



### general notice

Computing pairings fast is quite technical.

Better suited for papers than slides



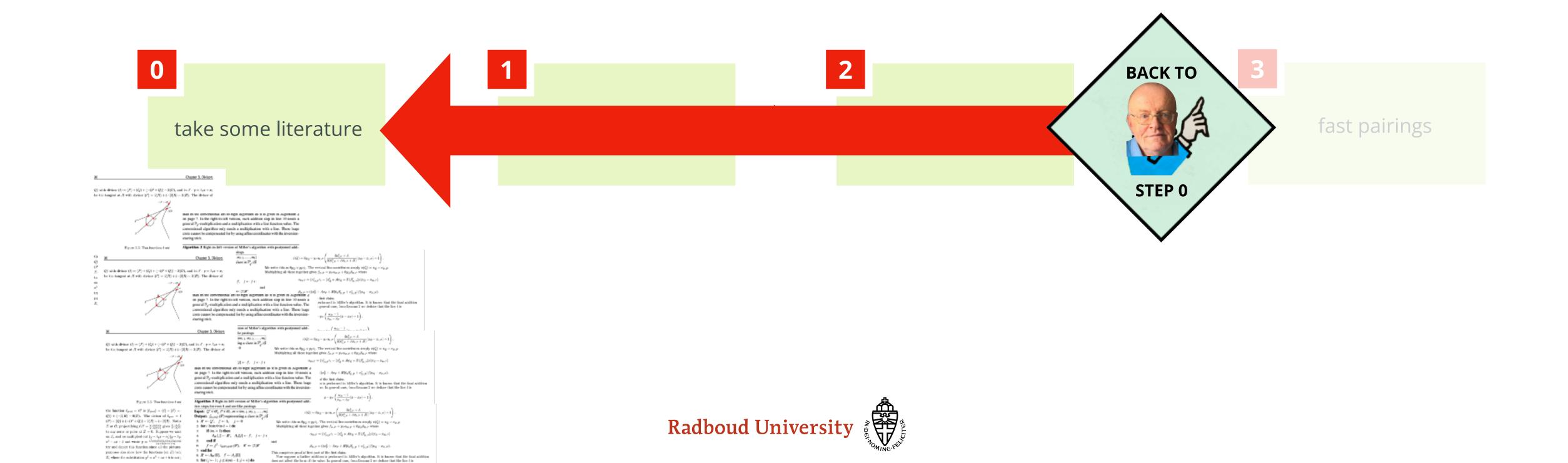
#### core idea

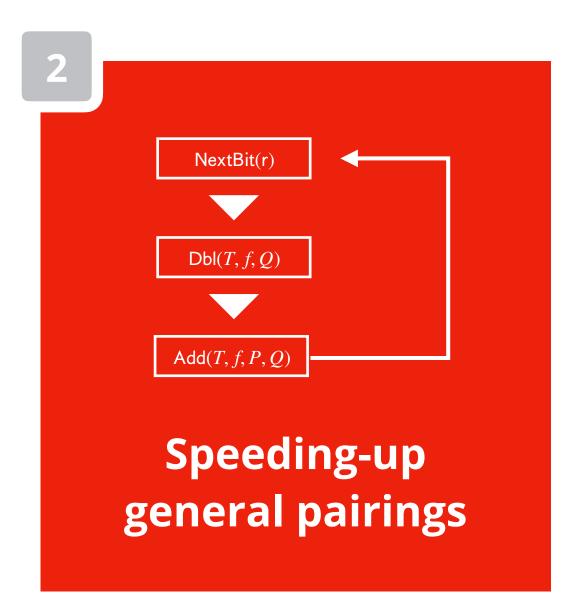
For  $P \in E(\mathbb{F}_p)$  and  $Q \in E^t(\mathbb{F}_p)$ , don't use curve arithmetic but pairing e(P,Q) to get overlap in orders!



# general approach

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





Q) with divisor (I) = (P) + (Q) + (-(P + Q)) - 3(D), and is  $I : p = \lambda_1 x + p_1$  be the tangent at II with divisor (I') = 2(X) + (-(2(X) - 2)X). The divisor of

the function  $\ell_{prot} = \ell \ell^*$  is  $(\ell_{prot}) = (\ell) - (\ell') = \ell \ell \ell + (-\ell, k) - 0.05$ . The distant of  $\ell_{prot} = \ell \ell \ell \ell + (-\ell' + k) + 0.07 - (-\ell, k)$ . Notice if  $\ell \in \mathcal{O}(\ell) + (-\ell' + k) + 0.07 - (-\ell, k)$  where  $\ell \in \mathcal{O}(\ell)$  is  $\ell \in \mathcal{O}(\ell)$  proportions  $\ell \ell' = \frac{1}{2} \frac{(\ell + k)}{2} \frac{(\ell + k)}$ to any zeros or point at Z=0. Suppose we want



 $\langle q_{ij,j} = (g_{ij,j}^* c_i - (g_{ij}^* + Ax_{ij} + B) S_{ij,i} | x(x_i - x_{ij,i}) \rangle$ 

where the convenience artises regarding measurement at the region of the properties of the page 2. In the right intent version, which interfaces within The convenience displacement of a multiplication with a fine. These larger tents caused by compensated for by using affine coordinates with the inventional species.

In propose the compensated for by using affine coordinates with the inventional species.

In propose the proposed in the first order of the proposed in the pro

**Experime 3 light to left version of Miller's algorithm with postposed sales.**  $y = yx \left( \frac{x_0 - 1}{x_0 - x_0} (x - x_0) - 1 \right)$ , the same  $y = yx \left( \frac{x_0 - 1}{x_0 - x_0} (x - x_0) - 1 \right)$ .

The trainer be composed of the first trainer for the problem of the first trainer for first trainer for the f

Against the B right in Lett version of Miller's steps than steps for even L and miller printings. Expect  $Q' + G_q P + G_{q'} = \{m_1, m_2, \dots, m_l\}$ Output:  $f_{m_1 m_2}(P) = \{m_1, m_2, \dots, m_l\}$ Output:  $f_{m_2 m_2}(P) = \{m_1, \dots, m_l\}$  $0 + R + G_q' = \{m_1, \dots, m_l\}$  $0 + R + G_q' = \{m_1, \dots, m_l\}$  $0 + R + G_q' = \{m_1, \dots, m_l\}$  $0 + R + G_q' = \{m_1, \dots, m_l\}$ 

### general notice

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



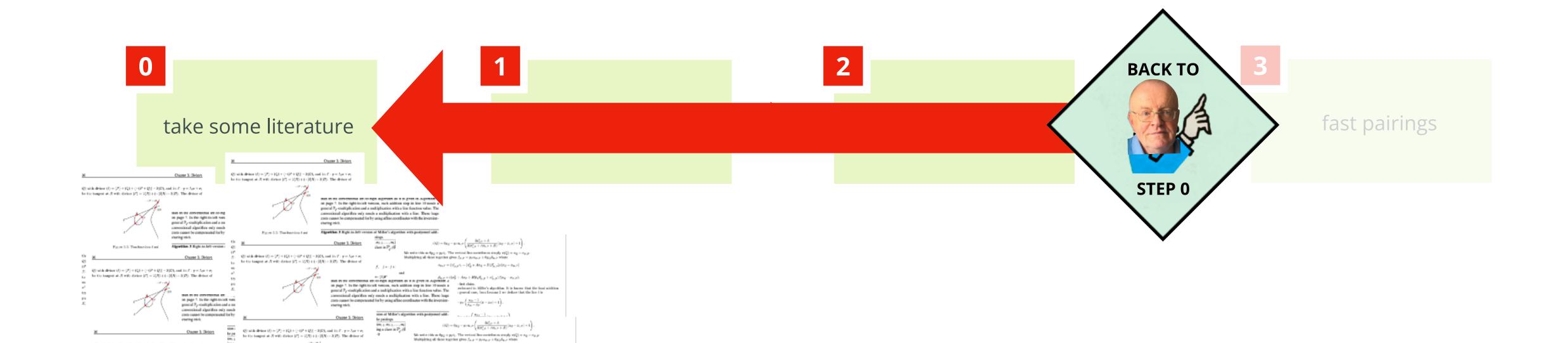
#### core idea

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