Paper Reading Report: NP-Hardness of Approximating Meta-Complexity: A Cryptographic Approach

Jingyi Lyu

April 22, 2025

We will briefly summarize the result, technique, and impact of ***NP-Hardness of Approximating Meta-Complexity: A Cryptographic Approach***. [HIR23]

1 Introduction

Meta-complexity refers to a series of problems concerning hardness of computing complexity of general objects (e.g., binary strings or boolean functions) over different complexity measures. For example, major (and also long-standing) questions in this area ask whether it is **NP**-hard to compute circuit complexity of boolean functions (MCSP) or time-bounded Kolmogorov complexity of binary strings (K^t).

Hardness results in meta-complexity has various applications in computational complexity, learning theory, cryptography, etc. For example:

- Worst-case to average-case reduction; [Hir21]
- Proving circuit lower bound; [KC00]
- Basing one-way function on natural complexity assumptions (e.g. $\mathbf{P} \neq \mathbf{NP}$); [LP20]
- Learning constant-depth circuits with parity gates in quasi-polynomial time. [CIKK16]

To partially understand the property, intuition, and connections behind these tough problems, variants of complexity measures are proposed and investigated, and surprisingly, computational hardness of some variants is provable with cryptographic techniques, either conditionally or unconditionally. Especially, [HIR23] makes progress on showing ***NP-hardness of approximation*** of some meta-complexity problems, with different cryptographic primitives applied.

2 Result

Preliminaries. The result we present here (among all the main results, others will be sketched later) investigates MOCSP, a conditional variant of MCSP. Given boolean functions $f : \{0,1\}^n \to \{0,1\}$ and $\mathcal{O} : \{0,1\}^{O(n)} \to \{0,1\}$, MOCSP asks to find the minimum size of the **oracle boolean circuit** $C^{\mathcal{O}}$ that computes f. Here, $C^{\mathcal{O}}$ is defined by the boolean circuit, but with oracle access to $\mathcal{O}$, in the form of single fan-in $O(n)$ gate that computes $\mathcal{O}$.

The cryptographic primitive used here is **witness encryption with oracle**, which is almost same as standard witness encryption, but all participants (encryption, decryption, and adversary) in this context of computation have oracle access to same $\mathcal{O}$. The security under this variant is defined with probabilistic notion on oracles, i.e., it is secure as long as security holds w.p. $1 - o(1)$ over $\mathcal{O} \leftarrow \mathcal{U}_{\mathcal{O}}$.

Main result. The result consists of two parts:

(a) For $L \in \mathbf{NP}$ and oracle distribution $\mathcal{U}_{\mathcal{O}}$, if secure witness encryption w.r.t. L and $\mathcal{U}_{\mathcal{O}}$ exists with exponential security, then randomized polynomial reduction from L to distinguishing

- Minimum size of $C^{\mathcal{O}}$ that completely computes f is less than $2^{\epsilon n}$;

- Minimum size of $C^{\mathcal{O}}$ that computes f correctly on *non-trivial fraction of inputs* (i.e., slightly larger than $\frac{1}{2}$) is greater than $2^{0.3n}$.

with truth table of $f : \{0,1\}^n \to \{0,1\}$ and $\mathcal{O} : \{0,1\}^{O(n)} \to \{0,1\}$ provided.

(b) There indeed exists $L \in \mathbf{NP}$ and $\mathcal{U}_{\mathcal{O}}$ such that witness encryption w.r.t. L and $\mathcal{U}_{\mathcal{O}}$ is exponentially secure and computable in polynomial time.

One can see the combination of two parts forms unconditional **NP**-hardness of approximating MOCSP with polynomial approximation factor.

3 Techniques

In this section we briefly conclude the technical contributions of this result.

(a) Reduction. Assume $(L, \mathcal{U}_{\mathcal{O}}, \mathsf{Encrypt}^{\mathcal{O}}, \mathsf{Decrypt}^{\mathcal{O}})$ forms exponentially secure witness encryption scheme with oracle. Furthermore, randomly fix an $\mathcal{O} \leftarrow \mathcal{U}_{\mathcal{O}}$ for encryption scheme as long as it has $1 - o(1)$ probability sustaining security. As input of reduction we have $x \in \{0,1\}^*$ as instance of L. By definition of witness encryption, any ciphertext produced with instance x is decrypt-able if and only if $x \in L$.

Consider uniformly random $f : \{0,1\}^n \to \{0,1\}$. To relate decrypt-ability to circuit complexity of computing f with oracle $\mathcal{O}'$, we construct $\mathcal{O}'$ by concatenating the following two ingredients:

- $\mathcal{O}_{\mathsf{ct}}$, which is bit-wise encryption of truth table of f. In other words, $\mathcal{O}_{\mathsf{ct}}$ concatenating all $\mathsf{Encrypt}^{\mathcal{O}}(x, f(s), r_s)$ over $s \in \{0,1\}^n$. Here r_s is fresh randomness.
- $\mathcal{O}$, without which one can decrypt nothing ($\mathsf{Decrypt}^{\mathcal{O}}$ has oracle access to $\mathcal{O}$);

So intuitively, given oracle access to $\mathcal{O}' = (\mathcal{O}, \mathcal{O}_{\mathsf{ct}})$, we have:

- For $x \in L$, fast algorithm computes f by invoking $\mathsf{Decrypt}^{\mathcal{O}}$ over $\mathcal{O}_{\mathsf{ct}}$ and get f. Thus a small circuit $C^{\mathcal{O}}$ exists, since we can derive non-uniform computation from uniform algorithms with polynomial blow up.
- For $x \notin L$, with security guarantee of witness encryption, $\mathcal{O}'$ provides no information about f. Namely, this is equivalent to computing f on raw boolean circuits. By randomness of f and counting argument, the circuit complexity is large w.h.p.

Proof of this part makes use of hybrid arguments and counting argument regarding probabilistic notions of incompressibility (namely, pK^t [GKLO22]), etc.

(b) Encryption scheme. The paper builds witness encryption scheme with oracle based on idea from [GGSW13]. Recall the multi-linear map model applied in [GGSW13], i.e., a sequence of order-p cyclic groups $G_1 = \langle g_1 \rangle, \cdots, G_n = \langle g_n \rangle$ and map

$$e_{i,j} : G_i \times G_j \to G_{i+j}, \quad (g_i^a, g_j^b) \mapsto g_{i+j}^{a+b}$$

, [HIR23] modified it into **generic multi-linear map model** by shuffling each group with random permutation. Namely, assume some random oracle provides bijection $\sigma_i : [p] \to G_i$ for all i, then we can define oracle $\mathcal{O}_{i,j}$ by

$$\mathcal{O}_{i,j} : [p] \times [p] \to [p], \quad (a, b) \mapsto \sigma_{i+j}^{-1}(e_{i,j}(\sigma_i(a), \sigma_j(b)))$$

[HIR23] then constructed witness encryption w.r.t. $\mathcal{O} = (\mathcal{O}_{i,j})$ with approach from [GGSW13], and unconditionally proved security of the construction.

The proof follows a tedious hybrid argument. We try to propose brief intuition here: Eventually it can be transformed into security game where each oracle access from adversary obtains a linear combination of formal variables (rather than elements from $[p]$). The formal variable used to represent message bit is identical for 0/1, then (with condition that witness does not exist) a deterministic adversary cannot tell any difference about values returned from oracle.

4 Contributions and Impact

The most noticeable advantage of [HIR23] is **improvement of approximation factor**. Hardness of approximating MOCSP is proved in previous work [Ila20] with poly-logarithmic approximation factor, while current result has polynomial factor.

Besides the approximation factor, another main result from [HIR23] also shows **improvement of time regime**. It states that conditional version of time-bounded Kolmogorov complexity $\mathsf{K}^t(x|y)$ is hard to approximate when t is super-linear in $|y|$ and indistinguishability obfuscation (iO) exists, while the previous results only hold with sub-linear t. [Hir22b] This improvement of time regime can satisfy *one of* major conditions from which **worst-case to average-case reduction of NP** (i.e., eliminating *Heuristica*) can be derived. [Hir22b]

Basing **NP**-hardness of meta-complexity on cryptographic primitives (or techniques) is not a new idea. For example, [IKV18] shows if iO exists, then $\mathsf{MCSP} \in \mathbf{ZPP}$ if and only if $\mathbf{NP} = \mathbf{ZPP}$; [Hir22a] shows partial function version of K^t with one-time padding scheme. However, these works have different drawbacks, such as:

- First, [IKV18] implies **non-black-box** reduction from SAT to MCSP, while usual definition of **NP**-hardness concerns **black-box** reduction;
- Second, [Hir22a] makes use of information-theoretic cryptography. [HIR23] provides intuition that, **NP**-hardness of MCSP (under different types of reduction) implies highly non-trivial circuit lower bound [SS20][HP15], which is hard to imagine without deterministically generating instances with large circuit complexity. So **structured computational hardness** from computational cryptography primitives may help, while information-theoretic ones (that relies purely one randomness) may not.

In comparison, this work provides black-box reduction with help of computational cryptography primitives, namely, witness encryption. It fits our intuition better and somehow fills these drawbacks. We can therefore be more confident that such applications of cryptographic primitives in [HIR23] is likely to be a successful approach toward major breakthroughs.

We would like to mention [Ila23] as an intriguing following work strengthening our confidence here. This paper proposed a construction of **cryptographic proof work** scheme from hash function. This scheme can be used to do "encryption", and the paper proved that if the hash function is **random oracle**, then efficient "decryption" exists if and only if witness to some **NP**-complete language instance exists.

By intuition, this reduction from [Ila23] is very similar to the one in [HIR23]. Furthermore, once we find approach to replace random oracle by practical hash function, we immediately get a randomized reduction from **NP**-complete language to MCSP, which will be a big breakthrough. That potentially existing hash function definitely holds a deterministic structure that makes it hard to invert - this exactly fits the intuition of [HIR23]. From this perspective, we can say the cryptographic approach proposed in [HIR23] deserves much expectation.

References

[CIKK16] Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonima Kolokolova. Learning algorithms from natural proofs., 2016.

[GGSW13] Sanjam Garg, Craig Gentry, Amit Sahai, and Brent Waters. Witness encryption and its applications., 2013.

[GKLO22] Halley Goldberg, Valentine Kabanets, Zhenjian Lu, and Igor Carboni Oliveira. Probabilistic kolmogorov complexity with applications to average-case complexity., 2022.

[Hir21] Shuichi Hirahara. Average-case hardness of np from exponential worst-case hardness assumptions., 2021.

[Hir22a] Shuichi Hirahara. Np-hardness of learning programs and partial mcsp., 2022.

[Hir22b] Shuichi Hirahara. Symmetry of information from meta-complexity., 2022.

[HIR23] Yizhi Huang, Rahul Ilango, and Hanlin Ren. Np-hardness of approximating meta-complexity: A cryptographic approach, 2023.

[HP15] John M. Hitchcock and Aduri Pavan. On the np-completeness of the minimum circuit size problem., 2015.

[IKV18] Russell Impagliazzo, Valentine Kabanets, and Ilya Volkovich. The power of natural properties as oracles., 2018.

[Ila20] Rahul Ilango. Approaching mcsp from above and below: Hardness for a conditional variant and ac0[p]., 2020.

[Ila23] Rahul Ilango. Sat reduces to minimum circuit size problem with a random oracle, 2023.

[KC00] Valentine Kabanets and Jin-Yi Cai. Circuit minimization problem., 2000.

[LP20] Yanyi Liu and Rafael Pass. On one-way functions and kolmogorov complexity., 2020.

[SS20] Michael Saks and Rahul. Santhanam. Circuit lower bounds from np-hardness of mcsp under turing reductions., 2020.