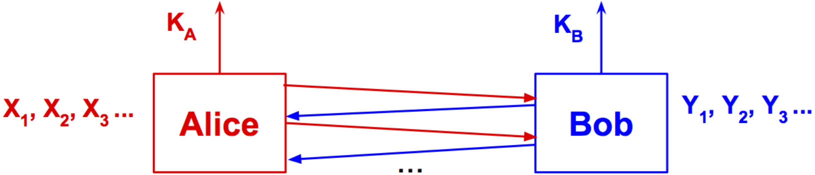
Communication-Rounds Tradeoffs for Common Randomness and Secret Key Generation

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

† Harvard University   * Google Research

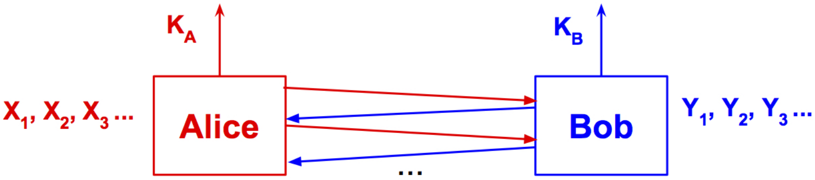
January 8, 2019

Common Randomness Generation (CRG)



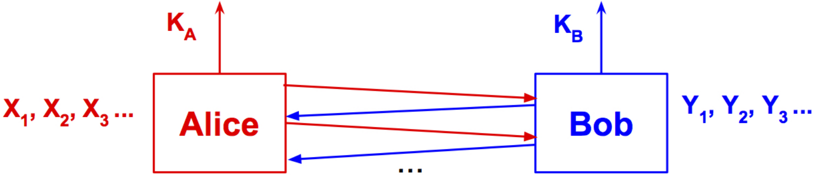
- $(X_i, Y_i) \sim \mu$ (**source**), Alice $\leftarrow X_i$, Bob $\leftarrow Y_i$.

Common Randomness Generation (CRG)



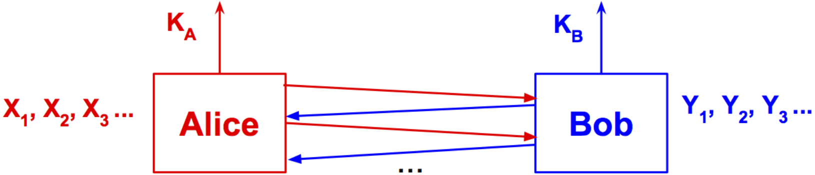
- $(X_i, Y_i) \sim \mu$ (**source**), Alice $\leftarrow X_i$, Bob $\leftarrow Y_i$.
- Several **rounds** of commun., starting w/ Alice:
  - $m_1 = m_1(\{X_i\})$;
  - $m_2 = m_2(m_1, \{Y_i\})$;
  - $m_3 = m_3(\{X_i\}, m_1, m_2), \ldots$.

Common Randomness Generation (CRG)



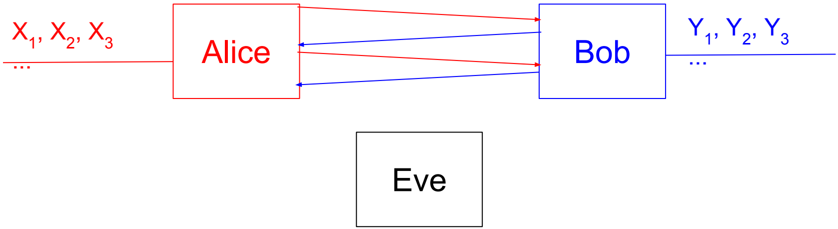
- $(X_i, Y_i) \sim \mu$ (**source**), Alice $\leftarrow X_i$, Bob $\leftarrow Y_i$.
- Several **rounds** of commun., starting w/ Alice:
  - $m_1 = m_1(\{X_i\})$;
  - $m_2 = m_2(m_1, \{Y_i\})$;
  - $m_3 = m_3(\{X_i\}, m_1, m_2), \ldots$.
- At end: Alice & Bob output K_A, K_B, resp., s.t.:
  - $K_A = K_A(\{X_i\}, m_1, \ldots, m_r)$;
    $K_B = K_B(\{Y_i\}, m_1, \ldots, m_r)$.

Common Randomness Generation (CRG)



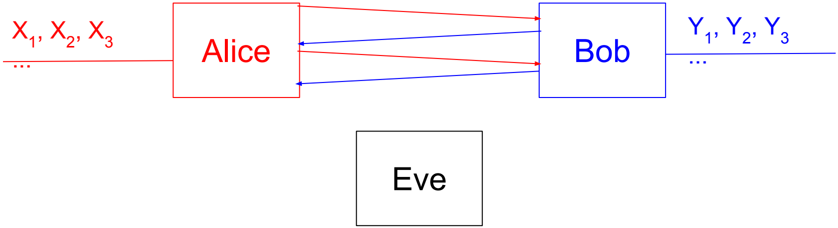
- $(X_i, Y_i) \sim \mu$ (**source**), Alice $\leftarrow X_i$, Bob $\leftarrow Y_i$.
- Several **rounds** of commun., starting w/ Alice:
  - $m_1 = m_1(\{X_i\})$;
  - $m_2 = m_2(m_1, \{Y_i\})$;
  - $m_3 = m_3(\{X_i\}, m_1, m_2), \ldots$.
- At end: Alice & Bob output K_A, K_B, resp., s.t.:
  - $K_A = K_A(\{X_i\}, m_1, \ldots, m_r)$; $K_B = K_B(\{Y_i\}, m_1, \ldots, m_r)$.
  - $K_A = K_B$ w.h.p., and
  - K_A, K_B have large min-entropy.

Secret Key Generation (SKG)



- 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 μ 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: $(X^N, Y^N) \sim \mu^{\otimes N}$;
  - Communication: $(C + \epsilon) \cdot N$;
  - Entropy of key: $(H - \epsilon) \cdot N$.

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

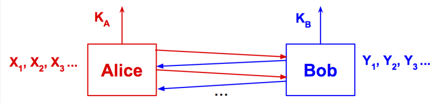
- Generalization of Ahlswede & Csiszár characterization to *multi-round protocols* by [Tyagi, '13] & [Liu et al., '16].
- For binary channels, additional rounds **does not** help reduce communication.
- [Tyagi, '13]: ternary source s.t. 2-round protocols require less communication than 1-round protocols.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

Formalizing Non-Amortized Setting

Definition ((r, c)-protocol)

Π is (r, c)-**protocol** if:

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

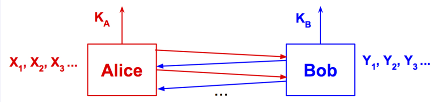


Formalizing Non-Amortized Setting

Definition ((r, c)-protocol)

Π is (r, c)-**protocol** if:

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



L represents number of bits of entropy in random keys:

Definition (L-CRG)

Π gives L-**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.:

- $\min\{H_\infty(K_A), H_\infty(K_B)\} \geq L$.
- $\Pr[K_A = K_B] \geq 1 - \epsilon$.

r vs. $r/2$ gap

Question: $\forall \delta > 0, r, L,$ $\exists \mu$ **s.t.**

- $\exists(r, \delta L)$-**protocol for** L-**CRG from** μ;
- **No** $(r-1, (1-\delta)L)$-**protocol for** L-**CRG from** μ?

r vs. $r/2$ gap

Question: $\forall \delta > 0, r, L$, $\exists \mu$ **s.t.**

- $\exists(r, \delta L)$**-protocol for** L**-CRG from** μ**;**
- **No** $(r-1, (1-\delta)L)$**-protocol for** L**-CRG from** μ**?**

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* $\left(\frac{r}{2}-2, \min\left\{o(L), \frac{n}{\operatorname{poly}\log(n)}\right\}\right)$*-protocol for L-CRG from* $\mu_{r,n,L}$.

r vs. $r/2$ gap

Question: $\forall \delta > 0, r, L$, $\exists \mu$ **s.t.**

- $\exists(r, \delta L)$**-protocol for** L**-CRG from** μ**;**
- **No** $(r-1, (1-\delta)L)$**-protocol for** L**-CRG from** μ**?**

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 $\left(\frac{r}{2} - 2, \min\left\{o(L), \frac{n}{\mathrm{poly}\log(n)}\right\}\right)$-protocol for L-CRG from $\mu_{r,n,L}$.*

Also: same theorem for L-SKG!

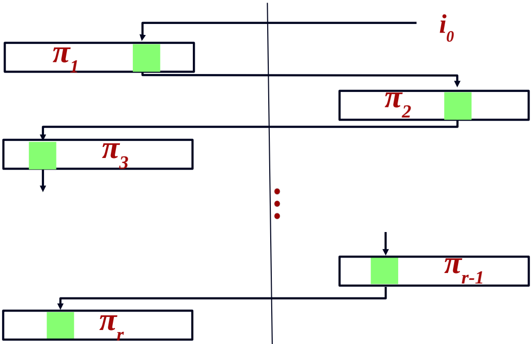
Pointer-chasing source for CRG: $\mu_{r,n,L}$

$i_0 \sim [n]$
$\pi_1, .., \pi_r \sim S_n$
$A_1, \ldots, A_n \sim \{0,1\}^L$
$B_1, \ldots, B_n \sim \{0,1\}^L$

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: $\mu_{r,n,L}$



$i_0 \sim [n]$

$\pi_1, .., \pi_r \sim S_n$

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

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

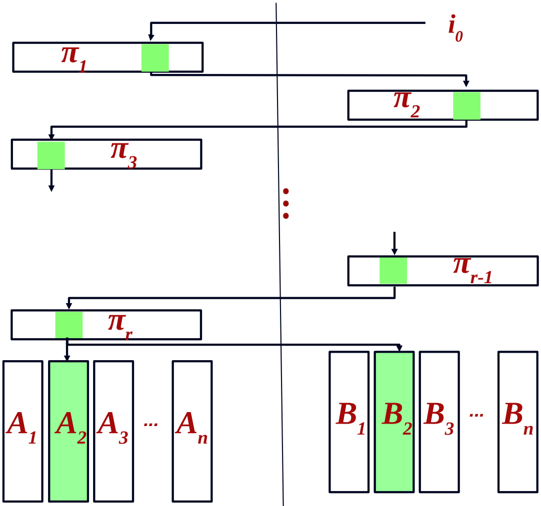
$i_{j+1} = \pi_{j+1}(i_j)$.

i_j = "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: $\mu_{r,n,L}$



$i_0 \sim [n]$
$\pi_1, .., \pi_r \sim S_n$
$A_1, \dots, A_n \sim \{0,1\}^L$
$B_1, \dots, B_n \sim \{0,1\}^L$
Where $A_{i_r} = B_{i_r}$,
$i_{j+1} = \pi_{j+1}(i_j)$.

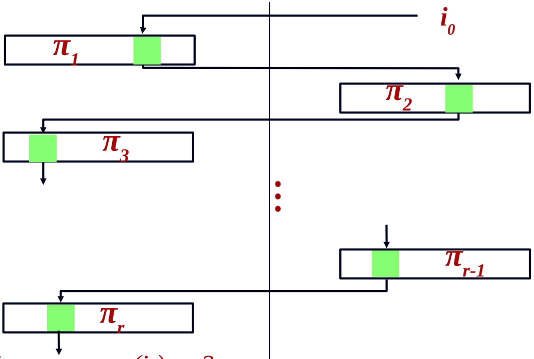
i_j = **"pointers"**

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

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

Background: Standard Pointer Chasing Problem

[Duris et al., '84] & [Nisan & Wigderson, '93], etc.:



$i_r = \pi_r \circ \ldots \circ \pi_1(i_0) = \ ?$

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

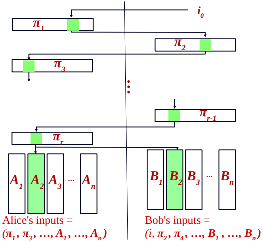
Bob's inputs = $(i_0, \pi_2, \pi_4, \ldots, \pi_{r-1})$

$i_0 \sim [n]$

$\pi_1, .., \pi_r \sim S_n$

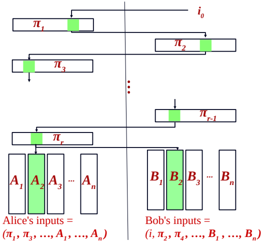
Upper/lower bounds for CRG from $\mu_{r,n,L}$

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



Upper/lower bounds for CRG from $\mu_{r,n,L}$

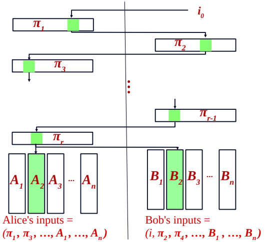
- *Upper bound*: follow pointers:
  $(r+1)$ *rounds*,
  communication $(r+1)\lceil \log n \rceil$.



- *Lower bound for protocols w/ $\leq r$ rounds*:
  - [Duris et al., '84] & [Nisan & Wigderson, '93], etc.: Pointer chasing is hard (for det. & rand. protocols).

Upper/lower bounds for CRG from $\mu_{r,n,L}$

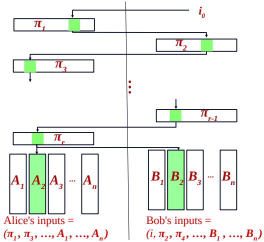
- *Upper bound*: follow pointers: $(r+1)$ *rounds*, communication $(r+1)\lceil \log n \rceil$.



- *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!

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 $\mu_{r,n,L}$: $X = (\pi_1, \pi_3, \ldots, \pi_r, A_1, \ldots, A_n)$, $Y = (i_0, \pi_2, \ldots, \pi_{r-1}, B_1, \ldots, B_n)$.
- Π *distinguishes* μ, ν if $\mathrm{TVD}(\Pi_\mu, \Pi_\nu) \geq \mathit{const}$.

Reduction 1: Indistinguishability

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

Claim

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

Reduction 1: Indistinguishability

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

Claim

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

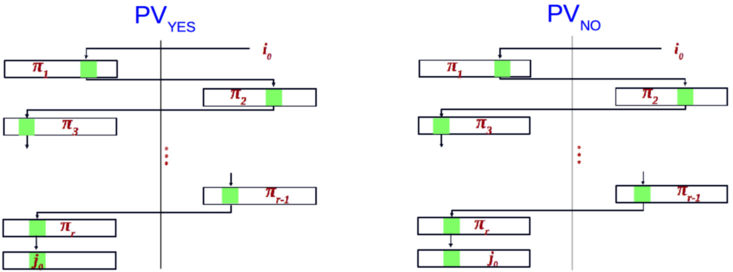
Idea of proof: L-CRG is impossible with communication $\ll L$ when parties have indep. inputs (e.g., [Cannone et al., '17]).

Overview of Reductions

$(r/2-2, \min\{o(L), o(n)\})$-protocol for L-CRG from μ → μ, $\mu_X \times \mu_Y$ distinguishable by $(r/2-1, o(n))$-protocol → PV_{YES}, PV_{NO} distinguishable by $(r/2-1, o(n))$-protocol

Reduction 1 *Reduction 2*

Ultimate goal: prove indistinguishability of PV_{YES}, PV_{NO}



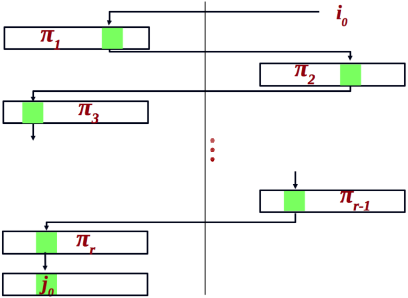
Reduction 2: Pointer Verification

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

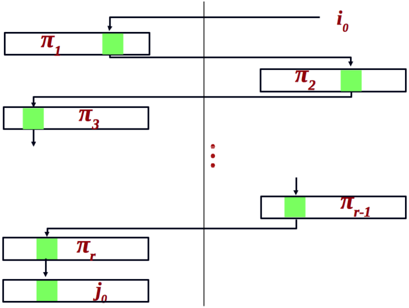
Reduction 2: Pointer Verification

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

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



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

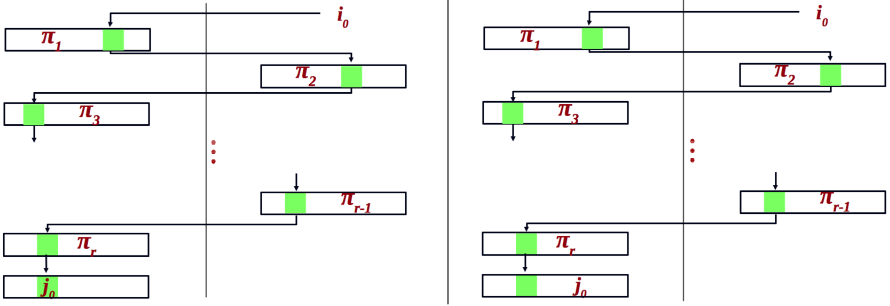


Reduction 2: Pointer Verification

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

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

$\mathrm{PV_{NO}}$: j_0 random.

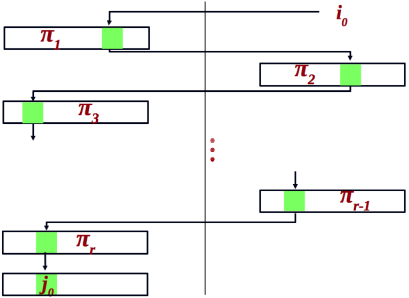


- **Protocol distinguishing $\mu = \mu_{r,n,L}$ & $\mu_X \times \mu_Y$ gives protocol distinguishing $\mathrm{PV_{YES}}$ & $\mathrm{PV_{NO}}$**

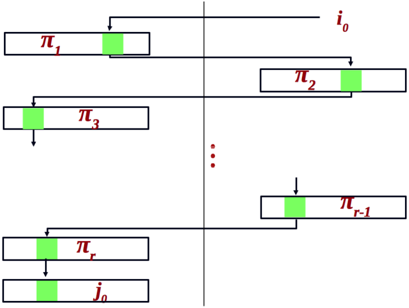
Reduction 2: Pointer Verification

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

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



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



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

Overview of Reductions

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

→ *Reduction 1* →

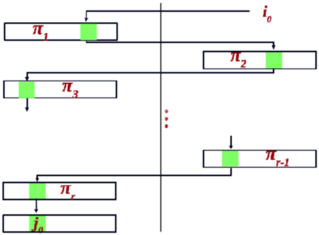
μ, $\mu_X \times \mu_Y$ distinguishable by $(r/2-1, o(n))$-protocol

→ *Reduction 2* →

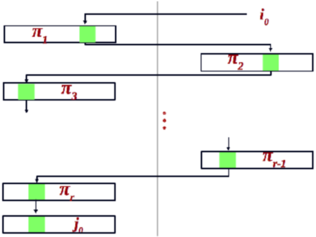
PV_{YES}, PV_{NO} distinguishable by $(r/2-1, o(n))$-protocol

Ultimate goal: prove indistinguishability of PV_{YES}, PV_{NO}

PV_{YES}



PV_{NO}



Indistinguishability of $\mathsf{PV}_{\mathsf{YES}}$, $\mathsf{PV}_{\mathsf{NO}}$

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

Theorem (BGGS, '19)

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

Indistinguishability of $\mathrm{PV_{YES}}$, $\mathrm{PV_{NO}}$

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

Theorem (BGGS, '19)

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

- Why only $\frac{r-1}{2}$ rounds?

Indistinguishability of $\mathrm{PV}_{\mathrm{YES}}$, $\mathrm{PV}_{\mathrm{NO}}$

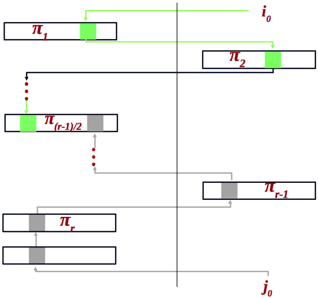
r, n implicit: $\mathrm{PV}_{\mathrm{YES}} = \mathrm{PV}_{\mathrm{YES}}(n, r)$, $\mathrm{PV}_{\mathrm{NO}} = \mathrm{PV}_{\mathrm{NO}}(n, r)$:

Theorem (BGGS, '19)

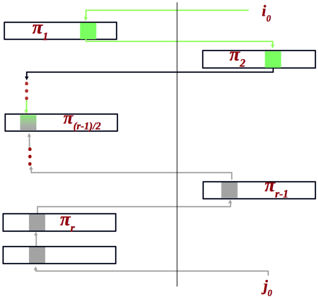
$\forall r, n$, $\mathrm{PV}_{\mathrm{NO}}$ & $\mathrm{PV}_{\mathrm{YES}}$ *are* $\left(\frac{r-1}{2}, \frac{n}{\mathrm{poly}\log(n)}\right)$*-indisting.*

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

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



$\mathrm{PV}_{\mathrm{YES}}$:



Proof of indist. of $\mathsf{PV}_{\mathsf{YES}}$ & $\mathsf{PV}_{\mathsf{NO}}$

- Idea: "round elimination" ([Nisan & Wigderson, '93]).
- Dealing with non-independence of inputs under $\mathsf{PV}_{\mathsf{YES}}$ makes proof more difficult.[1]

[1] Technically under $\frac{1}{2}(\mathsf{PV}_{\mathsf{YES}} + \mathsf{PV}_{\mathsf{NO}})$.

Proof of indist. of $\mathrm{PV}_{\mathrm{YES}}$ & $\mathrm{PV}_{\mathrm{NO}}$

- Idea: "round elimination" ([Nisan & Wigderson, '93]).
- Dealing with non-independence of inputs under $\mathrm{PV}_{\mathrm{YES}}$ 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 $\frac{1}{2}(\mathrm{PV}_{\mathrm{YES}} + \mathrm{PV}_{\mathrm{NO}})$.

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 $\tilde{\Omega}(\min\{L, n\})$.

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.

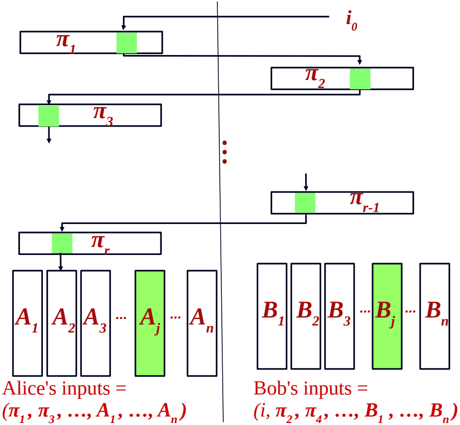
Thank you!

Proof Outline of Reduction 2

Overall goal: μ & $\mu_X \times \mu_Y$ are indistinguishable to (r', c)-protocols.

Intermediate distr. μ_{mid}:

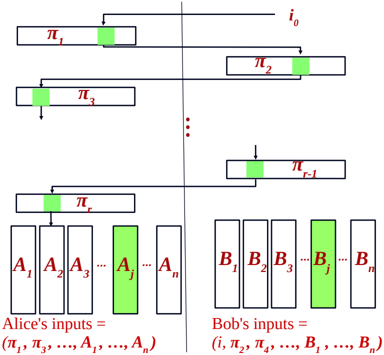
- $A_j = B_j$ for random j.
- I.e., j is independent of $\pi_r \circ \cdots \circ \pi_1(i_0)$.



Proof Outline of Reduction 2

Intermediate distr. μ_{mid}:

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

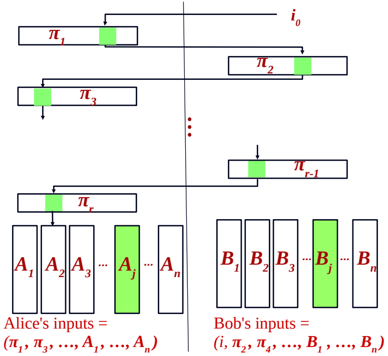


- $\mu_X \times \mu_Y$ **indist. from** μ_{mid} to protocols w/ communication $o(n)$ (*set disjointness hard*).

Proof Outline of Reduction 2

Intermediate distr. μ_{mid}:

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



- $\mu_X \times \mu_Y$ **indist. from** μ_{mid} to protocols w/ communication $o(n)$ (*set disjointness hard*).
- PV_{YES} & PV_{NO} indist. to (r', c)-protocols $\Rightarrow \mu$ **indist. from** μ_{mid} to (r', c)-protocols.

Proof of indisting. of $\mathsf{PV}_{\mathsf{YES}}$ & $\mathsf{PV}_{\mathsf{NO}}$

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

$$\begin{aligned} & \Pi \text{ disting. } \mathsf{PV}_{\mathsf{YES}} \text{ \& } \mathsf{PV}_{\mathsf{NO}} \\ \Leftrightarrow \quad & \Pi \text{ outputs } \mathbb{1}[j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)] \text{ whp} \\ & \text{under } \mathsf{PV}_{\mathsf{MIX}} = \tfrac{1}{2}(\mathsf{PV}_{\mathsf{YES}} + \mathsf{PV}_{\mathsf{NO}}). \end{aligned}$$

Proof of indisting. of $\mathrm{PV}_{\mathrm{YES}}$ & $\mathrm{PV}_{\mathrm{NO}}$

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

$$\begin{aligned} & \Pi \text{ disting. } \mathrm{PV}_{\mathrm{YES}} \;\&\; \mathrm{PV}_{\mathrm{NO}} \\ \Leftrightarrow\; & \Pi \text{ outputs } \mathbb{1}[j_0 = \pi_r \circ \cdots \circ \pi_1(i_0)] \text{ whp} \\ & \text{under } \mathrm{PV}_{\mathrm{MIX}} = \tfrac{1}{2}(\mathrm{PV}_{\mathrm{YES}} + \mathrm{PV}_{\mathrm{NO}}). \end{aligned}$$

- "Problem" 2: Players' inputs under $\mathrm{PV}_{\mathrm{MIX}}$ aren't independent.