```
Algorithm $\texttt{gen}'(1^k)$:
    $(sk_0, pk_0) := \texttt{gen}(1^k)$
    return $(sk_0, pk_0)$
```

```
Algorithm $\texttt{sgn}'(sk_0, m)$:
    $i :=$ number of calls to $\texttt{sgn}'$
    $(sk_i, pk_i) := \texttt{gen}(1^k)$
    $\eta_i := \texttt{sgn}(sk_{i-1}, m_i \| pk_i)$
    memorise $m_i \| pk_i \| \eta_i$
    return $(m_j \| pk_j \| \eta_j)_{1 \leq j \leq i}$
```

```
Algorithm $\texttt{vrf}'(pk_0, m, \sigma)$:
    unpack $\sigma =: (m_j \| pk_j \| \eta_j)_{1 \leq j \leq i}$
    if $m \neq m_i$ then
        return $\texttt{false}$
    for $j = 1 \ldots i$ do
        if $\neg\texttt{vrf}(pk_{j-1}, m_j \| pk_j, \eta_j)$ then
            return $\texttt{false}$
    return $\texttt{true}$
```