Communication-Rounds Tradeoffs for Common Randomness and Secret Key Generation

Mitali Bafna†, Badih Ghazi*, Noah Golowich†, and Madhu Sudan†

† Harvard University  * Google Research

January 8, 2019
Common Randomness Generation (CRG)

\[(X_i, Y_i) \sim \mu (\text{source}), \text{Alice} \leftarrow X_i, \text{Bob} \leftarrow Y_i.\]
Common Randomness Generation (CRG)

\((X_i, Y_i) \sim \mu (\text{source}),\) Alice \(\leftarrow X_i,\) Bob \(\leftarrow Y_i.\)

Several rounds of commun., starting w/ Alice:

- \(m_1 = m_1(\{X_i\});\)
- \(m_2 = m_2(m_1, \{Y_i\});\)
- \(m_3 = m_3(\{X_i\}, m_1, m_2), \ldots\)
Common Randomness Generation (CRG)

$(X_i, Y_i) \sim \mu \text{ (source)}, \text{ Alice } \leftarrow X_i, \text{ Bob } \leftarrow Y_i.$

Several rounds of commun., starting w/ Alice:

- $m_1 = m_1(\{X_i\});$
- $m_2 = m_2(m_1, \{Y_i\});$
- $m_3 = m_3(\{X_i\}, m_1, m_2), \ldots$

At end: Alice & Bob output $K_A, K_B$, resp., s.t.:

- $K_A = K_A(\{X_i\}, m_1, \ldots, m_r);$ 
- $K_B = K_B(\{Y_i\}, m_1, \ldots, m_r).$
(X_i, Y_i) \sim \mu \text{ (source)}, \text{ Alice } \leftarrow X_i, \text{ Bob } \leftarrow Y_i.
Several rounds of commun., starting w/ Alice:
- m_1 = m_1(\{X_i\});
- m_2 = m_2(m_1, \{Y_i\});
- m_3 = m_3(\{X_i\}, m_1, m_2), \ldots.

At end: Alice & Bob output K_A, K_B, resp., s.t.:
- K_A = K_A(\{X_i\}, m_1, \ldots, m_r);
- K_B = K_B(\{Y_i\}, m_1, \ldots, m_r).
- K_A = K_B \text{ w.h.p., and}
- K_A, K_B have large min-entropy.
Same as CRG, but key must be secure against eavesdropper Eve that watches the communication.
Secret Key Generation (SKG)

- Same as CRG, but key must be secure against eavesdropper Eve that watches the communication.
- **Question:** Are there sources $\mu$ such that having more rounds can lead to more efficient (i.e. lower communication) protocols for CRG or SKG?
Background: 1-Round & 2-Round Communication

- [Ahlswede & Csiszár, ’93 & ’98]: CRG and SKG for
  
  **1-round, 2-round protocols in amortized setting**: For $\epsilon \to 0$, characterize $(H, C)$ pairs s.t.
  
  - Samples: $(X^N, Y^N) \sim \mu^N$;
  - Communication: $(C + \epsilon) \cdot N$;
  - Entropy of key: $(H - \epsilon) \cdot N$. 

- [Guruswami & Radhakrishnan, ’16] & [Ghazi & Jayram, ’18]: non-amortized setting (our work): near-optimal tradeoff between communication, key length, & agreement probability for “simple” sources: BSC, BEC, BGS.
Background: 1-Round & 2-Round Communication

[Ahlswede & Csiszár, ’93 & ’98]: CRG and SKG for 1-round, 2-round protocols in amortized setting: For $\epsilon \to 0$, characterize $(H, C)$ pairs s.t.
- Samples: $(X^N, Y^N) \sim \mu^\otimes N$;
- Communication: $(C + \epsilon) \cdot N$;
- Entropy of key: $(H - \epsilon) \cdot N$.

[Guruswami & Radhakrishnan, ’16] & [Ghazi & Jayram, ’18]: non-amortized setting (our work): near-optimal tradeoff between communication, key length, & agreement probability for “simple” sources: BSC, BEC, BGS.
Background: Multi-Round Communication

- Generalization of Ahlswede & Csiszár characterization to *multi-round protocols* by [Tyagi, '13] & [Liu et al., '16].
- For binary channels, additional rounds **does not** help reduce communication.
- [Tyagi, '13]: ternary source s.t. 2-round protocols require less communication than 1-round protocols.
- Otherwise: no rounds vs. communication tradeoffs *(incl. in non-amortized case)!*
Formalizing Non-Amortized Setting

Definition \(((r, c)\text{-protocol})\)

\(\Pi\) is \((r, c)\text{-protocol}\) if:

- \(\leq r\) rounds (messages).
- \(\leq c\) bits total.

\(L\) represents number of bits of entropy in random keys:

Definition \((L\text{-CRG})\)

\(\Pi\) gives \(L\text{-CRG}\) if Alice, Bob, given samples \((X_1, Y_1), \ldots, (X_T, Y_T)\) \(\sim \mu \otimes T\), output \(K_A, K_B\), s.t.:

\[
\min\{H_\infty(K_A), H_\infty(K_B)\} \geq L.
\]

\[
\Pr[K_A = K_B] \geq 1 - \epsilon.
\]
Formalizing Non-Amortized Setting

Definition \(((r, c)\text{-protocol})\)

\(\Pi\) is \((r, c)\text{-protocol}\) if:
- \(\leq r\) rounds (messages).
- \(\leq c\) bits total.

\(L\) represents number of bits of entropy in random keys:

Definition \((L\text{-CRG})\)

\(\Pi\) gives \(L\text{-CRG}\) if Alice, Bob, given samples \((X_1, Y_1), \ldots, (X_T, Y_T) \sim \mu \otimes T\), output \(K_A, K_B\), s.t.:
- \(\min\{H_\infty(K_A), H_\infty(K_B)\} \geq L\).
- \(\Pr[K_A = K_B] \geq 1 - \epsilon\).
Question: \(\forall \delta > 0, r, L, \exists \mu \text{ s.t.}

- \exists (r, \delta L)\)-protocol for \(L\)-CRG from \(\mu\);
- No \((r - 1, (1 - \delta)L)\)-protocol for \(L\)-CRG from \(\mu\)?
Question: $\forall \delta > 0, r, L, \exists \mu$ s.t.
- $\exists (r, \delta L)$-protocol for $L$-CRG from $\mu$;
- No $(r - 1, (1 - \delta)L)$-protocol for $L$-CRG from $\mu$?

Theorem (BGGS, '19)

$\forall n, r, L$ construct $\mu_{r,n,L}$ s.t.
- $\exists (r + 1, O(r \log n))$-protocol for $L$-CRG from $\mu_{r,n,L}$;
- No $\left(\frac{r}{2} - 2, \min \left\{ o(L), \frac{n}{\text{poly} \log(n)} \right\} \right)$-protocol for $L$-CRG from $\mu_{r,n,L}$. 
**r vs. r/2 gap**

**Question:** \( \forall \delta > 0, r, L, \exists \mu \text{ s.t.} \)
- \( \exists (r, \delta L)\)-protocol for \( L \)-CRG from \( \mu \);
- No \( (r - 1, (1 - \delta)L)\)-protocol for \( L \)-CRG from \( \mu \)?

**Theorem (BGGS, ’19)**

\( \forall n, r, L \) construct \( \mu_{r,n,L} \) s.t.
- \( \exists (r + 1, O(r \log n))\)-protocol for \( L \)-CRG from \( \mu_{r,n,L} \);
- No \( \left( \frac{r}{2} - 2, \min \left\{ o(L), \frac{n}{\text{poly log}(n)} \right\} \right)\)-protocol for \( L \)-CRG from \( \mu_{r,n,L} \).

Also: same theorem for \( L \)-SKG!
Alice's inputs =
\((\pi_1, \pi_3, \ldots, A_1, \ldots, A_n)\)

Bob's inputs =
\((i_0, \pi_2, \pi_4, \ldots, B_1, \ldots, B_n)\)
Pointer-chasing source for CRG: $\mu_{r,n,L}$

$\pi_1, \ldots, \pi_r \sim S_n$

$A_1, \ldots, A_n \sim \{0,1\}^{L}$

$B_1, \ldots, B_n \sim \{0,1\}^{L}$

$i_{j+1} = \pi_{j+1}(i_j)$.  

$i_j = \text{“pointers”}$

Alice's inputs =  
$$(\pi_1, \pi_3, \ldots, A_1, \ldots, A_n)$$

Bob's inputs =  
$$(i_0, \pi_2, \pi_4, \ldots, B_1, \ldots, B_n)$$
Pointer-chasing source for CRG: $\mu_{r,n,L}$

Bob's inputs = $(i_0, \pi_2, \pi_4, \ldots, B_1, \ldots, B_n)$

Alice's inputs = $(\pi_1, \pi_3, \ldots, A_1, \ldots, A_n)$

Where $A_i = B_i$, $i_{j+1} = \pi_{j+1}(i_j)$.

$i_j = \text{“pointers”}$

$i_0 \sim [n]$

$\pi_1, \ldots, \pi_r \sim S_n$

$A_1, \ldots, A_n \sim \{0,1\}^L$

$B_1, \ldots, B_n \sim \{0,1\}^L$
Background: Standard Pointer Chasing Problem

[Duris et al., ’84] & [Nisan & Wigderson, ’93], etc.:
Upper/lower bounds for CRG from $\mu_{r,n,L}$

- **Upper bound**: follow pointers: $(r + 1)$ rounds, communication $(r + 1) \lceil \log n \rceil$.

Alice's inputs = $(\pi_1, \pi_3, ..., A_1, ..., A_n)$
Bob's inputs = $(i, \pi_2, \pi_4, ..., B_1, ..., B_n)$
Upper/lower bounds for CRG from $\mu_{r,n,L}$

- **Upper bound**: follow pointers: $(r + 1)$ rounds, communication $(r + 1)[\log n]$.

- **Lower bound for protocols w/ $\leq r$ rounds**:  
  - [Duris et al., ’84] & [Nisan & Wigderson, ’93], etc.: Pointer chasing is hard (for det. & rand. protocols).
Upper/lower bounds for CRG from $\mu_{r,n,L}$

- **Upper bound**: follow pointers: $(r + 1)$ rounds, communication $(r + 1)[\log n]$.

- **Lower bound for protocols w/ $\leq r$ rounds**:
  - [Duris et al., ’84] & [Nisan & Wigderson, ’93], etc.: Pointer chasing is hard (for det. & rand. protocols).
  - **Problem**: don’t have to solve pointer chasing for $L$-CRG!
  - “Guess” index $j$ such that $A_j = B_j \Rightarrow \lceil \log n \rceil$-bit non-deterministic protocol!
Upper/lower bounds for CRG from $\mu_{r,n,L}$

**Upper bound:** follow pointers: $(r + 1)$ rounds, communication $(r + 1)\lceil \log n \rceil$.

**Lower bound for protocols w/ $\leq r$ rounds:**

- [Duris et al., ’84] & [Nisan & Wigderson, ’93], etc.: Pointer chasing is hard (for det. & rand. protocols).
- **Problem:** don’t have to solve pointer chasing for $L$-CRG!
- “Guess” index $j$ such that $A_j = B_j \Rightarrow \lceil \log n \rceil$-bit non-deterministic protocol!
- Modular solution?
Reduction 1: Indistinguishability

- Marginals of $\mu_{r,n,L}$: $X = (\pi_1, \pi_3, \ldots, \pi_r, A_1, \ldots, A_n)$, $Y = (i_0, \pi_2, \ldots, \pi_{r-1}, B_1, \ldots, B_n)$.
- $\Pi$ distinguishes $\mu, \nu$ if $\text{TVD}(\Pi_{\mu}, \Pi_{\nu}) \geq \text{const}$.
Reduction 1: Indistinguishability

- Marginals of $\mu_{r,n,L}$: $X = (\pi_1, \pi_3, \ldots, \pi_r, A_1, \ldots, A_n)$, $Y = (i_0, \pi_2, \ldots, \pi_{r-1}, B_1, \ldots, B_n)$.
- $\Pi$ distinguishes $\mu, \nu$ if $\text{TVD}(\Pi_\mu, \Pi_\nu) \geq \text{const}$. 

Claim

Suppose $c \ll L$. If $\exists (r/2 - 2, c)$ protocol for L-CRG from $\mu = \mu_{r,n,L}$, then $\mu \& \mu_X \times \mu_Y$ are distinguishable by $(r/2 - 1)$-round protocol w/ communication $c + O(1)$. 

Idea of proof:

L-CRG is impossible with communication $\ll L$ when parties have indep. inputs (e.g., [Cannone et al., '17]).
Reduction 1: Indistinguishability

- Marginals of $\mu_{r,n,L}$: $X = (\pi_1, \pi_3, \ldots, \pi_r, A_1, \ldots, A_n)$, $Y = (i_0, \pi_2, \ldots, \pi_{r-1}, B_1, \ldots, B_n)$.
- $\Pi$ distinguishes $\mu, \nu$ if $\text{TVD}(\Pi_\mu, \Pi_\nu) \geq \text{const}$.

Claim

Suppose $c \ll L$. If $\exists (r/2 - 2, c)$ protocol for $L$-CRG from $\mu = \mu_{r,n,L}$, then $\mu \& \mu_X \times \mu_Y$ are distinguishable by $(r/2 - 1)$-round protocol w/ communication $c + O(1)$.

Idea of proof: $L$-CRG is impossible with communication $\ll L$ when parties have indep. inputs (e.g., [Cannone et al., '17]).
Overview of Reductions

Reduction 1

\[(r/2 - 2, \min\{o(L), o(n)\})\)-protocol for \(L\)-CRG from \(\mu\)

Reduction 2

\(\mu, \mu_x \times \mu_y\) distinguishable by 
\((r/2 - 1, o(n))\)-protocol

\(\text{PV}_{YES}, \text{PV}_{NO}\) distinguishable by 
\((r/2 - 1, o(n))\)-protocol

Ultimate goal: prove indistinguishability of \(\text{PV}_{YES}, \text{PV}_{NO}\)

Diagram:

- \(\text{PV}_{YES}\):
  - \(\pi_1\)
  - \(\pi_2\)
  - \(\pi_3\)
  - \(\cdots\)
  - \(\pi_{r-1}\)
  - \(\pi_r\)
  - \(i_0\)

- \(\text{PV}_{NO}\):
  - \(\pi_1\)
  - \(\pi_2\)
  - \(\pi_3\)
  - \(\cdots\)
  - \(\pi_{r-1}\)
  - \(\pi_r\)
  - \(i_0\)
Reduction 2: Pointer Verification

- $\text{PV}_{\text{YES}}(r, n), \text{PV}_{\text{NO}}(r, n)$ distributions on $(\tilde{X}, \tilde{Y})$:
  \[ \tilde{X} = (\pi_1, \pi_3, \ldots, \pi_r), \quad \tilde{Y} = (i_0, j_0, \pi_2, \pi_4, \ldots, \pi_{r-1}) \]
Reduction 2: Pointer Verification

- $\text{PV}_{\text{YES}}(r, n), \text{PV}_{\text{NO}}(r, n)$ distributions on $(\tilde{X}, \tilde{Y})$: 
  $\tilde{X} = (\pi_1, \pi_3, \ldots, \pi_r), \tilde{Y} = (i_0, j_0, \pi_2, \pi_4, \ldots, \pi_{r-1})$:

\[
\text{PV}_{\text{YES}}: \quad j_0 = \pi_r \circ \cdots \circ \pi_1(i_0).
\]

\[
\text{PV}_{\text{NO}}: \quad j_0 \text{ random.}
\]
Reduction 2: Pointer Verification

- $PV_{YES}(r, n), PV_{NO}(r, n)$ distributions on $(\tilde{X}, \tilde{Y})$: $\tilde{X} = (\pi_1, \pi_3, \ldots, \pi_r)$, $\tilde{Y} = (i_0, j_0, \pi_2, \pi_4, \ldots, \pi_{r-1})$:

  - $PV_{YES}$: $j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)$.

  - $PV_{NO}$: $j_0$ random.

  - Protocol distinguishing $\mu = \mu_{r, n, L}$ & $\mu_X \times \mu_Y$ gives protocol distinguishing $PV_{YES}$ & $PV_{NO}$
Reduction 2: Pointer Verification

- $\text{PV}_{\text{YES}}(r, n), \text{PV}_{\text{NO}}(r, n)$ distributions on $(\tilde{X}, \tilde{Y})$: 
  $\tilde{X} = (\pi_1, \pi_3, \ldots, \pi_r)$, $\tilde{Y} = (i_0, j_0, \pi_2, \pi_4, \ldots, \pi_{r-1})$:

  $\text{PV}_{\text{YES}}$: $j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)$.

  $\text{PV}_{\text{NO}}$: $j_0$ random.

- Protocol distinguishing $\mu = \mu_{r, n, L}$ & $\mu_X \times \mu_Y$ gives protocol distinguishing $\text{PV}_{\text{YES}}$ & $\text{PV}_{\text{NO}}$ (using $\Omega(n)$ disjointness lower bound).
Overview of Reductions

\((r/2 - 2, \min\{o(L), o(n)\})\)-protocol for \(L\)-CRG from \(\mu\)

\(\mu, \mu_x \times \mu_y\) distinguishable by \((r/2 - 1, o(n))\)-protocol

\(PV_{YES}, PV_{NO}\) distinguishable by \((r/2 - 1, o(n))\)-protocol

Ultimate goal: prove indistinguishability of \(PV_{YES}, PV_{NO}\)
Indistinguishability of \( PV_{\text{YES}}, PV_{\text{NO}} \)

\( r, n \) implicit: \( PV_{\text{YES}} = PV_{\text{YES}}(n, r), \ PV_{\text{NO}} = PV_{\text{NO}}(n, r) \):

Theorem (BGGS, ’19)

\( \forall r, n, PV_{\text{NO}} \& PV_{\text{YES}} \ are \ \left( \frac{r-1}{2}, \frac{n}{\text{poly log}(n)} \right)\)-indisting.
Indistinguishability of $PV_{\text{YES}}, PV_{\text{NO}}$

$r, n$ implicit: $PV_{\text{YES}} = PV_{\text{YES}}(n, r), PV_{\text{NO}} = PV_{\text{NO}}(n, r)$:

**Theorem (BGGS, ’19)**

$\forall r, n, PV_{\text{NO}} \& PV_{\text{YES}}$ are $\left(\frac{r-1}{2}, \frac{n}{\text{poly log}(n)}\right)$-indisting.

- Why only $\frac{r-1}{2}$ rounds?
Indistinguishability of $\text{PV}_{\text{YES}}$, $\text{PV}_{\text{NO}}$

$r, n$ implicit: $\text{PV}_{\text{YES}} = \text{PV}_{\text{YES}}(n, r)$, $\text{PV}_{\text{NO}} = \text{PV}_{\text{NO}}(n, r)$:

Theorem (BGGS, ’19)

$\forall r, n, \text{PV}_{\text{NO}} \& \text{PV}_{\text{YES}}$ are $\left(\frac{r-1}{2}, \frac{n}{\text{poly log}(n)}\right)$-indisting.

Why only $\frac{r-1}{2}$ rounds? $\exists \left(\frac{r+1}{2}, O(r \log n)\right)$-protocol:

$\text{PV}_{\text{NO}}$:

$\text{PV}_{\text{YES}}$: 
Proof of indist. of $PV_{\text{YES}}$ & $PV_{\text{NO}}$

- Idea: “round elimination” ([Nisan & Wigderson, '93]).
- Dealing with non-independence of inputs under $PV_{\text{YES}}$ makes proof more difficult.\textsuperscript{1}

\textsuperscript{1}Technically under $\frac{1}{2}(PV_{\text{YES}} + PV_{\text{NO}})$. 
Proof of indist. of $PV_{YES}$ & $PV_{NO}$

- Idea: “round elimination” ([Nisan & Wigderson, ’93]).
- Dealing with non-independence of inputs under $PV_{YES}$ makes proof more difficult.\(^1\)
- Idea: “peel” off 2 permutations (1 round) at a time, maintaining invariants:
  - $H(\pi_1, \ldots, \pi_r | \text{transcript}) \geq r \log(n!) - O(c)$.
  - $H(i_0 | \pi_1, \ldots, \pi_r, \text{transcript}) \geq \log(n) - o(1)$.
  - $H(j_0 | \pi_1, \ldots, \pi_r, \text{transcript}) \geq \log(n) - o(1)$.
  - $H(\mathbb{1}[\pi_r \circ \cdots \circ \pi_1(i_0) = j_0] | i_0, \pi_1, \ldots, \pi_r, \text{transcript}) \geq 1 - o(1)$.
  - Few others...

\(^1\)Technically under $\frac{1}{2}(PV_{YES} + PV_{NO})$. 
Conclusion

- First round/communication tradeoffs for CRG & SKG for $r > 2$ rounds.
- Explicitly constructed source $\mu = \mu_{r,n,L}$ s.t.:
  - $\exists$ efficient (i.e. $O(r \log n)$ communication) $(r + 1)$-round protocol for $L$-CRG/SKG
  - Any $(r/2 - 2)$-round protocol for $L$-CRG/SKG has communication $\tilde{\Omega}(\min\{L, n\})$.  

Open questions:
- Improve $(r + 1)$-vs-$(r/2 - 2)$ tradeoff to $(r + 1)$-vs-$r$ for $\mu_{r,n,L}$?
- Extend analysis to amortized case?
Conclusion

- First round/communication tradeoffs for CRG & SKG for \( r > 2 \) rounds.
- Explicitly constructed source \( \mu = \mu_{r,n,L} \) s.t.:
  - \( \exists \) efficient (i.e. \( O(r \log n) \) communication) \((r + 1)\)-round protocol for \( L \)-CRG/SKG
  - Any \((r/2 - 2)\)-round protocol for \( L \)-CRG/SKG has communication \( \tilde{\Omega}(\min\{L, n\}) \).
- Open questions:
  - Improve \((r + 1)\)-vs-\((r/2 - 2)\) tradeoff to \((r + 1)\)-vs-\( r \) for \( \mu_{r,n,L} \)?
  - Extend analysis to amortized case?
I am grateful to the NSF for a SODA travel grant.

Thank you!
Overall goal: $\mu \land \mu_X \times \mu_Y$ are indistinguishable to $(r', c)$-protocols.

Intermediate distr. $\mu_{\text{mid}}$:

- $A_j = B_j$ for random $j$.
- I.e., $j$ is independent of $\pi_r \circ \cdots \circ \pi_1(i_0)$.

Alice's inputs = $(\pi_1, \pi_3, \ldots, A_1, \ldots, A_n)$

Bob's inputs = $(i, \pi_2, \pi_4, \ldots, B_1, \ldots, B_n)$
Proof Outline of Reduction 2

Intermediate distr. $\mu_{\text{mid}}$:

- $A_j = B_j$ for random $j$.
- I.e., $j$ is independent of $\pi_r \circ \cdots \circ \pi_1(i_0)$.

- $\mu_X \times \mu_Y \overset{\text{indist. from}}{\rightarrow} \mu_{\text{mid}}$ to protocols w/ communication $o(n)$ (set disjointness hard).

\[ \begin{array}{c}
A_1 \ A_2 \ A_3 \ \cdots \ A_j \ \cdots \ A_n \\
\downarrow \quad \downarrow \\
\pi_r \\
\vdots \\
\pi_r \\
B_1 \ B_2 \ B_3 \ \cdots \ B_j \ \cdots \ B_n \\
\end{array} \]

Alice's inputs = $(\pi_1, \pi_3, \ldots, A_1, \ldots, A_n)$

Bob's inputs = $(i, \pi_2, \pi_4, \ldots, B_1, \ldots, B_n)$
Proof Outline of Reduction 2

Intermediate distr. $\mu_{\text{mid}}$:

- $A_j = B_j$ for random $j$.
- I.e., $j$ is independent of $\pi_r \circ \cdots \circ \pi_1(i_0)$.

- $\mu_X \times \mu_Y \text{ indist. from } \mu_{\text{mid}} \text{ to protocols w/ communication } o(n)$ (set disjointness hard).

- $\text{PV}_{\text{YES}}$ & $\text{PV}_{\text{NO}}$ indist. to $(r', c)$-protocols
  $\Rightarrow \mu \text{ indist. from } \mu_{\text{mid}} \text{ to } (r', c)$-protocols.
Proof of indisting. of $\mathcal{PV}_{\text{YES}} & \mathcal{PV}_{\text{NO}}$

- Idea: “round elimination” ([Nisan & Wigderson, ’93]).
- “Problem” 1: Want to work with a functional problem.

Solution 1:

$$\Pi \text{ disting. } \mathcal{PV}_{\text{YES}} & \mathcal{PV}_{\text{NO}}$$

$$\Leftrightarrow \Pi \text{ outputs } \mathbb{1}[j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)] \text{ whp}$$
under $\mathcal{PV}_{\text{MIX}} = \frac{1}{2}(\mathcal{PV}_{\text{YES}} + \mathcal{PV}_{\text{NO}})$. 
Proof of indisting. of $\text{PV}_{\text{YES}} \& \text{PV}_{\text{NO}}$

- Idea: “round elimination” ([Nisan & Wigderson, '93]).
- “Problem” 1: Want to work with a functional problem.
- Solution 1:
  \[\Pi \text{ disting. } \text{PV}_{\text{YES}} \& \text{PV}_{\text{NO}}\]
  \[\iff \Pi \text{ outputs } 1[j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)] \text{ whp under } \text{PV}_{\text{MIX}} = \frac{1}{2}(\text{PV}_{\text{YES}} + \text{PV}_{\text{NO}}).\]

- “Problem” 2: Players’ inputs under $\text{PV}_{\text{MIX}}$ aren’t independent.