

Judge J

► $A.m_1, \dots, A.m_l$
 $(sk, pk) := \text{gen}(1^k)$
for $i = 1 \dots l$:
 $\sigma_i := \text{sgn}(sk, A.m_i)$

► $A.m, A.\sigma$
return $\text{vrf}(pk, A.m, A.\sigma)$
 $\wedge (\forall i \in [l], A.m \neq A.m_i)$

Adversary A

select m_1, \dots, m_l

► $J.pk$
► $J.\sigma_1, \dots, J.\sigma_l$
forge (m, σ)