Asymmetry of Information, Cryptography, and Complexity Lower Bounds

Igor Oliveira

Based on joint work with Jinqiao Hu and Yahel Manor

Proof Complexity Workshop

University of Bath

June 2026

Overview of the Talk

- **Algorithmic information theory** precisely captures problems from **cryptography** and **complexity theory**.

  "*In a secure cryptographic protocol, the ciphertext should reveal a negligible amount of information about the message to any computationally bounded adversary.*"

- Recent results allow us to formalize this perspective and **characterize one-way functions**.

- A connection to **Meta-Complexity** leads to unconditional results on the **information asymmetry** needed in cryptography.

Algorithmic Information Theory (Kolmogorov Complexity)

$$x = 01100100111110101011001101001001010100111$$

Given a string $x \in \{0,1\}^*$, $\mathrm{K}(x)$ denotes the length of the smallest program Π that prints x.

$\mathrm{K}(x \mid y)$ denotes the length of the smallest program Π such that $\Pi(y) = x$.

$\mathrm{K}(x) - K(x \mid y)$ measures the **amount of information that y contains about x.**

Symmetry of Information (SoI) – Levin-Kolmogorov, 1970

Symmetry of Information (SoI): The amount of information that an n-bit string x reveals about another n-bit string y is essentially the same in either direction:

$$\mathrm{K}(x,y) \;=\; \mathrm{K}(x) + \mathrm{K}(y \mid x) \;=\; \mathrm{K}(y) + \mathrm{K}(x \mid y) \quad \text{up to} \quad \pm O(\log n).$$

Leonid Levin

Andrey Kolmogorov

The nontrivial part is to show that $\mathrm{K}(x,y) \gtrsim \mathrm{K}(y) + \mathrm{K}(x \mid y)$.

The proof requires an **exhaustive search** and does not extend to **time-bounded** settings.

Cryptography: One-Way Functions

An efficiently computable function $f\colon \{0,1\}^n \to \{0,1\}^n$ is a **one-way function** (OWF) if for every probabilistic poly-time algorithm A,

$$\Pr_{x\sim\{0,1\}^n,\, y=f(x)}[\, A(y) \in f^{-1}(y)\,] \;\leq\; 1/n^{\omega(1)}.$$

The **existence of secure cryptographic primitives**, such as

private-key encryption, digital signatures, bit commitment, pseudorandom generators, etc.,

is **equivalent to the existence of OWFs**.

Time-Bounded Kolmogorov Complexity

In cryptography and complexity, the **efficiency** of computations is relevant. Levin (1984) introduced the following notion:

$$\mathrm{Kt}(x) \triangleq \min_{\substack{\Pi \in \{0,1\}^* \\ t \in \mathbb{N}}} \{|\Pi| + \lceil \log t \rceil \mid \Pi \text{ outputs } x \text{ within } t \text{ steps}\}.$$

We also need to consider **randomized** computations (Oliveira, 2019):

$$\mathrm{rKt}(x) \triangleq \min_{\substack{\text{randomized } \Pi \in \{0,1\}^* \\ t \in \mathbb{N}}} \{|\Pi| + \lceil \log t \rceil \mid \Pi \text{ outputs } x \text{ with prob. } \geq 2/3 \text{ within } t \text{ steps}\}.$$

We can define **conditional** $\mathrm{Kt}(x \mid y)$ and $\mathrm{rKt}(x \mid y)$ in the natural way.

Information Asymmetry and Cryptography (Longpré-Watanabe, 1995)

- Longpré-Watanabe (1995): Information asymmetry is **necessary** for cryptography.

  Let $\boldsymbol{f : \{0,1\}^n \to \{0,1\}^n}$, and assume $\boldsymbol{f}$ is a **permutation** for simplicity.

  Consider a random $x \sim \{0,1\}^n$, set $y \triangleq f(x)$. Now if SoI holds with error $e(n)$ and

  $$\mathrm{rKt}(x, y) = \mathrm{rKt}(y) + \mathrm{rKt}(x \mid y) \pm e(n),$$

  then $\mathrm{rKt}(x \mid y) \lesssim e(n)$.

  But then x can be recovered from y in randomized time $\approx 2^{e(n)}$.

- **Note:** The error bound $e(n)$ controls the cryptographic security.

Equivalence (Hirahara-Ilango-Lu-Nanashima-Oliveira, 2023 & 2024)

- Information asymmetry is also **sufficient** for cryptography!
- Formally, if there is a poly-time samplable distribution $\mathcal{D}$ over $(\boldsymbol{x}, \boldsymbol{y}) \in \{0,1\}^n \times \{0,1\}^n$ such that

$$\Pr_{(\boldsymbol{x},\boldsymbol{y})\sim\mathcal{D}}[\text{SoI for rKt fails for } (\boldsymbol{x},\boldsymbol{y}) \text{ with error } e(n) = \omega(\log n)] \;=\; \Omega(1/\text{poly}(n))$$

  then one-way functions exist (**[HILNO'23]**, **[HLO'24]**, **[HLN'24]**).

- **Failure of SoI** for a non-negligible fraction of pairs (x, y) produced by a samplable distribution is all we need to construct basic cryptographic primitives.

Deterministic vs Randomized

Ronneburger (2004) employed a diagonalization argument to show that **SoI fails for** Kt.

A key step is to construct in exponential time a string that has large Kt.

This brute-force construction **does not work** in the **randomized setting relevant for cryptography**: the output is not canonical (pseudodeterministic).

Does Symmetry of Information hold for randomized computation?

We show that this is tightly related to **Meta-Complexity**.

Meta-Complexity

Meta-Complexity refers to the complexity of problems and tasks that are themselves about computations and their complexity.

Connections to learning algorithms, cryptography, proof complexity, and lower bounds.

We will be concerned with the complexity of the following task:

Given an input string $x \in \{0,1\}^n$, estimate the value $\mathrm{rKt}(x)$.

Trivial Upper Bound: Given x, $\mathrm{rKt}(x)$ can be estimated up to error $O(\log n)$ in randomized time $2^n \cdot \mathrm{poly}(n)$.

First Result: A Tight Correspondence

Theorem 1: Equivalence Between SoI for rKt and Its Meta-Complexity

For a monotone function $n \leq T(n) \leq 2^n$, the following are equivalent up to polylog(n) factors:

- SoI holds for **rKt** with error $e(n) = \widetilde{O}(\log T(n))$.
- Given $x \in \{0,1\}^n$, the value $\mathbf{rKt}(x)$ can be approximated within an additive term $\widetilde{O}(\log T(n))$ in randomized time

$$2^{\widetilde{O}(\log T(n))}.$$

For instance, SoI for rKt holds with error $e(n) = \text{poly}(\log n)$ if and only if $\mathbf{rKt}(x)$ can be approximated up to additive error $\text{poly}(\log n)$ in time $n^{\text{poly}(\log n)}$.

Consequence: SoI Fails for Randomized Computations

Combining the correspondence with the **unconditional** result from (Oliveira, 2019) that rKt **cannot** be approximated up to error $\varepsilon \cdot n$ in randomized time $n^{\mathrm{poly}(\log n)}$:

Theorem 2: SoI Fails for rKt with Polylogarithmic Error

For every constant $c \geq 1$, there are infinitely many values of n and strings $x, y \in \{0,1\}^n$ such that SoI for rKt fails for (x, y) with error $(\log n)^c$:

$$\mathrm{rKt}(x, y) < \mathrm{rKt}(x) + \mathrm{rKt}(x \mid y) - (\log n)^c.$$

I: From SoI to Meta-Complexity

- In hindsight, the connection from **SoI to Meta-Complexity** is obvious.

  Goal: Given $x \in \{0,1\}^n$, estimate $\mathbf{rKt}(x)$.

  Assume SoI with error $e(n)$ holds: $\mathrm{rKt}(x) = \mathrm{rKt}(x_1) + \mathrm{rKt}(x_2 \mid x_1) \pm e(n)$.

  – We can estimate $\mathbf{rKt}(x_1)$ up to error $O(\log n)$ in time $\approx 2^{n/2}$.

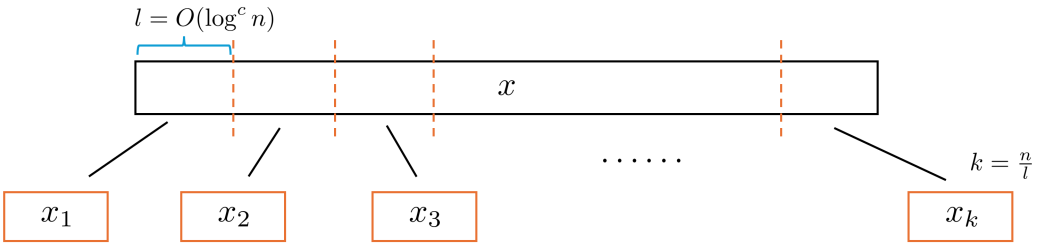
  – Similarly, $\mathbf{rKt}(x_2 \mid x_1)$ can be estimated up to error $O(\log n)$ in time $\approx 2^{n/2}$.

  $\Longrightarrow$ We can estimate $\mathrm{rKt}(x)$ up to error $e(n) + O(\log n)$ in time $\approx 2^{n/2}$. **Nontrivial!**

- It is possible to iterate this idea using that **SoI $\rightarrow$ conditional SoI** (with a small loss).

A Weaker Bound: Kabanets-Kolokolova (2025)

- Break x into n/ℓ blocks of length $\ell \triangleq \mathbf{poly}(\log n)$.



- Estimate $\widetilde{k_i} = \mathrm{rKt}(x_i \mid x_1 \ldots x_{i-1})$ up to error $O(\log n)$ in time $n^{\mathbf{poly}(\log n)}$.
- **From Sol**, $\mathrm{rKt}(x) = \sum_{i=1}^{\ell} \mathrm{rKt}(x_i \mid x_1 \ldots x_{i-1}) \pm O(e(n) \cdot n/\ell)$.
- If $e(n) = \mathrm{poly}(\log n)$, we can estimate $\mathrm{rKt}(x)$ up to error $n/\mathbf{poly}(\log n)$ in time $n^{\mathrm{poly}(\log n)}$.

The Stronger Connection

- We obtain a much tighter connection from **SoI $\rightarrow$ Meta-Complexity**.
- If $\boldsymbol{e(n) = \mathbf{poly}(\log n)}$, we can estimate $\mathrm{rKt}(x)$ up to error $\mathbf{poly}(\log n)$ in the same time.
- To minimize the total error, we reduce the number of times we apply SoI to just $O(\log n)$.
- Proof relies on a **recursive decomposition of x using properties of** rKt **+ techniques from search-to-decision reductions in meta-complexity**.

II: From Meta-Complexity to SoI

- For the other direction, we must show that if

  rKt is easy to estimate $\Rightarrow$ SoI holds for rKt.

- The argument is an adaptation of existing techniques:

  Proof follows from work of **[Goldberg-Kabanets'22]** and **[Hirahara'22]** showing that **Meta-Complexity $\Rightarrow$ SoI** using **techniques from computational pseudorandomness**.

- Running time and accuracy of rKt estimator controls the error $e(n)$ in SoI.

Back to Cryptography

The previous result shows the existence of pairs (x, y) such that SoI for rKt fails for (x, y).

For crypto, we need an efficient distribution such that SoI fails for many pairs $(x, y) \sim \mathcal{D}$.

Second Result: Average-Case Failure of SoI

Theorem 3: Average-Case Failure of SoI with Error $e(n) = O(\log n)$

For every constant $c \geq 1$, there is a poly-time samplable distribution family $\mathcal{D} = \{\mathcal{D}_n\}_{n \geq 1}$, where each $\mathcal{D}_n$ is supported over $\{0,1\}^n \times \{0,1\}^n$, for which the following holds:

There is $k > 0$ such that, for infinitely many values of n, we have

$$\Pr_{(x,y)\sim\mathcal{D}_n}\left[\mathrm{rKt}(x,y) \leq \mathrm{rKt}(y) + \mathrm{rKt}(x \mid y) - c \cdot \log n\right] \geq \frac{1}{n^k}.$$

Note: This is necessary but does not establish the existence of OWFs: we need $e(n) = \omega(\log n)$.

Average-Case: Techniques

- The failure of SoI in the **worst case** combines two ingredients:

$$\text{SoI} \to \text{Meta-Complexity } \textbf{[KK'25]} \quad + \quad \text{rKt lower bound } \textbf{[Oli'19]}.$$

- From **average case SoI**, we only get an algorithm that estimates rKt on **most strings**.
- While **[Oli'19]** gives a 1-sided average-case lower bound, the algorithm obtained above **errs on the "wrong" side**.
- We build on the argument behind **[Oli'19]**, which is extended with the following ideas:
  - **Win-win** arguments over the distributions of pairs (x, y) induced in the relevant pseudorandom constructions;
  - **Random-self-reducibility** of a relevant PSPACE-complete problem to tolerate errors.

How Asymmetric is Randomized Computation?

- SoI fails with error $e(n) = \text{poly}(\log n)$ for **randomized computations**.
- Meanwhile, we know from Ronneburger's result that SoI fails with error $e(n) = \Omega(n)$ for **deterministic computations** (i.e., for Kt complexity).
- Asymmetry bound relates to level of cryptographic hardness against randomized adversaries.

By the correspondence between **SoI** $\iff$ **Meta-Complexity**, larger error bounds are equivalent to stronger complexity lower bounds.

Third Result: New Exponential Complexity Lower Bound

Theorem 4: Exponential Hardness of Estimating Conditional rKt

For every $0 < \alpha < \beta < 1$ there is a constant $\varepsilon > 0$ such that the following holds:

There is no randomized algorithm running in time $2^{\varepsilon \cdot |x|} \cdot \mathrm{poly}(|y|)$ that

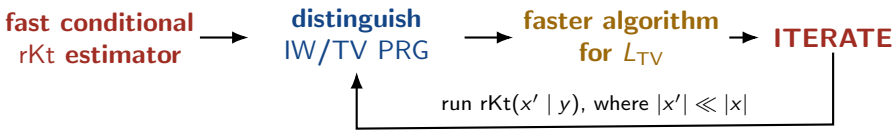
- **accepts** every pair (x, y) with $\mathbf{rKt}(x \mid y) \geq \beta \cdot |x|$,
- **rejects** every pair (x, y) with $\mathbf{rKt}(x \mid y) \leq \alpha \cdot |x|$.

– The lower bound is **essentially optimal**.

– Incomparable to the lower bound against $\mathbf{BPTIME}[2^{o(n)}]$ from **[Hirahara'22]**, which does not require a conditional string but cannot be extended to **prBPTIME**$[\cdot]$.

A New Technique: Iterative Bootstrapping

- We build on the lower bound proof from **[Oli'19]**: $L_{\mathsf{TV}} \in \mathsf{BPP}^{\text{Gap-MrKtP}[\alpha n, \beta n]}$.
- **Key Idea:** **Iterative Bootstrapping** using an algorithm for estimating $\mathrm{rKt}(x \mid y)$.



- We eventually get $L_{\mathsf{TV}} \in \mathsf{BPP}$ (without oracle), which can be used to derive a contradiction.

Consequence: Strong Failure of Conditional SoI

We say that **conditional Symmetry of Information** holds for rKt with error $e(n)$ if for every large enough length $n \in \mathbb{N}$, strings $x, y \in \{0,1\}^n$, and $w \in \{0,1\}^*$,

$$\mathrm{rKt}(x, y \mid w) \;\geq\; \mathrm{rKt}(y \mid w) + \mathrm{rKt}(x \mid y, w) - e(n).$$

(**Note:** The error term $e(n)$ **does not depend** on the length of w.)

Theorem 5: Failure of Conditional SoI with Linear Error

There is a constant $\varepsilon > 0$ such that conditional SoI with error $\boldsymbol{e(n) = \varepsilon \cdot n}$ fails for rKt.

Summary

- **Symmetry of Information** precisely captures **Meta-Complexity**:

  SoI holds for rKt with error $e(n)$ $\iff$ rKt can be estimated in time $\approx 2^{e(n)}$

- **SoI fails for** rKt **with error** $\mathrm{poly}(\log n)$.

- $\forall c$, SoI for rKt **fails on average** with error $c \cdot \log n$ over a poly-time samplable distribution.

- We show an **exponential lower bound** on the complexity of estimating $\mathrm{rKt}(x \mid y)$.

Open Problems

- Prove that **SoI fails for** rKt with error

$$e(n) = n^{\varepsilon}$$

for some $\varepsilon > 0$.

- Equivalently, prove that **rKt(x) cannot be approximated** up to an additive term of order n^{ε} in randomized time $2^{n^{\varepsilon}}$.

Thank You