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

- **for** $i = 1 \ldots q$ **do**
  - $(sk_i, pk_i) := \mathtt{gen}(1^k)$
- $sk := sk_1 \| \ldots \| sk_q$
- $pk := pk_1 \| \ldots \| pk_q$
- **return** (sk, pk)

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

- unpack $sk =: sk_1 \| \ldots \| sk_q$
- $i :=$ number of calls of $\mathtt{sgn}'$
- **return** $i \| \mathtt{sgn}(sk_i, m)$

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

- unpack $pk := pk_1 \| \ldots \| pk_q$
- unpack $\sigma =: i \| \eta$
- **return** $\mathtt{vrf}(pk_i, m, \eta)$