

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

└ **return** (\emptyset, \emptyset)

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

┌ $i :=$ number of calls to sgn'

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

└ **return** $pk_i \parallel \text{sgn}(sk_i, m)$

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

┌ unpack $\sigma =: pk_i \parallel \eta$

└ **return** $\text{vrf}(pk_i, m, \eta)$