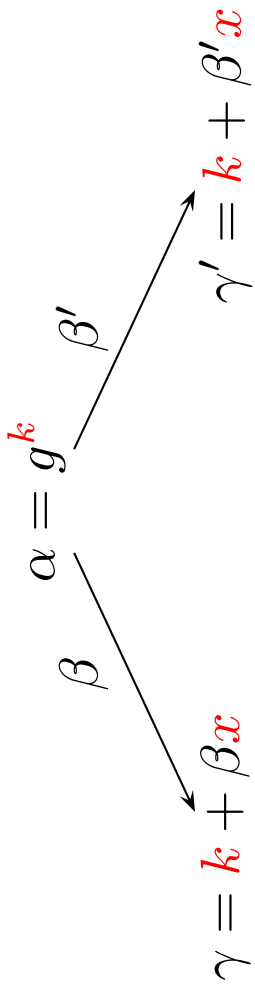


Given two runs with a coinciding prefix  $\alpha$



We can extract the secret key  $x = \frac{\gamma - \gamma'}{\beta - \beta'}$ .