

A tropical sunset scene with palm trees and the ocean. The sun is low on the horizon, casting a golden glow over the water and silhouetting the palm trees. The sky is a mix of orange, yellow, and blue.

CSIDH

[ˈsiː,saɪd]

Lorenz Panny, TU/e

Post-quantum Diffie–Hellman?

Traditionally, Diffie–Hellman works in a **group** G via the map

$$\begin{aligned}\mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x.\end{aligned}$$

Post-quantum Diffie–Hellman?

Traditionally, Diffie–Hellman works in a **group** G via the map

$$\begin{aligned}\mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x.\end{aligned}$$

Shor's algorithm quantumly computes discrete logarithms in any group in polynomial time.

Post-quantum Diffie–Hellman!

Traditionally, Diffie–Hellman works in a **group** G via the map

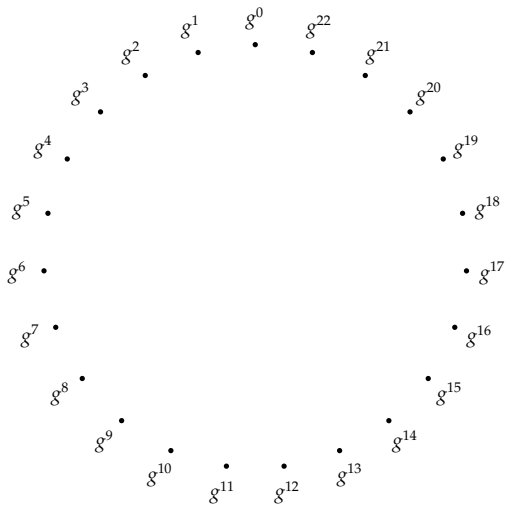
$$\begin{aligned}\mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x.\end{aligned}$$

Shor's algorithm quantumly computes discrete logarithms in any group in polynomial time.

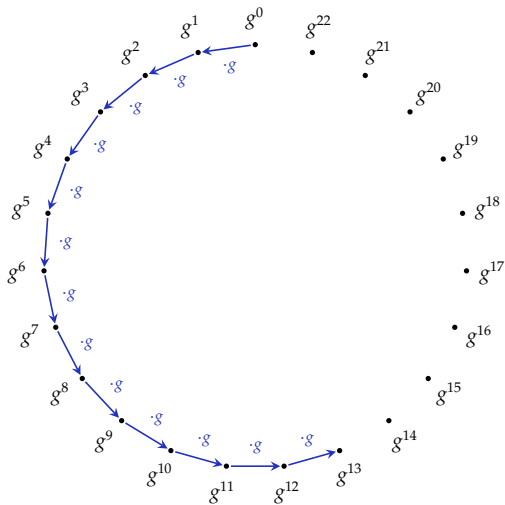
Shor relies on composing public keys: $g^x \cdot g^y = g^{x+y}$. \rightsquigarrow Idea:

Replace exponentiation on the group G by a **group action** of a group H on a **set** S :

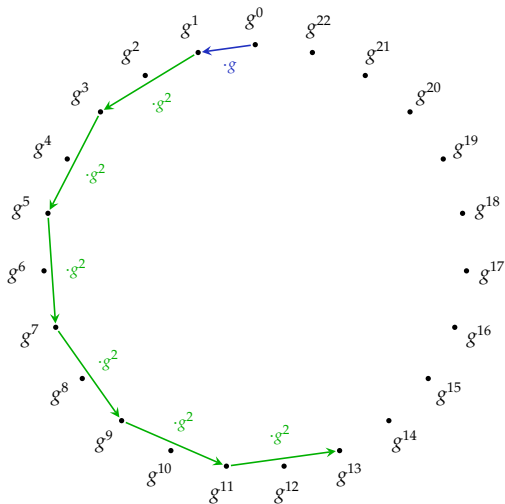
$$H \times S \rightarrow S.$$



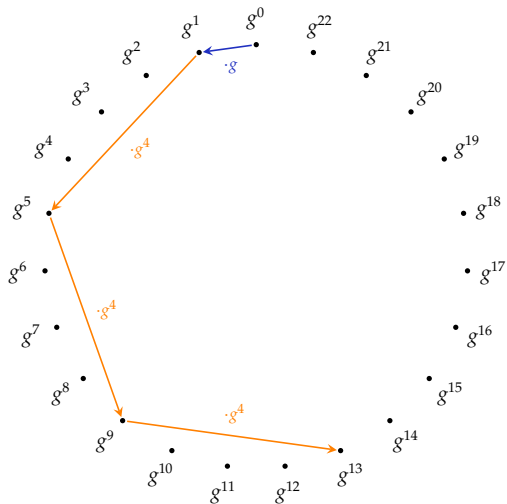
multiply



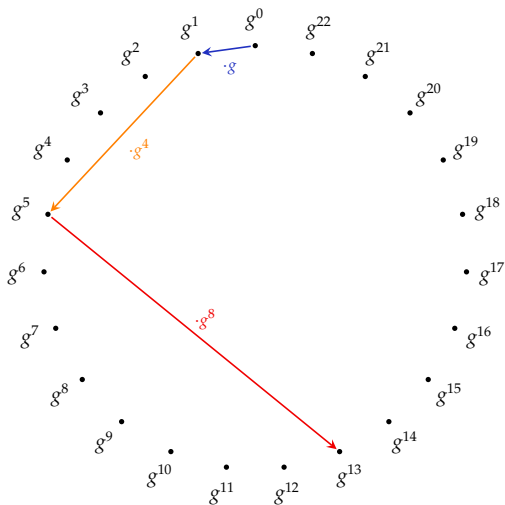
Square-and-multiply



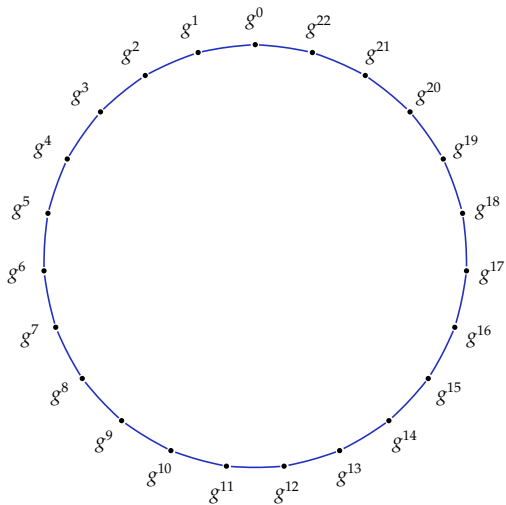
Square-and-multiply-and-square-and-multiply



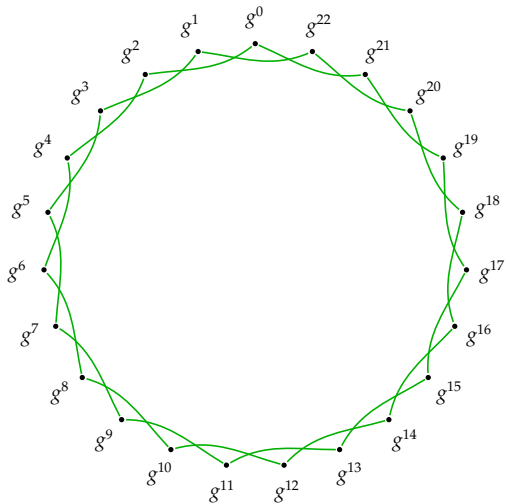
Square-and-multiply-and-square-and-multiply-and-squ



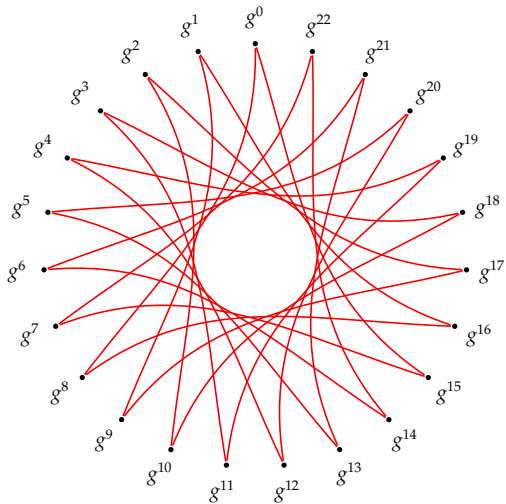
cycles



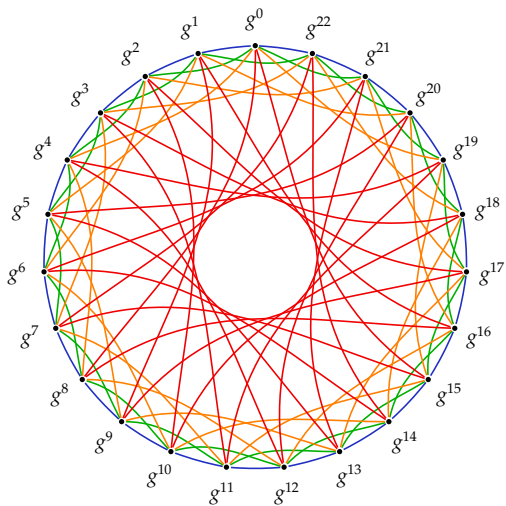
cycles



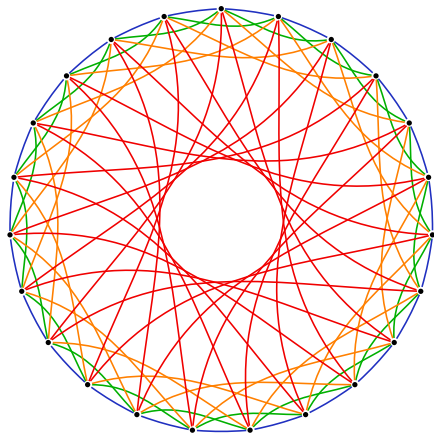
cycles



A union of cycles

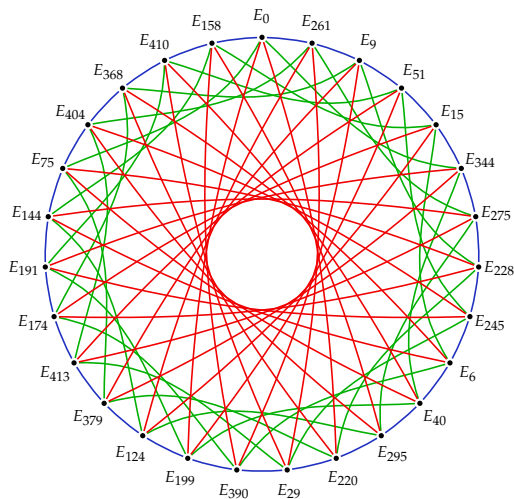


A union of cycles



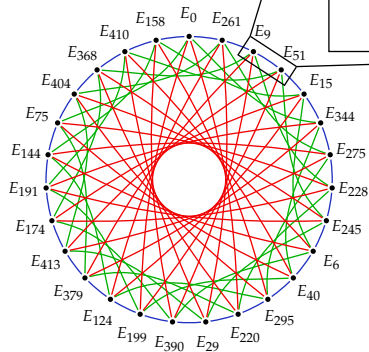
CSIDH: Nodes are now **elliptic curves** and edges are **isogenies**.

A union of cycles of elliptic curves

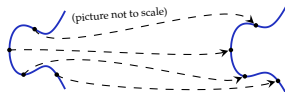


Nodes: Supersingular curves $E_A: y^2 = x^3 + Ax^2 + x$ over \mathbb{F}_{419} .
Edges: 3-, 5-, and 7-isogenies (certain kinds of maps).

A union of cycles of elliptic curves and isogenies



A 3-isogeny



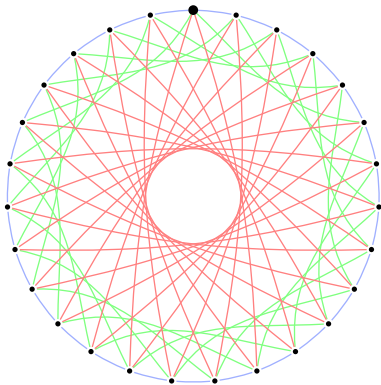
$$E_{51}: y^2 = x^3 + 51x^2 + x \longrightarrow E_9: y^2 = x^3 + 9x^2 + x$$

$$(x, y) \longmapsto \left(\frac{97x^3 - 183x^2 + x}{x^2 - 183x + 97}, \right. \\ \left. y \cdot \frac{133x^3 + 154x^2 - 5x + 97}{-x^3 + 65x^2 + 128x - 133} \right)$$

Diffie–Hellman on graphs!

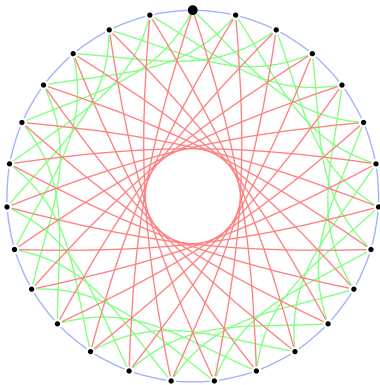
Alice

[+, -, +, -]



Bob

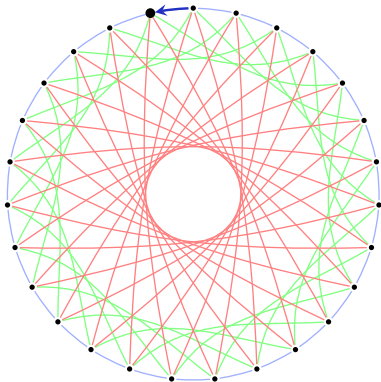
[+, +, -, +]



Diffie–Hellman on graphs!

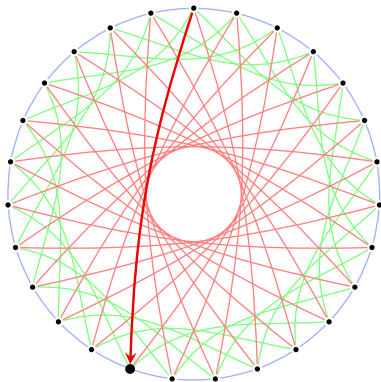
Alice

[\uparrow , -, +, -]



Bob

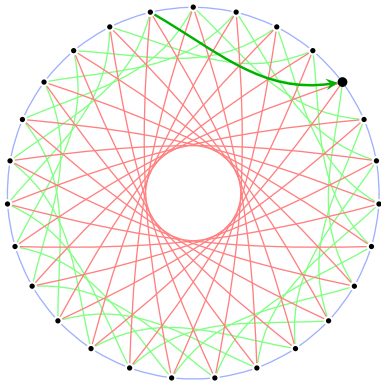
[\uparrow , +, -, +]



Diffie–Hellman on graphs!

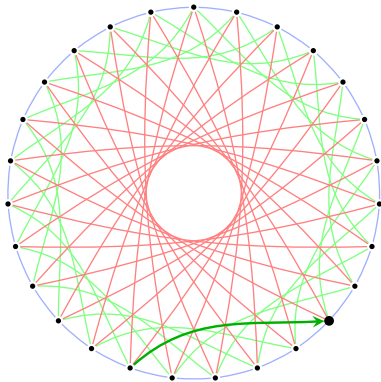
Alice

[+, -, +, -]
↑



Bob

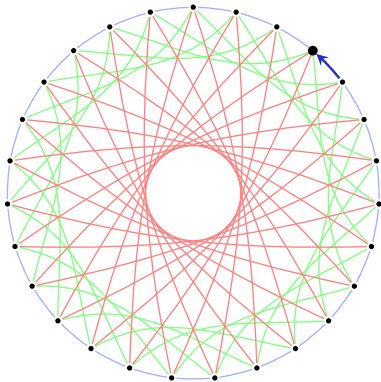
[+, +, -, +]
↑



Diffie–Hellman on graphs!

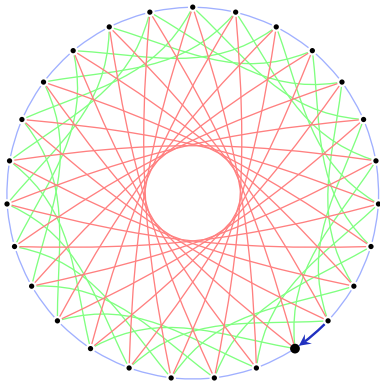
Alice

[+, -, +, -]
↑



Bob

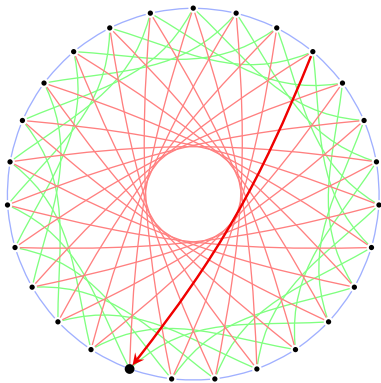
[+, +, -, +]
↑



Diffie–Hellman on graphs!

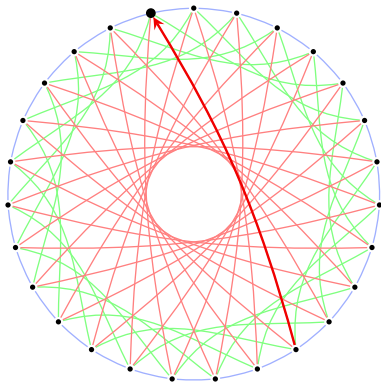
Alice

[+, -, +, -]
↑



Bob

[+, +, -, +]
↑



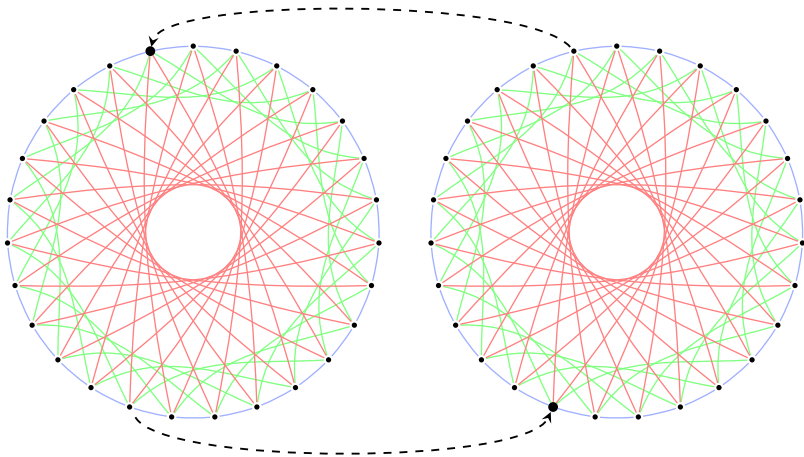
Diffie–Hellman on graphs!

Alice

[+, -, +, -]

Bob

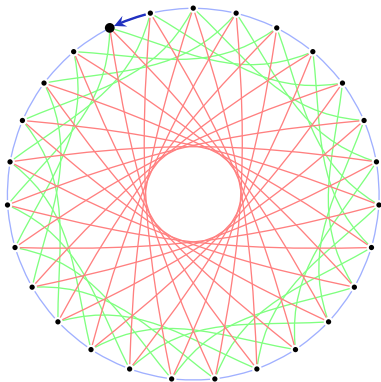
[+, +, -, +]



Diffie–Hellman on graphs!

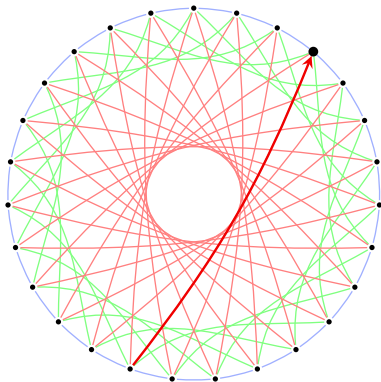
Alice

[+, -, +, -]
↑



Bob

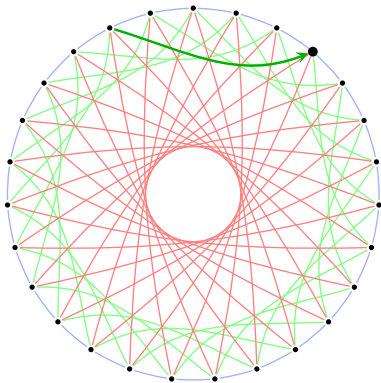
[+, +, -, +]
↑



Diffie–Hellman on graphs!

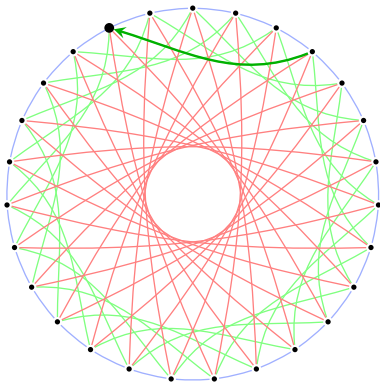
Alice

[+, -, +, -]
↑



Bob

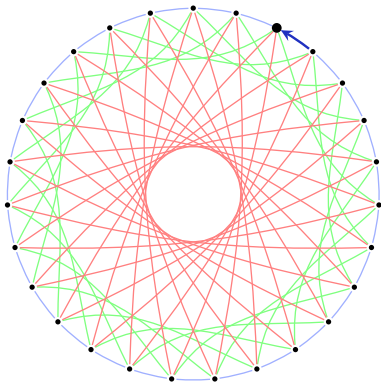
[+, +, -, +]
↑



Diffie–Hellman on graphs!

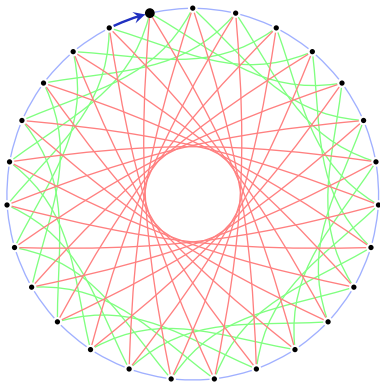
Alice

[+, -, +, -]
↑



Bob

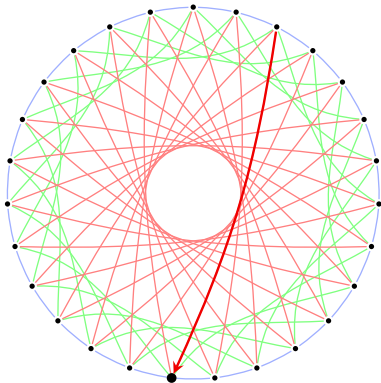
[+, +, -, +]
↑



Diffie–Hellman on graphs!

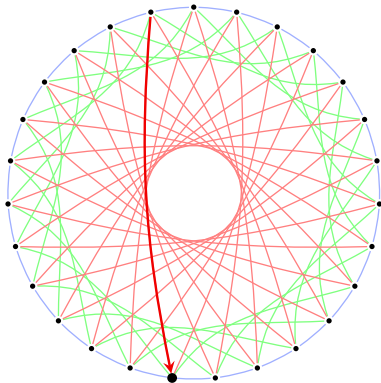
Alice

[+, -, +, -]
↑



Bob

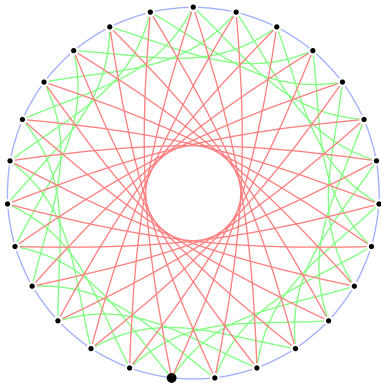
[+, +, -, +]
↑



Diffie–Hellman on graphs!

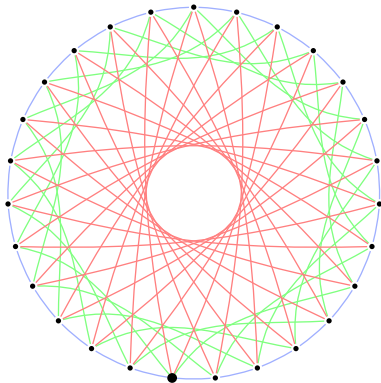
Alice

[+, -, +, -]



Bob

[+, +, -, +]



Welcome to the CSIDH!

- ▶ Our contribution:
Huge speed-up by switching to supersingular curves.

Welcome to the CSIDH!

- ▶ Our contribution:
Huge speed-up by switching to supersingular curves.
- ▶ 'An efficient post-quantum commutative group action'.

Welcome to the CSIDH!

- ▶ Our contribution:
Huge speed-up by switching to supersingular curves.
 - ▶ 'An efficient post-quantum commutative group action'.
- ⇒ Post-quantum non-interactive key exchange.
(Efficient public-key validation!)
- ▶ Public keys: 64 bytes (conjectured AES-128 security level).
 - ▶ Full key exchange: ~ 80 ms. (Optimizations in progress!)

Welcome to the CSIDH!

- ▶ Our contribution:
Huge speed-up by switching to supersingular curves.
 - ▶ 'An efficient post-quantum commutative group action'.
- ⇒ Post-quantum non-interactive key exchange.
(Efficient public-key validation!)
- ▶ Public keys: 64 bytes (conjectured AES-128 security level).
 - ▶ Full key exchange: ~ 80 ms. (Optimizations in progress!)

Thanks!