CSIDH: an efficient post-quantum commutative group action

Class group action on elliptic curve isogeny volcanoes.

- Couveignes–Rostovtsev–Stolbunov use ordinary curves. (**slow!**)
- De Feo–Kieffer–Smith use small-order rational points. (**still slow...**)
- We switch to supersingular curves defined over $\mathbb{F}_p$.
  (Galbraith–Delfs: essentially the same structure as the ordinary case)

$\Longrightarrow$ yields an easy Diffie–Hellman key agreement.

$\Longrightarrow$ PoC implementation takes $\sim 50\,\text{ms}$ per operation.

$\Longrightarrow$ small public keys ($\sim$ 64 bytes for NISTPQC level 1)
(taking into account Childs–Jao–Soukharev's subexponential quantum attack)

$\Longrightarrow$ public-key validation: doesn't need Fujisaki–Okamoto.
$\Longrightarrow$ post-quantum static–static key exchange!

Expect our paper in a week or two!
More details and applications still work in progress.

---

interested? talk to: Wouter Castryck, Tanja Lange, Lorenz Panny, Joost Renes