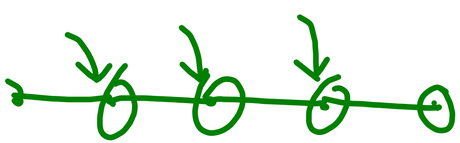
Chain-based signature

- Stateful signature

- verification time is linear to the # of msg signed
- signature releases the previous msgs.

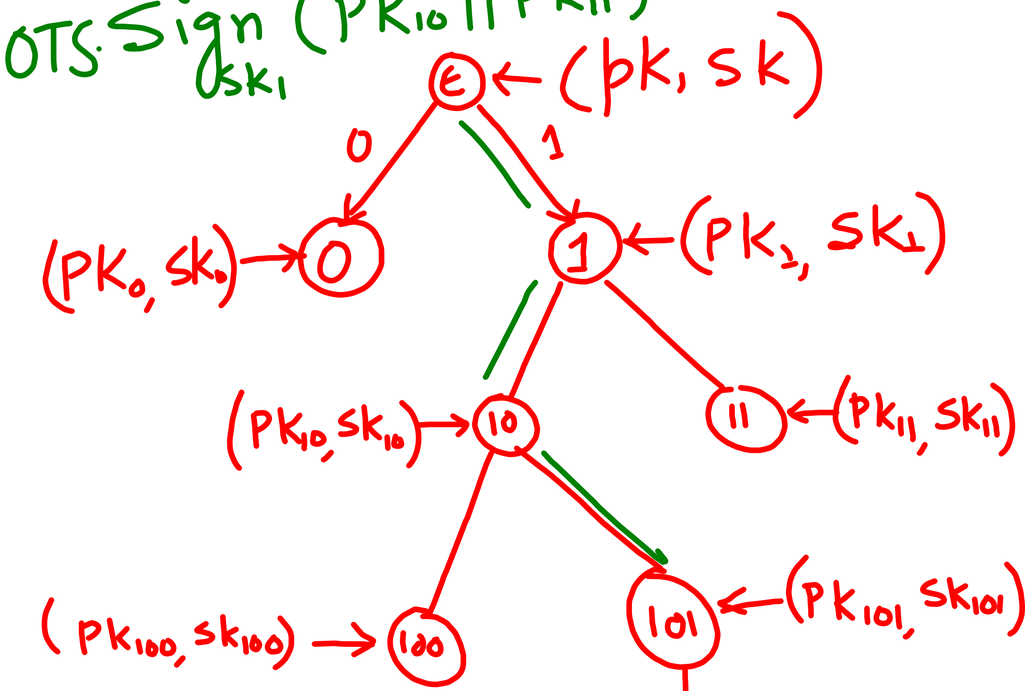


Suppose msg. space $M = \{0,1\}^n$

Binary tree construct of depth n.

$\sigma_1 = \text{OTS.Sign}_{sk}(pk_0 \| pk_1)$.

$\sigma_2 = \text{OTS.Sign}_{sk_1}(pk_{10} \| pk_{11})$



Tree-Based Signature

$n = 3$. $m = 101$ $\quad \Pi_T = (\text{KGen}, \text{Sign}, \text{Vrfy})$

$\text{KGen}(1^n) \to (pk, sk)$

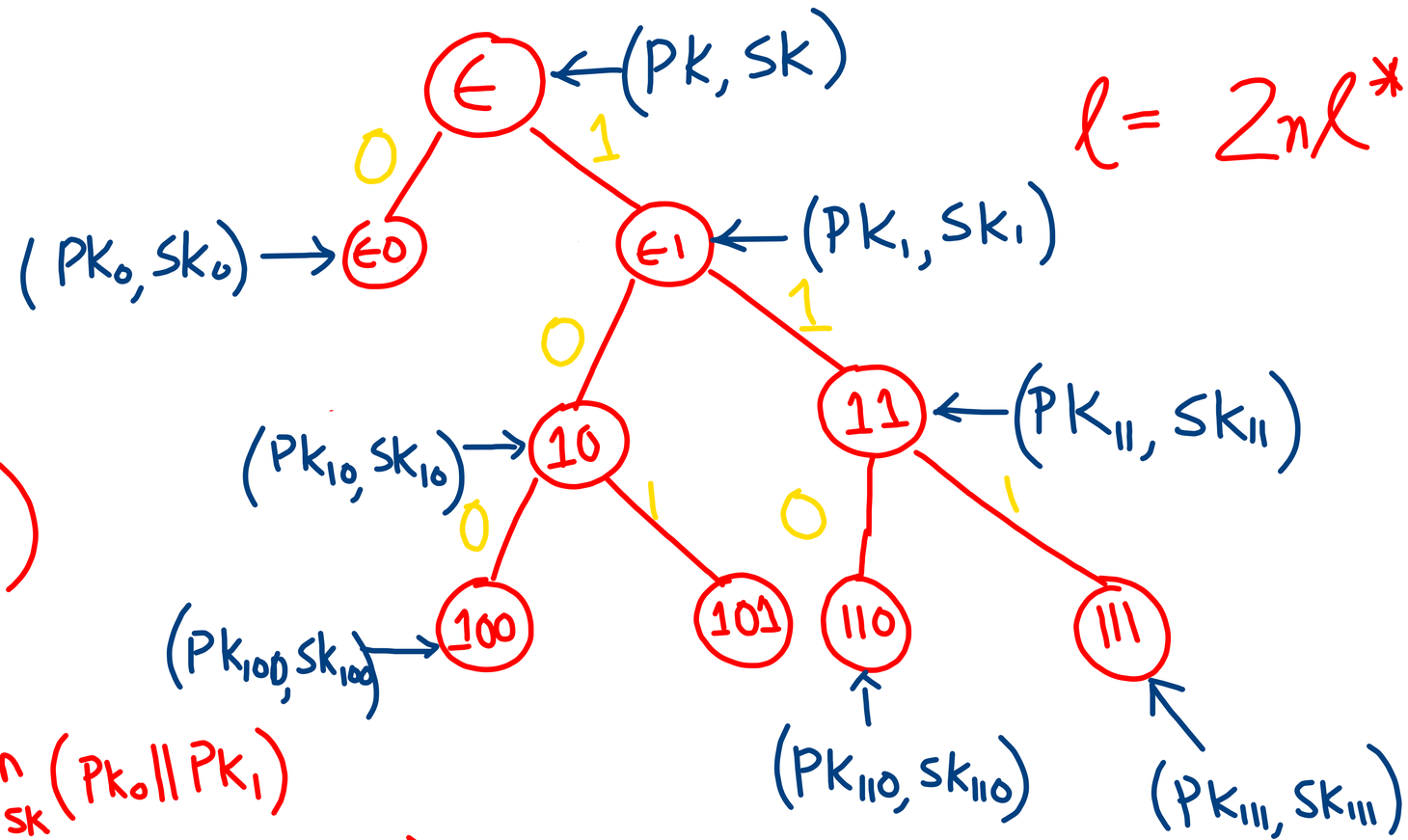
$\hat{\sigma} = \{ (\sigma_1, pk_0 \| pk_1), (\sigma_2, pk_{10} \| pk_{11}), (\sigma_3, pk_{100} \| pk_{101}), \sigma_m \}, 101$

$\sigma_3 = \text{OTS.Sign}_{sk_{10}}(pk_{100} \| pk_{101})$

$\sigma_m = \text{OTS.Sign}_{sk_{101}}(101)$

Suppose $m' = 110$

$m = 101$



$\ell = 2n\ell^* + 1$ many $\langle pk, sk \rangle$

$\sigma_1' = \sigma_1$

$\sigma_2' = \sigma_2$

$\sigma_3' \neq \sigma_3$

$\sigma_m' \neq \sigma_m$

i^*

$(pk_{i^*} \leftarrow pk)$

$sk_{i^*} = (?)$

$\sigma_1' = \text{OTS.Sign}_{sk}(pk_0 \| pk_1)$

$\sigma_2' = \text{OTS.Sign}_{sk_1}(pk_{10} \| pk_{11})$

$\sigma_3' = \text{OTS.Sign}_{sk_{11}}(pk_{110} \| pk_{111})$

$\sigma_m' = \text{OTS.Sign}_{sk_{110}}(110)$

$\hat{\sigma} = \{(\sigma_1', pk_0 \| pk_1), (\sigma_2', pk_{10} \| pk_{11}), (\sigma_3', pk_{110} \| pk_{111}), \sigma_m'\}$

Stateless soln.

We store two keys $\underline{k}$, $\underline{k'}$

$F_K(w) \rightarrow r_w \rightarrow$ Random string.

$(pk_w, sk_w) \leftarrow Gen(r_w)$

$F_{K'}(w) \rightarrow r'_w$

$\sigma = Sign_{sk}(m^*, r'_w)$