



general notice

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



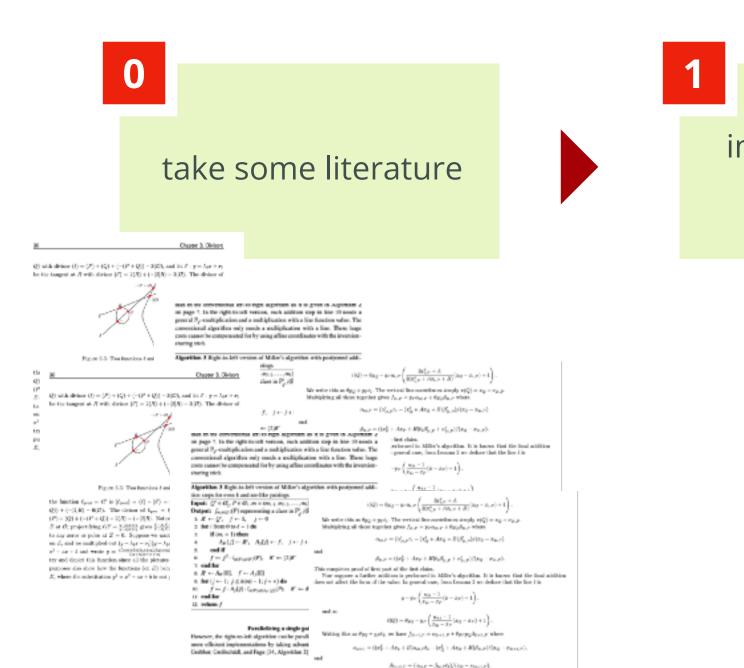
core idea

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

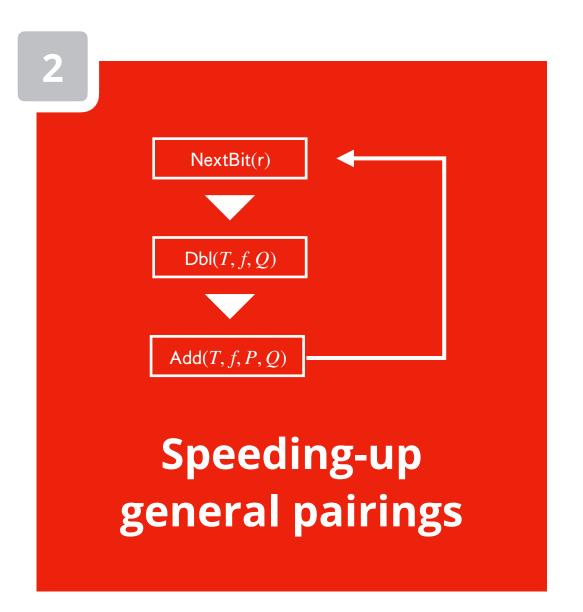
Instead I describe the general approach, and leave all details out



 $\beta_{(i-1),i'} = (x_{(i),i'} + \beta_{(i),i'}t_1)/(x_{(i')} - x_{(i+1),i'}).$

implement all tricks that apply





K, where the substitution $p^2 = p^2 + ap + b$ is not :

 $i(Q) = \theta_{N3} - y_{iT} \left(\frac{x_{i,t} - 1}{z_{iy} - x_{T}} (x_{ij} - x_{T}) + 1 \right).$

 $\beta_{(i-1),i'} = (x_{(i),i'} + \beta_{(i),i'}t_1)/(x_{(i')} - x_{(i+1),i'}).$

Functioning a single gat However, the right an left algorithm can be parall some efficient imprintmentations by taking admit Coubber, Coubbankli, and Fage (H., Algorithm 2) and

general notice

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



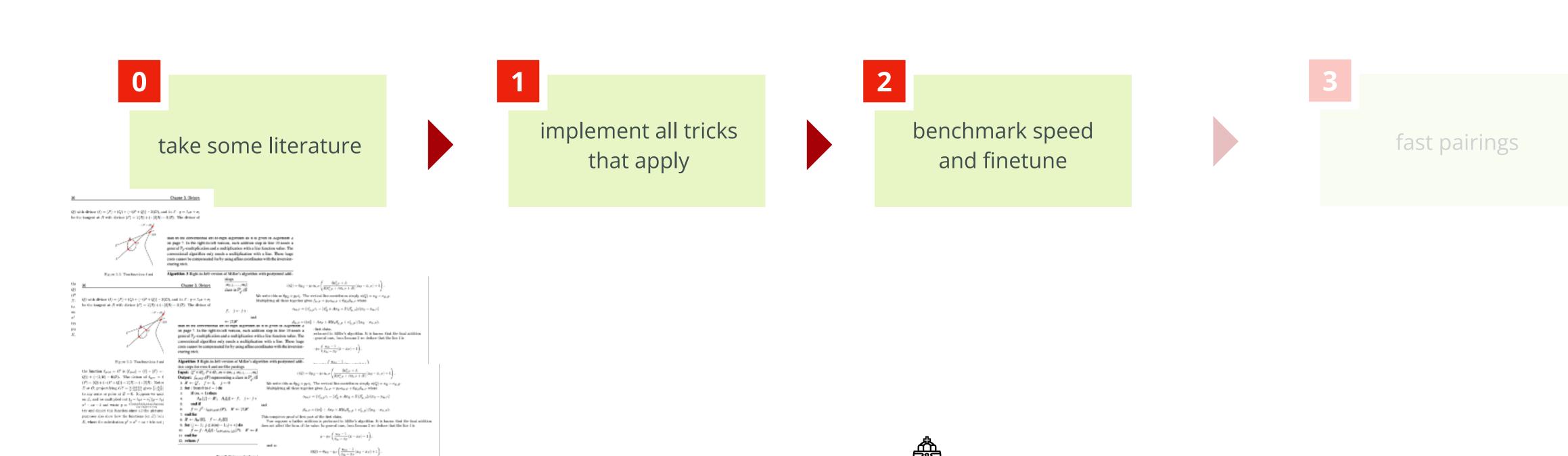
core idea

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



Radboud University