

•  $r \sim \{0, 1\}^\ell$  and  $h_1, \dots, h_t: \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$  2-wise independent

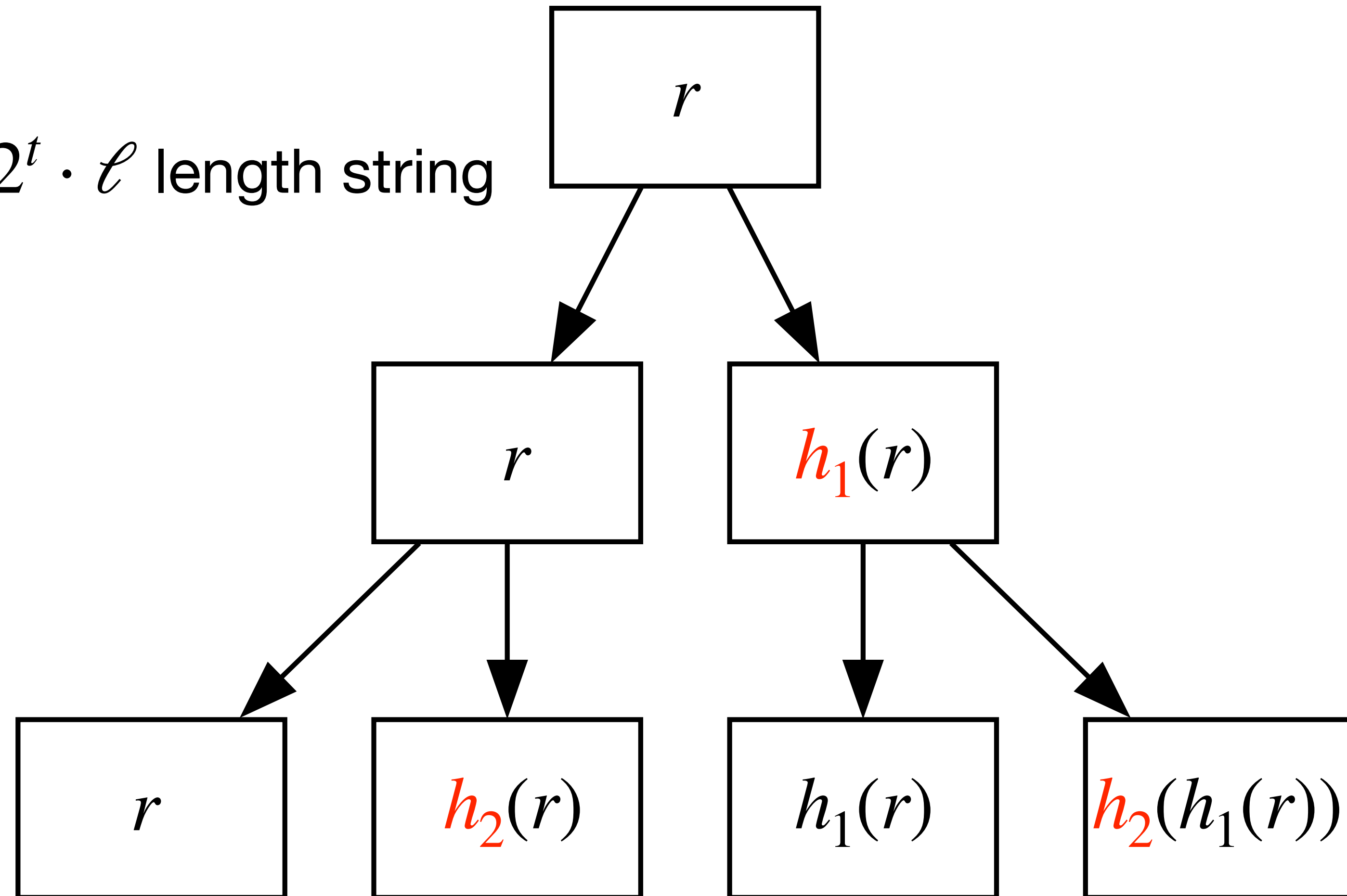
- Seed length of  $\mathcal{O}(t \cdot \ell)$

- Extending the tree gives a length  $2^t \cdot \ell$  length string

**Nissan's PRG**

# Nisan's PRG

- $r \sim \{0,1\}^\ell$  and  $h_1, \dots, h_t : \{0,1\}^\ell \rightarrow \{0,1\}^\ell$  2-wise independent
- Seed length of  $O(t \cdot \ell)$
- Extending the tree gives a length  $2^t \cdot \ell$  length string



# Nisan's Guarantees