

ullet $r \sim \{0,1\}^\ell$ and $h_1,\dots,h_t\colon \{0,1\}^\ell o \{0,1\}^\ell$ 2-wise independent

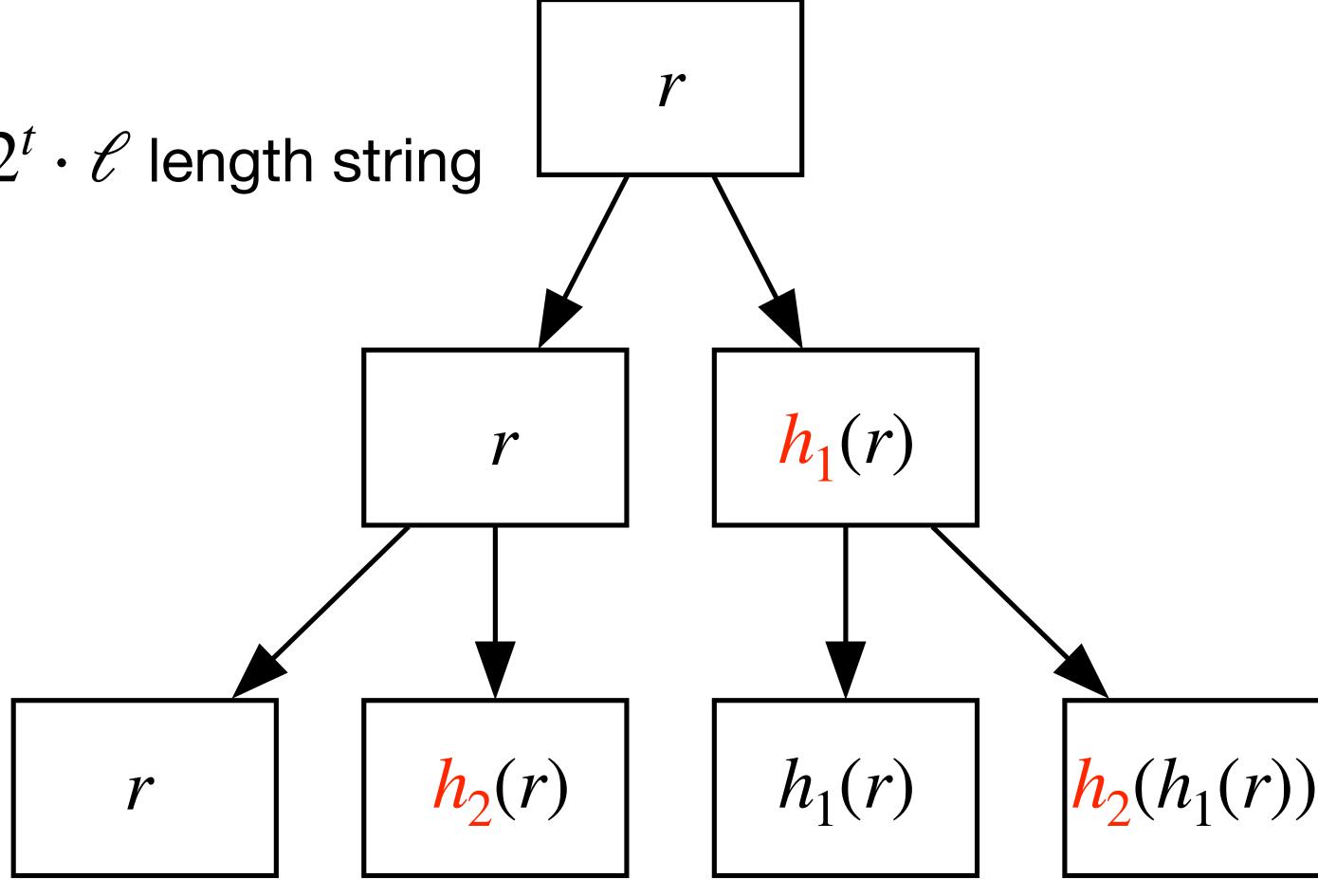
• Seed length of $O(t \cdot \mathscr{C})$

ullet Extending the tree gives a length $2^t \cdot \mathscr{E}$ length string

Nisan's PRG

Nisan's PRG

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



Nisan's Guarantees