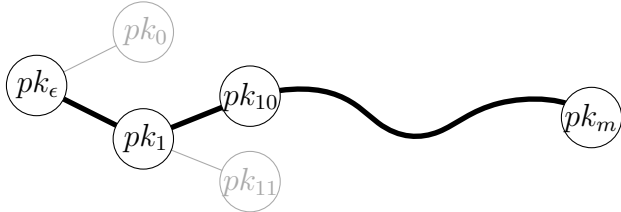


Algorithm $\text{gen}'(1^k)$:

```
┌  $(sk_\epsilon, pk_\epsilon) := \text{gen}(1^k)$   
└ return  $(sk_\epsilon, pk_\epsilon)$ 
```

Algorithm $\text{sgn}'(sk_0, m)$:

```
┌ assume  $m =: b_1 \dots b_L$   
┌ for  $i = 1 \dots L$  do  
┌    $x := b_1 \dots b_{i-1}$   
┌   if  $x$  not visited before then  
┌     ┌  $(sk_{x0}, pk_{x0}) := \text{gen}(1^k)$   
┌     ┌  $(sk_{x1}, sk_{x1}) := \text{gen}(1^k)$   
┌     └  $\eta_x := \text{sgn}(sk_x, pk_{x0} \| pk_{x1})$   
┌  $\eta_m := \text{sgn}(sk_m, m)$   
└ return  $\eta_m \| (pk_{x0} \| pk_{x1} \| \eta_x)_{x \sqsubseteq m}$ 
```



Algorithm $\text{vrf}'(pk_0, m, \sigma)$:

```
┌ assume  $m =: b_1 \dots b_L$   
┌ unpack  $\sigma =: \eta_m \| (pk_{x0} \| pk_{x1} \| \eta_x)_{x \sqsubseteq m}$   
┌ for  $i = 1 \dots L$  do  
┌    $x := b_1 \dots b_{i-1}$   
┌   if  $\neg \text{vrf}(pk_x, pk_{x0} \| pk_{x1}, \eta_x)$  then  
┌     └ return false  
└ return  $\text{vrf}(pk_m, m, \eta_m)$ 
```