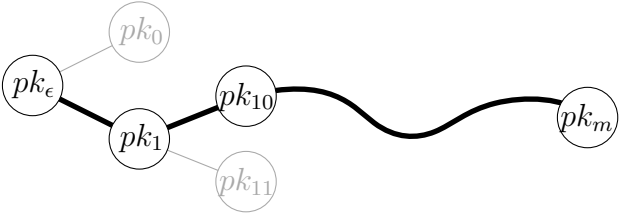
Algorithm $\mathtt{gen}'(1^k)$**:**

$(sk_\epsilon, pk_\epsilon) := \mathtt{gen}(1^k)$

return $(sk_\epsilon, pk_\epsilon)$



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

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**

$(sk_{x0}, pk_{x0}) := \mathtt{gen}(1^k)$

$(sk_{x1}, sk_{x1}) := \mathtt{gen}(1^k)$

$\eta_x := \mathtt{sgn}(sk_x,\ pk_{x0} \| pk_{x1})$

$\eta_m := \mathtt{sgn}(sk_m, m)$

return $\eta_m \parallel (pk_{x0} \| pk_{x1} \| \eta_x)_{x \sqsubset m}$

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

assume $m =: b_1 \dots b_L$

unpack $\sigma =: \eta_m \parallel (pk_{x0} \| pk_{x1} \| \eta_x)_{x \sqsubset m}$

for $i = 1 \dots L$ **do**

$x := b_1 \dots b_{i-1}$

if $\neg \mathtt{vrf}(pk_x,\ pk_{x0} \| pk_{x1},\ \eta_x)$ **then**

return `false`

return $\mathtt{vrf}(pk_m, m, \eta_m)$