



Applying pairings in isogeny crypto

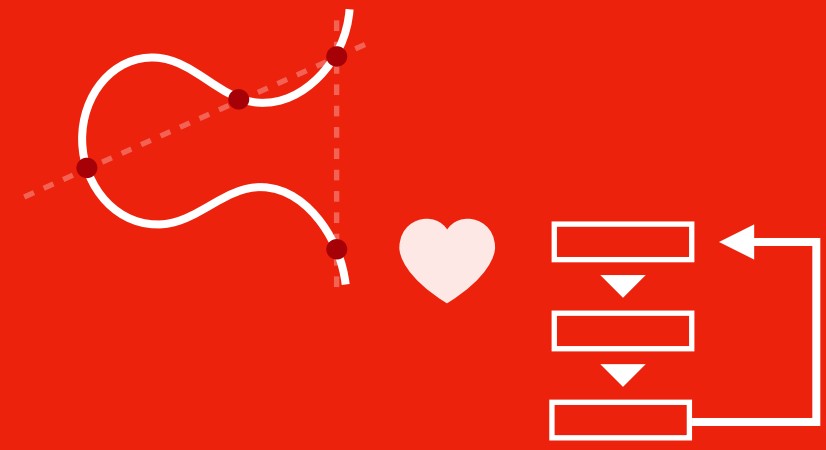
why pairings at all?

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



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