Kolmogorov Comes to Cryptomania:

On Interactive Kolmogorov Complexity and Key-Agreement

Marshall Ball	(NYU)
Yanyi Liu	(Cornell)
Noam Mazor	(Cornell Tech)
Rafael Pass	(Tel Aviv University & Cornell Tech)

Kolmogorov Complexity

- Measure randomness of a string
  - The minimal description length of a string

Def: Fix universal TM U

$$K(x) = \min\{|\mathrm{P}| : U(\mathrm{P}) = x\}$$

- $\mathrm{P} = \langle M, w \rangle$
- (Almost) independent of the choice of U
- $K(x) \leq |x| + O(1)$
- $\Pr_{x \leftarrow \{0,1\}^n}[K(x) \geq n - i] \geq 1 - 2^{-i}$

Time-Bounded Kolmogorov Complexity

Def: Fix universal TM U. For a function $t\colon \mathrm{N} \to \mathrm{N}$:

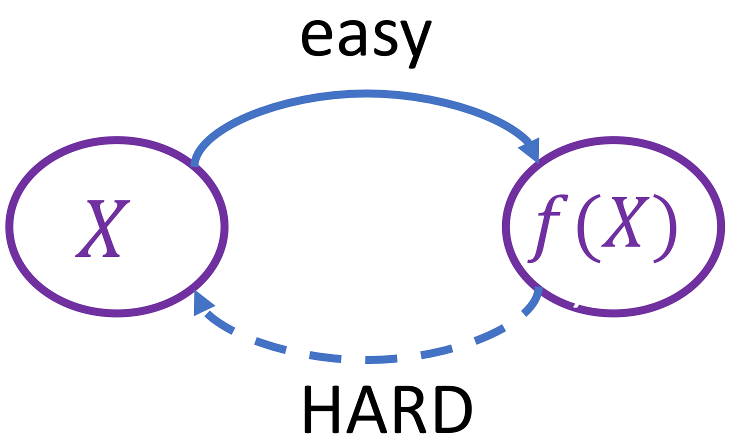
$$K^t(x) = \min\{|\mathrm{P}| : U\left(\mathrm{P}, 1^{t(|x|)}\right) = x\}$$

- Usually, fix $t \in poly$
- $K(x) \leq K^t(x) \leq |x| + O(1)$

Question: How hard is it to compute $K^t(x)$?

- Meta Complexity
- Perebor Conjecture

One-Way Functions



- The minimal assumption in cryptography
- Can be used to construct many useful primitives:

  PRGs, symmetric encryptions, digital signatures, commitments,…
- Want to base on complexity assumptions ($P \neq NP$)

Pseudorandom Generators (PRGs):

$G:\{0,1\}^n \to \{0,1\}^\ell$ s.t. for every poly-time algorithm A,

$$\left|\Pr\left[A\left(G(U_n)\right) = 1\right] - \Pr[A(U_\ell) = 1]\right| \leq negl(n)$$

Kolmogorov Complexity and One-Way Functions

- Assuming one-way functions (PRGs), K^t is hard
  - Random ℓ-bit string has K^t-compleixy ℓ
  - Output of a PRG has has K^t-compleixy $n \ll \ell$
  - (Worst-case hardness)

- Other direction?
  - Basing one-way function on the perebor conjecture

Kolmogorov Complexity and OWFs [LP’20]

Thm: OWF exists iff K^t is hard on average on U_n

- OWF exists iff there is no algorithm, that given uniform input $x \leftarrow \{0,1\}^n$ outputs (approximation of) $K^t(x)$ with probability $1 - n^{-c}$.

- To get OWFs, need to assume hardness on average
- [LP’23, Hirahara-Nanashima’23] OWFs from worst-case hardness of related promise problem

Beyond One-Way Functions: Key Agreement

- Key Agreement is one of the most important cryptographic primitives
- Allows two parties to agree on a secret over a public channel
- Cannot be based on OWF in black-box way
- Less candidates and more structured assumptions

- Can we base KA on complexity assumptions?
  - Hardness of K^t?

Overview of Our Results

- New: (time-bounded) Interactive Kolmogorov Complexity
- Hardness of Interactive Kolmogorov Complexity ⇔ KA

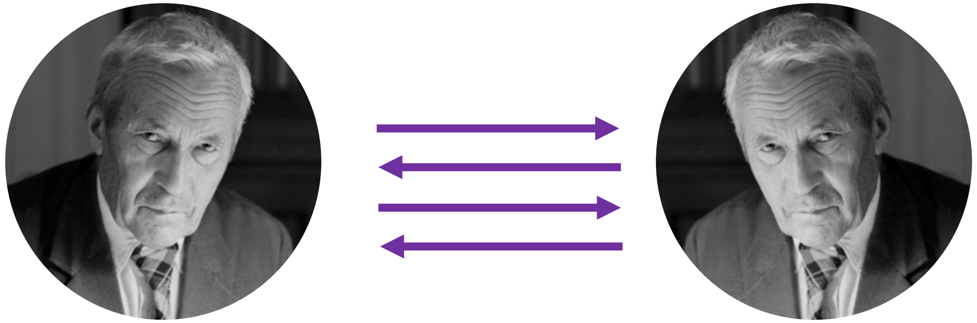
Interactive Kolmogorov Complexity

Def: $IK^t(\pi; x; y)$ is the minimal total length $|P_A| + |P_B|$ of two programs,

such that when P_A and P_B interacte:

- Both programs halt in time $t(|\pi|)$
- The transcript is π
- The output of P_A is x
- The output of P_B is y

- $IK^t(\pi; x; y) \geq K^t(\pi, x, y)$
- $IK^t(\pi; x; y) \leq |\pi| + |x| + |y| + O(1)$



The Relative IK^t Problem (RIK^tP)

RIK^tP: Given π, x, y with $|\pi| = |x| = |y| = n$, detrimine if:

- Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10 \log n$
- No: $K(\pi, x, y) \geq K(\pi) + 50 \log n$

(arbitrary choice of constants)

Thm 1 (informal):

Worst-case hardness of RIK^tP ⇔ OWFs

The Relative IK^t Problem (RIK^tP)

$RIK^tP|_{x=y}$: Given $\pi, x, y = x$ with $|\pi| = |x| = |y| = n$, detrimine if:

- Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10 \log n$
- No: $K(\pi, x, y) \geq K(\pi) + 50 \log n$

Thm 2 (informal):

Worst-case hardness of $RIK^tP|_{x=y}$ ⇔ KA

- Both in uniform/non-uniform setting
- Non black-box proof

The Relative IK^t Problem (RIK^tP)

Thm 1: Worst-case hardness of RIK^tP ⇔ OWFs

Thm 2: With the restriction that $x = y$:

- Worst-case hardness of $RIK^tP|_{x=y}$ ⇔ KA

Threshold transition:

- Let $\Delta(x, y) = \max\{K^t(x|y), K^t(y|x)\}$
- With the restriction that $\Delta(x, y) \leq s$:
  - $s \leq \log n$ => charactirizes KA
  - $s \geq 55 \log n$ => charactrizes OWF

The Relative IK^t Problem (RIK^tP)

RIK^tP: Given π, x, y with $|\pi| = |x| = |y| = n$, detrimine if:

- Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10 \log n$
- No: $K(\pi, x, y) \geq K(\pi) + 50 \log n$

- Not clear that $\mathrm{R}IK^tP \in NP$
  - $K(\pi)$ is not computable
- If $P = NP$, there is no KA and $\mathrm{R}IK^tP \in prBPP$

- Assuming KA, $\mathrm{R}IK^tP$ is hard even given $K(\pi)$
- Can replace with average-case hardness on some distributions.

Worst-case Hardness

[Antunes, Fortnow, Van Melkebeek, Vinodchandran] (informal):

Worst-case hardness on inputs with small computational depth $\Rightarrow$ Average-case Hardness (on sampleable distribution)

- Computational depth: $cd^t(x) = K^t(x) - K(x)$
- Here: small "interactive computational depth": $IK^t(\pi; x; y) - K(\pi)$

Rest of this Talk

Thm 2: Worst-case hardness of $RIK^tP|_{x=y}$ ⇔ KA

- $RIK^tP|_{x=y} \notin prBPP \quad \Rightarrow \quad$ KA
- (Overview) KA $\quad \Rightarrow \quad RIK^tP|_{x=y} \notin prBPP$

$RIK^tP|_{x=y} \notin prBPP \Rightarrow$ KA: The (weak) KA Protocol

	Alice	Bob
1. Sample:	$\ell_A \leftarrow [n], P_A \leftarrow \{0,1\}^{\ell_A}.$	$\ell_B \leftarrow [n], P_B \leftarrow \{0,1\}^{\ell_B}.$

2. Interact:

$$x \quad \boxed{\begin{matrix} P_A \Leftrightarrow P_B \\ \pi \end{matrix}} \quad y$$

3. Equality Check:

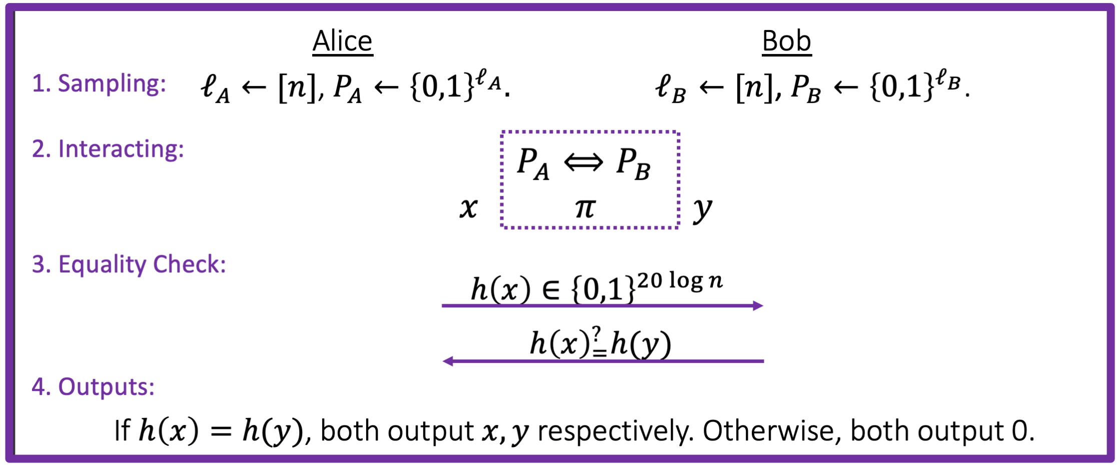
$$\xrightarrow{\quad h(x) \in \{0,1\}^{20 \log n} \quad}$$

$$\xleftarrow{\quad h(x) \overset{?}{=} h(y) \quad}$$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

$RIK^tP|_{x=y} \notin prBPP \Rightarrow$ KA: Analysis



Alice Bob

1. Sampling: $\ell_A \leftarrow [n], P_A \leftarrow \{0,1\}^{\ell_A}$. $\ell_B \leftarrow [n], P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: $P_A \Leftrightarrow P_B$ x π y

3. Equality Check: $h(x) \in \{0,1\}^{20 \log n}$ $h(x) \overset{?}{=} h(y)$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

Claim (Agreement):

Alice and Bob agree w.p. $1 - n^{-20}$.

Claim (Security):

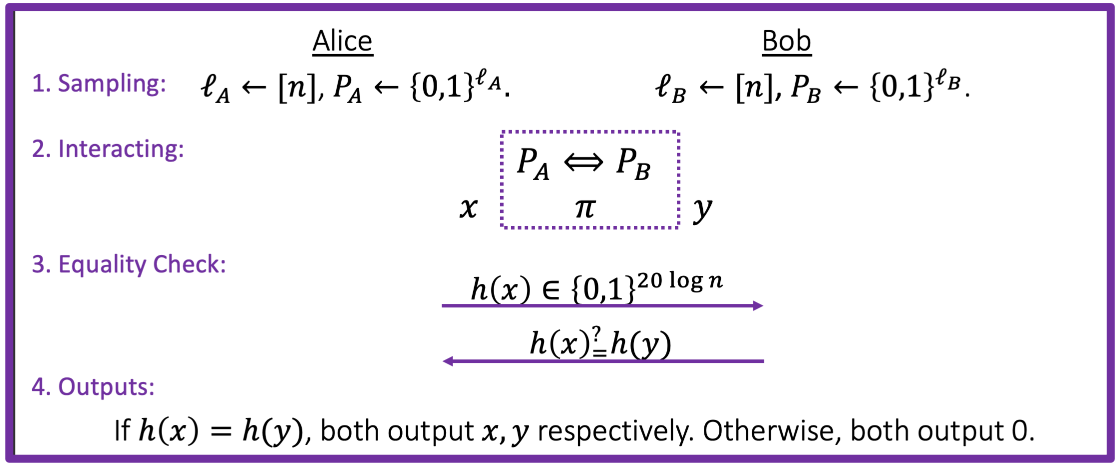
Assuming $RIK^tP|_{x=y} \notin prBPP$, Eve guesses Alice's output with probability at most $1 - n^{-19}$.

$\Rightarrow$ By [Holenstien], the protocol can be amplified to KA

Agreement

Claim (Agreement):

Alice and Bob agree w.p. $1 - n^{-20}$.



Alice

Bob

1. Sampling: $\ell_A \leftarrow [n]$, $P_A \leftarrow \{0,1\}^{\ell_A}$. $\ell_B \leftarrow [n]$, $P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: $P_A \Leftrightarrow P_B$ x π y

3. Equality Check: $\xrightarrow{h(x) \in \{0,1\}^{20 \log n}}$ $\xleftarrow{h(x) \overset{?}{=} h(y)}$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

Pf: If $x \neq y$, $\Pr[h(x) = h(y)] \leq n^{-20}$.

Security

Claim (Security):

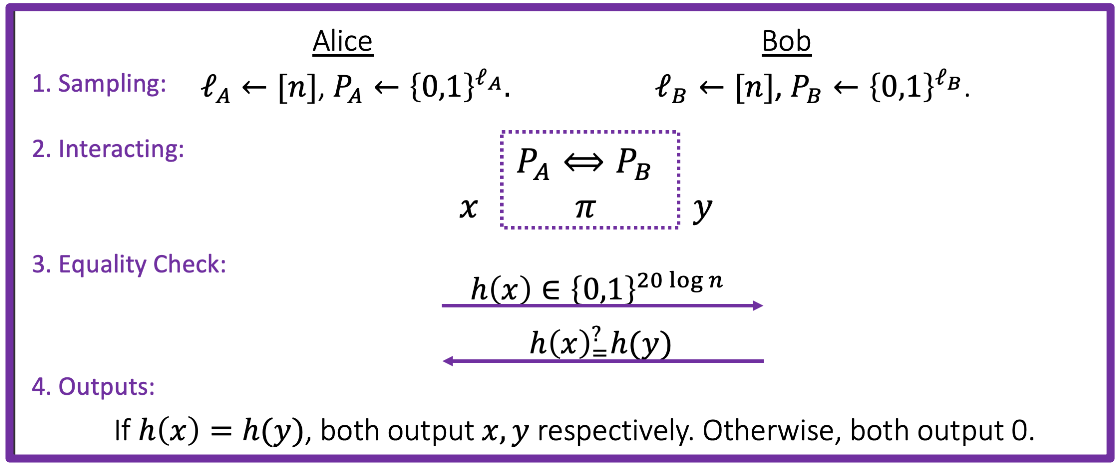
Assuming $RIK^tP|_{x=y} \notin prBPP, \boldsymbol{Eve}$ guesses Alice's output with probability at most $1 - n^{-19}$.

- In the following, assume $\boldsymbol{Eve}$ breaks the security
- We construct decider for $RIK^tP|_{x=y}$
- For simplicity, assume $\boldsymbol{Eve}$ is deterministic

The Decider

The $RIK^tP|_{x=y}$ decider D:

- On input $\pi, x, y := x$:
    - Compute $h(x)$
    - Run $Eve(\pi, h(x), "h(x) = h(y)")$
    - If Eve outputs x, output True.
      Otherwise, output False.



Alice — Bob

1. Sampling: $\ell_A \leftarrow [n]$, $P_A \leftarrow \{0,1\}^{\ell_A}$. — $\ell_B \leftarrow [n]$, $P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: x $P_A \Leftrightarrow P_B$ π y

3. Equality Check: $h(x) \in \{0,1\}^{20 \log n}$ $\xrightarrow{\hspace{2em}}$; $h(x) \overset{?}{=} h(y)$ $\xleftarrow{\hspace{2em}}$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

$RIK^tP|_{x=y}$:

Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10 \log n$

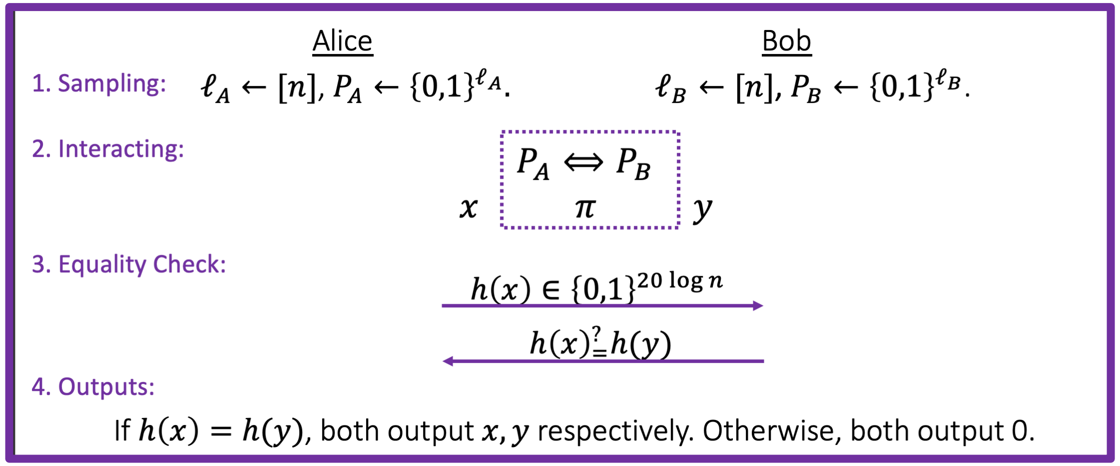
No: $K(\pi, x, y) \geq K(\pi) + 50 \log n$

The Decider

The $RIK^tP|_{x=y}$ decider D:

- On input $\pi, x, y \coloneqq x$:
  - Compute $h(x)$
  - Run $Eve(\pi, h(x))$
  - If Eve outputs x, output True.

    Otherwise, output False.



Alice

Bob

1. Sampling: $\ell_A \leftarrow [n]$, $P_A \leftarrow \{0,1\}^{\ell_A}$. $\ell_B \leftarrow [n]$, $P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: $P_A \Leftrightarrow P_B$ x π y

3. Equality Check: $h(x) \in \{0,1\}^{20 \log n}$ $h(x) \overset{?}{=} h(y)$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

$RIK^tP|_{x=y}$:

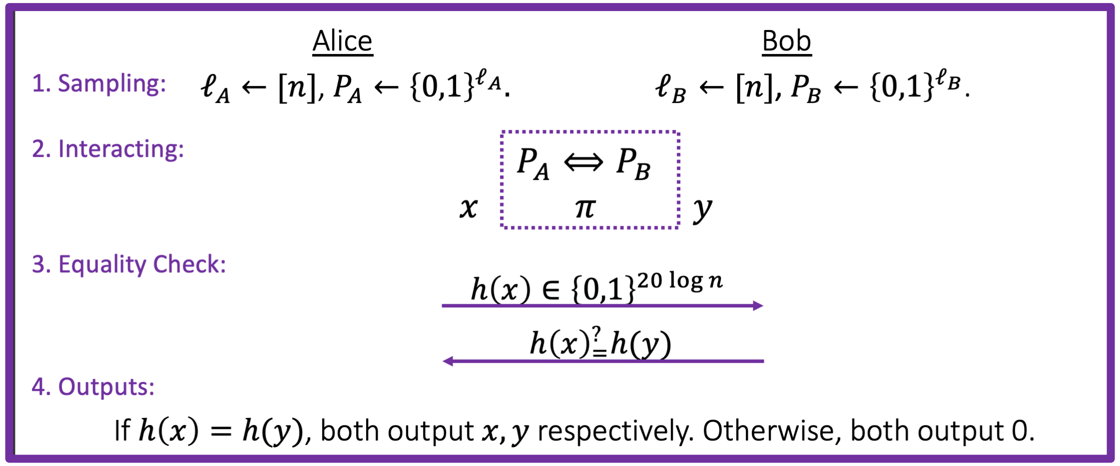
Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10 \log n$

No: $K(\pi, x, y) \geq K(\pi) + 50 \log n$

Soundness

The $RIK^tP|_{x=y}$ decider D:

- On input $\pi, x, y \coloneqq x$:
  - Compute $h(x)$
  - Run $Eve(\pi, h(x))$
  - If Eve outputs x, output True.
    Otherwise, output False.



Alice

Bob

1. Sampling: $\ell_A \leftarrow [n]$, $P_A \leftarrow \{0,1\}^{\ell_A}$. $\ell_B \leftarrow [n]$, $P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: $P_A \Leftrightarrow P_B$ x π y

3. Equality Check: $h(x) \in \{0,1\}^{20 \log n}$ $h(x) \overset{?}{=} h(y)$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

$RIK^tP|_{x=y}$:

Yes: $IK^t(\pi, x, y) \le K(\pi) + 10 \log n$

No: $K(\pi, x, y) \ge K(\pi) + 50 \log n$

Claim: If D outputs True, the input is not No-instance

Non Black-Box

Pf: Assume $Eve(\pi, h(x)) = x$,

$\Rightarrow K(\pi, x, y) \le K(\pi) + |h(x)| + |Eve| + O(1) < K(\pi) + 50 \log n$

Completeness

- Assume towards a contradiction that D answers False on Yes-Instance $(\pi, x, y = x)$.

$\Rightarrow Eve\big(\pi, h(x)\big) \neq x$.

- Let $\ell = IK^t(\pi; x; y)$.

Claim: $K(\pi) \leq \ell - 14\log n$

$\Rightarrow$ $(\pi, x, y = x)$ is not Yes-Instance

$RIK^tP|_{x=y}$:

Yes: $IK^t(\pi, x, y) \leq K(\pi) + 10\log n$

No: $K(\pi, x, y) \geq K(\pi) + 50\log n$

Idea: Eve errs with small probability => Eve errs on transcripts with small K-complexity

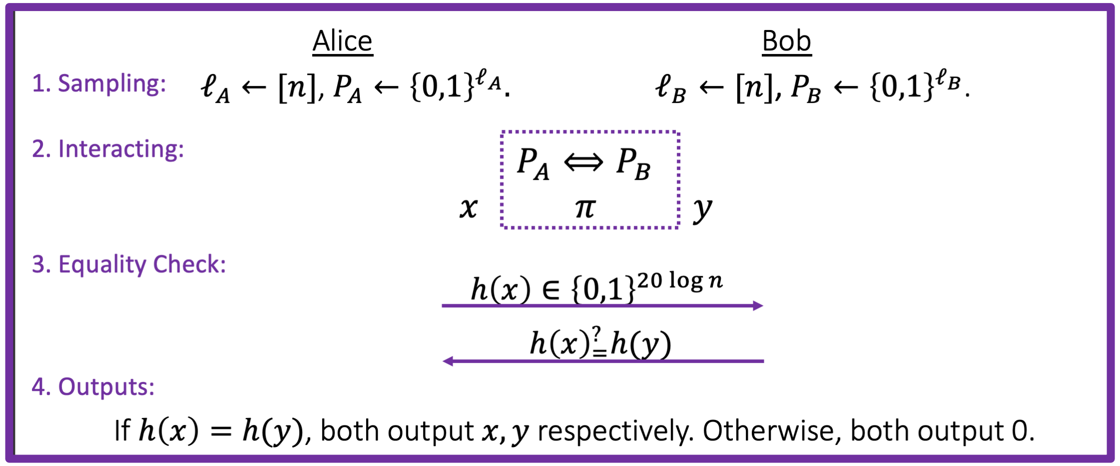
[LP'23]

Completeness

- Fix $(\pi, x, y = x)$ with $Eve(\pi, h(x)) \neq x$.
- $\ell = IK^t(\pi; x; y)$.

Claim: $K(\pi) \leq \ell - 14 \log n$

Pf:



Alice Bob

1. Sampling: $\ell_A \leftarrow [n], P_A \leftarrow \{0,1\}^{\ell_A}$. $\ell_B \leftarrow [n], P_B \leftarrow \{0,1\}^{\ell_B}$.

2. Interacting: $P_A \Leftrightarrow P_B$ x π y

3. Equality Check: $h(x) \in \{0,1\}^{20 \log n}$ $h(x) \overset{?}{=} h(y)$

4. Outputs:

If $h(x) = h(y)$, both output x, y respectively. Otherwise, both output 0.

- Alice and Bob sample (π, x, y) with probability $\frac{1}{n^2} \cdot 2^{-\ell}$.
- Eve errs w.p. at most n^{-19}

$\Rightarrow$ Eve errs on at most $\frac{n^{-19}}{\frac{1}{n^2} \cdot 2^{-\ell}} = 2^{\ell - 17 \log n}$ triplets (π', x', y') with

$$IK^t(\pi'; x'; y') = \ell$$

Completeness

Claim: $K(\pi) \leq \ell - 14 \log n$

Pf cont.: Eve errs on at most $2^{\ell - 17 \log n}$ triplets (π', x', y') with

$$IK^t(\pi'; x'; y') = \ell$$

- Let $S_\ell = \{(\pi', x', y') : IK^t(\pi', x', y') = \ell, Eve\big(\pi', h(x')\big) \neq x\}$.
- To encode π, encode S_ℓ, and the index of π in S_ℓ.
- Given n, ℓ and Eve, S_ℓ can be computed.
- $K(\pi) \leq 2 \log n + |Eve| + \log|S_\ell| \leq \ell - 14 \log n$

Non Black-Box

□

Universal KA

- The KA protocol is universal KA
  - If KA exists, the protocol is KA
- [Harnik-Kilian-Naor-Reingold-Rosen] different universal protocol

KA $\Rightarrow RIK^tP|_{x=y} \notin prBPP$

- Assume there exists KA protocol.
- Let (Π, K) be the distribution of the transcript and the key
- Security: It is hard to distinguish (Π, K) and (Π, U_n)
- $K(\Pi, U_n, U_n) \geq K(\Pi) + \Omega(n)$ with high probability.
- Not clear if $IK^t(\Pi, K, K)$ is small compare to $K(\Pi)$.
  - If $IK^t(\Pi, K, K) \leq K(\Pi) + 10\log n$, we finish

$RIK^tP|_{x=y}$:

Yes: $IK^t(\pi, x, y) \leq K(\pi) + \ 10\log n$

No: $K(\pi, x, y) \geq K(\pi) + \ 50\log n$

KA $\Rightarrow RIK^tP|_{x=y} \notin prBPP$

  - If $IK^t(\Pi, K, K) \leq K(\Pi) + 10\log n$, we finish
- When the randomness of the parties can be reconstructed from Π,

$$IK^t(\Pi, K, K) \approx K(\Pi)$$

- In Deffie-Hellman, the randomness can be reconstructed
- We show how to transform any KA protocol to have this property*
  - (cond entropy-preserving KA)

Conclusion & Open Questions

- Interactive Kolmpgorov complexity
- $RIK^{t}P$
- Characterization of KA (and OWF)

Open Questions:

- Public Key Encryption?
- Other cryptographic primitives?

Thanks!