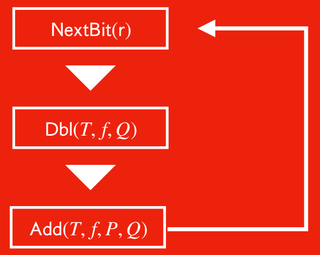
2



Speeding-up general pairings

general notice

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

core idea

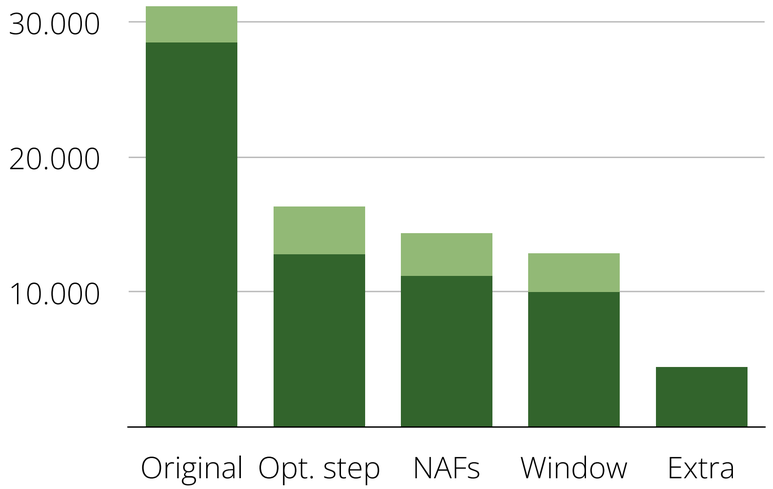
For $P \in E(\mathbb{F}_p)$ and $Q \in E^t(\mathbb{F}_p)$, don't use curve arithmetic but pairing $e(P, Q)$ to get overlap in orders!

general approach

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

3

fast pairings



extra pairings

if you have already computed $e(P, Q_1)$,

it is very efficient to compute $e(P, Q_2)$

Fast pairings

Isogeny crypto