Algorithm $\mathtt{gen}'(1^k)$**:**

for $i = 1 \dots \ell$ **do**

$(sk_i, pk_i) := \mathtt{gen}(1^k)$

$sk := (sk_1, pk_1) \| \dots \| (sk_\ell, pk_\ell)$

return $(sk, \varnothing)$

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

unpack $sk := (sk_1, pk_1) \| \dots \| (sk_\ell, pk_\ell)$

$i :=$ number of calls to $\mathtt{sgn}'$

return $pk_i \| \mathtt{sgn}(sk_i, m)$

Algorithm $\mathtt{vrf}'(\varnothing, m, \sigma)$**:**

unpack $\sigma =: pk_i \| \eta$

return $\mathtt{vrf}(pk_i, m, \eta)$