

Judge J

► m_1, \dots, m_ℓ

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

for $i = 1 \dots \ell$:

$\sigma_i := \text{sgn}(sk, m_i)$

► m, σ

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

$\wedge (\forall i \in [\ell], m \neq m_i)$

Adversary A

select m_1, \dots, m_ℓ

► $pk, \sigma_1, \dots, \sigma_\ell$

forge (m, σ)