Judge J

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

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

  ▶ m_i

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

▶ m, σ

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

$\wedge(\forall i,\ m \neq m_i)$

Adversary A

▶ pk

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

  select m_i

  ▶ σ_i

  break when appropriate

forge (m, σ)