Algorithm $\mathtt{sgn}^+(sk, m)$**:**

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

return

$pk^1 \| \mathtt{sgn}(sk, pk^1) \| \mathtt{sgn}(sk^1, m)$

Algorithm $\mathtt{vrf}^+(pk, m, \sigma)$**:**

unpack $\sigma =: pk^1 \| \eta \| \zeta$

return

$\mathtt{vrf}(pk, pk^1, \eta) \wedge \mathtt{vrf}^1(pk^1, m, \zeta)$