Meta-Complexity as a Tool in the Foundations of Cryptography

Rahul Santhanam

(University of Oxford)

Plan of the Talk

- Background and Motivation
- Meta-Complexity and One-Way Functions
- Applications of Crypto to Meta-Complexity
- Future Directions

Plan of the Talk

- *Background and Motivation*
- Meta-Complexity and One-Way Functions
- Applications of Crypto to Meta-Complexity
- Future Directions

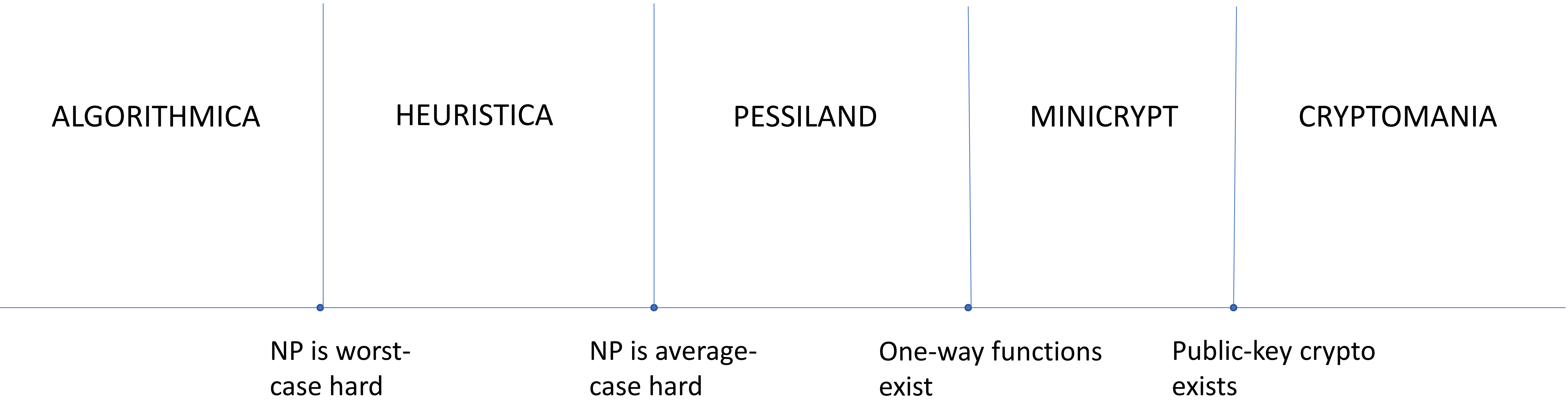
Cryptographic Foundations

- Theory of cryptography is one of the most successful areas of theoretical computer science
- Principled protocols for a variety of cryptographic tasks, including private-key encryption, public-key encryption, pseudorandom generation, zero-knowledge proofs, secure multi-party computation, homomorphic encryption, indistinguishability obfuscation etc.
- These protocols are often built out of a small number of basic primitives, such as one-way functions, trapdoor functions and oblivious transfer, for each of which there are many candidate constructions based on computational hardness of natural problems (such as Factoring, lattice problems, Planted Constraint Satisfaction)

Some Fundamental Questions that Remain

- Can assumptions be reduced even further? Can public-key encryption be based on one-way functions, and one-way functions on NP ≠ P? There is a rich theory of black-box reductions, but how much does this tell us?
- Standard assumptions for tasks such as indistinguishability obfuscation? Much progress recently, but we still don’t have a clear picture
- More generally, how much can we bridge complexity theory and cryptography? By this we mean using assumptions that are about standard complexity classes, or about problems that play important roles in complexity theory

Impagliazzo’s Five Worlds



ALGORITHMICA

HEURISTICA

PESSILAND

MINICRYPT

CRYPTOMANIA

NP is worst-case hard

NP is average-case hard

One-way functions exist

Public-key crypto exists

World Annihilation?

- Current proof techniques cannot properly distinguish between Algorithmica and Cryptomania: we might live in a world where everything is easy or we might live in a world where problems are generically hard
- However, we could hope to simplify the picture by ruling out intermediate worlds

A Dream Scenario for Foundations of Crypto

- Minimal Foundations for Cryptography: For each cryptographic primitive, find complexity-theoretic hardness assumptions that are both necessary and sufficient, in both classical and post-quantum worlds
- These hardness assumptions should relate to natural complexity-theoretic problems. Average-case hardness assumptions ok, though worst-case hardness assumptions would be better
- Potential way to attack longstanding open problems, eg., annihilating Impagliazzo’s worlds

The Role of Meta-Complexity

- Which computational problems to consider when working toward the dream scenario?
- For standard combinatorial NP-hard problems, it seems hard to come up with natural distributions for which hardness can be connected to crypto primitives
- For structured problems such as Factoring or LWE, it is unclear whether their hardness gives a characterization of any given crypto primitive
- Most suitable problems seem to be *meta-complexity* problems

What is Meta-Complexity?

- Complexity of computational problems that are themselves about complexity, eg., the Minimum Circuit Size Problem (MCSP) and the problem K of determining the Kolmogorov complexity of a string
  - These problems seem both hard to *solve* and hard to *understand*
- In some sense, these problems are about measuring the inherent randomness/lack of structure in an object, which does seem relevant to cryptography
- A nice feature of these problems is that the uniform distribution is a candidate hard distribution

Meta-Complexity Problems

- MCSP: Given the truth table of a Boolean function F, and a parameter s, does F have Boolean circuits of size s?
- K: Given a string x and a parameter s, does x have Kolmogorov complexity at most s?
  - K(x) = min{|p|: U(p, ε) = x} (where U is a universal Turing machine we fix in advance)
- K^t: Given a string x and a parameter s, does x have time t-bounded Kolmogorov complexity at most s (where t is a polynomially bounded function we fix in advance)?
  - $K^t(x)$ = min{|p|: U(p, ε) outputs x within t(|x|) steps}
- Kt: Given a string x and a parameter s, is Kt(x) [Levin84] at most s?
  - Kt(x) = min{|p|+log(t): U(p, ε) outputs x within t steps}

Meta-Complexity Problems (Parameterized Versions)

- MCSP[s]: Given the truth table of a Boolean function F, does F have Boolean circuits of size s?
- K[s]: Given a string x, does x have Kolmogorov complexity at most s?
  - $K(x) = \min\{|p| : U(p, \varepsilon) = x\}$ (where U is a universal Turing machine we fix in advance)
- $K^t[s]$: Given a string x, does x have time t-bounded Kolmogorov complexity at most s (where t is a polynomially bounded function we fix in advance)?
  - $K^t(x) = \min\{|p| : U(p, \varepsilon) \text{ outputs } x \text{ within } t(|x|) \text{ steps}\}$
- Kt[s]: Given a string x, is Kt(x) [Levin84] at most s?
  - $Kt(x) = \min\{|p| + \log(t) : U(p, \varepsilon) \text{ outputs } x \text{ within } t \text{ steps}\}$

Questions

- What is the complexity of these problems? Are they hard for natural complexity classes? Are they hard unconditionally for weak models of computation?
- How do these problems relate to each other?
- How is the complexity of these problems relevant to cryptography, learning theory, circuit complexity, proof complexity, etc.?

Computational Problems about Complexity

- MCSP: Given the truth table of a Boolean function F, and a parameter s, does F have Boolean circuits of size s?
  - In NP; unknown if NP-complete
- K: Given a string x and a parameter s, does x have Kolmogorov complexity at most s?
  - Uncomputable
- K^t: Given a string x and a parameter s, does x have time t-bounded Kolmogorov complexity at most s (where t is a polynomially bounded function we fix in advance)?
  - In NP; unknown if NP-complete
- Kt: Given a string x and a parameter s, is Kt(x) at most s?
  - In EXP; complete for EXP with respect to poly-size reductions [ABKvMR06]

Some Historical Landmarks

- Pre-history: [Trakhtenbrot84] surveyed how meta-complexity was a focus of research in the Soviet world from as early as the 1950s
- Natural Proofs: the "natural proofs" barrier of Razborov and Rudich [RR97] indicated deep links between meta-complexity, cryptography and proof complexity
- The Minimum Circuit Size Problem: first defined and studied by Kabanets and Cai [KC00]
- Power from Random Strings: [ABKvMR06] showed that natural variants of Kolmogorov complexity are complete for standard classes such as PSPACE and EXP
- Learning from Natural Proofs: [CIKK16] showed how to get learning algorithms for a circuit class C from natural proofs useful against C

Plan of the Talk

- Background and Motivation
- *Meta-Complexity and One-Way Functions*
- Applications of Crypto to Meta-Complexity
- Future Directions

Meta-Complexity and Crypto

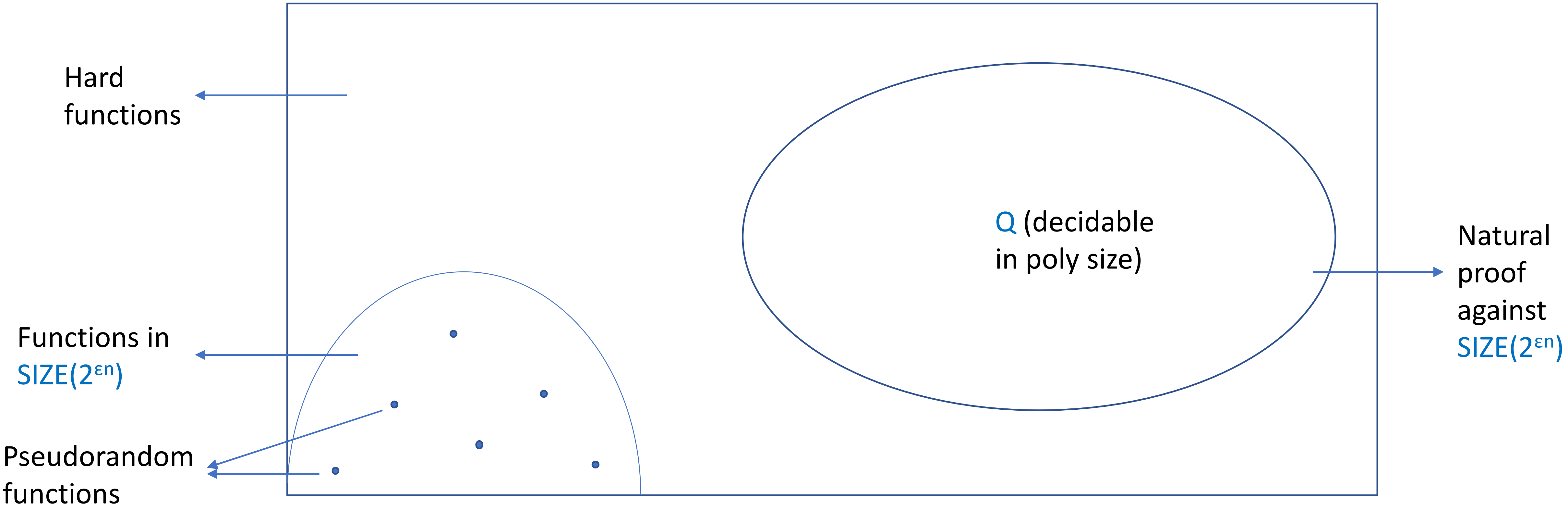
- The existence of one-way functions (OWFs) turns out to be closely related to the average-case complexity of meta-complexity problems
- The first such connection is implicit in the “Natural Proofs” paper of Razborov and Rudich [RR97]
- They implicitly show that if OWFs exist, then for each $\varepsilon > 0$, MCSP[$2^{\varepsilon n}$] is zero-error hard on average over the uniform distribution

Average-Case Complexity of MCSP

- There is a natural distribution on inputs to MCSP, namely the uniform distribution
- However, under this distribution, MCSP[s] is highly biased (since most Boolean functions are hard) for any reasonable s
- Hence we adopt a *zero-error* notion of average-case complexity
  - We say MCSP[s] is average-case hard if for any sequence of polynomial-size Boolean circuits that, on each input, either answer correctly or output ‘?’, there is a negligible fraction of inputs on which a non-’?’ answer is given
- Proposition [HS17]: MCSP[$2^{\varepsilon n}$] is average-case hard iff natural proofs against SIZE($2^{\varepsilon n}$) do not exist

Natural Proofs: Main Theorem of [RR97]

Lemma [GGM86]: If one-way functions exist, then for each $\varepsilon > 0$ there is pseudorandom function family in SIZE($2^{\varepsilon n}$) against SIZE($2^{O(n)}$)


Hard functions
Functions in SIZE($2^{\varepsilon n}$)
Pseudorandom functions
Q (decidable in poly size)
Natural proof against SIZE($2^{\varepsilon n}$)

Q distinguishes random from pseudorandom, and is poly-time computable. Contradiction!

OWFs and Hardness of MCSP

- [RR97] result shows that OWFs imply average-case hardness of MCSP
- Could there be a converse? If so, zero-error average-case hardness of MCSP would be a characterizing hardness assumption for OWFs, and we would make progress toward our dream scenario
- In [S20], I showed that this is the case if a certain "Universality Conjecture" about pseudorandom sets supported on easy functions holds. This would yield a very clean picture, with equivalences between hardness of MCSP for various size parameters, existence of OWFs and impossibility of learning circuits over the uniform dist
- However, status of the conjecture is unclear

The Liu-Pass Breakthrough

- Liu and Pass [LP20] obtained an unconditional characterization of one-way functions by hardness of a meta-complexity problem!
- They work with (the function version of) K^t rather than with MCSP, and crucially use *bounded-error* average-case hardness rather than zero-error average-case hardness
- We say that K^t is mildly average-case hard to compute if any probabilistic poly-time algorithm A fails to compute K^t on at least an inverse polynomial fraction of instances
- Theorem [LP20]: There is poly bounded t such that K^t is mildly average-case hard to compute iff OWFs exist

The Liu-Pass Construction

- The construction of OWF f is very direct: Given p of length n and an integer r in $[n]$, $f(p,r) = (U^t(p|_{r,}\ \varepsilon)\ ,\ r)$, where $p|_r$ is the r-bit prefix of p
- Intuitively, we just run the r-bit prefix of the input program for t steps and output the answer together with r
- To show that mild average-case hardness of K^t implies that f is a weak OWF, suppose that some probabilistic poly time algorithm A inverts f on almost all instances
  - We can compute the K^t complexity of x for almost all instances x by running the inversion algorithm on (x,r) for all r in $[n]$, and outputting the minimum r for which the inversion algorithm succeeds

The Liu-Pass Construction

- The construction of OWF f is very direct: Given p of length n and an integer r in $[n]$, $f(p,r) = (U^t(p|_{r,}\ \varepsilon)\ ,\ r)$, where $p|_r$ is the r-bit prefix of p
- Intuitively, we just run the r-bit prefix of the input program for t steps and output the answer together with r
- To show that K^t is mildly average-case hard if f is an OWF, use [HILL99] to construct PRG G based on f and use a presumed average-case algorithm for K^t to break G
    - This is not straightforward because the average-case algorithm is *bounded-error* – some work is needed to make sure the generator is "entropy-preserving"

Takeaways from Liu-Pass

- Proof of principle that standard crypto primitives can be characterized by complexity assumptions on natural problems
  - Raises the question of whether average-case hardness of other meta-complexity problems is also connected to crypto?
- Yields some non-trivial robustness results for the K^t problem
  - The functional version and the decision versions for $s = n-O(\log(n))$ are equivalent in complexity

How about MCSP?

- It would be very interesting to show an analogue of [LP20] for MCSP
- One challenge with working with MCSP is that circuit size is not known to be tightly concentrated around its expectation, and the tight concentration of time-bounded Kolmogorov complexity plays a crucial role in [LP20]
- In [RS21], we consider the MKTP problem, which is a Kolmogorov version of MCSP [Allender01]
- Theorem [RS21]: MKTP is mildly hard on average iff there are OWFs in NC^0

How about MCSP?

- Theorem [RS21]: MKTP is mildly hard on average iff there are OWFs in NC^0
- We crucially use the fact that “typical” strings are computed from their shortest programs in a small amount of time, which then allows us to exploit the randomizing polynomials machinery of [AIK06]
- We also derive OWFs in NC^0 from exponential average-case hardness of MCSP, and a partial converse as well, but we don’t get an equivalence in this case
- Moreover, we give fine-grained equivalences enabling us to get OWFs with almost maximal hardness from plausible meta-complexity assumptions

The Case of Kt

- Kt is complete for EXP, and hence we might not expect its average-case complexity to be related to crypto
- Somewhat surprisingly, the mild average-case hardness of Kt also turns out to be equivalent to OWFs [RS21, LP21] !
  - Intuitively, the reason is that "typical" strings are produced from their optimal programs in polynomial time, and hence the average-case complexity of Kt and the average-case complexity of K^{poly} behave similarly
- [LP21] build on earlier work of [ABKvMR06] to show that *zero-error* average-case hardness of Kt is equivalent to EXP ≠ BPP!

A Different Approach to Characterizing OWFs

- [LP20] and approaches that build on it use hardness assumptions tailored to a specific distribution, i.e., the uniform distribution. Can similar results be shown for other distributions?
- Theorem [IRS22] : The following are equivalent
  - OWFs exist
  - Kolmogorov complexity is hard to $\omega(\log(n))$-additively approximate over some samplable distribution
  - Kolmogorov complexity is hard to $n^{1-\varepsilon}$-multiplicatively approximate over some samplable distribution for some $\varepsilon > 0$
- Note that Kolmogorov complexity is *uncomputable* in the worst case, yet its average-case complexity characterizes OWFs!

OWFs from Samplers

- The approach in [IRS22] departs fundamentally from the approach in [LP20, LP21, RS21]
  - In the earlier line of work, the OWF is tailored to the parameters of the meta-complexity problem, and the security of the OWF follows from the average-case hardness assumption over the uniform distribution
  - In [IRS22], the OWF is defined based on the sampler for the hard distribution, and the security of the OWF corresponds to the parameters of the meta-complexity problem
- The latter approach shows that meta-complexity problems are very robust in terms of average-case complexity, when considering hardness with respect to samplable distributions

An Equivalence for MCSP

- Theorem [IRS22]: For any $\varepsilon > 0$, OWFs exist iff Circuit Size is hard to $N^{3\varepsilon}$-multiplicatively approximate over some N^{ε}-locally samplable distribution
- Our techniques seem to require that the meta-complexity notion is “stronger” than the sampler in terms of computational power

Plan of the Talk

- Background and Motivation
- Meta-Complexity and One-Way Functions
- *Applications of Crypto to Meta-Complexity*
- Future Directions

Connecting i0 and MCSP

- Theorem [IKV18, KMNPRY14]: If MCSP in ZPP and iO exists, then SAT in ZPP
- Note that NP-hardness of MCSP is a long-standing open problem – the theorem above shows that MCSP is “effectively” NP-complete if iO exists

Secret Sharing and the Quest for NP-Completeness

- Theorem [H22]: The “partial function” version of MCSP is NP-complete
- Partial function version: the truth table is allowed to have ? in addition to 0 and 1
- Proof of theorem relies heavily on results about monotone secret sharing

Plan of the Talk

- Background and Motivation
- Meta-Complexity and One-Way Functions
- Applications of Crypto to Meta-Complexity
- *Future Directions*

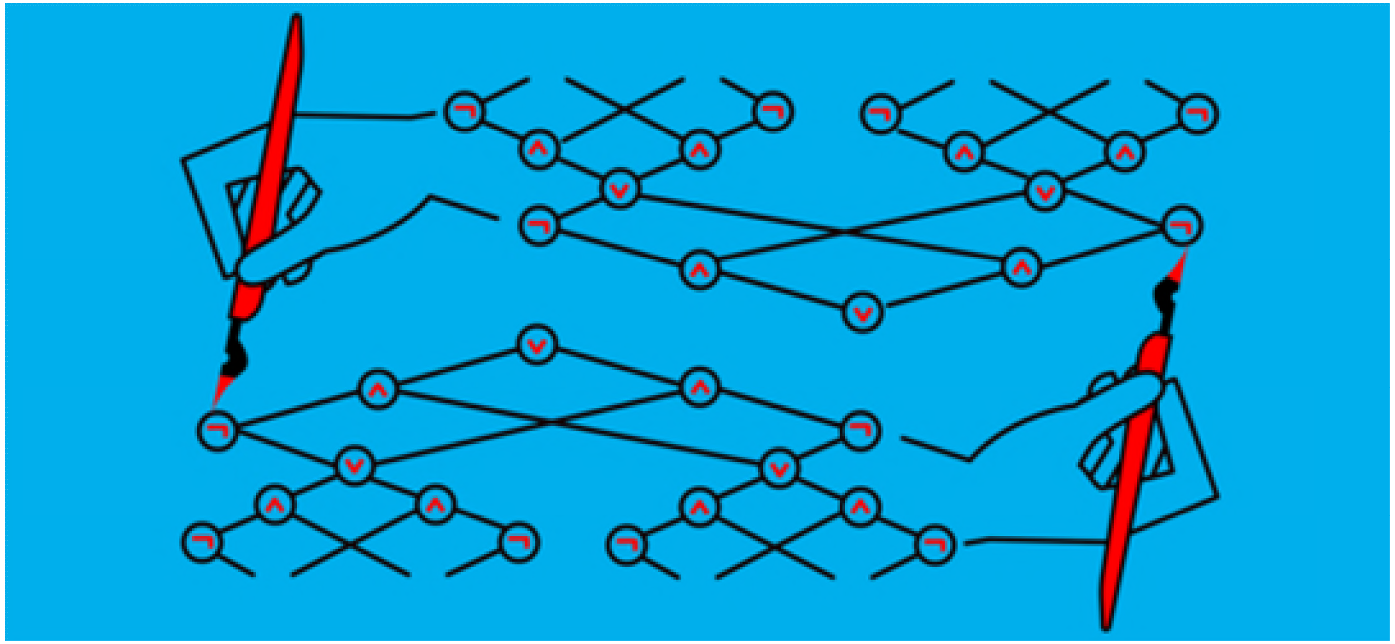
Open Problems

- It would be interesting to have characterizations of other crypto notions using meta-complexity, eg., public-key crypto or XiO
- Are there characterizations of OWFs or other crypto primitives based on worst-case complexity of natural computational problems?
- Are there examples of other natural average-case hard problems, perhaps even combinatorial ones, that characterize OWFs? This would be analogous to Karp's theory of NP-completeness
- Explore other applications of iO and other crypto assumptions in complexity theory

Open Problems

- Might it be possible to build practical cryptosystems from minimal assumptions?
- Does the meta-complexity perspective lead to new possibilities for post-quantum crypto?
- There has been a lot of recent work on connections between TFNP and crypto – can we identify any interesting and relevant meta-complexity problems in TFNP?

Advertisement



Simons Semester in Meta-Complexity: Jan 10 – May 12, 2023

Minimal Complexity Assumptions for Crypto: May 1 – May 5
(organised by Yuval Ishai, Yael Tauman Kalai, Rafael Pass)