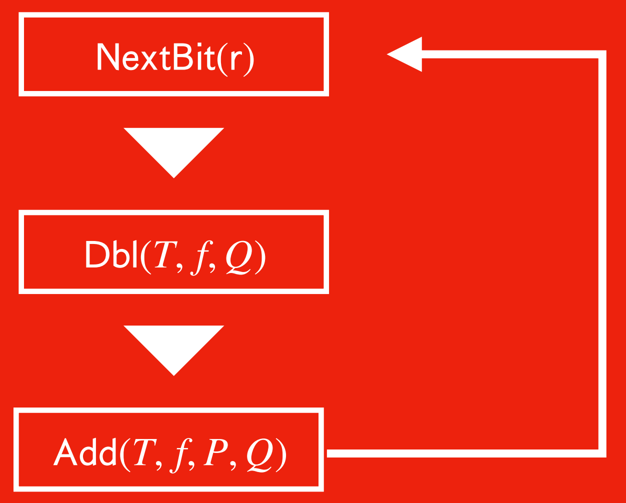
2



NextBit(r)

Dbl(T, f, Q)

Add(T, f, P, Q)

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

MAIN RESULTS

1 make pairings great again

2 apply **core idea**

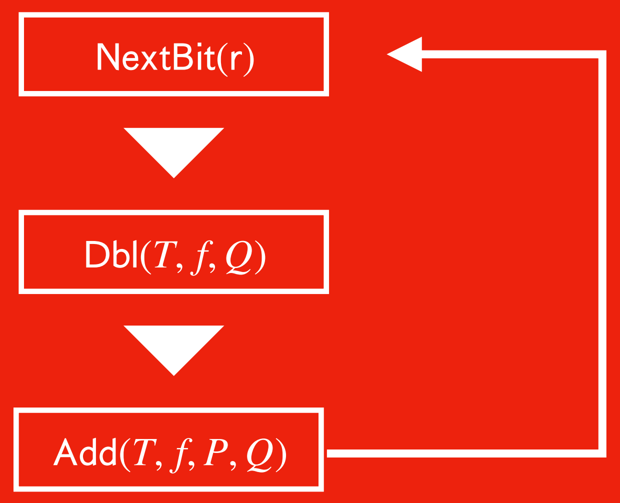
3 faster isogeny algorithms!

first this

then this

Radboud University

2



Speeding-up general pairings

!

general notice

Computing pairings fast is quite technical.
Better suited for papers than slides

✓

general approach

Instead I describe the general approach,
and leave all details out

✓

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!