Judge J

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

for $i = 1, 2, \ldots$:

- ▶ $A.m_i$
- $\sigma_i := \mathtt{sgn}(sk, A.m_i)$

▶ $A.m, A.\sigma$

return $\mathtt{vrf}(pk, A.m, A.\sigma)$
$\wedge(\forall i,\ A.m \neq A.m_i)$

Adversary A

▶ $J.pk$

for $i = 1, 2, \ldots$:

- select m_i
- ▶ $J.\sigma_i$
- compute; break if appropriate

forge (m, σ)