Judge J

▶ $A.\widetilde{m}$

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

$\widetilde{\sigma} := \mathtt{sgn}(sk, A.m_1)$

▶ $A.m, A.\sigma$

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

Adversary A

select $\widetilde{m}$

▶ $J.pk, \ J.\widetilde{\sigma}$

forge (m, σ)