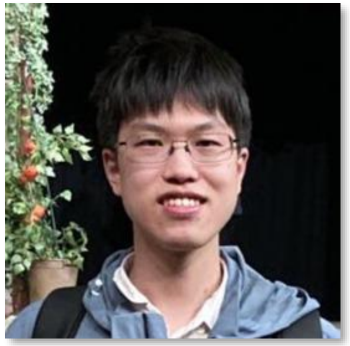
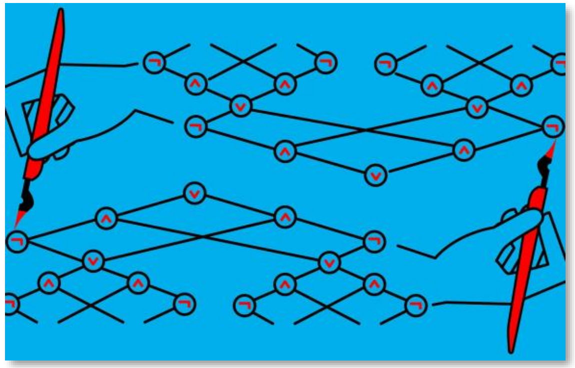
NP-Hardness of Approximating Meta-Complexity: A Cryptographic Approach



Yizhi Huang
(Tsinghua)

Rahul Ilango
(MIT)

<u>Hanlin Ren</u>
(Oxford)



Minimal Complexity Assumptions for Cryptography
Meta-Complexity @ Simons

In this talk, you will see

(For complexity theorists)

Minimum Oracle Circuit Size Problem (MOCSP)

NP-hardness of meta-complexity

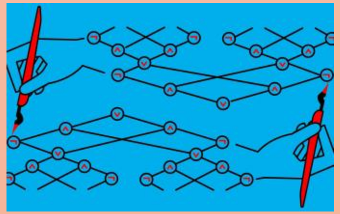
approximating

with optimal inapprox gap

NO ADDED ~~PRESERVATIVES~~ PCPs

(For cryptographers)

Cryptography



Meta-complexity

Witness encryption
(the one proposed in GGSW)

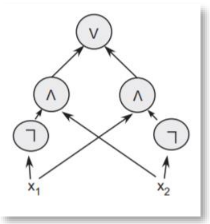
How we used crypto constructions to prove something interesting in complexity theory… Unconditionally!

YOU can make progress in meta-complexity!

Minimum Circuit Size Problem

- MCSP (Minimum Circuit Size Problem)
  - Given a truth table, compute its circuit complexity

Input length $= N = 2^n$



$\boldsymbol{x}$	$\mathbf{0}^{\boldsymbol{n}}$	…	$\mathbf{1}^{\boldsymbol{n}}$
f	$f(0^n)$	…	$f(1^n)$

$\mathrm{Circuit\_Complexity}(f)$

- What's the complexity of MCSP?

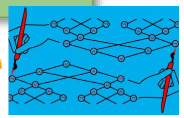
The (meta-)complexity of circuit complexity!

MCSP is in $\mathbf{NP}$.

MCSP is intractable under standard crypto assumptions.

[RR97, KC00]

Cryptography



Meta-complexity

Is MCSP $\mathbf{NP}$-complete?

NP-completeness of MCSP: Why care about it?

[Murray-Williams 17]: If MCSP is $\mathbf{NP}$-hard under deterministic mapping reductions, then $\mathbf{EXP} \neq \mathbf{ZPP}$.

Is it $\mathbf{NP}$-hard? This problem will be “hard to solve”, but Yes or No?

Curiosity

Excluding Heuristica

[LP20, LP22]: Average-case complexity of “cousins” of MCSP characterizes one-way functions!

MCSP is a natural problem whose complexity remain unidentified… for 50 yrs!

OWF from $\mathbf{NP} \not\subseteq \mathbf{BPP}$?

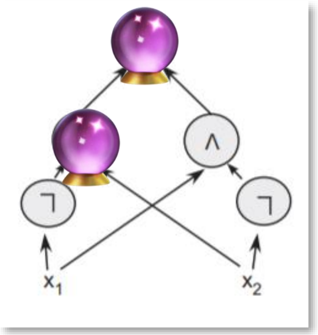
[Hirahara18]: If $\mathrm{GapMCSP}$ is $\mathbf{NP}$-hard, then the worst- and average-case complexity of $\mathbf{NP}$ are equivalent.

Minimum Oracle Circuit Size Problem

- "Approaching MCSP from above" [Ilango'20]
- Given a function f and an oracle O, compute the O-oracle circuit complexity of f 

x	$\mathbf{0}^n$	...	$\mathbf{1}^n$
f	$f(0^n)$	...	$f(1^n)$

x	$\mathbf{0}^m$	...	$\mathbf{1}^m$
O	$O(0^m)$	...	$O(1^m)$



- A "testing ground" for MCSP?
  - $\mathbf{NP}$-hardness of MOCSP under deterministic reductions $\Longrightarrow$ $\mathbf{EXP} \neq \mathbf{ZPP}$ (still!)
  - [Ilango'20]: $\mathbf{NP}$-hard under randomized reductions! 

Hardness of Approximation…?

Yes instances: complexity $\leq s$
No instances: complexity $\geq 2^{(1-\varepsilon)n} s$
$\left(s \text{ vs } 2^{(1-\varepsilon)n} s\right)$

Theorem (Hirahara'18): If $\boxed{\mathrm{Gap}_\varepsilon}\mathrm{MCSP}$ is $\mathbf{NP}$-hard for every $\varepsilon > 0$, then Heuristica doesn't exist.

$(s \text{ vs } 0.1n \cdot s)$

Theorem (Ilango'20): $\boxed{\mathrm{Gap}}\mathrm{MOCSP}$ is $\mathbf{NP}$-hard!

Comment: reduction from set cover, so $\Theta(\log N)$-approx is optimal

$\left(s \text{ vs } 2^{(1-\varepsilon)n} s\right)$

This work: $\boxed{\mathrm{Gap}_\varepsilon}\mathrm{MOCSP}$ is $\mathbf{NP}$-hard for every $\varepsilon > 0$!

Yes instances: exactly computed by size s
No instances: hard on average against size $2^{(1-\varepsilon)n} s$

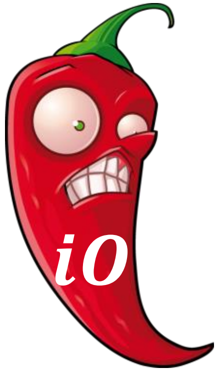
Why Cryptography Helps

Intuition I: “Structured” Hardness

- If we “merely” assume circuit lower bounds, seems unclear how to use it and prove MCSP is $\mathbf{NP}$-hard.
- What if we assume cryptographic hardness?

Intuition II: Arguments

- Argument systems = $\mathbf{NP}$-hardness of “meta-complexity”
- More on the next slide ☺



Warm-Up: Arguments = $\mathbf{NP}$-Hardness of Meta-Complexity

- Arguments: proof systems sound against computationally bounded provers

An argument system for L

- L: some language in $\mathbf{NP}$
- $x \in L$: $\exists$ a size-s prover (with a witness of x) that convinces the verifier
- $x \notin L$: any size-s^{10} prover cannot convince the verifier (except with negl probability)

L reduces to "meta-complexity"

- "meta-complexity" problem: what's the complexity of convincing the verifier?
- $x \in L$: complexity $\leq s$
- $x \notin L$: complexity $> s^{10}$

Remark 1: hardness of approximation! (Arbitrarily large inapprox, by adjusting the security parameter)

Remark 2: the No instances are average-case hard! Any size-s^{10} prover has only negl prob of convincing the verifier

Witness Encryption

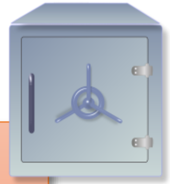
- Encryption using a (public) SAT instance!

Intuition: encrypt a message, but anyone knowing the solution to a Sudoku puzzle / a proof of Riemann Hypothesis can decrypt!

- $\text{Encrypt}(\varphi, msg; rand) \to ct$
- $\text{Decrypt}(\varphi, \alpha, ct) \to msg$

Assumption: Encrypt is randomized, but Decrypt is not

Correctness: If $\varphi(\alpha) = 1$, then Decrypt outputs the correct msg.



Security: If φ is unsatisfiable, then $\text{Encrypt}(\varphi, 0) \approx_c \text{Encrypt}(\varphi, 1)$.

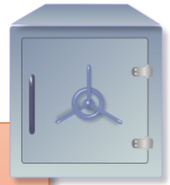
Oracle Witness Encryption

- Everybody has access to a (specifically designed) oracle $\mathcal{O}$
- $\mathrm{Encrypt}^{\mathcal{O}}(\varphi, msg; rand) \to ct$
- $\mathrm{Decrypt}^{\mathcal{O}}(\varphi, \alpha, ct) \to msg$

Caveat: the oracle fan-in is only $O(\lambda)$ where $\lambda \sim \log|\varphi|$ is the security parameter

Oracle length $= 2^{O(\lambda)} = \mathrm{poly}(|\varphi|)$
Need exponential security ($2^{\Omega(\lambda)}$)!

Correctness: If $\varphi(\alpha) = 1$, then $\mathrm{Decrypt}^{\mathcal{O}}$ outputs the correct msg.



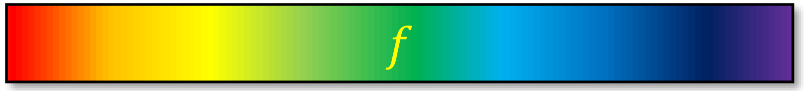
Security: If φ is unsatisfiable, then $\mathrm{Encrypt}^{\mathcal{O}}(\varphi, 0) \approx_c \mathrm{Encrypt}^{\mathcal{O}}(\varphi, 1)$.

Hope 1: if we design $\mathcal{O}$ carefully, then oracle witness encryption unconditionally exists…?

Hope 2: if oracle witness encryption exists, then MOCSP is $\mathbf{NP}$-hard (with large approx gap)?

Oracle WE $\Longrightarrow$ NP-hardness of MOCSP

- Given an instance φ, want to produce an instance (f, O)
  - φ is satisfiable if and only if f has small O-oracle circuit complexity!



(random truth table)

If φ is satisfiable, then by correctness of witness encryption, f has a small O-oracle circuit:

$f(i)$:
- Hardcode a witness α of φ
- Query O_2 to obtain $ct = \mathrm{Encrypt}^{O_1}(\varphi, f(i))$
- Run $\mathrm{Decrypt}^{O_1}(\varphi, \alpha, ct)$ and obtain $f(i)$

O

O_1: the oracle under which witness encryption exists

$O_2(i, j) = j$-th bit of $\mathrm{Encrypt}^{O_1}(\varphi, f_i)$

If φ is unsatisfiable, then any small O-oracle circuit for f violates the security of witness encryption! (Need a non-trivial proof)

How to construct oracle WE?

- Look at candidate witness encryptions in literature one by one, and find oracles that make them secure

Witness Encryption and its Applications

Sanjam Garg, UCLA
Craig Gentry[*], IBM Watson
Amit Sahai[†], UCLA
Brent Waters[‡], U.T. Austin

- GGSW works!
- GGSW uses multilinear maps, so our oracle implements the **generic multilinear map model**.
- Security proof highly non-trivial.

GGSW Witness Encryption

Starting point: $\mathrm{Exact\_Cover}$
- Input: universe $[n]$ and "pieces" $X_1, X_2, \ldots, X_m \subseteq [n]$
- Decide: Are there pieces $X_{i_1}, X_{i_2}, \ldots, X_{i_k}$ that exactly covers $[n]$?
  - (Their disjoint union is exactly $[n]$)

Idea
- Assign a random number r_i to element $i \in [n]$
- $r(S) \coloneqq \sum_{i \in S} r_i$
- Announce $r([n])$ and each $r(X_i)$ to the public
- Decryption reduces to finding $i_1, i_2, \ldots, i_k$ such that $r([n]) = r(X_{i_1}) + r(X_{i_2}) + \cdots + r(X_{i_k})$

Implementation
- $r_1, \ldots, r_n, r_{n+1}, r_{n+2} \leftarrow$ random numbers
- Wlog assume $msg \in \{n+1, n+2\}$
- Announce r_{n+1}, r_{n+2}, $r([n] \cup \{msg\})$, and each $r(X_i)$ to the public

Decryption:
1. Find $r([n]) = r(X_{i_1}) + \cdots + r(X_{i_k})$
2. Compare $r([n] \cup \{n+1\})$ and $r([n] \cup \{n+2\})$ with $r([n] \cup \{msg\})$

Unconditional security?
Use oracle to obfuscate the + operation!

Multilinear Map

- Groups $\mathbb{G}_1, \mathbb{G}_2, \dots, \mathbb{G}_{n+1}$, each $\mathbb{G}_i$ is the cyclic group of order p
- Each group $\mathbb{G}_i$ is paired with a random bijection $\sigma_i : \mathbb{G}_i \to [p]$
- For a set S, use the $|S|$-th group to obfuscate $r(S) = \sum_{i \in S} r_i$
- Multilinear map:

Intuition: $\sigma_i(j)$ is the label of j.
Given $\sigma_i(j)$, it's hard to infer j back

"Obfuscation of $r(S)$" $= \sigma_{|S|}\big(r(S)\big)$

$$e_{i,j} : [p] \times [p] \to [p], \qquad e_{i,j}\Big(\sigma_i(a), \sigma_j(b)\Big) = \sigma_{i+j}(a+b)$$

$\big(i, j, \sigma_i(a), \sigma_j(b)\big)$ →  → $\sigma_{i+j}(a+b)$

Note: this enables us to compute $\sigma_{i_1+i_2+\cdots+i_k}(a_1 + a_2 + \cdots + a_k)$ from $\left\{\sigma_{i_j}(a_j)\right\}$!

GGSW, revisited

Secure Implementation

- $r_1, \dots, r_n, r_{n+1}, r_{n+2} \leftarrow \mathbb{G}_1$
- Wlog assume $msg \in \{n+1, n+2\}$
- Announce $\sigma_1(r_{n+1})$, $\sigma_1(r_{n+2})$, $\sigma_{n+1}\left(r([n] \cup \{msg\})\right)$, and each $\sigma_{|X_i|}\left(r(X_i)\right)$ to the public

"Obfuscation of $r(S)$" = $\sigma_{|S|}\left(r(S)\right)$

Intuition: if $\nexists$ exact cover, then $\sigma_n\left(r([n])\right)$ and $\sigma_{|X_i|}\left(r(X_i)\right)$ are "independent"!

$$e_{i,j}: [p] \times [p] \to [p], \qquad e_{i,j}\left(\sigma_i(a), \sigma_j(b)\right) = \sigma_{i+j}(a+b)$$

$\left(i, j, \sigma_i(a), \sigma_j(b)\right)$ →  → $\sigma_{i+j}(a+b)$

Note: this enables us to compute $\sigma_{i_1+i_2+\cdots+i_k}(a_1 + a_2 + \cdots + a_k)$ from $\left\{\sigma_{i_j}(a_j)\right\}$!

Wrap Up

Oracle Witness Encryption

- $\mathrm{Encrypt}^{\mathcal{O}}(\varphi, msg; rand) \to ct$
- $\mathrm{Decrypt}^{\mathcal{O}}(\varphi, \alpha, ct) \to msg$

Oracle WE $\Longrightarrow$ NP-Hardness of MOCSP

O_1: the oracle under which witness encryption exists

$O_2(i, j) = j$-th bit of $\mathrm{Encrypt}^{O_1}(\varphi, f_i)$

Reducing $\mathrm{Exact\_Cover}$ to MOCSP:

- $\mathrm{Exact\_Cover}$ instance: universe $[n]$ and "pieces" $X_1, X_2, \ldots, X_m \subseteq [n]$
- $f \leftarrow$ random truth table
- $O_1 \leftarrow$ generic multilinear map model

$\boxed{\big(i, j, \sigma_i(a), \sigma_j(b)\big)} \rightarrow$  $\rightarrow \boxed{\sigma_{i+j}(a+b)}$

- $O_2 \leftarrow$ stores the ciphertexts
  - Obfuscations of r_{n+1}, r_{n+2}, $r([n] \cup \{f(i)\})$, and each $r(X_i)$
- $O \leftarrow O_1 \cup O_2$

Summary

For complexity theorists: new techniques for **NP**-hardness of meta-complexity!

For cryptographers: YOU can make progress on central problems in meta-complexity!

GGSW

"generic multilinear map"

Oracle witness encryption (with unconditional security!)

(unconditional) **NP**-hardness of $\mathrm{GapMOCSP}$

- Large inapprox gap
- Average-case hardness in the No case

Thank you!

Questions are welcome!

Discussion 1: PCP Theorems from Meta-Complexity?

Previous results

- Starts from inapprox results (using PCP theorem)
- Weak hardness of approx (s vs $0.1s \log N$)

Our results

- Strong hardness of approx ($N^{0.0001}$ vs $N^{0.9999}$)
- Direct reduction from $\mathrm{Exact\_Cover}$

GapMOCSP

- Yes instances: f admits size-s O-oracle circuits
- No instances: f is 0.9-avg hard against size-$2s$ O-oracle circuits

PCP Theorem from Meta-Complexity?

Randomly choose x and verify $C^O(x) = f(x)$…

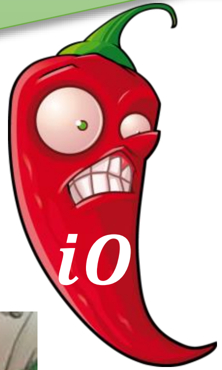
Wait, computing $C^O(x)$ takes too much time ☹

Discussion 2: MCSP?

Question: Is MCSP **NP**-complete under "reasonable" crypto assumptions?

What are "reasonable" assumptions?

Arguments? What type of arguments do we need?



Combinations of fancy cryptos?