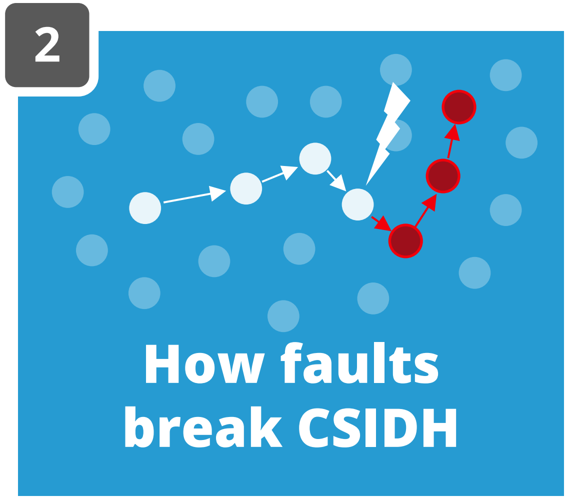


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

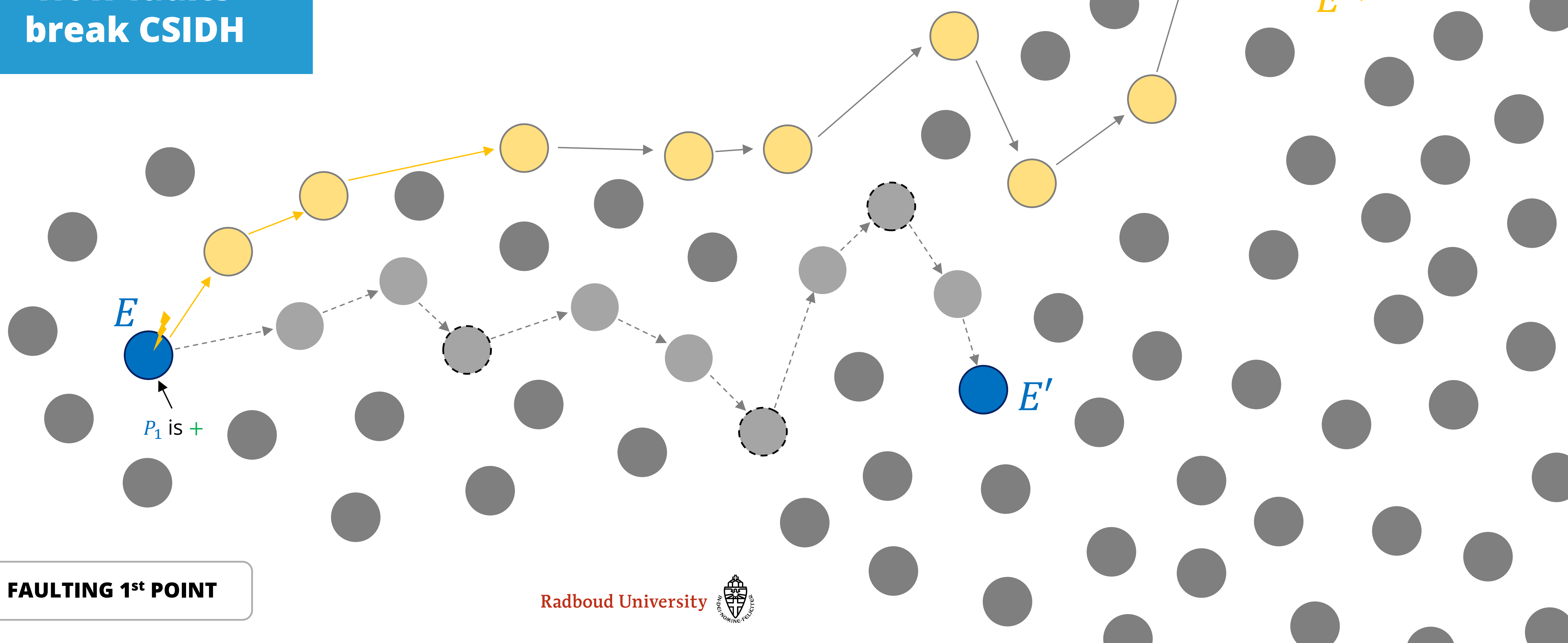


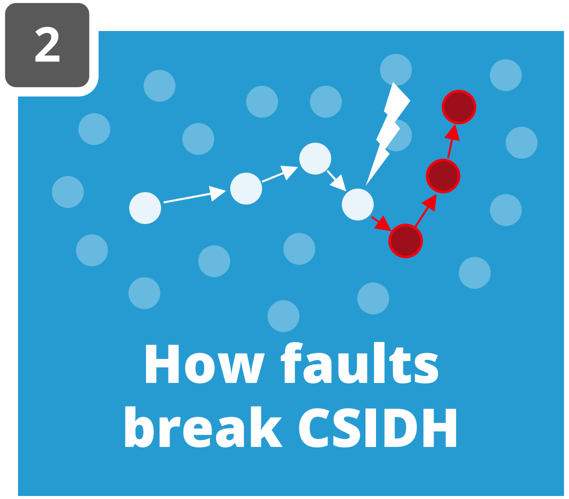
NORMAL



Back to example

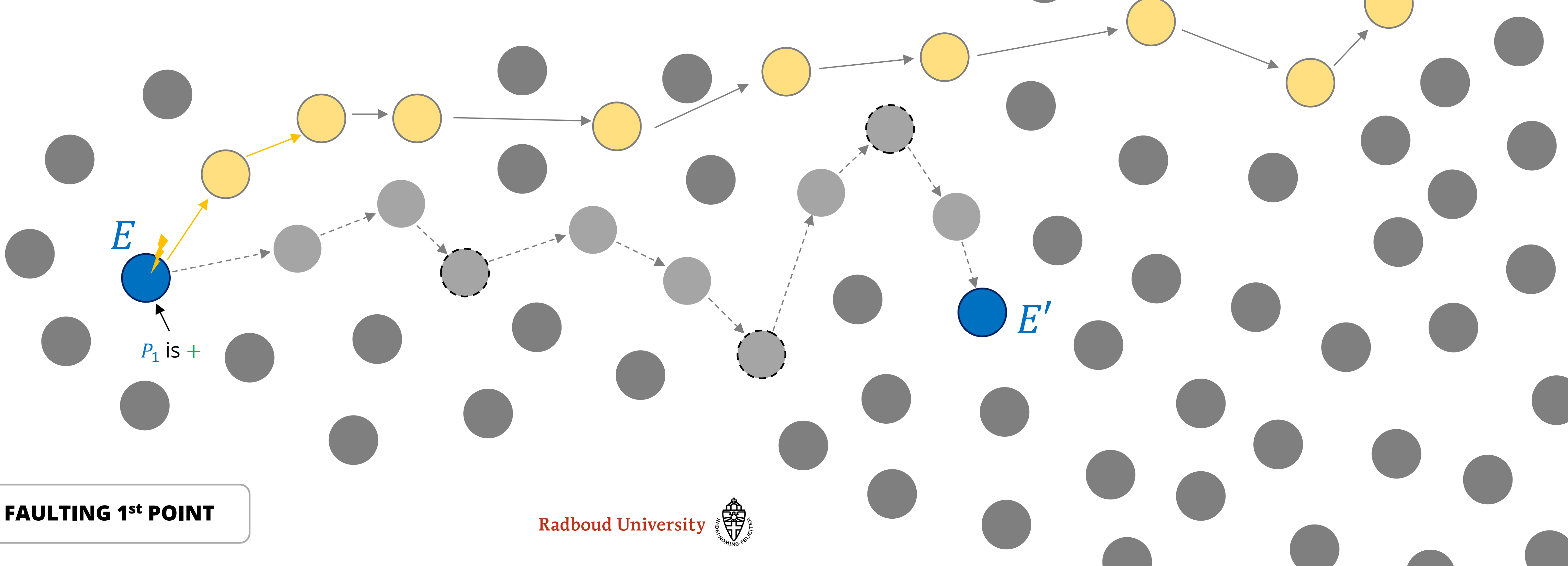
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

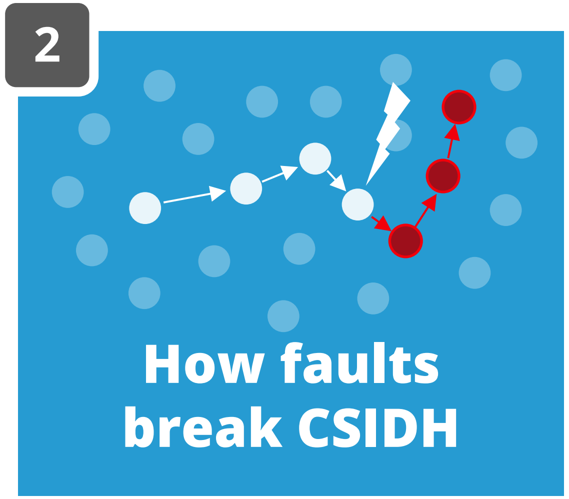




Back to example

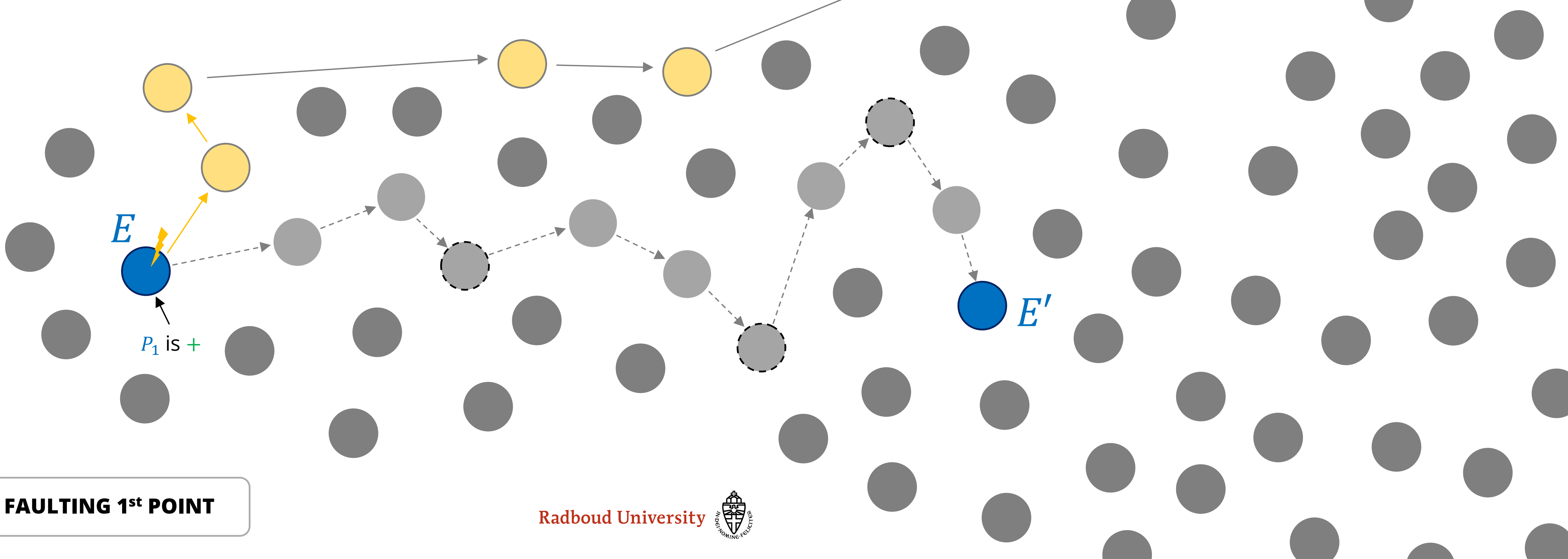
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

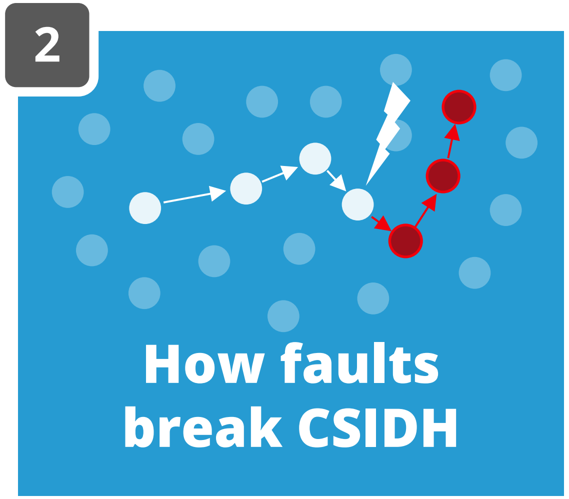




Back to example

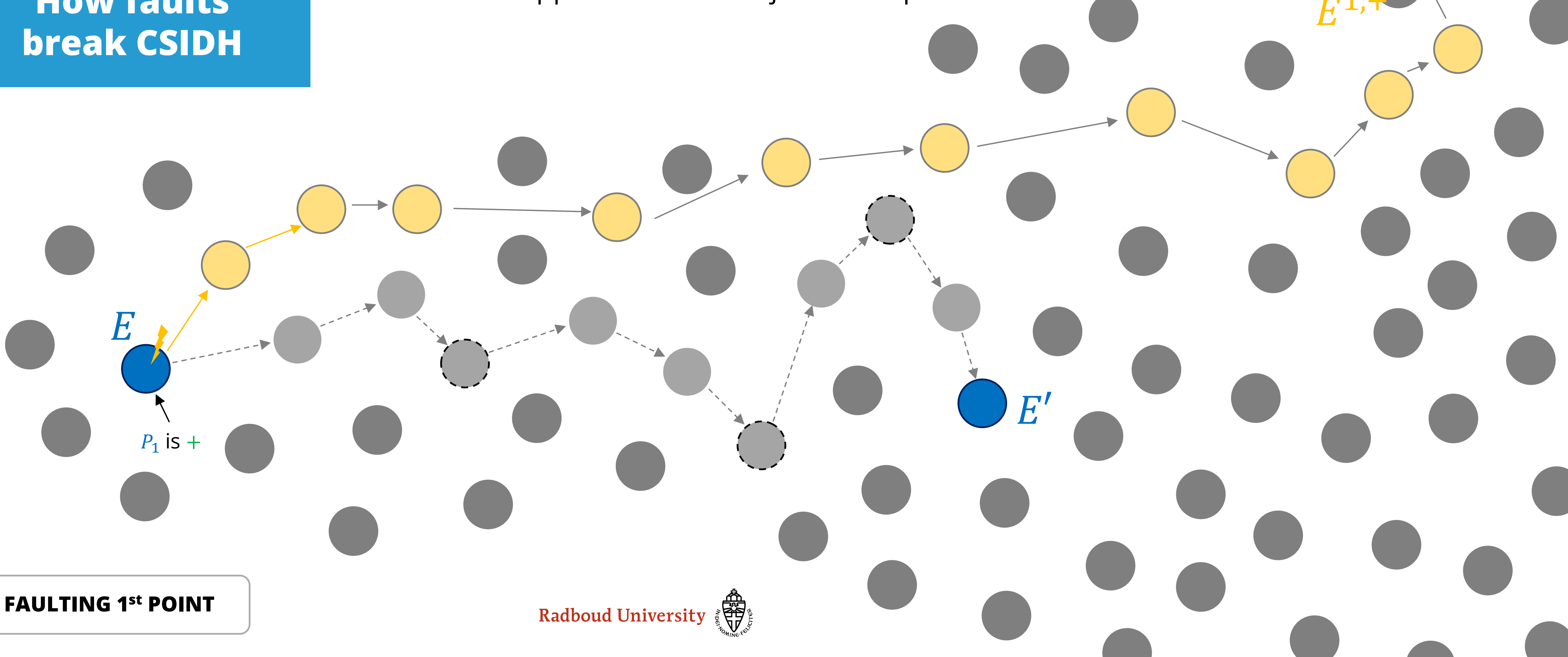
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



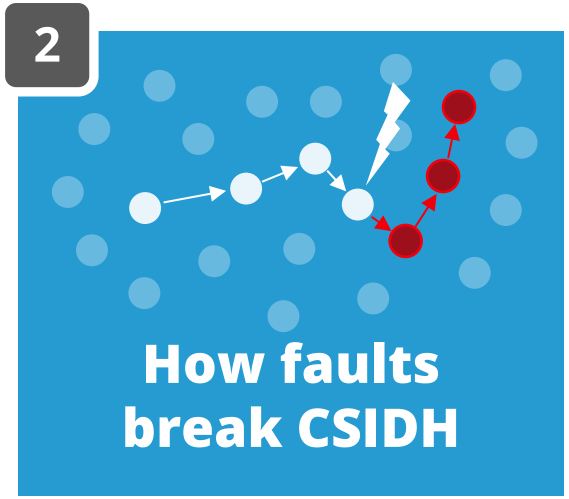


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

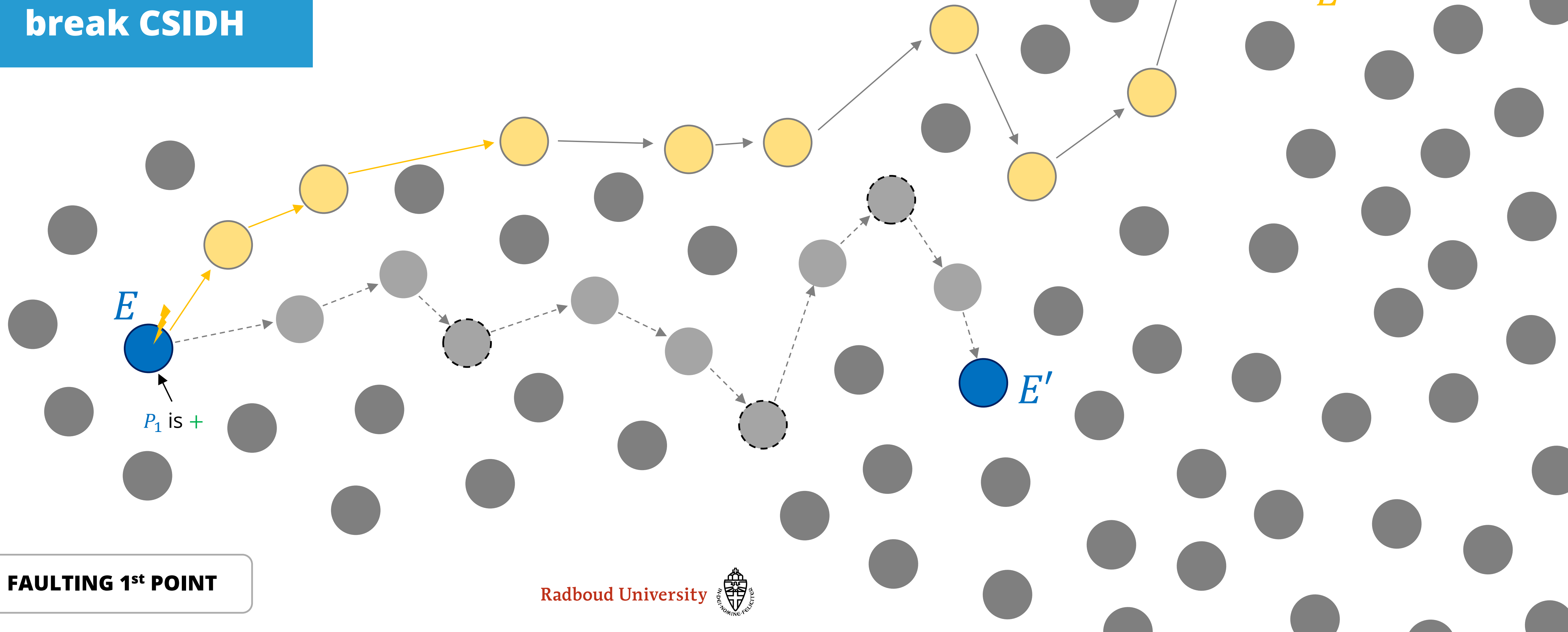


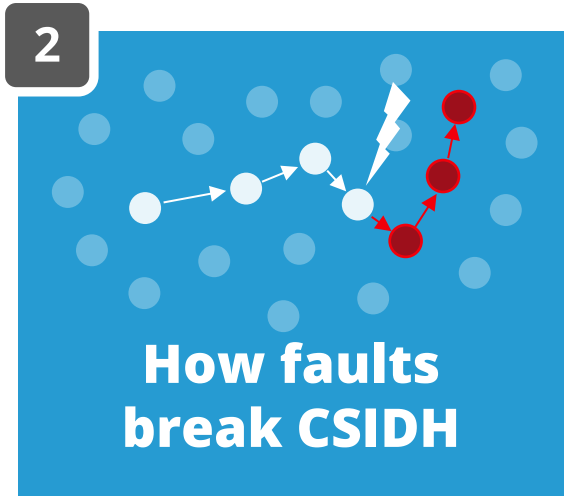
FAULTING 1st POINT



Back to example

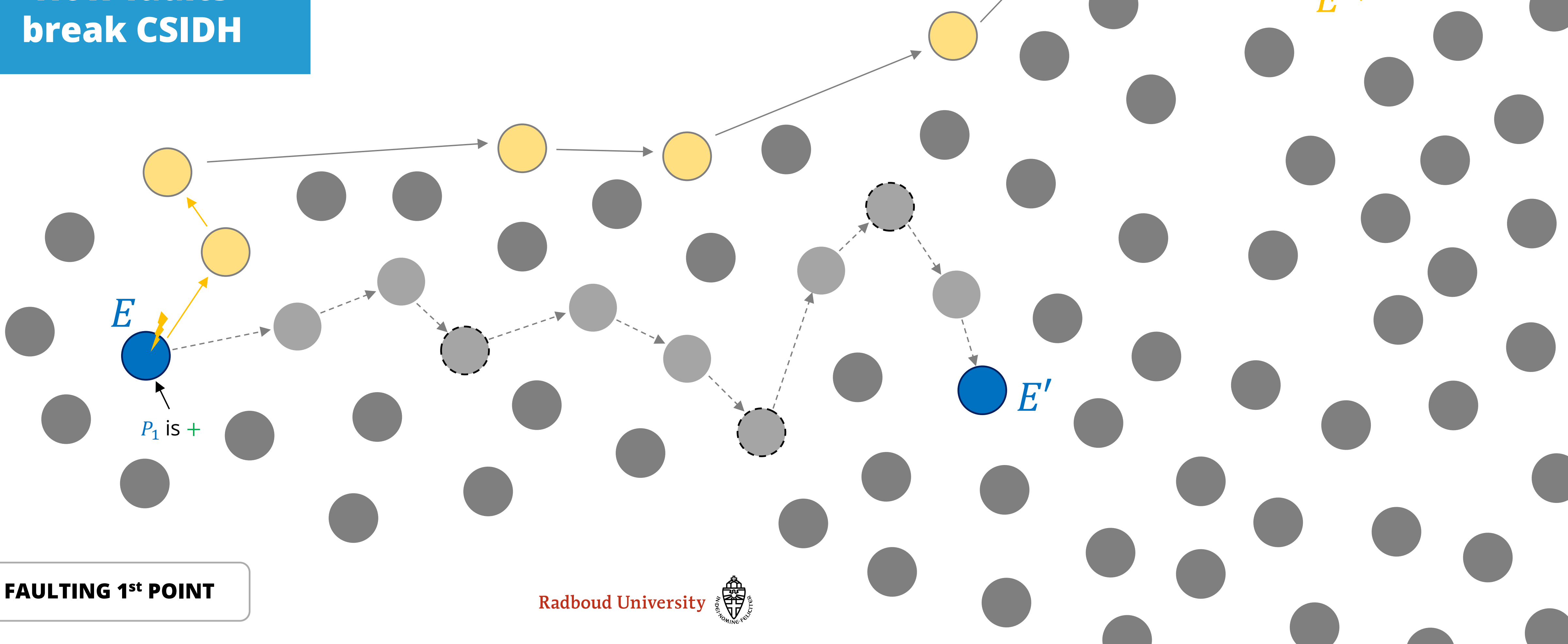
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?





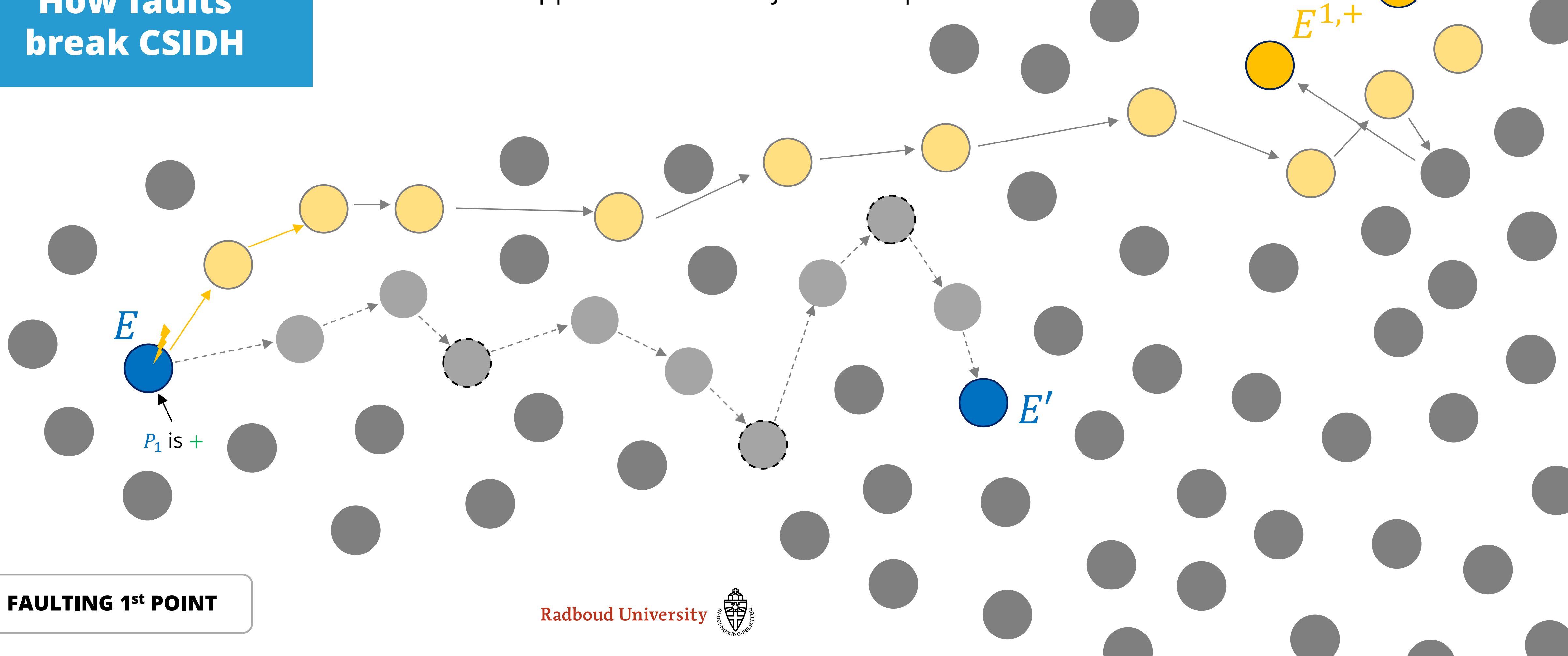
Back to example

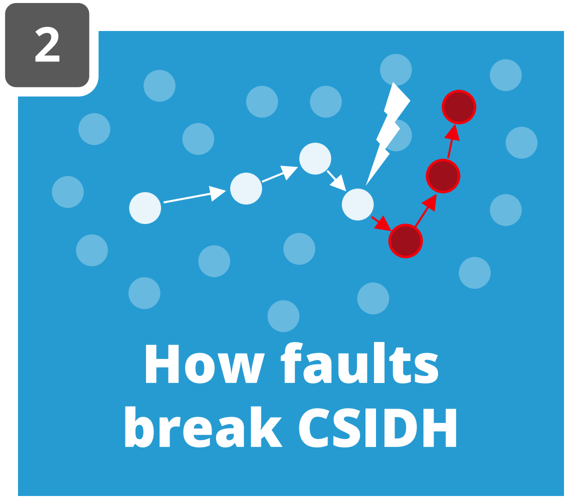
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



Back to example

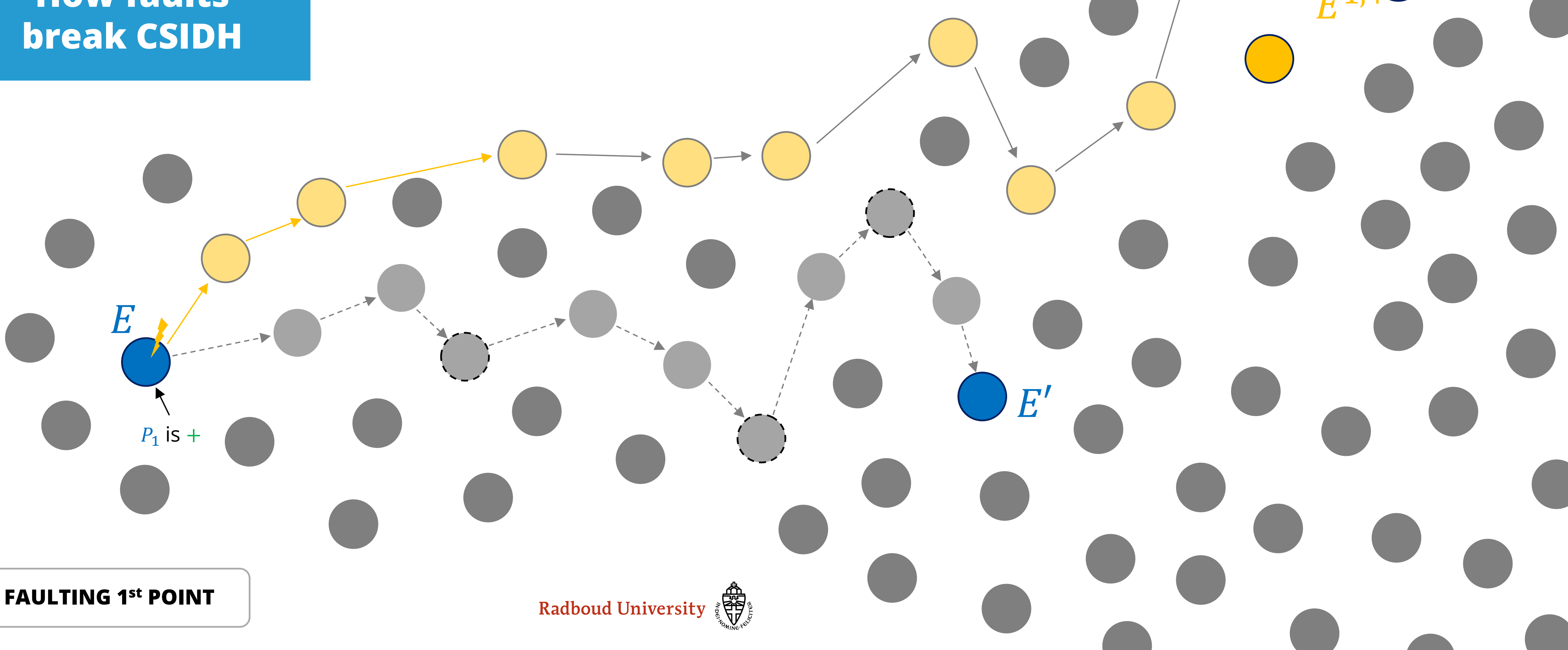
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



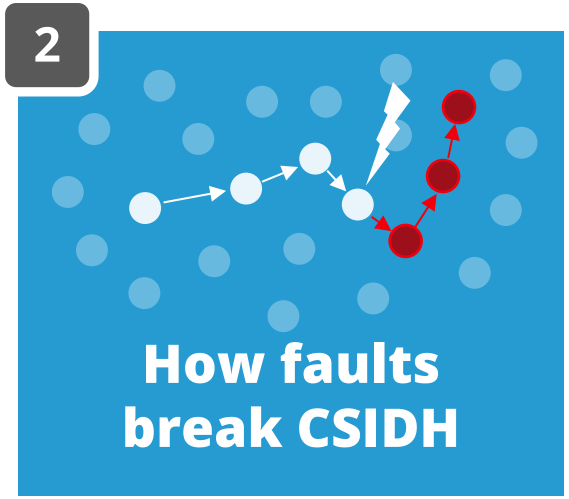


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

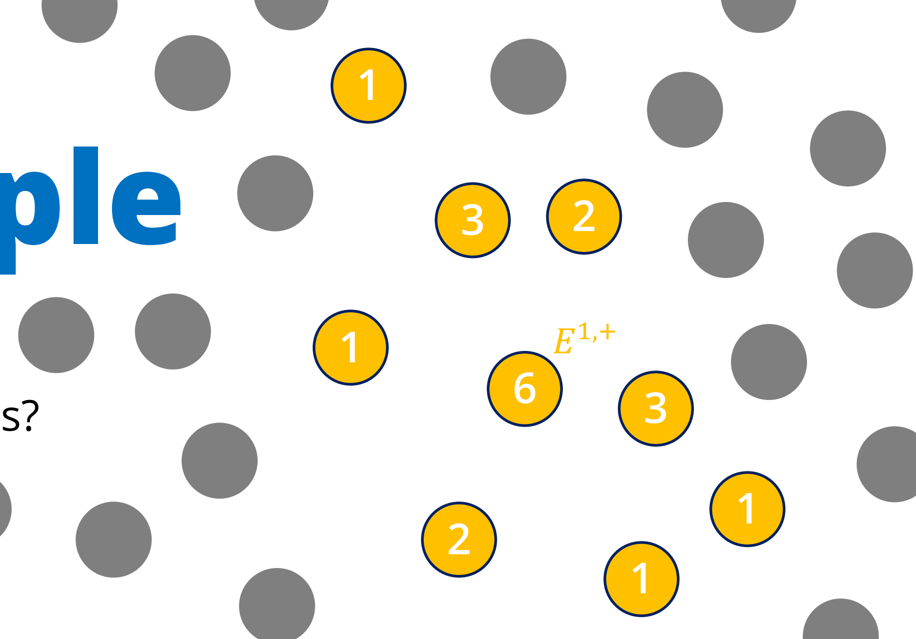


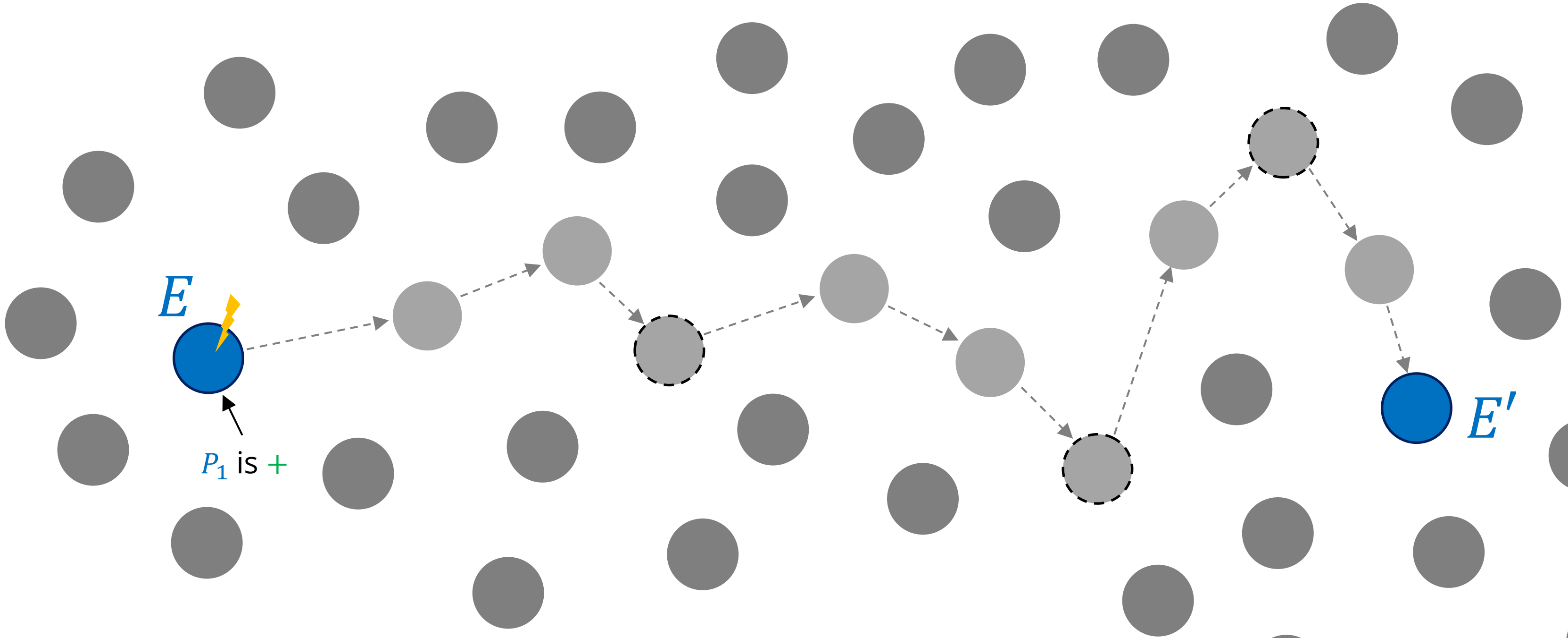
FAULTING 1st POINT

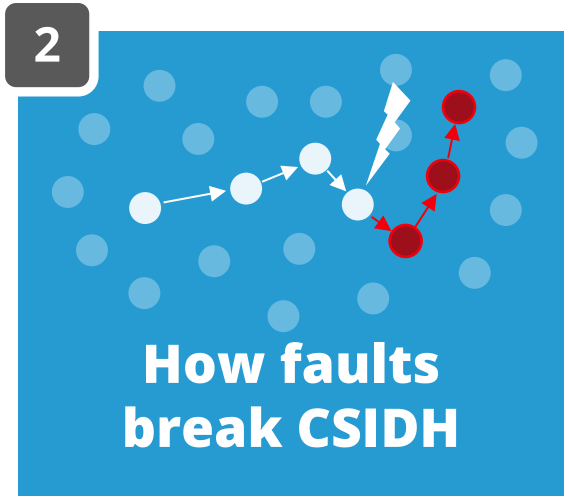


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

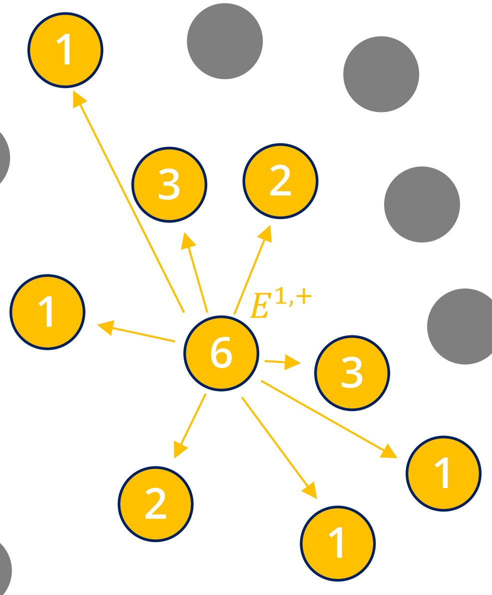


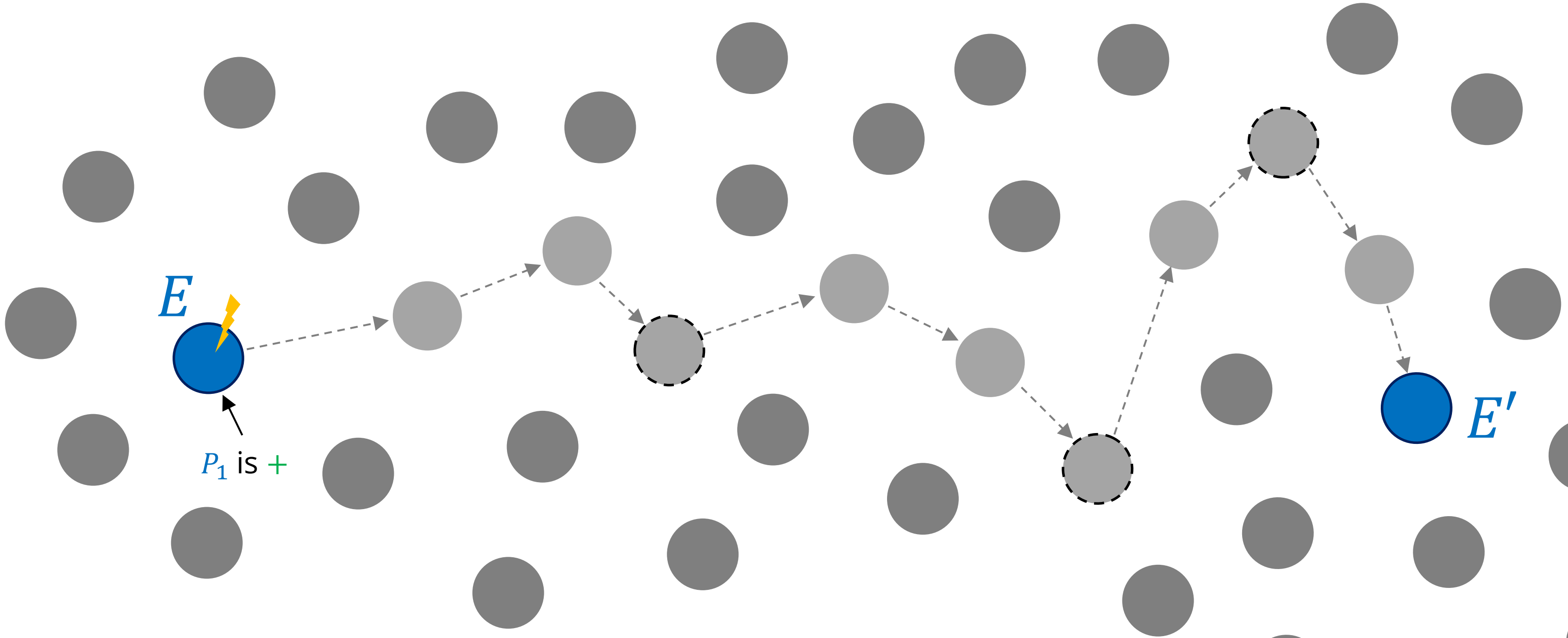




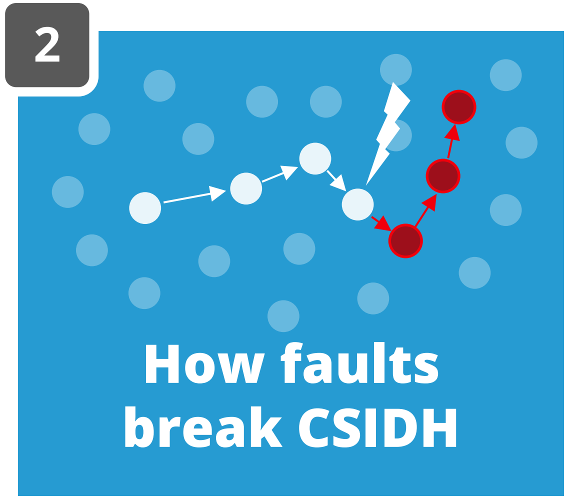
Back to example

- Path $E \to E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



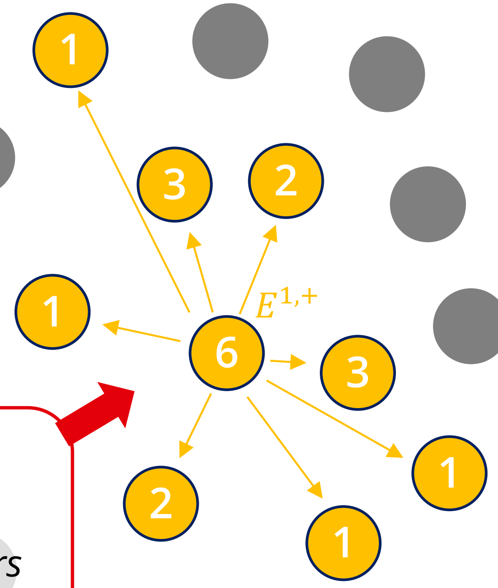


FAULTING 1st POINT

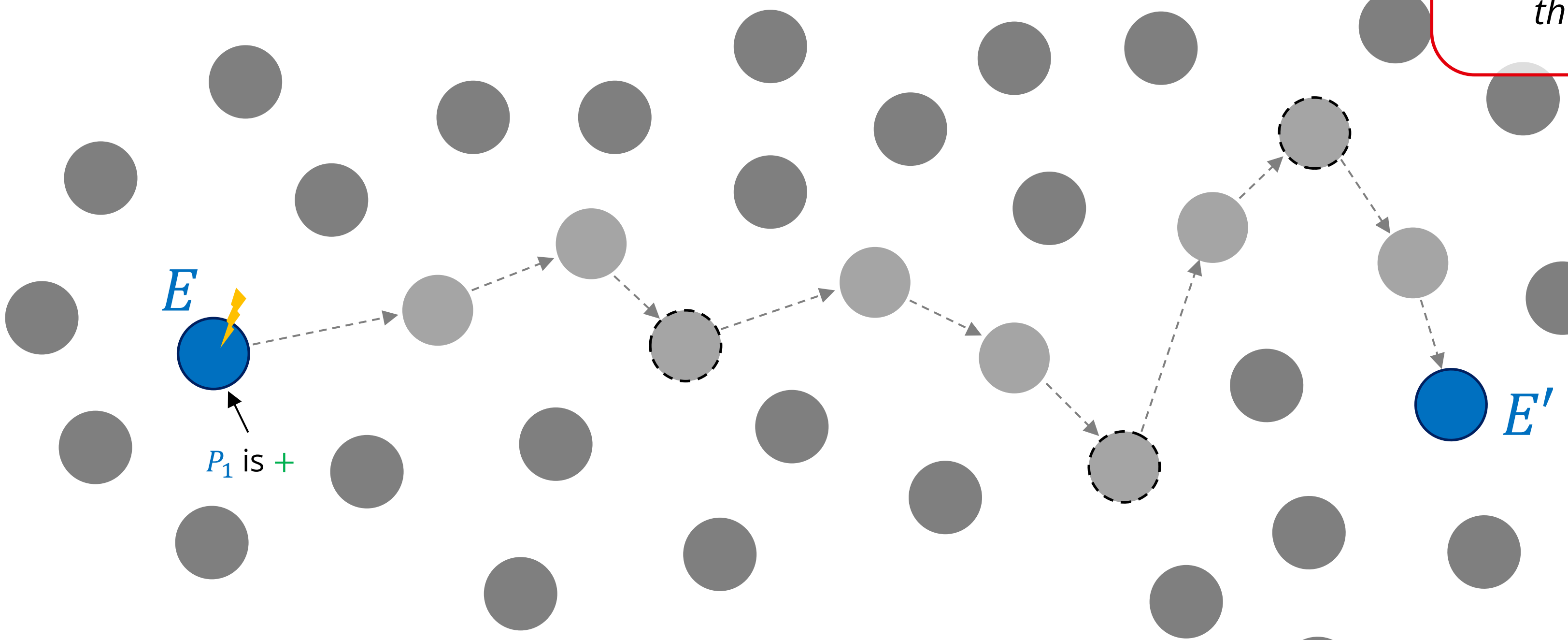


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

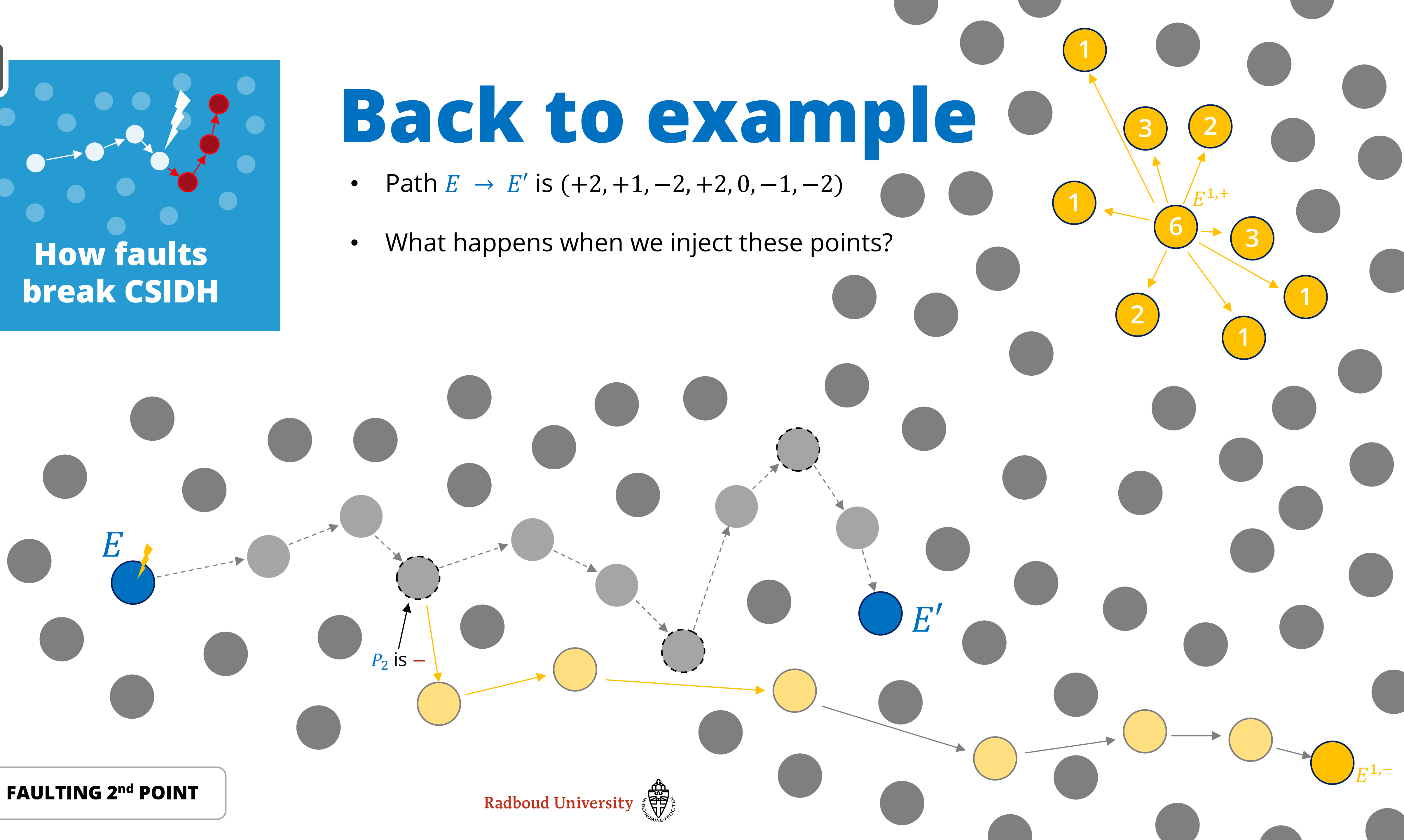


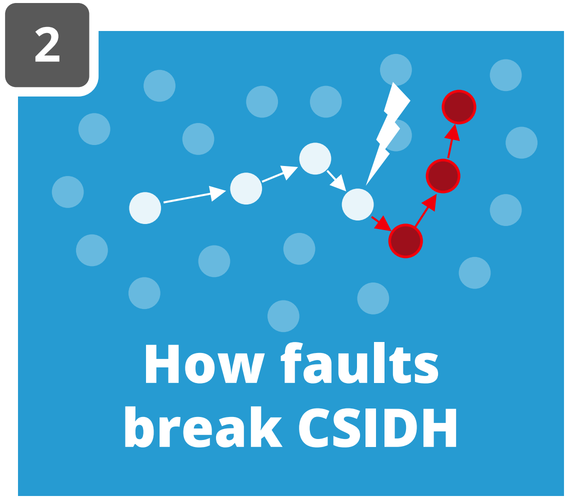
- *easy to find*
- *if* ℓ_i *appears then* $e_i \geq +1$



Back to example

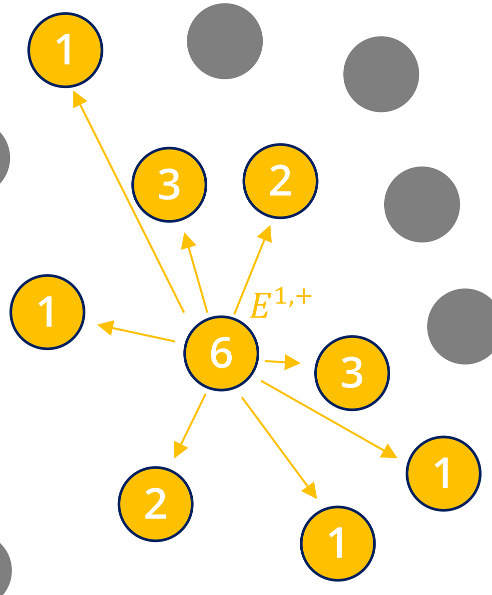
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

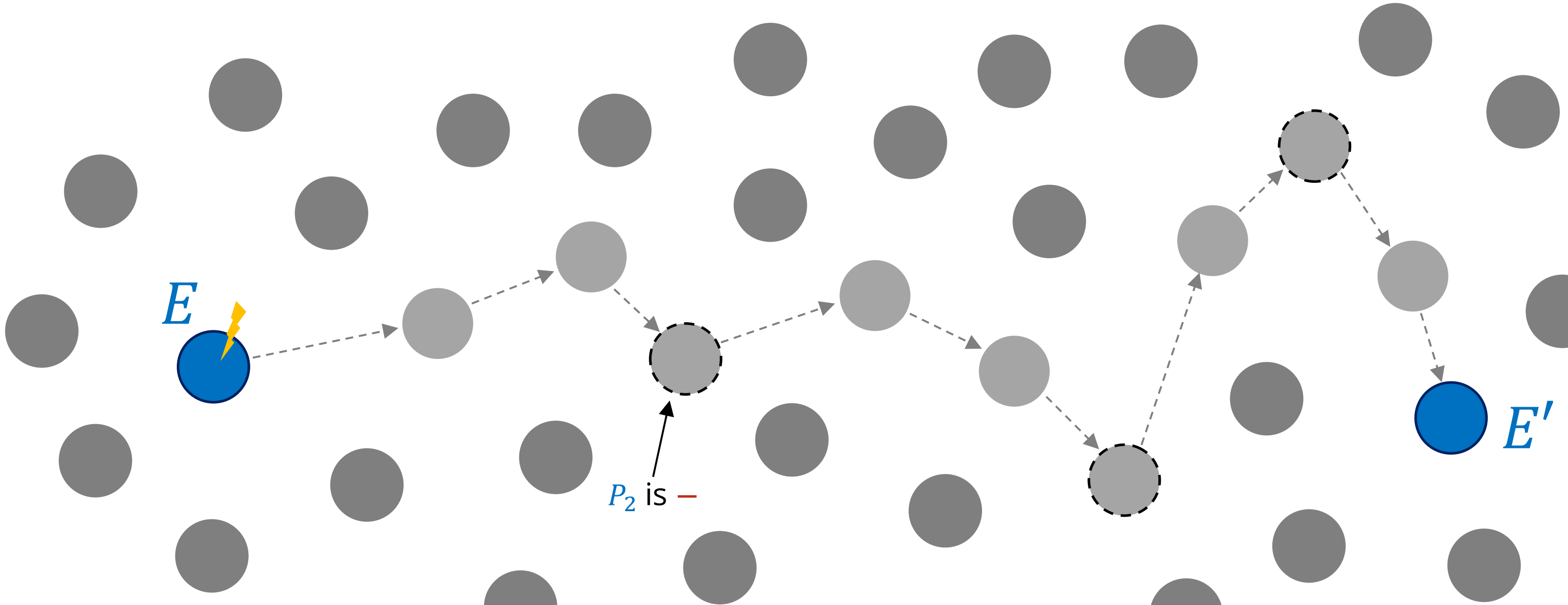


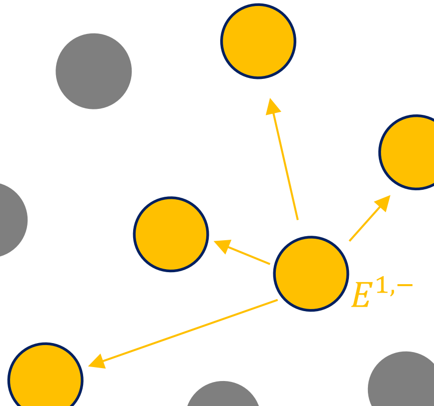


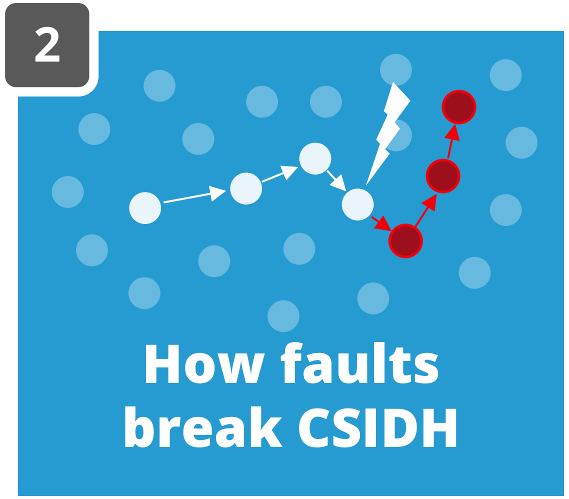
Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



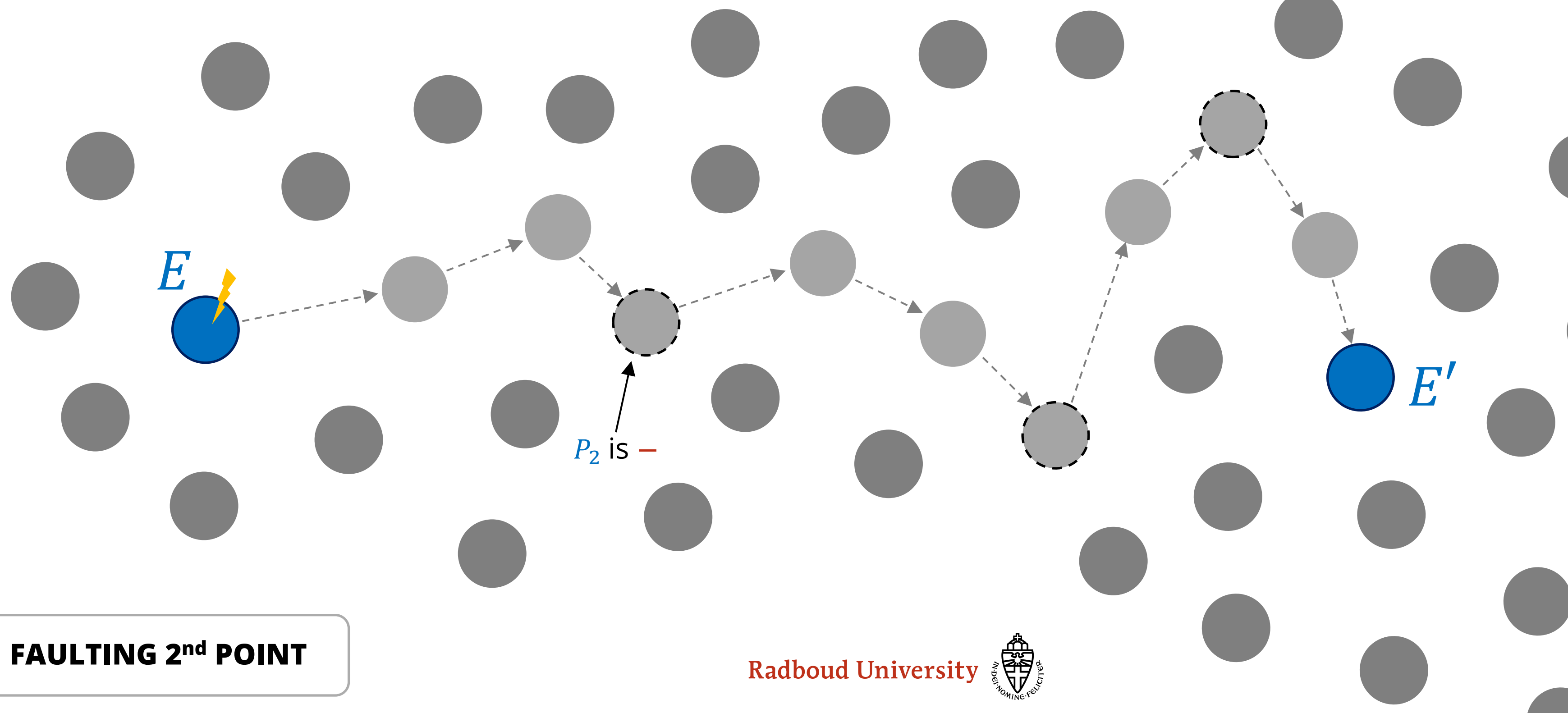


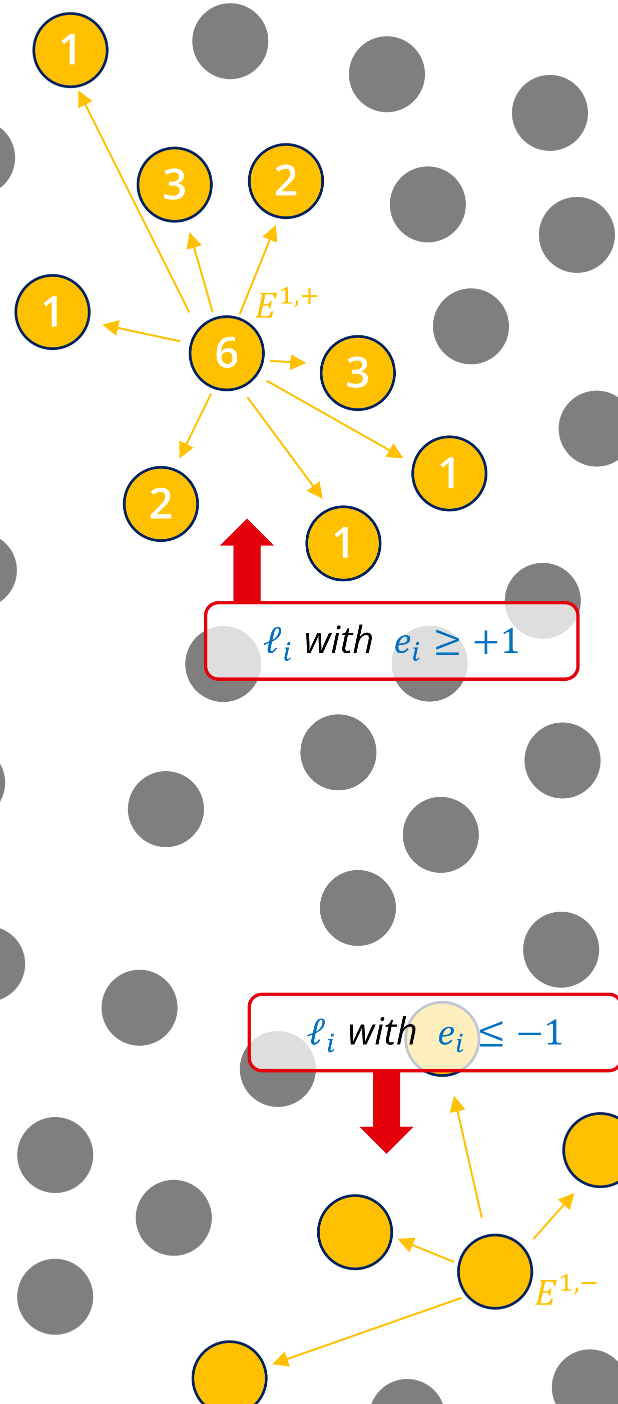




Back to example

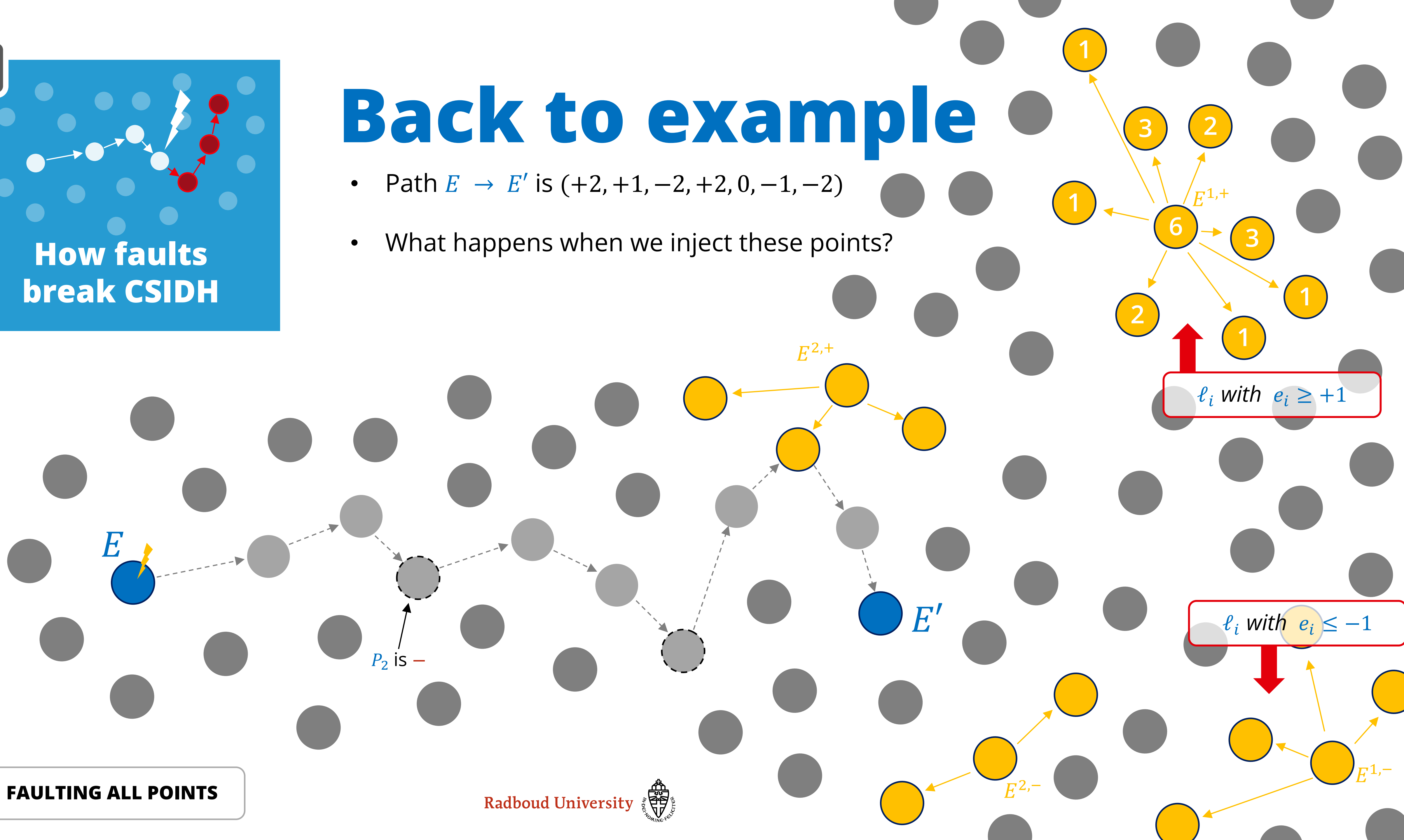
- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

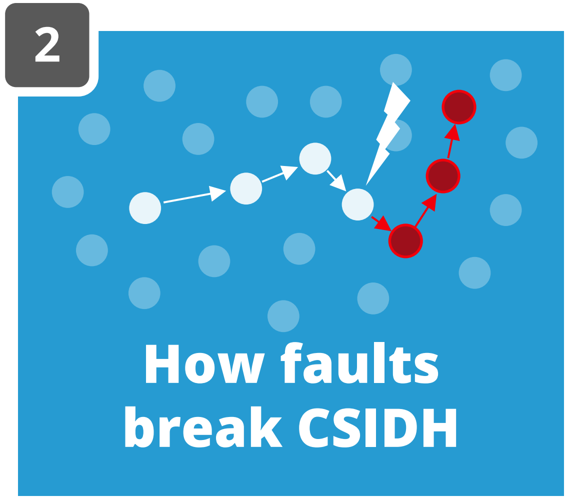




Back to example

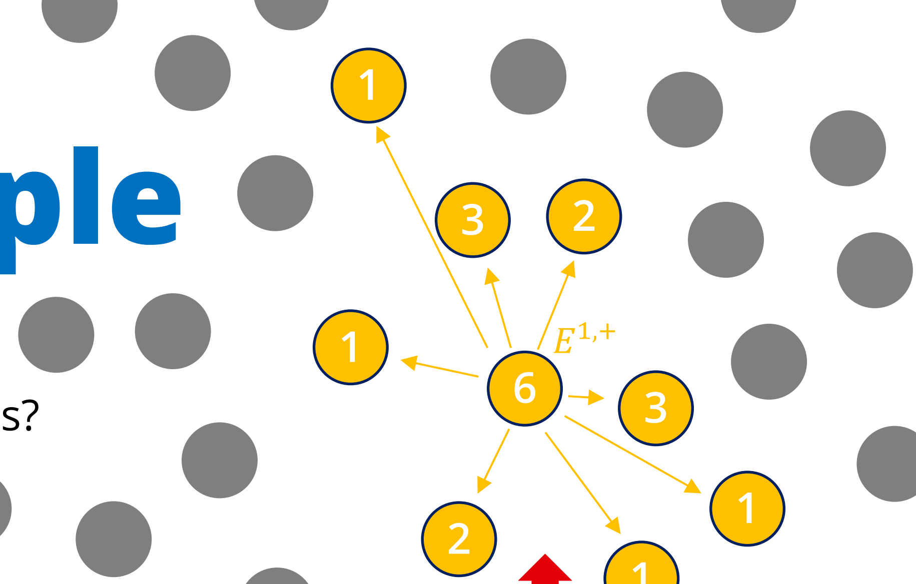
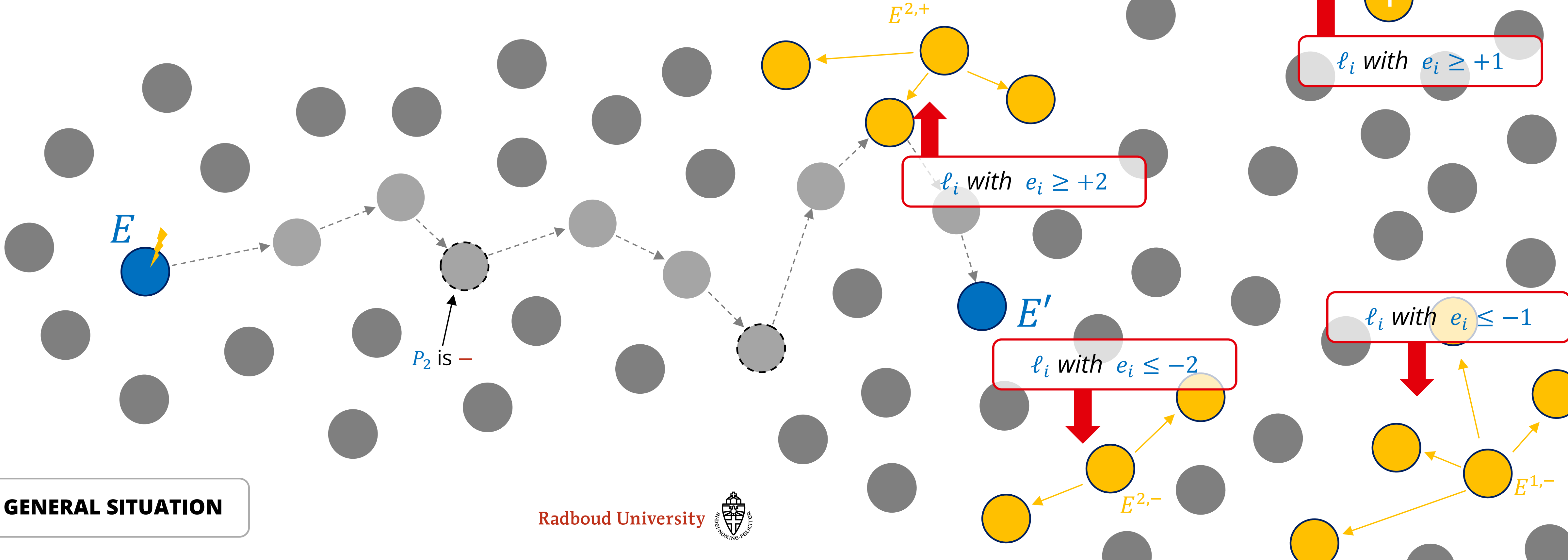
- Path $E \rightarrow E'$ is $(+2,+1,-2,+2,0,-1,-2)$
- What happens when we inject these points?



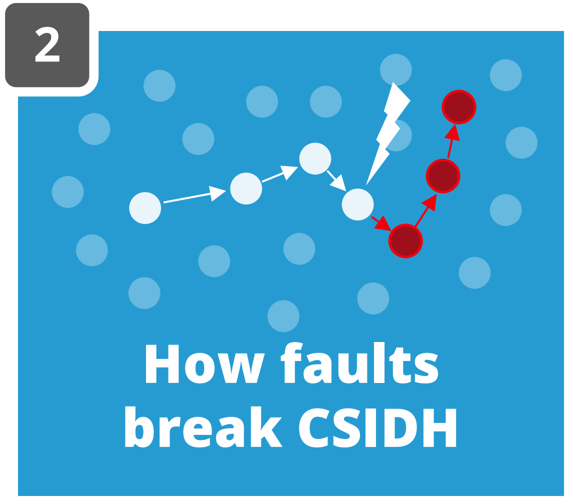


Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?

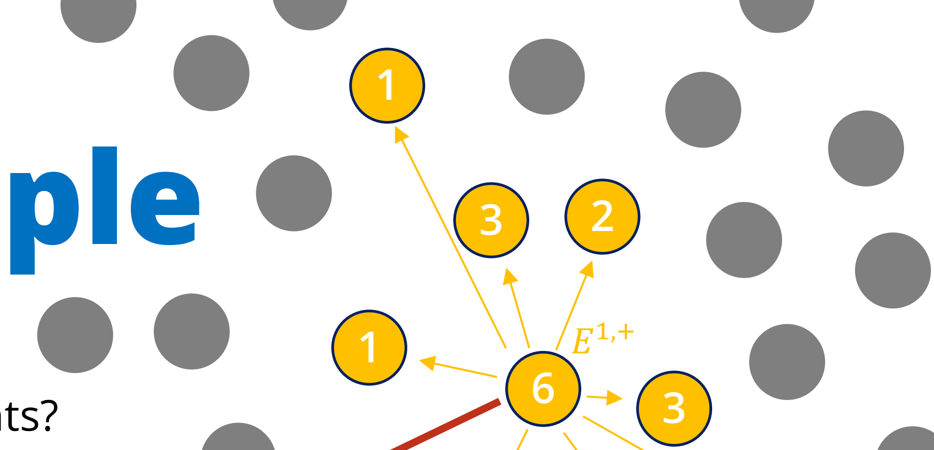



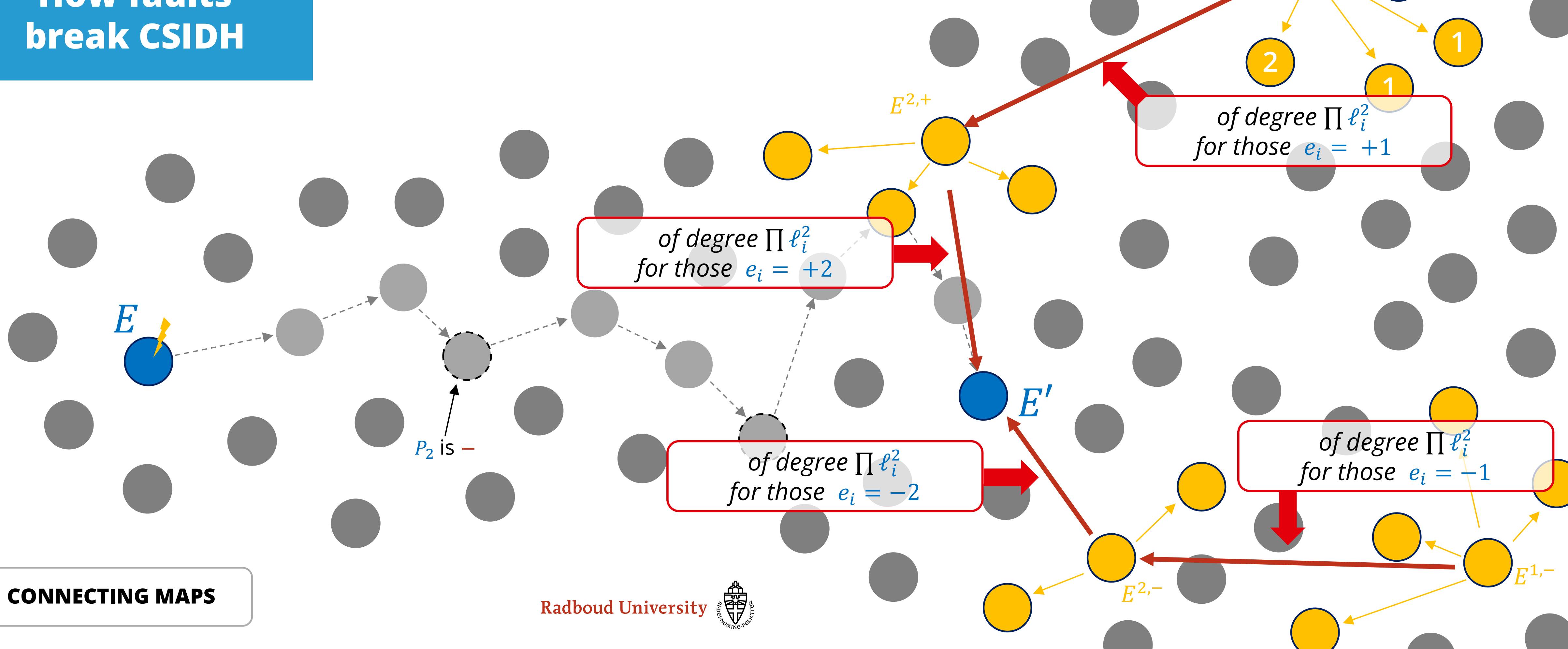
GENERAL SITUATION



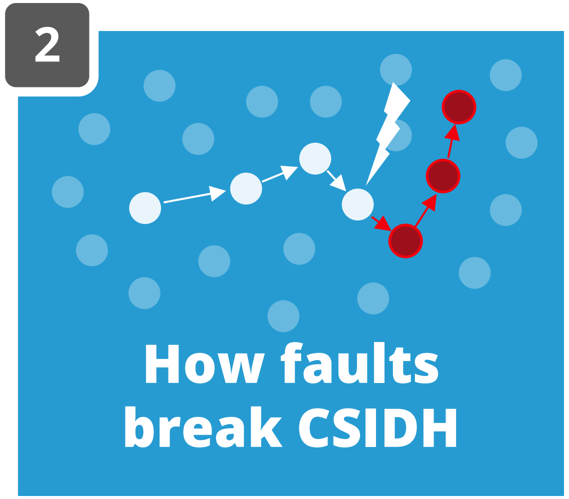
Back to example

- Path $E \rightarrow E'$ is $(+2, +1, -2, +2, 0, -1, -2)$
- What happens when we inject these points?



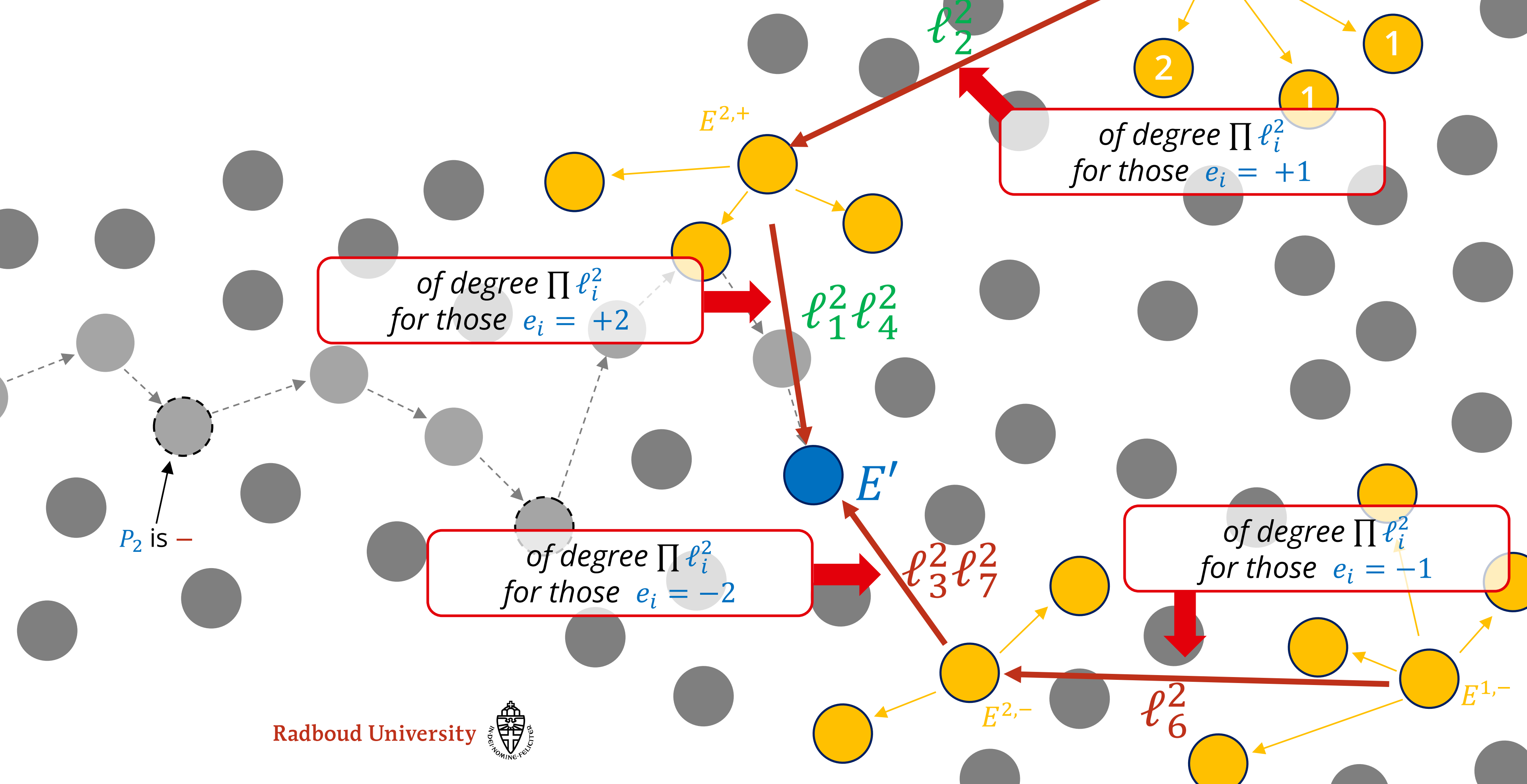


2

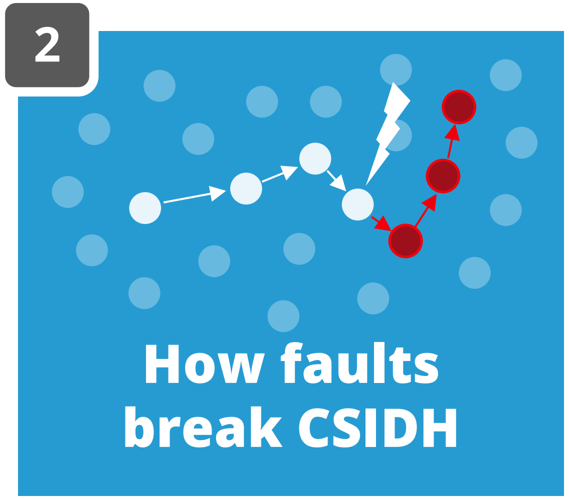


Back to example

- Path $E \rightarrow E'$ is $(+2,+1,-2,+2,0,-1,-2)$
- What happens when we inject these points?

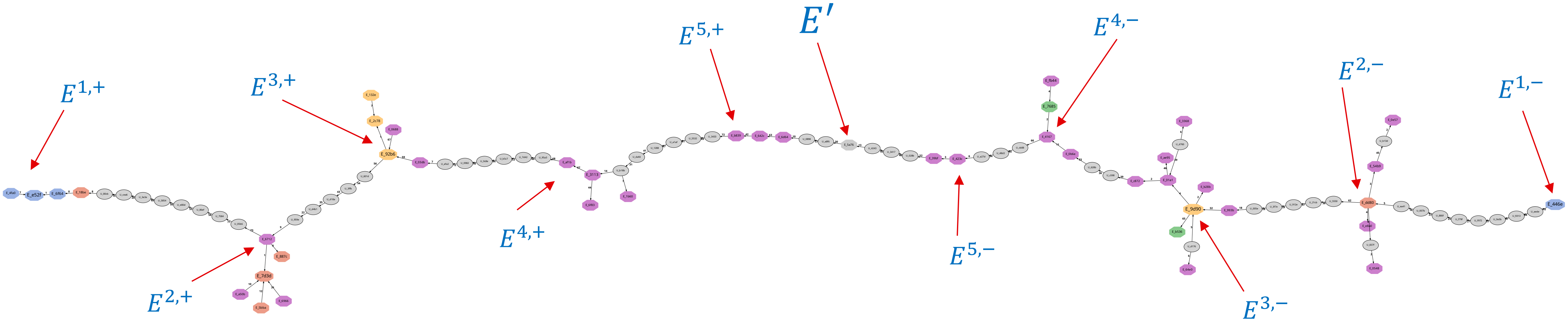


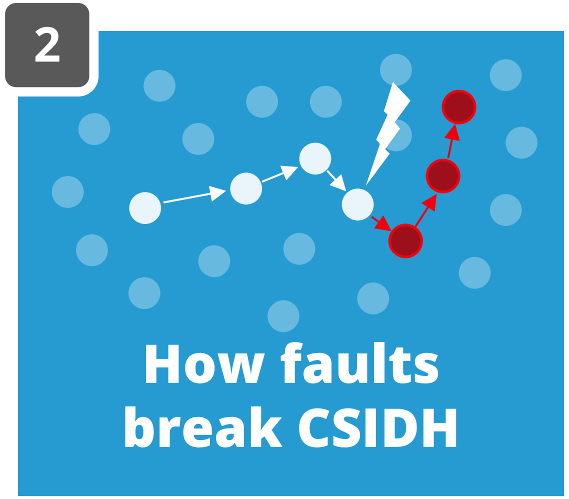
RECOVERING KEY



Real world: CSIDH-512

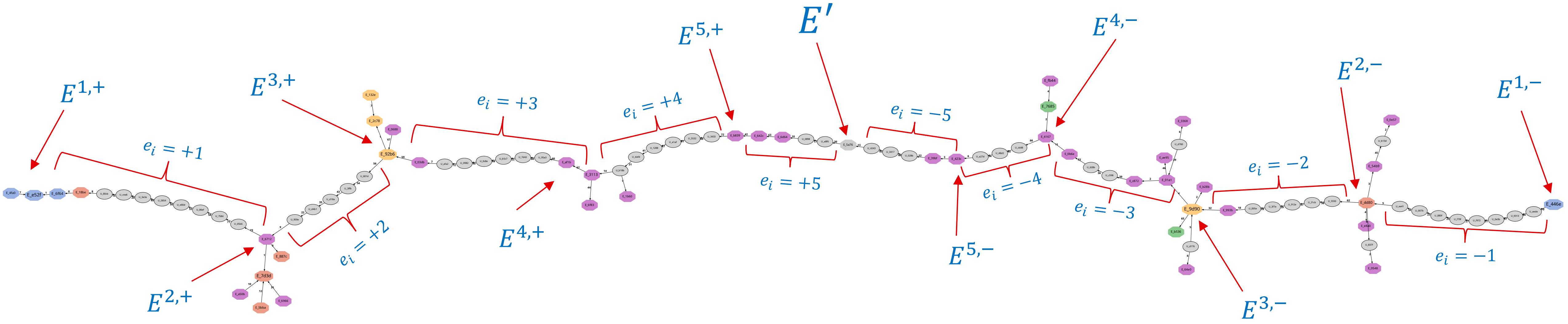
- uses 74 ℓ_i with $\mathrm{e_i} \in [-5, \dots, 5]$ for secret $(e_1, \dots, e_{74})$
- hence, need 10 points to perform computation so we get $E^{1,\pm}, \dots, E^{5,\pm}$ and a much larger graph
- overall strategy is exactly the same as before

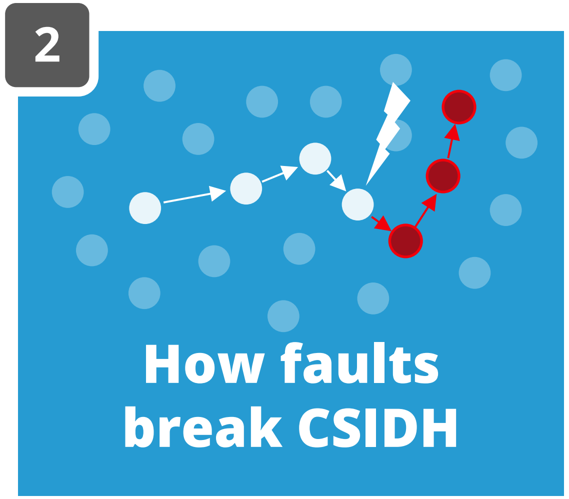




Real world: CSIDH-512

- uses 74 ℓ_i with $\mathrm{e_i} \in [-5, \dots, 5]$ for secret $(e_1, \dots, e_{74})$
- hence, need 10 points to perform computation so we get $E^{1,\pm}, \dots, E^{5,\pm}$ and a much larger graph
- overall strategy is exactly the same as before

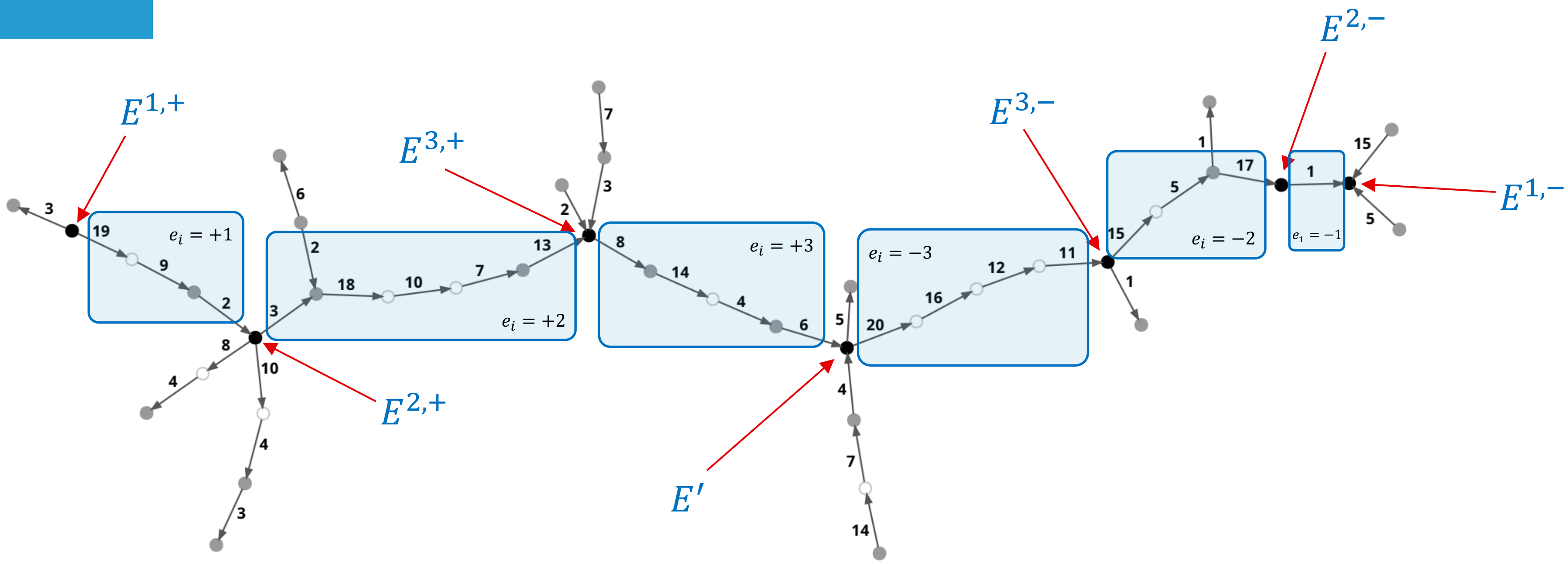




MORE READABLE: CSIDH-103

- uses 21 ℓ_i with $e_i \in [-3, \ldots, 3]$ for secret $(e_1, \ldots, e_{21})$
- hence, need 6 points to perform computation so we get $E^{1,\pm}, \ldots, E^{3,\pm}$ and a much larger graph

CSIDH-103



$[\mathfrak{a}] \sim (-1, +1, +2, +3, -2, +3, +2, +3, +1, +2, -3, -3, +2, +3, -2, -3, -2, +2, +1, -3, 0)$

IN SUMMARY

- fault injections allow us to break CSIDH-512 in about **100 samples**
  (one sample is a computation of group action with a single fault injection)
- similar strategy applied to CTIDH-512 needs only **40 samples**
- more advanced tricks (using the twist) moves most of computational effort to break CTIDH-512 to **one-off precomputation**
- countermeasure: **Elligreator.** (about 5% extra cost)
- hashed version: requires more samples and computations, still feasible