

Judge J

► \tilde{m}

$(sk, pk) := \text{gen}(1^k)$

$\tilde{\sigma} := \text{sgn}(sk, \tilde{m})$

► m, σ

return $\text{vrf}(pk, m, \sigma)$
 $\wedge (m \neq \tilde{m})$

Adversary A

select \tilde{m}

► $pk, \tilde{\sigma}$

forge (m, σ)