

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

for $i = 1 \dots q$ **do**
 $(sk_i, pk_i) := \text{gen}(1^k)$
 $sk := (sk_1, pk_1) \parallel \dots \parallel (sk_q, pk_q)$
 return (sk, \emptyset)

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

 unpack $sk := (sk_1, pk_1) \parallel \dots \parallel (sk_q, pk_q)$
 $i :=$ number of calls of sgn'
 return $pk_i \parallel \text{sgn}(sk_i, m)$

Algorithm $\text{vrf}'(\emptyset, m, \sigma)$:

 unpack $\sigma =: pk_i \parallel \eta$
 return $\text{vrf}(pk_i, m, \eta)$