



## Applying pairings in isogeny crypto



### fast pairings

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



### core idea

For  $P \in E(\mathbb{F}_p)$  and  $Q \in E'(\mathbb{F}_p)$ , 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  $Q \in E'(\mathbb{F}_p)$ .

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

**A:** compute  $\zeta = e(P, Q)$  and check that order  $\zeta$  is  $p + 1$ .

speedup: -75%



### compute full torsion $P$

In some CSIDH variants, we get  $E$

**Q:** find  $P \in E(\mathbb{F}_p)$  and  $Q \in E'(\mathbb{F}_p)$  of order  $p + 1$ , e.g. full torsion points

**A:** take random,  $P, Q$ , then find  $\zeta = e(P, Q)$ . Compute order  $\zeta$  and apply Gauss' algorithm.

speedup: case dependent, up to -75%





## Applying pairings in isogeny crypto



### fast pairings

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



### core idea

For  $P \in E(\mathbb{F}_p)$  and  $Q \in E'(\mathbb{F}_p)$ , 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  $Q \in E'(\mathbb{F}_p)$ .

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

**A:** compute  $\zeta = e(P, Q)$  and check that order  $\zeta$  is  $p + 1$ .



speedup: -75%

### compute full torsion $P$

In some CSIDH variants, we get  $E$

**Q:** find  $P \in E(\mathbb{F}_p)$  and  $Q \in E'(\mathbb{F}_p)$  of order  $p + 1$ , e.g. full torsion points

**A:** take random,  $P, Q$ , then find  $\zeta = e(P, Q)$ . Compute order  $\zeta$  and apply Gauss' algorithm.



speedup: case dependent, up to -75%

### verify supersingularity

In some CSIDH variants, we get  $E$

**Q:** is  $E$  even supersingular? verify that it is!