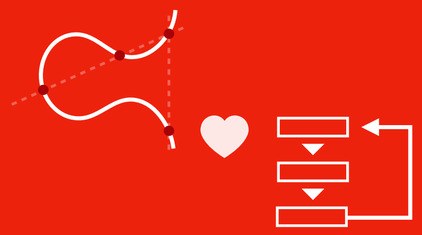


Applying pairings in isogeny crypto

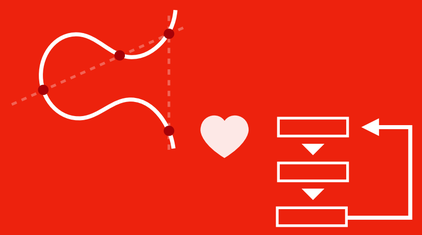
why pairings at all?

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



Applying pairings in isogeny crypto

why pairings at all?

scheme maturity	CSIDH's maturity?
• classical security well understood	✓ classical security well understood
• quantum security well understood	? quantum security well understood
• fast, constant-time implementation	? quite slow constant-time
• deterministic and dummy-free	✗ *very slow* deterministic, dummy-free

how do we achieve fast high-security CSIDH?

constant-time, deterministic, dummy-free