

Judge J

sample uniform $\theta \in \mathbb{Z}_{n_k}$

$y := g_k^\theta \in G_k$

► $I.\theta$

return $y \stackrel{?}{=} g_k^{I.\theta}$

Inverter I

► $J.y$
compute θ