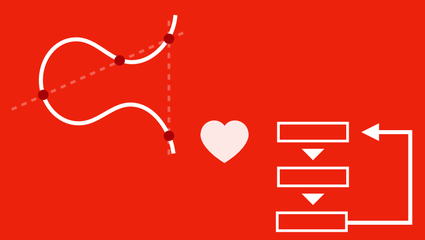


Applying pairings in isogeny crypto

✓ **fast pairings**

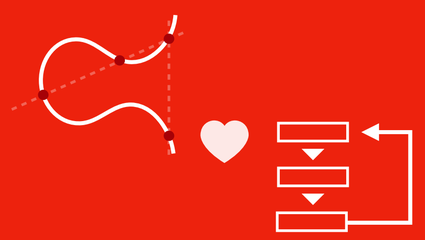
Optimized pairing computation for the specific scenario $P \in E(\mathbb{F}_p), Q \in E^t(\mathbb{F}_p)$

&

✓ **core idea**

For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$, don't use curve arithmetic but pairing $e(P, Q)$ to get overlap in orders!

Faster isogeny subroutines



Applying pairings in isogeny crypto

✓ **fast pairings**

Optimized pairing computation for the specific scenario $P \in E(\mathbb{F}_p), Q \in E^t(\mathbb{F}_p)$

&

✓ **core idea**

For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$, don't use curve arithmetic but pairing $e(P, Q)$ to get overlap in orders!

Faster isogeny subroutines

verify full torsion *P*

In some CSIDH variants, we are given $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$.

Q: verify that both P and Q have order $p + 1$, e.g. full torsion points