

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

- for**  $i = 1 \dots \ell$  **do**
  - $(sk_i, pk_i) := \text{gen}(1^k)$
- $sk := sk_1 \parallel \dots \parallel sk_\ell$
- $pk := pk_1 \parallel \dots \parallel pk_\ell$
- return**  $(sk, pk)$

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

- unpack  $sk := sk_1 \parallel \dots \parallel sk_\ell$
- $i :=$  number of calls to  $\text{sgn}'$
- return**  $i \parallel \text{sgn}(sk_i, m)$

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

- unpack  $pk := pk_1 \parallel \dots \parallel pk_\ell$
- unpack  $\sigma := i \parallel \eta$
- return**  $\text{vrf}(pk_i, m, \eta)$