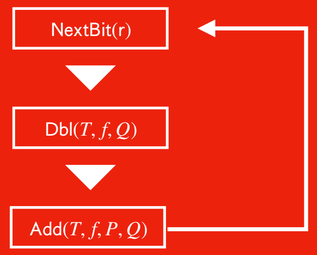
2



Speeding-up general pairings

pairing crypto

Choose a “nice” curve E,
Choose a “nice” prime p,
to do **pairings** with

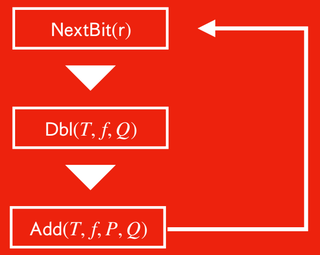
Computing $e(P, Q)$
is quite **fast**!

✓

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!

2



Speeding-up general pairings

pairing crypto

Choose a “nice” curve E,
Choose a “nice” prime p,
to do **pairings** with

Computing $e(P, Q)$
is quite **fast**!

isogeny crypto

Choose a “nice” curve E,
Choose a “nice” prime p,
to do **isogenies** with

These are mediocre curves,
and definitely bad primes,
to do **pairings** with

Computing $e(P, Q)$
seems way too **slow**!

✓

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!