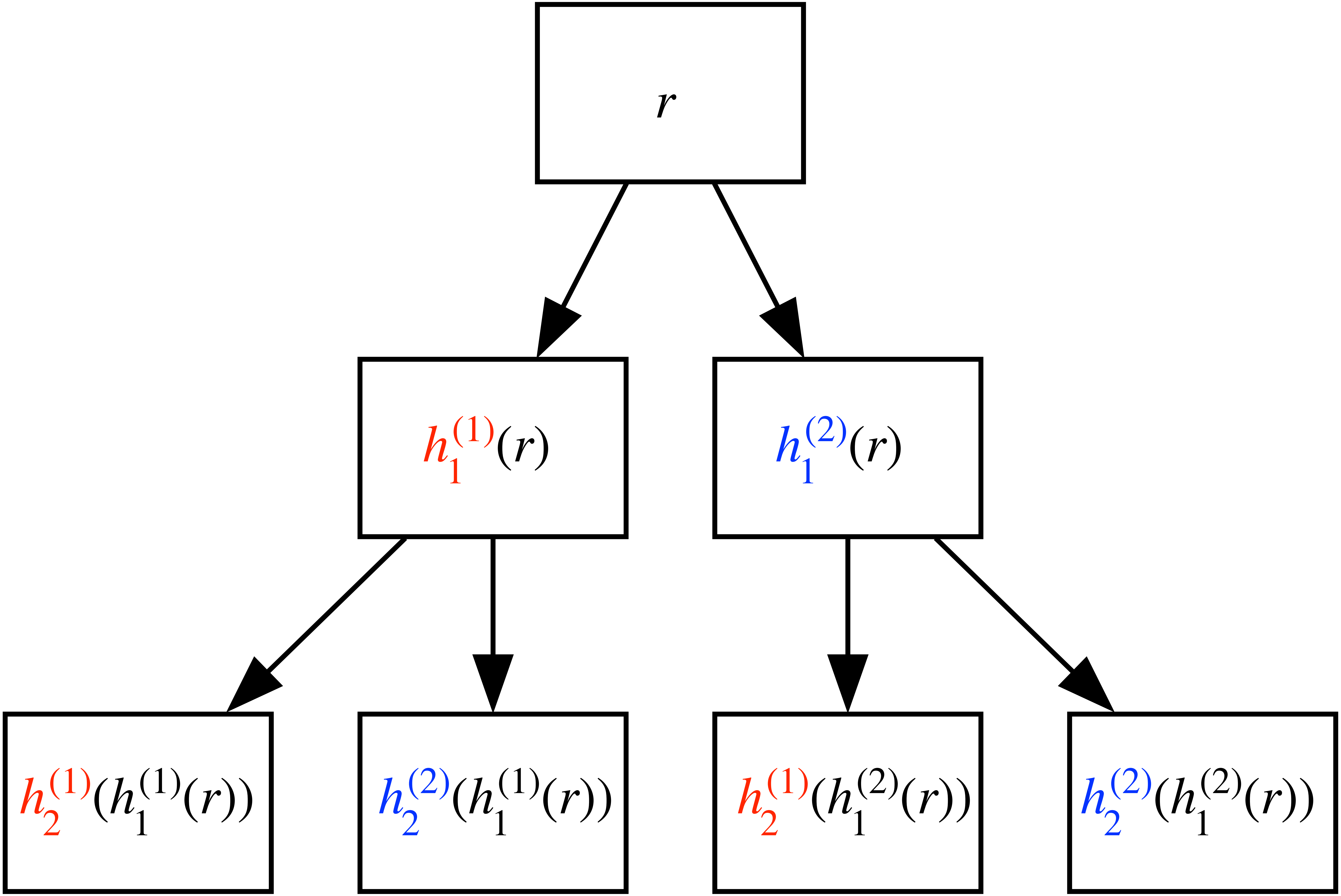

r
$h_1^{(1)}(r)$
$h_1^{(2)}(r)$
$h_2^{(1)}(h_1^{(1)}(r))$
$h_2^{(2)}(h_1^{(1)}(r))$
$h_2^{(1)}(h_1^{(2)}(r))$
$h_2^{(2)}(h_1^{(2)}(r))$

HashPRG : Our Construction

- **Two** hash functions per level

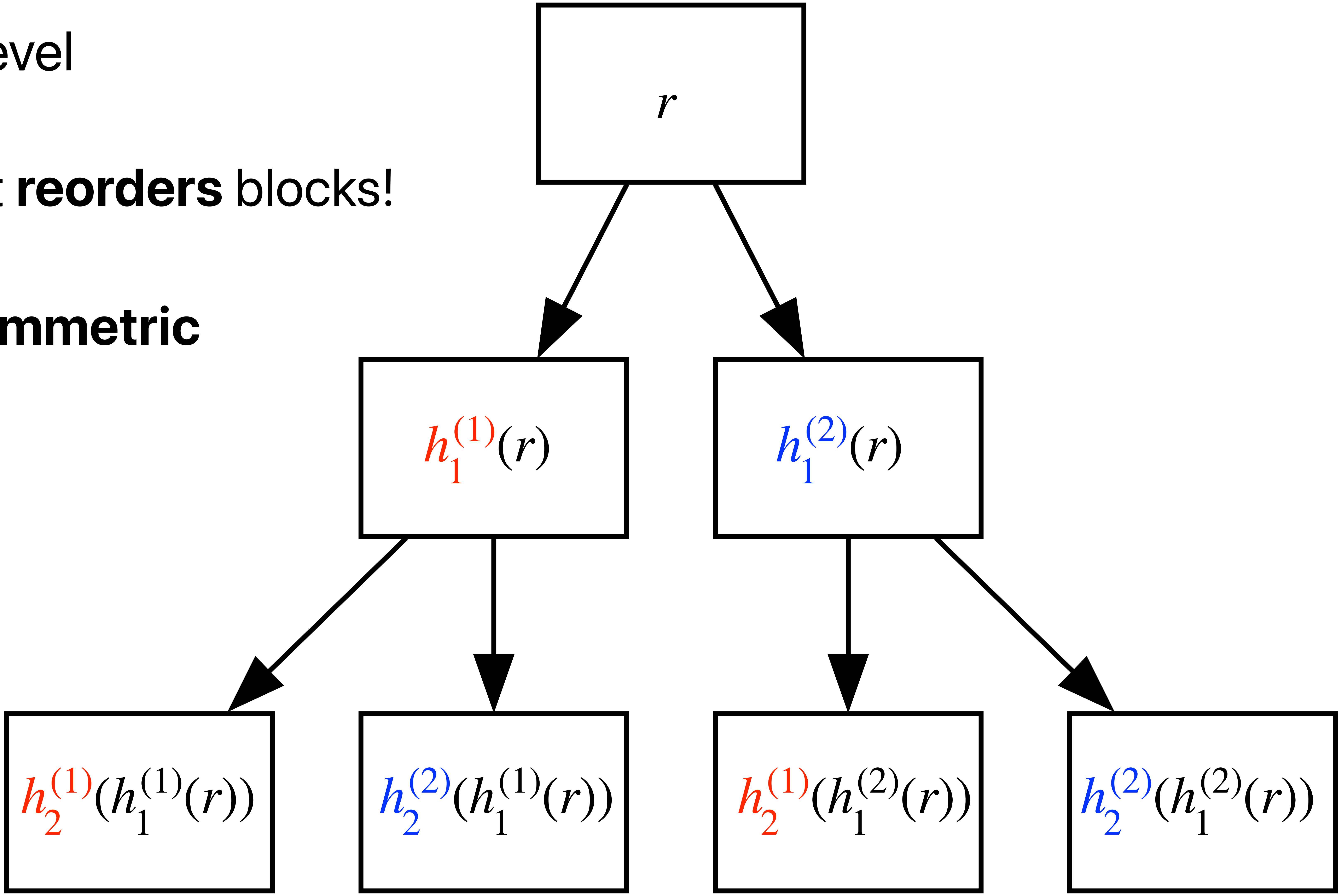
- Switching $h_1^{(1)}$ and $h_1^{(2)}$ just **reorders** blocks!

- Distribution of strings is **symmetric**

19

HashPRG : Our Construction

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


r
$h_1^{(1)}(r)$
$h_1^{(2)}(r)$
$h_2^{(1)}(h_1^{(1)}(r))$
$h_2^{(2)}(h_1^{(1)}(r))$
$h_2^{(1)}(h_1^{(2)}(r))$
$h_2^{(2)}(h_1^{(2)}(r))$

HashPRG