

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