

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

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

• 2^t • ℓ length string at the bottom

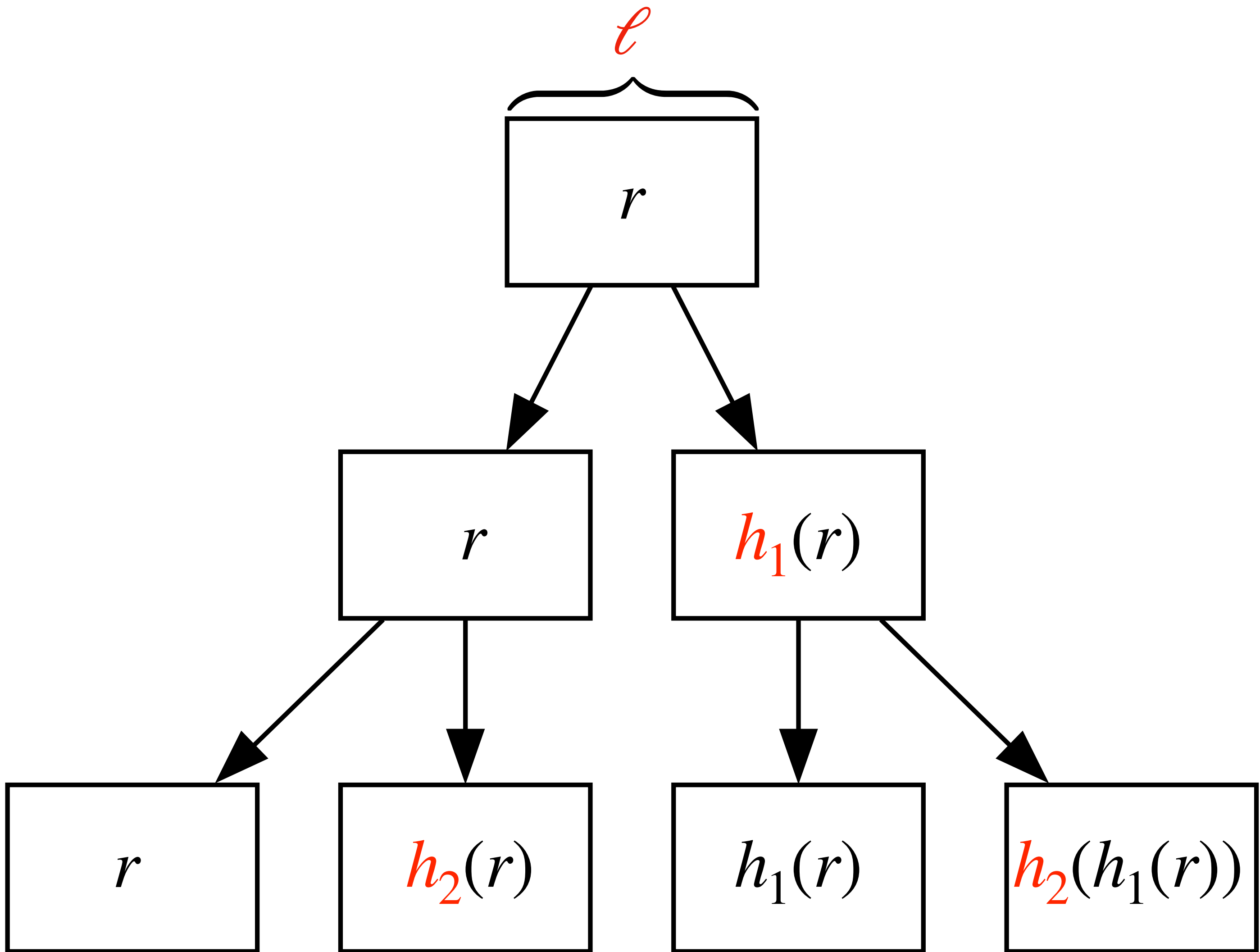
Nissan's PRG



- If $t, w \leq c \cdot \ell$, the PRG fools an algorithm which uses w bits of space

- Compute block with t hash evaluations

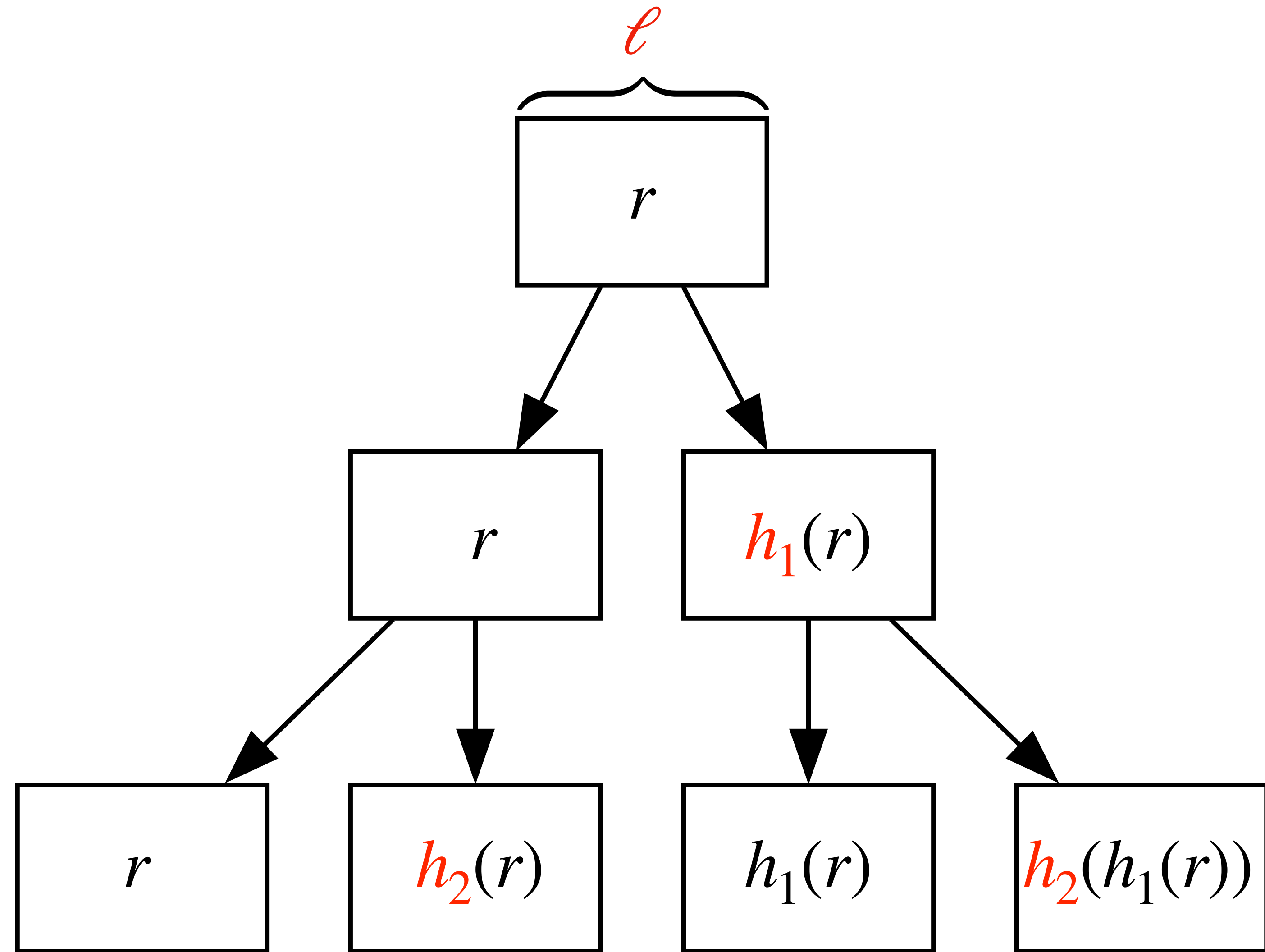
- Keep t and \mathcal{L} small



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 $O(t \cdot \ell)$
- $2^t \cdot \ell$ length string at the bottom

- If $t, w \leq c \cdot \ell$, the PRG fools an algorithm which uses w bits of space
- Compute block with t hash evaluations
 - Keep t and ℓ small



HashPRG : Our Construction