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