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

Radboud University

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

Radboud University