Disorientation faults in CSIDH
From disorientation attacks to key recovery

1. How did CSIDH work again…?

2. How faults break CSIDH
CSIDH FOR BEGINNERS
CSIDH for beginners

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

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

1. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $\#E_A(\mathbb{F}_p) = p + 1$
How did CSIDH work again...?

CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $#E_A(\mathbb{F}_p) = p + 1$
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $\ell$ 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 $\ell$ 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 $\ell$ 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 \( \ell \) 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 \( \ell \) 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 \( \ell \in \{3, 5, 7\} \)
How did CSIDH work again…?

CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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. For $\ell$ 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. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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. For $\ell$, 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. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $\ell$ 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 $\ell$ 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 $\ell$ 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. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $\ell$ we can take either a positive or a negative step
4. Magic!

$\begin{align*}
p &= 419 = 4 \cdot 3 \cdot 5 \cdot 7 - 1 \\
gives 27 “special” A \in \mathbb{F}_p with \#E_A(\mathbb{F}_p) = p + 1 steps by \ell \in \{3, 5, 7\}\end{align*}$
CSIDH for beginners

1. Pick some field $\mathbb{F}_p$ with many primes $\ell$ 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 $\ell$ 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 $\ell \in \{3, 5, 7\}$
CSIDH key exchange

1. Pick somewhere to start
1. How did CSIDH work again...
2. CSIDH key exchange

1. Pick somewhere to start
2. Alice picks \textbf{secret path} \( a = (e_1, e_2, e_3) \)
CSIDH key exchange

1. Pick somewhere to start
2. Alice picks secret path $a = (e_1, e_2, e_3)$
3. Bob picks secret path $b = (e_1, e_2, e_3)$
How did CSIDH work again...

CSIDH key exchange

1. Pick somewhere to start
2. Alice picks secret path $a = (e_1, e_2, e_3)$
3. Bob picks secret path $b = (e_1, e_2, e_3)$
4. Alice applies $a$ to Bob’s Public Key
   Bob applies $b$ to Alice’s Public Key
CSIDH key exchange

1. Pick somewhere to start
2. Alice picks secret path \( a = (e_1, e_2, e_3) \)
3. Bob picks secret path \( b = (e_1, e_2, e_3) \)
4. Alice applies \( a \) to Bob's Public Key
   Bob applies \( b \) to Alice's Public Key
1. Pick somewhere to start
2. Alice picks secret path $a = (e_1, e_2, e_3)$
3. Bob picks secret path $b = (e_1, e_2, e_3)$
4. Alice applies $a$ to Bob’s Public Key
   Bob applies $b$ to Alice’s Public Key
HOW TO WALK
How to compute walk
How did CSIDH work again…?

How to compute walk

Let’s say $E \rightarrow E'$ is path $(+2, +1, -2, +2, 0, -1, -2)$
How did CSIDH work again…?

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

e.g. take two negative steps for third $\ell$ that divides $p + 1$
How did CSIDH work again…?

How to compute walk

Let’s say $E \to E'$ 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 $\ell_i$
3. Repeat until path is performed
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 $\ell_i$
3. Repeat until path is performed

$(+2, +1, -2, +2, 0, -1, -2)$
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 $\ell_i$
3. Repeat until path is performed
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 $\ell_i$
3. Repeat until path is performed

$$(+1, +0, -2, +2, 0, -1, -2)$$
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 $\ell_i$
3. Repeat until path is performed

$(+1, +0, -2, +1, 0, -1, -2)$
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 $\ell_i$
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 $\ell_i$
3. Repeat until path is performed

$P$ is $-$

$(+1, +0, -2, +1, 0, -1, -2)$
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 $\ell_i$
3. Repeat until path is performed

$(+1, +0, -1, +1, 0, -1, -2)$
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 $\ell_i$
3. Repeat until path is performed

$(+1, +0, -1, +1, 0, -0, -2)$
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 $\ell_i$
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 \( \ell_i \)
3. Repeat until path is performed

\((-1, 0, -1, +1, 0, 0, -1)\)
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 $\ell_i$
3. Repeat until path is performed

$(+1, 0, -1, +1, 0, 0, -1)$
How did CSIDH work again…?

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 $\ell_i$
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 $\ell_i$
3. Repeat until path is performed

$(+1, 0, -0, +1, 0, 0, -0)$
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 $\ell_i$
3. Repeat until path is performed

$$(+1, 0, 0, +1, 0, 0, 0)$$
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 $\ell_i$
3. Repeat until path is performed

$(+0, 0, 0, +1, 0, 0, 0)$
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 $\ell_i$
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 $\ell_i$
3. Repeat until path is performed
FAULT INJECTIONS

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

• Let’s say \( E \rightarrow E' \) is path \((+1, +1, -1, -1, 0, 0, 0)\)
How faults break CSIDH

- 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
How faults break CSIDH

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

- 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
How faults break CSIDH

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

- Path $E \to E'$ 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?
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?
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?

- Easy to find
- If $\ell_i$ 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?
Back to example

• Path $E \to E'$ 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?

How faults break CSIDH
Real world: CSIDH-512

- uses 74 \( \ell_i \) with \( e_i \in [-5, \ldots, 5] \) for secret \((e_1, \ldots, e_{74})\)

- hence, need 10 points to perform computation so we get \( E^{1,\pm}, \ldots, E^{5,\pm} \) and a much larger graph

- overall strategy is exactly the same as before
Real world: CSIDH-512

- uses 74 $\ell_i$ with $e_i \in [-5, ..., 5]$ for secret $(e_1, ..., e_{74})$

- hence, need 10 points to perform computation so we get $E^{1,\pm}, ..., E^{5,\pm}$ and a much larger graph

- overall strategy is exactly the same as before
How faults break CSIDH

MORE READABLE: CSIDH-103

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

CSIDH-103

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