Disorientation faults in CSIDH

17 March 2023
Crypto Working Group meeting

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

Fault attacks

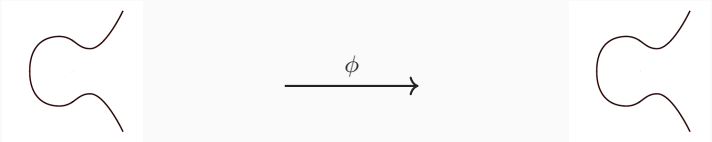
Nixdorf, CC BY-SA 3.0

Physical attacks: trigger an error during the execution of sensitive computations; infer secret information from faulty outputs;

Takeaway:

- We propose lightweight countermeasures.
- The security of CSIDH is not compromised.

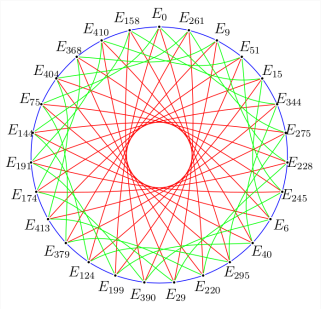
- Part of post-quantum public-key cryptography.
- **Isogeny:** rational function that maps points from curve E_1 to points on curve E_2.



- **Degree** of an isogeny: number of points on E_1 mapping to the neutral element on E_2. Computing an isogeny of degree $\ell_i \rightarrow$ an ℓ_i-step.
- **CSIDH**: commutative group action suitable for non-interactive key exchange.

The CSIDH isogeny graph

- Nodes $\to \mathbb{F}_p$-isomorphism classes of supersingular elliptic curves.
  Edges $\to$ isogenies between them.
- We can not compute the whole graph, but we can *walk* on it $\to$ compute a step and see on which node we arrive.
- $p = 4 \cdot \prod \ell_i - 1$, for $\ell_i \in \{3, 5, \ldots, 377, 587\} \to$ we can compute ℓ_i-steps in the positive or in the negative direction, for all ℓ_i.



Edges are 3, 5, and 7-isogenies. Image credit: Lorenz Panny.

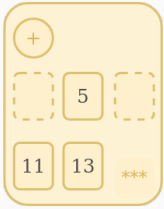
Supersingular Isogeny Path problem

Given E_1 and E_2 two supersingular elliptic curves over $\mathbb{F}_p$, find and isogeny from E_1 to E_2.

Walking on the graph

Magic box

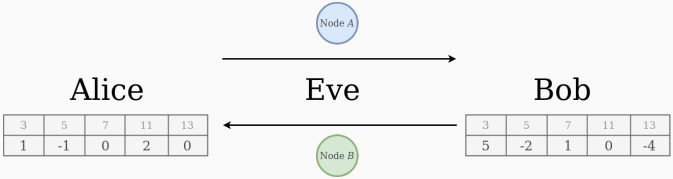
Cards with instructions on how to compute steps.

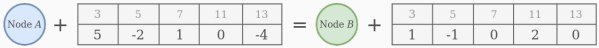


- Some cards are for walking in the positive, and some are for walking in the negative direction.
- Some cards are missing instructions for certain steps (unlucky).

Key exchange

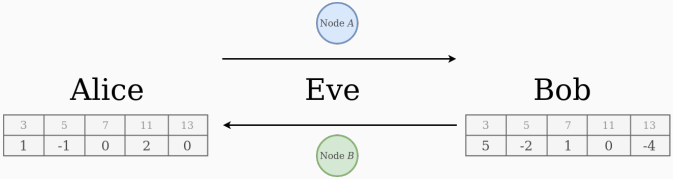
Key exchange

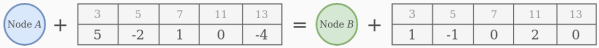




- Eve will relay the messages between Alice and Bob.

Key exchange





- Eve will relay the messages between Alice and Bob.
- She brings the magic box.

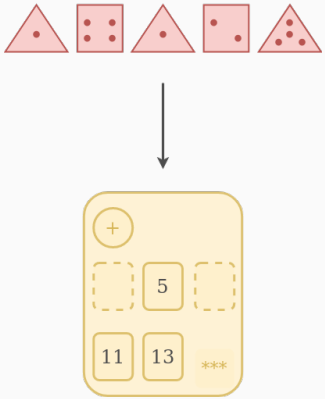
Computing the secret path

Alice gets a card with instructions.

Computing the secret path

Alice gets a card with instructions.

Computing the secret path



Cheat sheet

- Alice rolls 74 dice. Each dice has ℓ_i sides for $\ell_i \in \{3, 5, \ldots, 377, 587\}$.
- Getting a 'one' on the dice with ℓ_i sides : Alice gets a card *without* instructions for making ℓ_i-steps.
- Getting anything else: Alice gets a card *with* instructions for making ℓ_i-steps. Instructions are either for positive or negative steps, both with equal probability.
- Alice can compute all or some of the steps that she gets instructions for. Each step is computed at most once.
- **Round**: the process from rolling the dice to computing all possible steps.
- Alice performs as many rounds as she needs to compute all steps from the secret key.

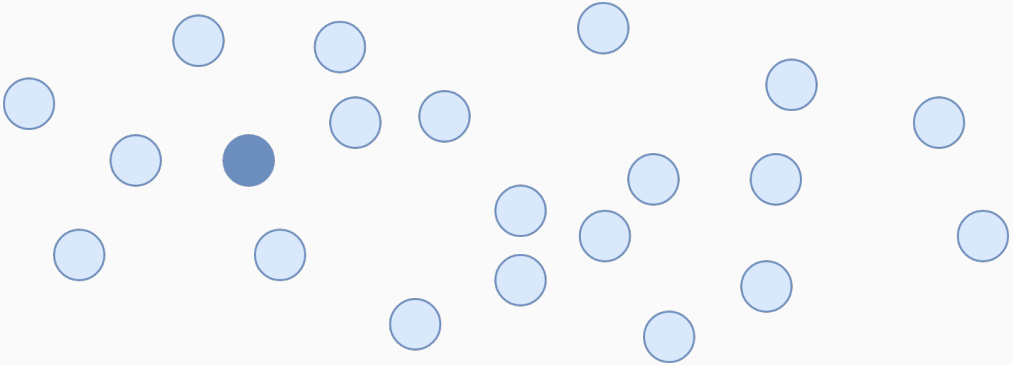
Computing the secret path (example)

Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
1	-1	0	3	0



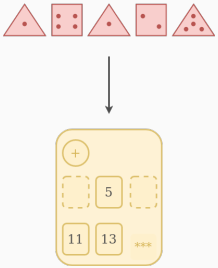
Computing the secret path (example)

Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
1	-1	0	3	0



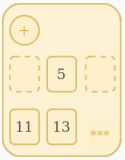
Computing the secret path (round 1)

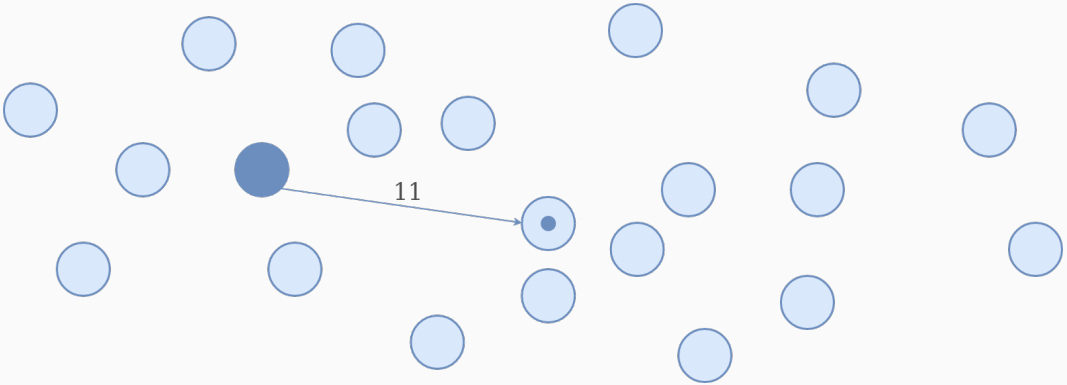
Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
1	-1	0	2	0





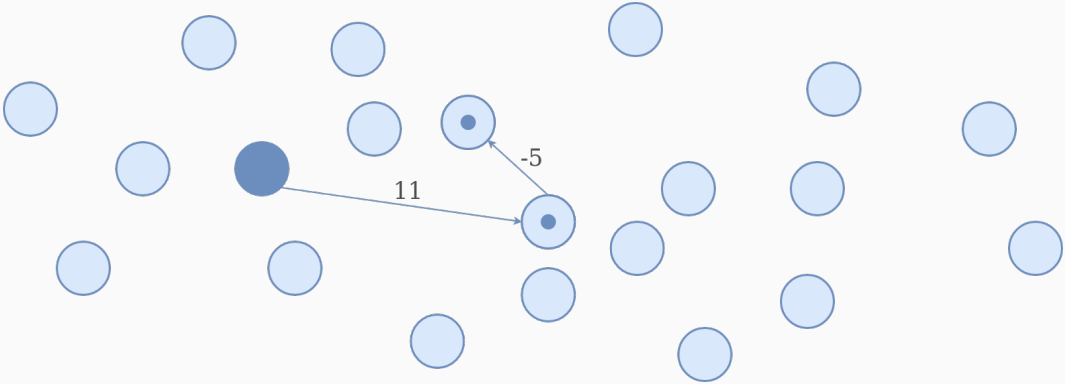
Computing the secret path (round 2)

Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
1	0	0	2	0



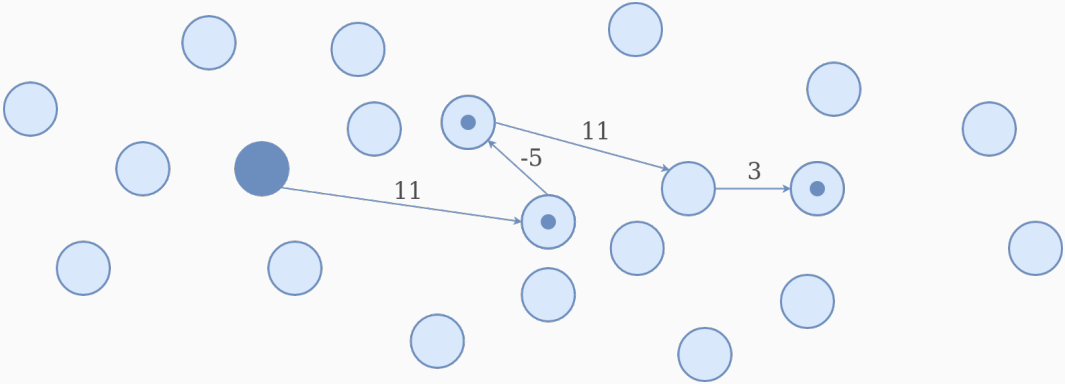
Computing the secret path (round 3)

Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
0	0	0	1	0



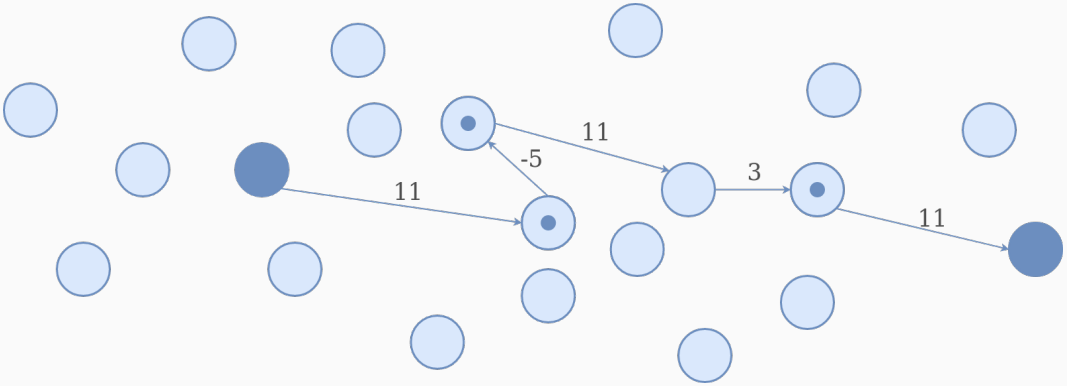
Computing the secret path (round 4)

Alice's secret key

3	5	7	11	13
1	-1	0	3	0

Left to compute

3	5	7	11	13
0	0	0	0	0

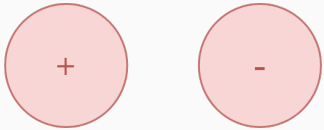


Cheat sheet

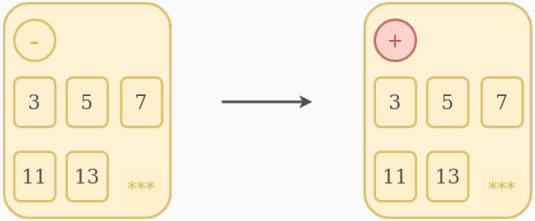
- Alice rolls 74 dice. Each dice has ℓ_i sides for $\ell_i \in \{3, 5, \ldots, 377, 587\}$.
- Getting a 'one' on the dice with ℓ_i sides : Alice gets a card *without* instructions for making ℓ_i-steps.
- Getting anything else: Alice gets a card *with* instructions for making ℓ_i-steps. Instructions are either for positive or negative steps, both with equal probability.
- Alice can compute all or some of the steps that she gets instructions for. Each step is computed at most once.
- **Round**: the process from rolling the dice to computing all possible steps.
- Alice performs as many rounds as she needs to compute all steps from the secret key.

Eve's mission

- You bring stickers to put over the direction sign on the cards.



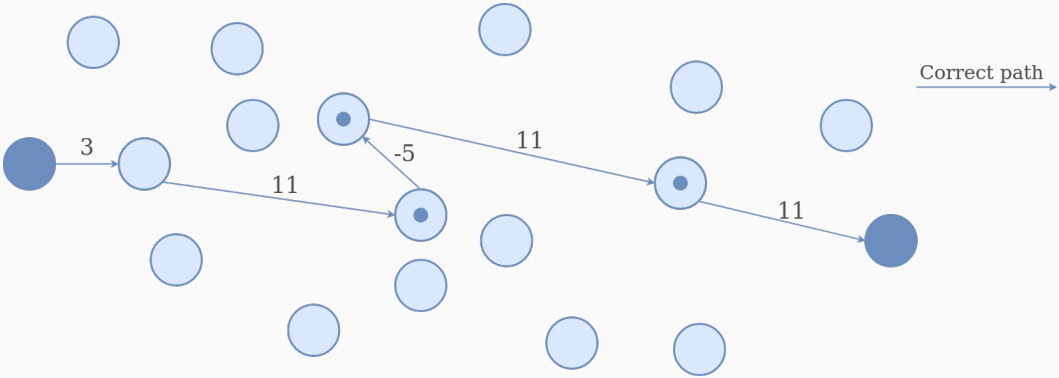
- Alice thinks she has a card with instructions for positive steps, but she has a card with instructions for negative steps.



Faulted paths

Alice's secret key

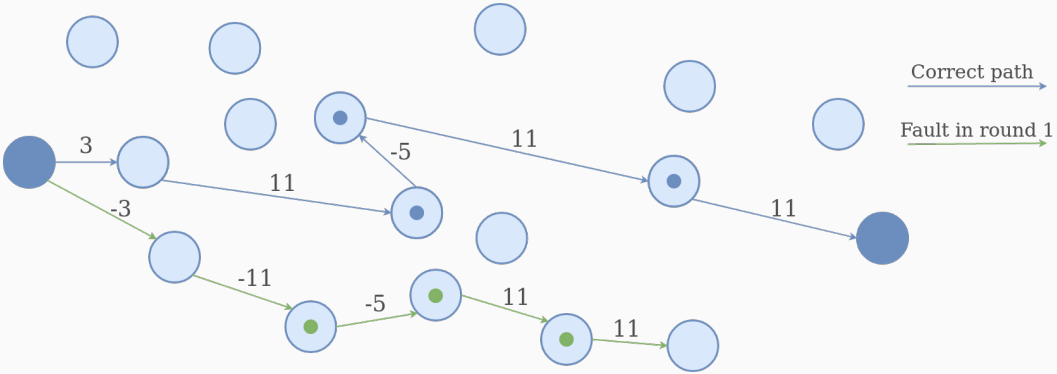
3	5	7	11	13
1	-1	0	3	0



Faulted paths

Alice's secret key

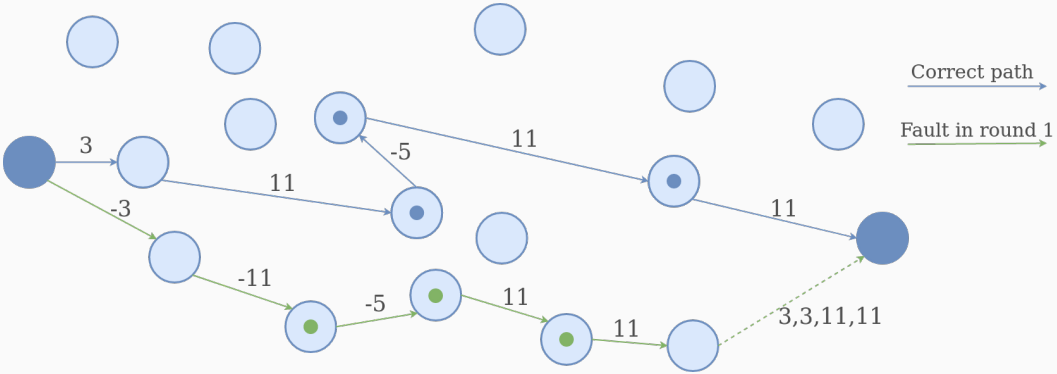
3	5	7	11	13
1	-1	0	3	0



Faulted paths

Alice's secret key

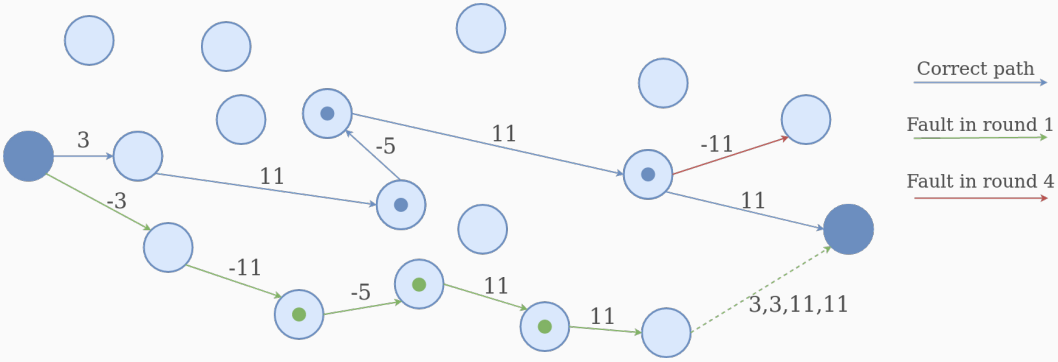
3	5	7	11	13
1	-1	0	3	0



Faulted paths

Alice's secret key

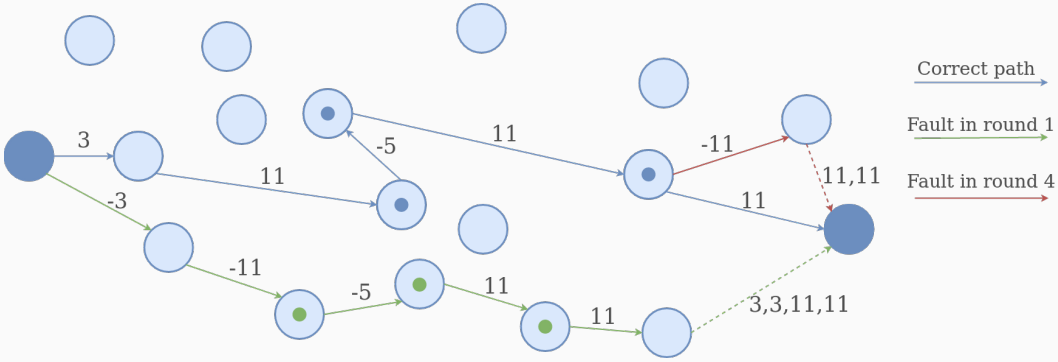
3	5	7	11	13
1	-1	0	3	0



Faulted paths

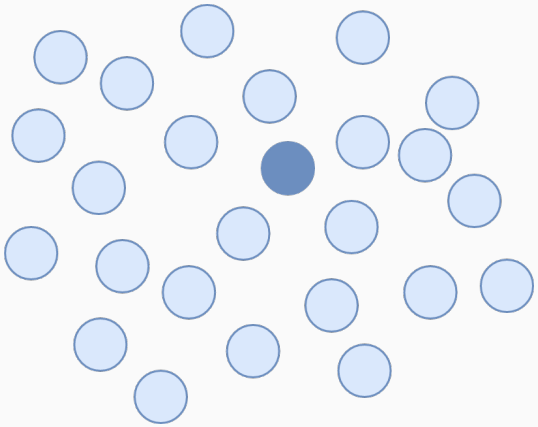
Alice's secret key

3	5	7	11	13
1	-1	0	3	0



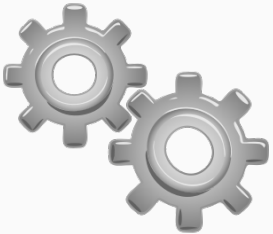
Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



Eve's graph

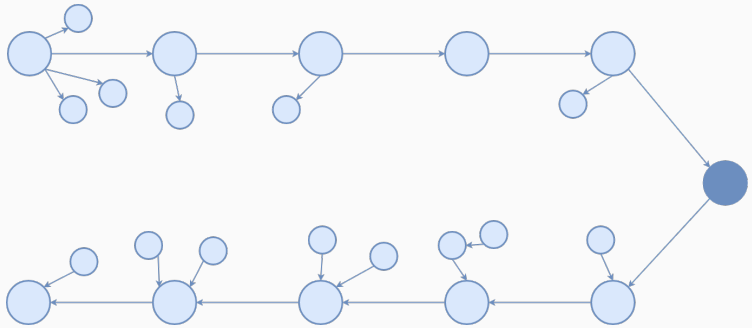
- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



`pubcrawl`

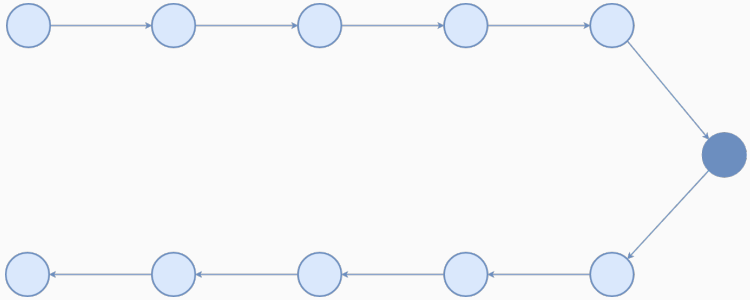
Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



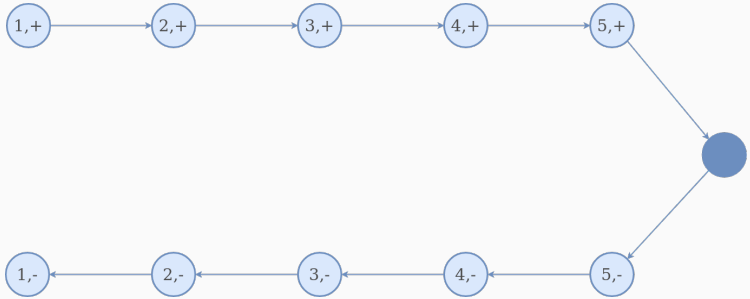
Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



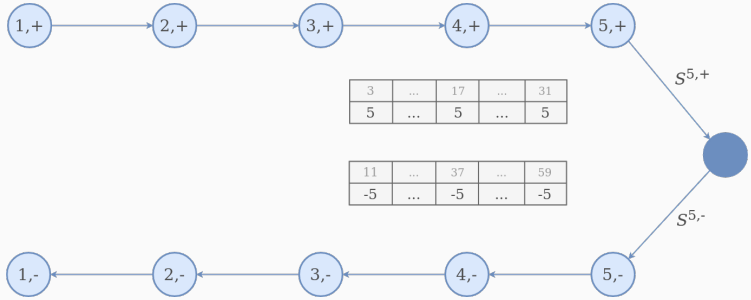
Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



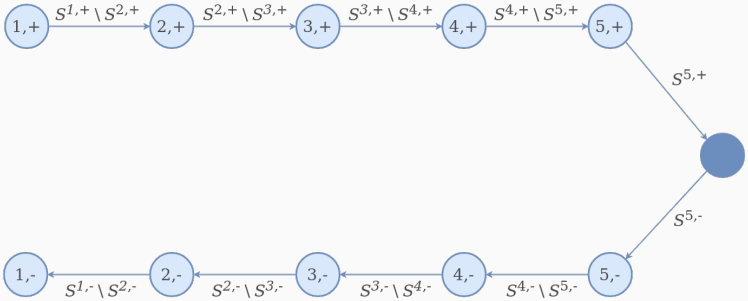
Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



Eve's graph

- Collecting faulty output nodes from the first 5 rounds, both from negative and positive steps.



In the full paper

- The isogeny details
- Attack on CSIDH
- Attack on CTIDH
- Exploiting the twist
- Lightweight countermeasures

eprint: 2022/1202