

## 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  $Q \in E'(\mathbb{F}_p)$ ,  
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

0

take some literature

1

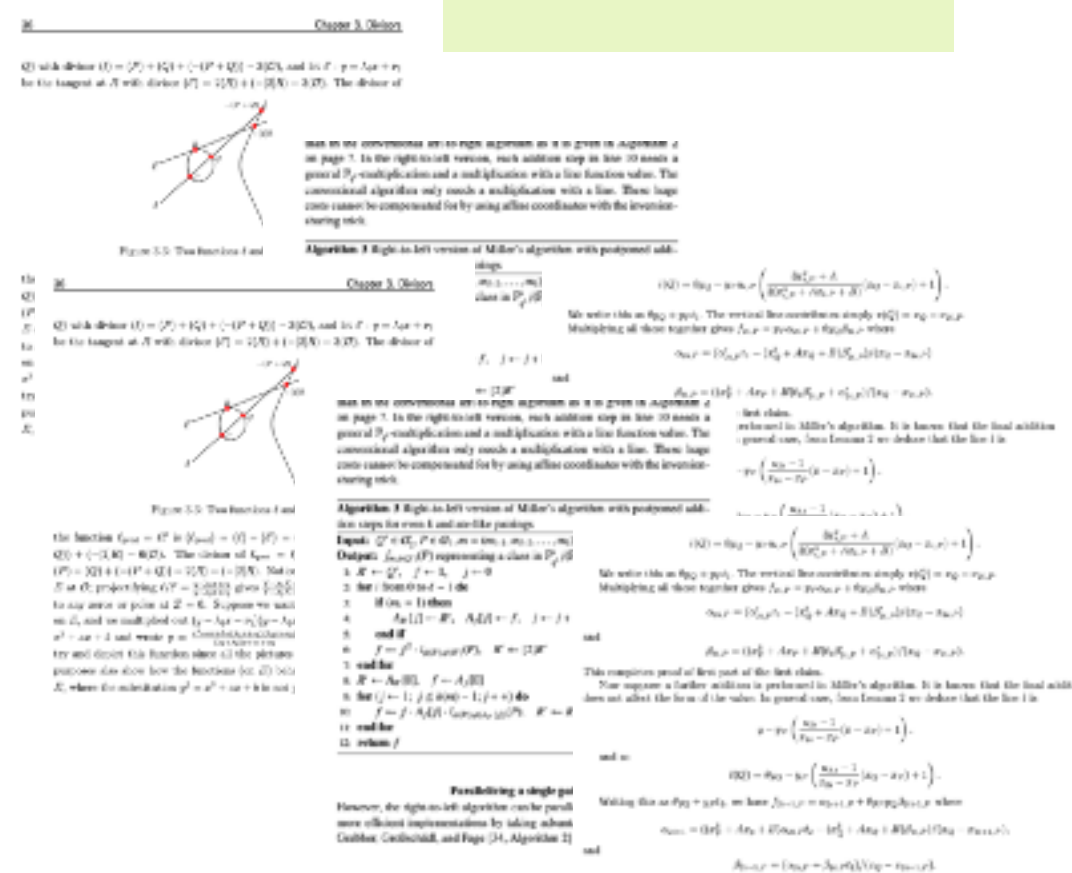
implement all tricks  
that apply

2

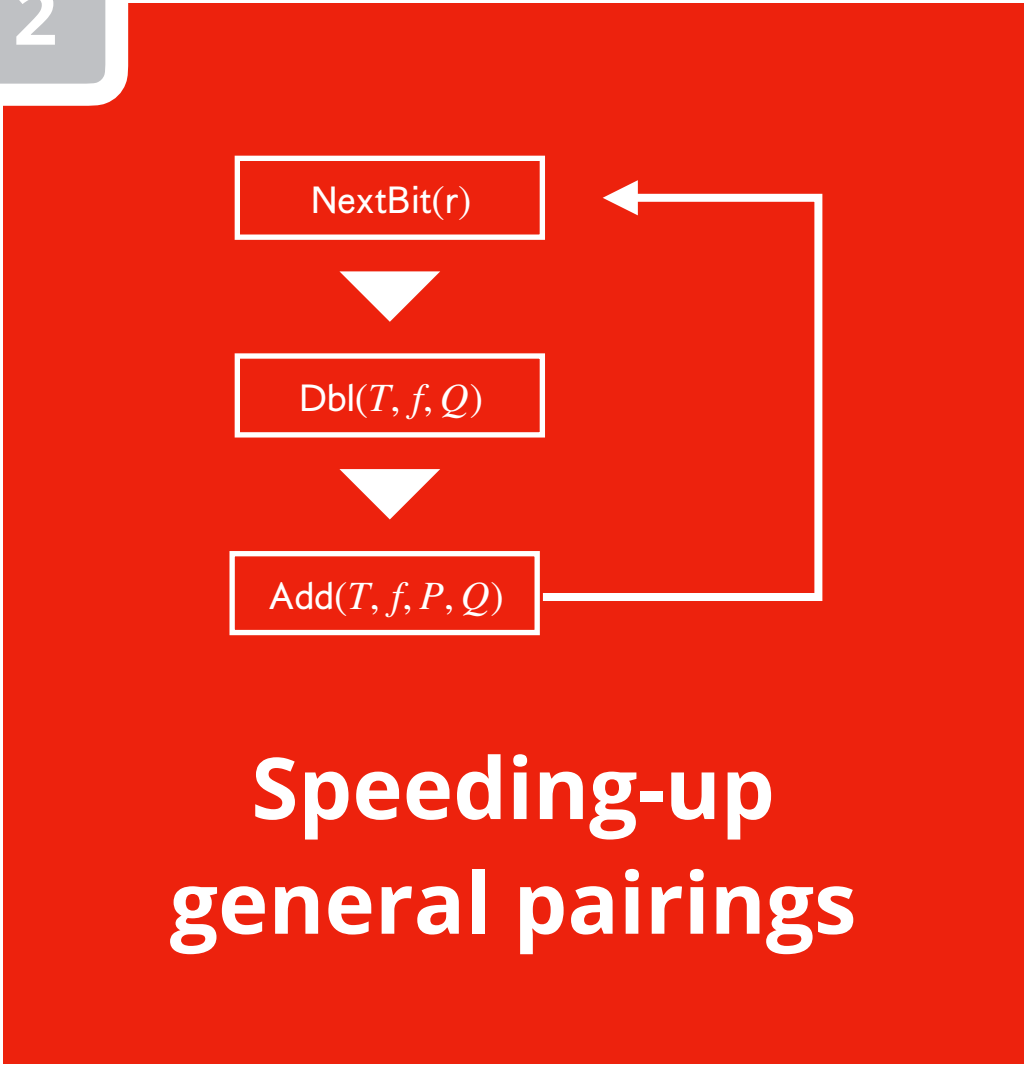
benchmark speed  
and finetune

3

fast pairings



2



**!**

**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

0

take some literature

Chapter 3: History

1

implement all tricks  
that apply

## 2 benchmark speed and finetune

