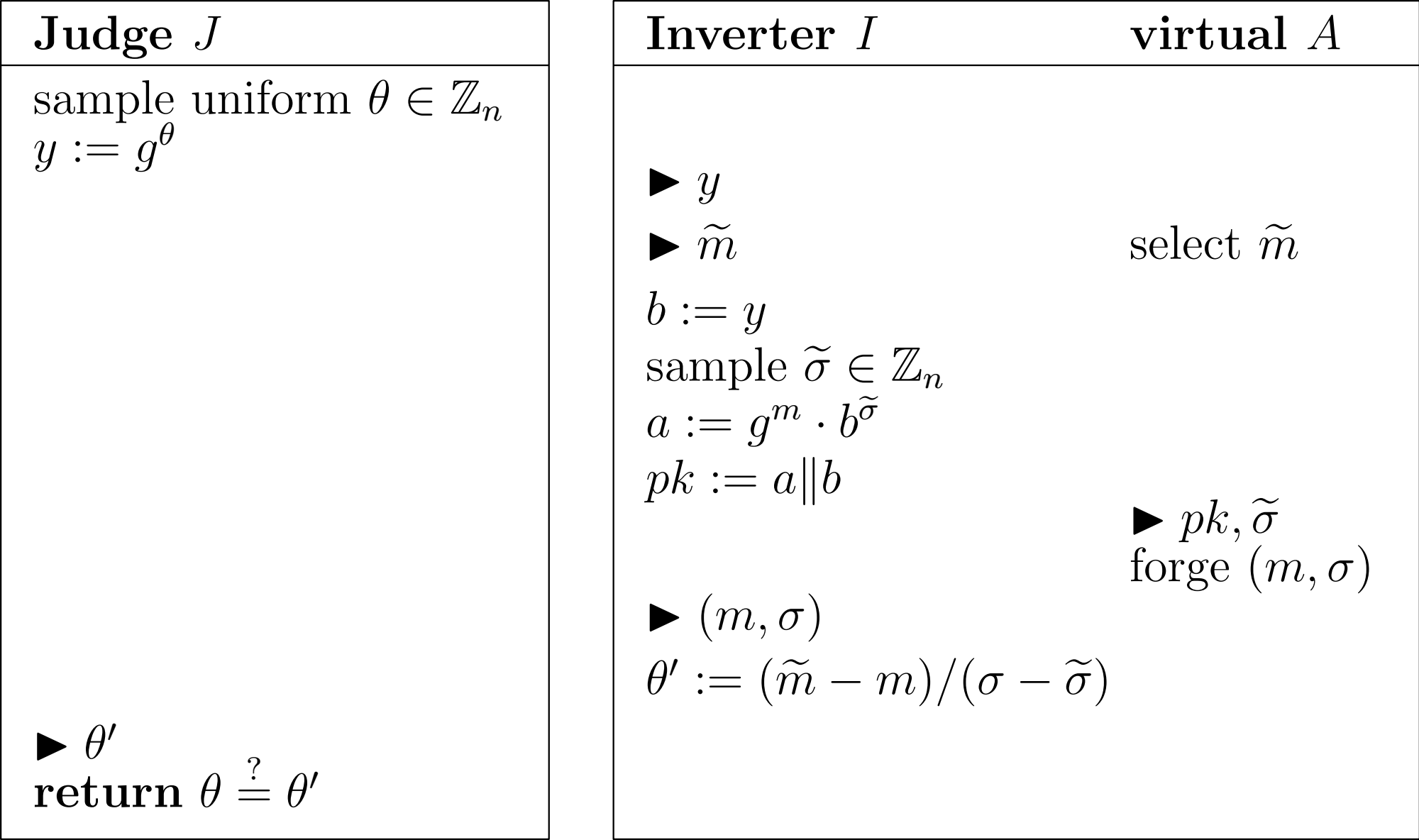
Judge J
sample uniform $\theta \in \mathbb{Z}_n$
$y := g^\theta$
▶ θ'
return $\theta \stackrel{?}{=} \theta'$
Inverter I
virtual A
▶ y
▶ $\widetilde{m}$
select $\widetilde{m}$
$b := y$
sample $\widetilde{\sigma} \in \mathbb{Z}_n$
$a := g^m \cdot b^{\widetilde{\sigma}}$
$pk := a \| b$
▶ $pk, \widetilde{\sigma}$
forge (m, σ)
▶ (m, σ)
$\theta' := (\widetilde{m} - m)/(\sigma - \widetilde{\sigma})$