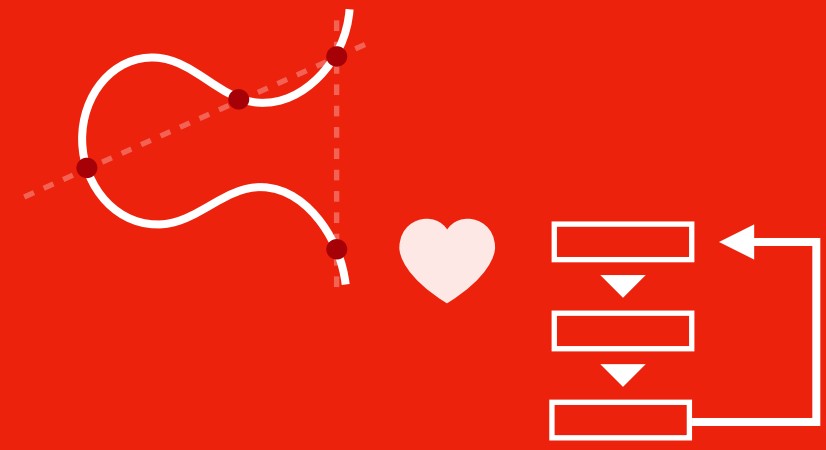


# Fast pairings ♥ Isogeny crypto



## 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