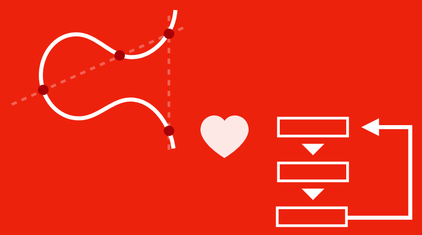

Applying pairings in isogeny crypto

why pairings at all?

scheme maturity

- classical security well understood
- quantum security well understood
- fast, constant-time implementation
- deterministic and dummy-free

CSIDH's maturity?

- ✓ classical security well understood
- ? quantum security well understood
- ? quite slow constant-time
- ✗ *very slow* deterministic, dummy-free

---

how do we achieve fast high-security CSIDH?

constant-time, deterministic, dummy-free

✗ **previously**

- add **seed** for torsion points in key
- **slow** verification of torsion points
- **slow** group action due to dummy-free

? **with pairings**

- **fast** verification of torsion points
- removes probability from CTIDH
- improved group action and ss verify!

✓ ***to do***

- analyse **optimal** use of torsion
- can we use **faster** torsion finding?
- can improve group action!

Thank you!

Any questions*?

*If not, I have a question for you...