

HashPRG: Our Construction

• Two hash functions per level

• Switching  $h_1^{(1)}$  and  $h_1^{(2)}$  just reorders blocks!

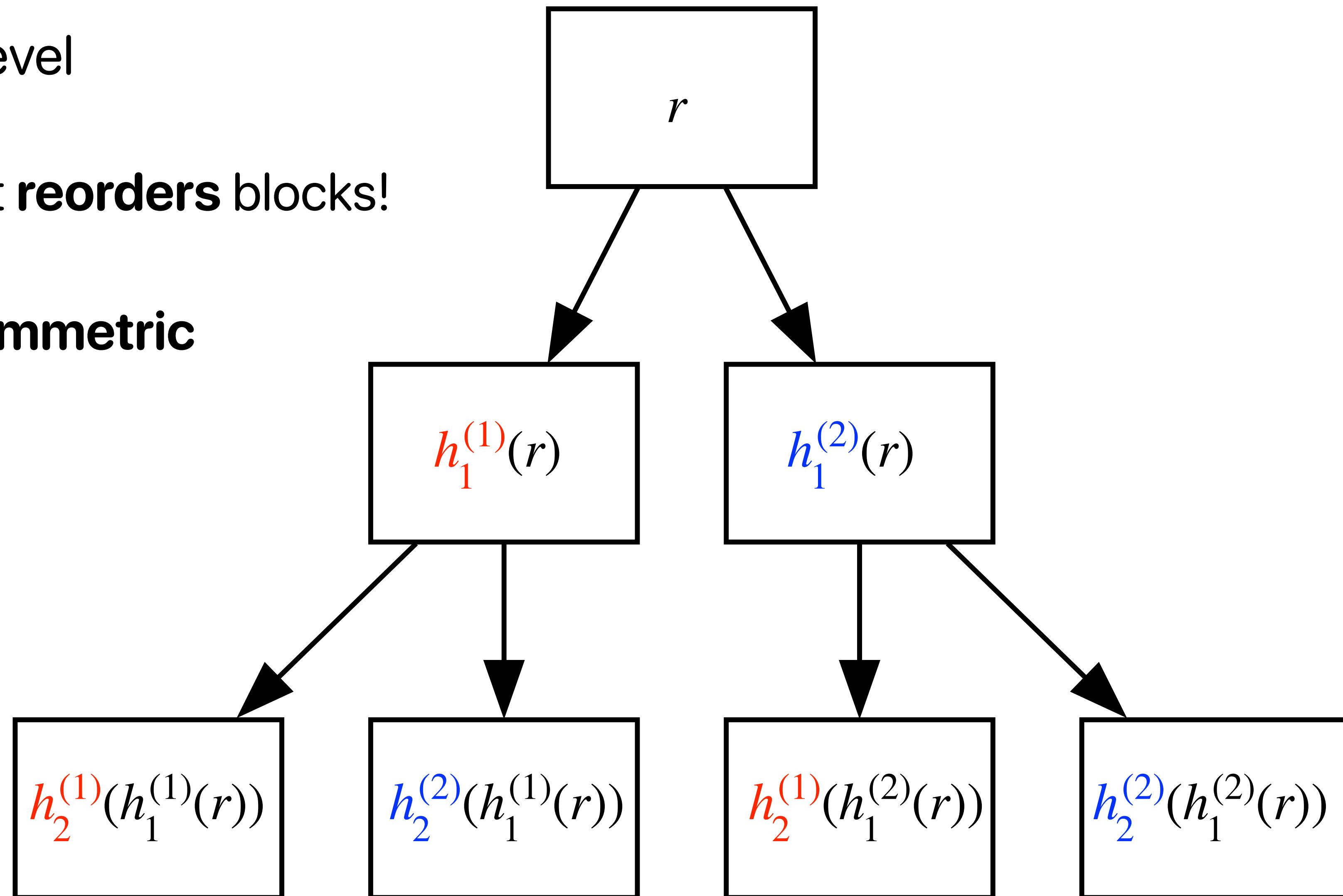
• Distribution of strings is symmetric

3

6

# HashPRG : Our Construction

- **Two** hash functions per level
- Switching  $h_1^{(1)}$  and  $h_1^{(2)}$  just **reorders** blocks!
- Distribution of strings is **symmetric**





# HashPRG