Capturing One-way Functions via NP-hardness of Meta-Complexity

Shuichi Hirahara
National Institute of Informatics, Japan

@Minimal Complexity Assumptions for Cryptography
May 2, 2023

One-way Function

- f is a one-way function if f is easy to compute but hard to invert *on average*.

  Example: $f(x,y) = x \times y$. $f^{-1} \approx \text{Integer Factorization.}$

- One of the most fundamental cryptographic primitives

- Equivalent to many cryptographic primitives.
  - Pseudorandom generator [Hastad-Impagliazzo-Levin-Luby'99]
  - Pseudorandom function generator [Goldreich-Goldwasser-Micali'86]
  - Private-key encryption
  - Digital signatures [Rompel'90]
  - Commitment schemes [Naor'91]

Worst-case characterization

Question: Can we characterize one-way functions by **worst-case assumptions**?

Main Theorem (informal)

The following are equivalent:

- There exists a one-way function secure against $\mathrm{P/poly}$.
- $\mathrm{NP} \not\subseteq \mathrm{ioP/poly}$, and

  "distributional Kolmogorov complexity ($\mathrm{dK^{poly}}$)" is NP-hard
  (under randomized polynomial-time reductions)

Informally: $\mathrm{dK^{poly}}$ is NP-hard iff Heursitica and Pessiland do not exist.

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

Minicrypt

Pessiland

Heuristica

$$P \neq NP$$

Algorithmica

$$P = NP$$

Impagliazzo’s Five Possible Worlds

[Impagliazzo ’95] classified five possible worlds consistent with our current knowledge.

Cryptomania

Minicrypt

Pessiland

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

☺ Any problem in **NP** can be solved efficiently.
Automated theorem proving is possible.
☹ Impossible to construct a secure cryptosystem.

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Impagliazzo's Five Possible Worlds

☹ There is an intractable problem in **NP**, but
☺ it is possible to construct a public-key cryptosystem.

…ossible worlds
consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto. & ∄ public-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ & ∄ private-key crypto.

("$\mathrm{P} \neq \mathrm{NP}$ on average")

Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

("$\mathrm{P} = \mathrm{NP}$ on average")

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

$\exists$ public-key crypto.

Minicrypt

$\exists$ private-

The "worst" possible world (a pessimistic world)

☹ Impossible to construct a private-key cryptosystem.

☹ **NP** can't be solved efficiently (on average).

Pessiland

$\text{DistNP} \not\subseteq \text{AvgP}$ ("$\text{P} \neq \text{NP}$ on average") & $\nexists$ private-key crypto.

Heuristica

$\text{P} \neq \text{NP}$ & $\text{DistNP} \subseteq \text{AvgP}$ ("$\text{P} = \text{NP}$ on average")

Algorithmica

$\text{P} = \text{NP}$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

$\exists$ public-

Impossible to construct a public-key cryptosystem.

Possible to construct a private-key cryptosystem.

Minicrypt

$\exists$ private-key crypto. & $\nexists$ public-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ ("$\mathrm{P} \neq \mathrm{NP}$ on average") & $\nexists$ private-key crypto.

Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$ ("$\mathrm{P} = \mathrm{NP}$ on average")

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto. & ∄ public-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ & ∄ private-key crypto.

("$\mathrm{P} \neq \mathrm{NP}$

Heuristica

A world where <u>heuristics</u> are efficient

☺ There are efficient heuristics that solve **NP** on average.

☹ Impossible to construct a cryptosystem.

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

("$\mathrm{P} = \mathrm{NP}$ on average")

Algorithmica

$$\mathrm{P} = \mathrm{NP}$$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

The Ultimate Goal of Complexity Theory

is to decide which world corresponds to our world.

(In particular, we would like to resolve the conjecture that our world is Cryptomania.)

Heuristica

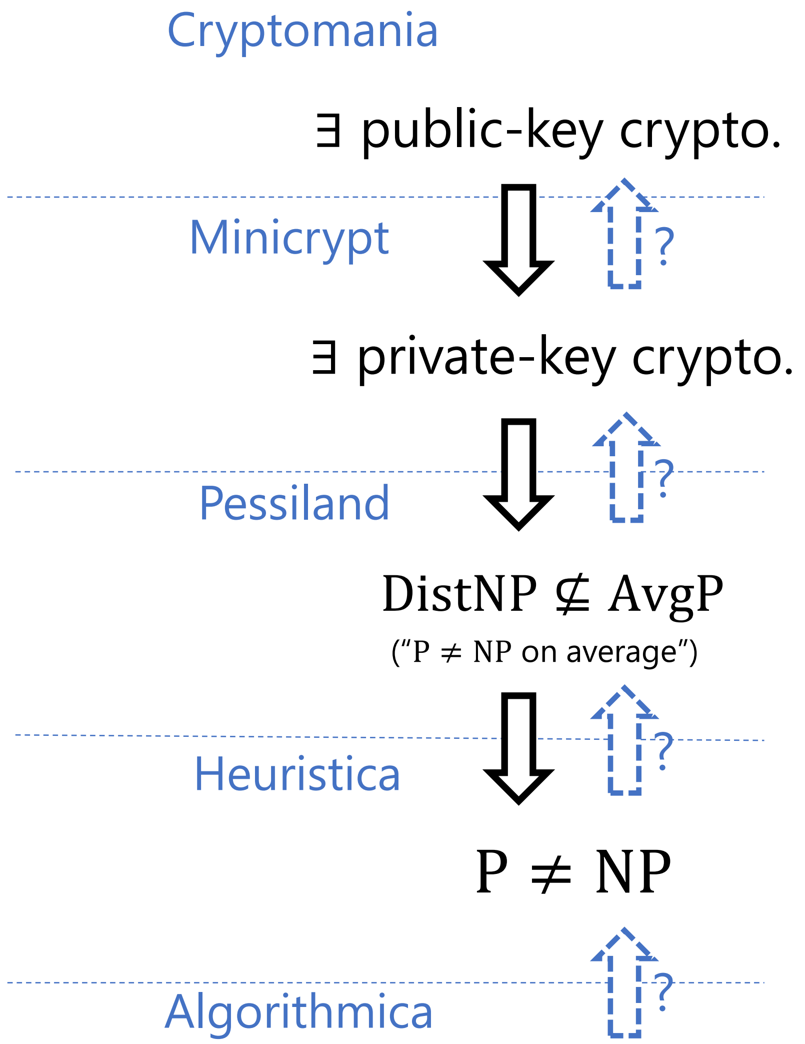
$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

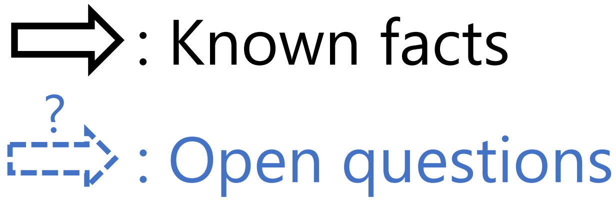
("P = NP on average")

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Known Facts and Open Questions





Toward Public-key Crypto.

⇨ : Known facts

? ⇨ : Open questions

Cryptomania

∃ public-key crypto.

Minicrypt

Important Open Question

Can we exclude Minicrypt?

∃ private-key crypto.

Pessiland

Important Open Question

Can we exclude Pessiland?

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

(“$\mathrm{P} \neq \mathrm{NP}$ on average”)

Heuristica

Important Open Question

Can we exclude Heuristica?

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

Important Open Question

$\mathrm{P} \neq \mathrm{NP}$ (Can we exclude Algorithmica?)

Proving the four implications

⟺

Our world is Cryptomania!

Proving one implication

⟺

Excluding one world

Toward Public-key Crypto.

⇨ : Known facts

⇢? : Open questions

Cryptomania

∃ public-key crypto.

Minicrypt

Important Open Question

Can we exclude Minicrypt?

∃ private-key crypto.

Pessiland

Important Open Question

Can we base the security of a one-way function on the worst-case hardness of NP?

Heuristica

$P \neq NP$

Algorithmica

Important Open Question

$P \neq NP$ (Can we exclude Algorithmica?)

Proving the four implications

$\Leftrightarrow$

Our world is Cryptomania!

Proving one implication

$\Leftrightarrow$

Excluding one world

Limits of Current Proof Techniques

⇨ : Known facts

? : Open questions

✕ : Barrier results

Several types of proof techniques are insufficient to resolve the open question.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

(“$\mathrm{P} \neq \mathrm{NP}$ on average”)

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

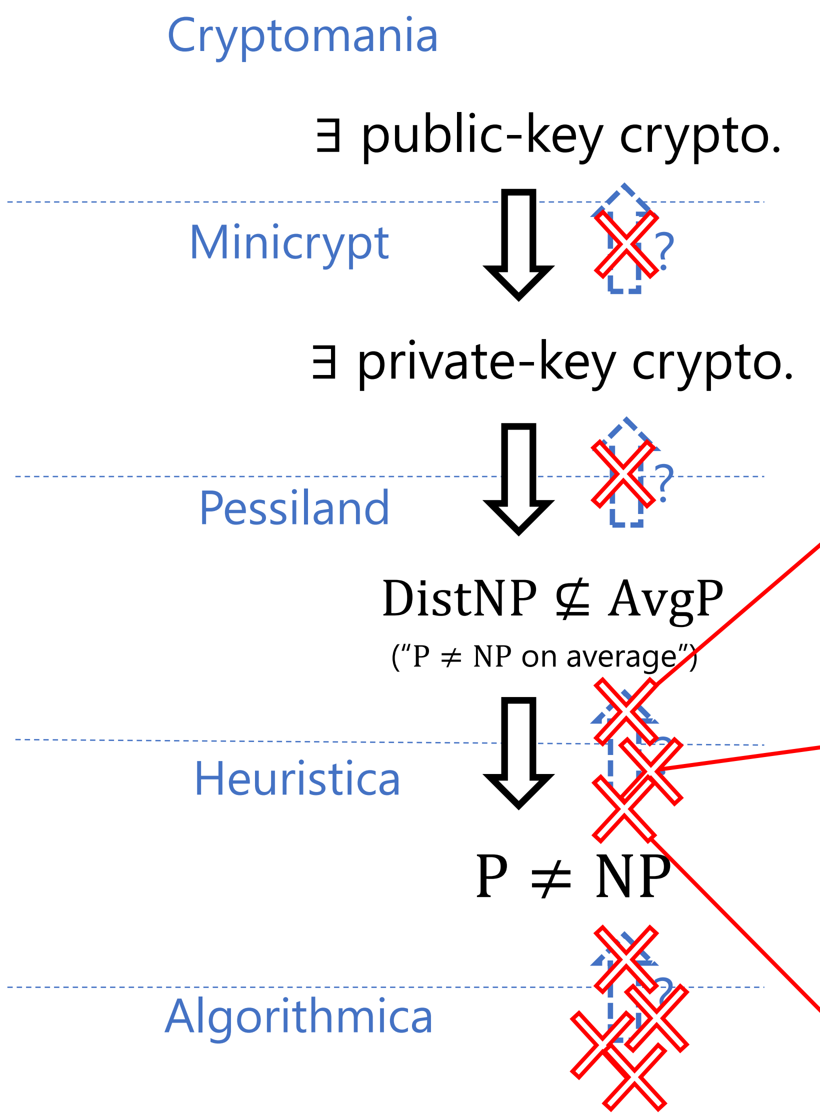
Relativization barrier [Baker-Gill-Solovay’75]

Algebrization barrier [Aaronson-Wigderson’09]

Natural proof barrier [Razborov-Rudich’97]

Locality barrier [Chen-H.-Oliveira-Pich-Rajgopal-Santhanam (ITCS’20)]

Limits of Current Proof Techniques



⇨ : Known facts

?⇢ : Open questions

✕ : Barrier results

Several types of proof techniques are insufficient to resolve the open question.

Relativization barrier

[Impagliazzo (2011)] [H. & Nanashima (FOCS'21)]

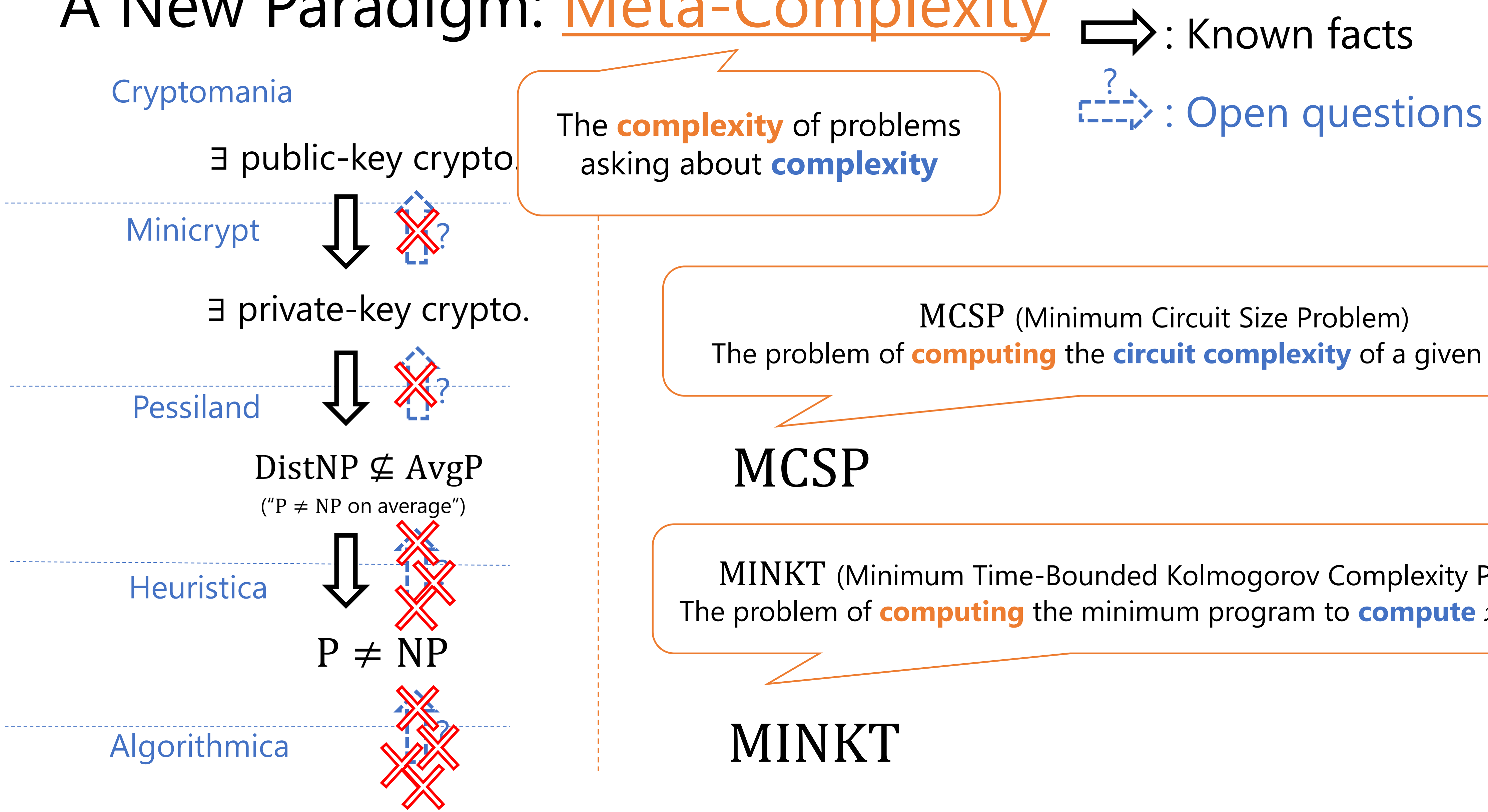
Limits of black-box reductions

[Feigenbaum & Fortnow (1993)]
[Bogdanov & Trevisan (2006)]

"Impossibility" of hardness amplification

[Viola (2005)]

A New Paradigm: Meta-Complexity



The **complexity** of problems asking about **complexity**

MCSP (Minimum Circuit Size Problem)
The problem of **computing** the **circuit complexity** of a given function f

MCSP

MINKT (Minimum Time-Bounded Kolmogorov Complexity Problem)
The problem of **computing** the minimum program to **compute** x efficiently

MINKT

Overcoming Limits of Black-box Reductions

Cryptomania

$\exists$ public-key crypto.

Minicrypt

$\exists$ private-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgBPP}$

("P ≠ NP on average")

Heuristica

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica

BPP — **Worst-case complexity**
(measures the runtime on the worst-case input)

AvgBPP — **Average-case complexity**
(measures the average-case runtime)

Theorem [H. (FOCS 2018)]
Worst- and average-case complexities of MCSP are equivalent.

$(\mathrm{MCSP}, \mathcal{U}) \notin \mathrm{AvgBPP} \iff \mathrm{GapMCSP} \notin \mathrm{BPP}$

Limits of
black-box reductions

[Bogdanov & Trevisan (2006)]

Any problem reducible to DistNP is in $\mathrm{NP/poly} \cap \mathrm{coNP/poly}$.

Conjecture: $\mathrm{GapMCSP} \notin \mathrm{coNP/poly}$ [Rudich'97]

[H. (FOCS'18)] is the first result that goes beyond the limits!

An Approach Towards Excluding Heuristica

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto.

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgBPP}$

(“P ≠ NP on average”)

Heuristica

$\mathrm{NP} \not\subseteq \mathrm{BPP}$

Algorithmica

BPP **Worst-case complexity**
(measures the runtime on the worst-case input)

AvgBPP **Average-case complexity**
(measures the average-case runtime)

[H. (FOCS 2018)]

$(\mathrm{MCSP}, \mathcal{U}) \notin \mathrm{AvgBPP} \Longleftrightarrow \mathrm{GapMCSP} \notin \mathrm{BPP}$

?

Open Problem

Is GapMCSP NP-hard?

Corollary of [H. (FOCS 2018)]

GapMCSP is NP-hard $\Longrightarrow$ Heuristica doesn’t exist

An Approach Towards Excluding Pessiland

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto.

Pessiland

DistNP $\not\subseteq$ AvgBPP

("P ≠ NP on average")

Heuristica

NP $\not\subseteq$ BPP

Algorithmica

[Impagliazzo-Levin 1990]

$\{\mathrm{Q}^t\} \times \mathrm{PSamp} \not\subseteq \mathrm{HeurBPP}$ $(t = n^{\omega(1)})$

[Liu-Pass (FOCS 2020)]

$(\mathrm{MINKT}, \mathcal{U}) \notin \mathrm{HeurBPP}$

[H. (FOCS 2018)]

$(\mathrm{MCSP}, \mathcal{U}) \notin \mathrm{AvgBPP}$ ⟺ $\mathrm{GapMCSP} \notin \mathrm{BPP}$

Q^t: t-time-bounded universal probability.

$\mathrm{Q}^t(x) \coloneqq \Pr_{d \sim \{0,1\}^t}[U^t(d) = x]$. $-\log \mathrm{Q}^{\mathrm{poly}}(x) \approx \mathrm{pK}^{\mathrm{poly}}(x)$.

Corollary of [Impagliazzo-Levin'90]

Q^t is NP-hard $\Longrightarrow$ Pessiland doesn't exist

(under t'-time reductions, where $t' \ll t$)

$\because$ $(\mathrm{Q}^t, \mathcal{D})$ is DistNP-hard for some $\mathcal{D} \in \mathrm{PSamp}$.

An Approach Towards Excluding Heuristica & Pessiland

Cryptomania

$\exists$ public-key crypto.

[Impagliazzo-Levin 1990]

$\{\mathrm{Q}^t\} \times \mathrm{PSamp} \not\subseteq \mathrm{HeurBPP}$ $(t = n^{\omega(1)})$

Minicrypt

[Liu-Pass (FOCS 2020)]

$\exists$ private-key crypto. $\Longleftrightarrow$ $(\mathrm{MINKT}, \mathcal{U}) \notin \mathrm{HeurBPP}$

Pessiland

[H. (FOCS 2018)]

$\mathrm{DistNP} \not\subseteq \mathrm{AvgBPP}$ $\Longleftarrow$ $(\mathrm{Q}^t, \mathcal{U}) \notin \mathrm{AvgBPP}$ $\Longleftrightarrow$ $\mathrm{GapQ}^t \notin \mathrm{BPP}$

("$\mathrm{P} \neq \mathrm{NP}$ on average")

Heuristica

$\mathrm{NP} \not\subseteq \mathrm{BPP}$

Algorithmica

Corollary of [H.'18] & [Impagliazzo-Levin'90]

Errorless (Avg) **Error-prone (Heur)**

GapQ^t is NP-hard $\Longrightarrow$ **Heuristica** & **Pessiland** do not exist

(under t'-time reductions, where $t' \ll t$)

This doesn't imply $\mathrm{NP} \not\subseteq \mathrm{BPP} \Longrightarrow \exists$ a one-way function.

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypto.

$(L, D) \in \mathrm{AvgP}$ iff
∃ an errorless heuristic scheme A such that
$A(x, \delta)$ outputs $\{L(x), \bot\}$ and $\Pr_{x \sim D}[A(x, \delta) \neq L(x)] \leq \delta$.
(Equivalent to average-polynomial-time [Levin'86])

Errorless Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ ("$\mathrm{P} \neq \mathrm{NP}$ on average") & ∄ private-key crypto.

Errorless Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$ ("$\mathrm{P} = \mathrm{NP}$ on average")

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Impagliazzo's Five Possible Worlds

[Impagliazzo '95] classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ private-key crypt

$(L, D) \in \mathrm{HeurP}$ iff
∃ an (error-prone) heuristic scheme A such that
~~$A(x,\delta)$ outputs $\{L(x), \bot\}$ and~~ $\Pr_{x\sim D}[A(x,\delta) \neq L(x)] \leq \delta$.

Error-prone Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{HeurP}$ & ∄ private-key crypto.
("P ≠ NP on average")

Error-prone Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{HeurP}$
("P = NP on average")

Algorithmica

$\mathrm{P} = \mathrm{NP}$

Impagliazzo's Five Possible Worlds

Minicrypt

$\exists$ private-key crypto. & $\nexists$ public-key crypto.

Error-prone Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{HeurP}$ & $\nexists$ private-key crypto.

("$\mathrm{P} \neq \mathrm{NP}$ on average")

(Errorless Pessiland) ∩ (Error-prone Heuristica)

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$ & $\mathrm{DistNP} \subseteq \mathrm{HeurP}$

These can be excluded from NP-hardness of Q^t.

Errorless Heuristica

$\mathrm{P} \neq \mathrm{NP}$ & $\mathrm{DistNP} \subseteq \mathrm{AvgP}$

("$\mathrm{P} = \mathrm{NP}$ on average")

Algorithmica

$$\mathrm{P} = \mathrm{NP}$$

Another Fundamental Difficulty

Theorem [Saks-Santhanam (CCC'22)]

Under some plausible assumptions, GapQ^t is not NP-hard under t'-time reductions, where $t' \ll t$.

(if the gap is an additive $\omega(\log n)$)

- Remember:

Corollary of [H.'18] & [Impagliazzo-Levin'90]

Errorless (Avg) **Error-prone (Heur)**

GapQ^t is NP-hard $\Longrightarrow$ **Heuristica** & **Pessiland** do not exist
(under t'-time reductions, where $t' \ll t$)

- This approach of excluding Pessiland does not work!

Important Questions Left Unanswered

- Is the approach of using meta-complexity ***necessary***?

  → Yes (NP-hardness of dK^t is necessary for excluding Heuristica & Pessiland)

- Is there a meta-computational problem (other than Q^t) whose NP-hardness is (plausible and) sufficient for excluding Pessiland?

  → NP-hardness of dK^t is sufficient

- Can we close the gap between ***errorless*** and ***error-prone*** average-case complexity?

  → Yes (assuming NP-hardness of dK^t)

Kolmogorov complexity

- The Kolmogorov complexity of a string $x \in \{0,1\}^*$

$$\mathrm{K}(x) \coloneqq \min \{ \, |M| : M \text{ prints } x \, \}.$$

Example: $\mathrm{K}(0 \cdots 0) = \log n + O(1)$ $\leftarrow$ M: print $'0' \times n$

Kolmogorov complexity

- The conditional Kolmogorov complexity of a string $x \in \{0,1\}^*$ given $y \in \{0,1\}^*$

$$\mathrm{K}(x|y) \coloneqq \min\{\,|M| : M \text{ prints } x \text{ on input } y\,\}.$$

Example: $\mathrm{K}(0 \cdots 0) = \log n + O(1)$ $\leftarrow$ M: print $'0' \times n$

- The t-time-bounded Kolmogorov complexity of a string $x \in \{0,1\}^*$

$$\mathrm{K}^t(x) \coloneqq \min\{\,|M| : M \text{ prints } x \text{ in time } t\,\}.$$

- The t-time-bounded distributional Kolmogorov complexity of a string x given $\mathcal{D}$:

$$\mathrm{dK}^t_\lambda(x|\mathcal{D}) \coloneqq \min\left\{|M| : \Pr_{y\sim\mathcal{D}}[M(y) = x] \geq \lambda\right\}.$$

$\lambda \in (0,1]$: a success probability.

$\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}$ (The Meta-complexity Problem of dK)

➢ Informally, $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}$ is the problem of approximating $\mathrm{dK}^t_\lambda(x|\mathcal{D})$.

Input

- A string $x \in \{0,1\}^n$
- A distribution $\mathcal{D}$ on $\{0,1\}^n$
  (represented by a circuit)
- A size parameter $s \in \mathbb{N}$
- A success probability λ

Output

$$\begin{cases} \mathrm{YES} & \text{if } \mathrm{dK}^{\tau(n)}_{\lambda}(x|\mathcal{D}) \leq s \\ \mathrm{NO} & \text{if } \mathrm{dK}^{\tau(n)}_{\lambda-n^{-100}}(x|\mathcal{D}) > (1+\epsilon)\cdot s \end{cases}$$

τ: a polynomial $\quad$ $\epsilon > 0$: a constant.

➢ **Fact:** $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP} \in \mathrm{PromiseMA}$

$\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{A}$ (The Meta-complexity Problem of dK)

- Informally, $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{A}$ is the problem of approximating $\mathrm{dK}^{t}_{\lambda}(x|\mathcal{D})$.

Input

- A string $x \in \{0,1\}^n$
- A distribution $\mathcal{D}$ on $\{0,1\}^n$
  (represented by a circuit)
- A size parameter $s \in \mathbb{N}$
- A success probability λ

Output

$$\begin{cases} \mathrm{YES} & \text{if } \mathrm{dK}^{\tau(n),A}_{\lambda}(x|\mathcal{D}) \le s \\ \mathrm{NO} & \text{if } \mathrm{dK}^{\tau(n),A}_{\lambda-n^{-100}}(x|\mathcal{D}) > (1+\epsilon)\cdot s \end{cases}$$

τ: a polynomial $\epsilon > 0$: a constant.

- **Fact:** $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{A} \in \mathrm{PromiseMA}^{A}$

$A \in \mathrm{P/poly}$

$\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^A$ (The Meta-complexity Problem of dK)

- Informally, $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^A$ is the problem of approximating $\mathrm{dK}_\lambda^t(x|\mathcal{D})$.

Input

- A string $x \in \{0,1\}^n$
- A distribution $\mathcal{D}$ on $\{0,1\}^n$
  (represented by a circuit)
- A size parameter $s \in \mathbb{N}$
- A success probability λ

Output

$$\begin{cases} \mathrm{YES} & \text{if } \mathrm{dK}_\lambda^{\tau(n)}(x|\mathcal{D}, A) \le s \\ \mathrm{NO} & \text{if } \mathrm{dK}_{\lambda - n^{-100}}^{\tau(n)}(x|\mathcal{D}, A) > (1+\epsilon)\cdot s \end{cases}$$

τ: a polynomial $\epsilon > 0$: a constant.

- **Fact:** $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^A \in \mathrm{PromiseMA}^A$ $A \in \mathrm{P/poly}$

The Theorem Statement

Main Theorem

The following are equivalent for any constant $\epsilon > 0$:

- There exists a one-way function secure against $\mathrm{P/poly}$.
- $\mathrm{NP} \not\subseteq \mathrm{ioP/poly}$, and

  "$(1+\epsilon)$-factor approx. of distributional Kolmogorov complexity (dK^{τ}) is NP-hard".

I.e., there exists **a** parametric-honest randomized nonadaptive reduction from NP to $\mathrm{Gap}_{\tau,\epsilon}\mathrm{MdKP}^{A}$ for any polynomial τ and any oracle $A \in \mathrm{P/poly}$.

- Parametric-honest: The size parameter s in any query of the reduction on input length n is at least $n^{0.01}$.
- The reduction must be **independent** of τ and A (so the running time of the reduction $\ll \tau(n)$).

Equivalently:

($\because$ $\exists$ a one-way function $\Longrightarrow \mathrm{NP} \not\subseteq \mathrm{ioP/poly}$)

Main Theorem (rephrased)

Assuming $\mathrm{NP} \not\subseteq \mathrm{ioP/poly}$ (our world is not Algorithmica),
the following are equivalent:

- There exists a one-way function secure against $\mathrm{P/poly}$.

  (Heuristica & Pessiland do not exist)

- "distributional Kolmogorov complexity ($\mathrm{dK^{poly}}$) is NP-hard".

  (NP-hardness of meta-complexity)

➢ NP-hardness of $\mathrm{dK^{poly}}$ characterizes the question of excluding Heuristica & Pessiland.

Proof Techniques in One Slide

- NP-hardness of $\mathrm{dK}^{\mathrm{poly}}$ under ∃ OWF: This is similar to NP-hardness of MCSP^* [H. FOCS'22].
- The converse: Very complicated! (≈ 30 pages proof)
  - We combine a lot of results in the literature.
- **High level idea:** Combine [Nanashima ITCS'21] and [H. FOCS'18]

[Nanashima ITCS'21]

If NP reduces to "avoiding a hitting set generator" via a black-box reduction,
then $\mathrm{NP} \not\subseteq \mathrm{BPP} \Longrightarrow$ ∃ a one-way function.

[H. FOCS'18]

$\mathrm{K}^{\mathrm{poly}}$ reduces to "avoiding a hitting set generator" via a non-black-box reduction.

[This work]

$\Longrightarrow$ $\mathrm{dK}^{\mathrm{poly}}$ reduces to "avoiding a hitting set generator" via a non-black-box reduction.

To combine these proof techniques, we need to develop a theory of non-black-box reductions.

How to Close the Errorless versus Error-prone Gap

- A Key Idea in [Nanashima ITCS'21]: One-way function is testable!

  Given oracle access to A, one can test whether A inverts f or not efficiently:

$$\Pr_{x \sim \{0,1\}^n}\left[A\left(f(x)\right) \in f^{-1}(f(x))\right] \geq \frac{1}{2}?$$

  poly.-time computable

- If we have a reduction to an (auxiliary-input) one-way function, then we obtain an errorless heuristic scheme using the testability.

  (If the oracle does not invert f, then we output $\perp$.)

Meta-Complexity Padding Conjecture

- It remains open whether a one-way function can be characterized by some natural worst-case intractability (instead of NP-hardness).
- Maybe worst-case hardness of approximating $\mathrm{K}^{\mathrm{poly}}$?

  $\mathrm{GapMINKT} \in \mathrm{P} \Leftrightarrow (\mathrm{MINKT}, \mathcal{U}) \in$ AvgP (assuming $\mathrm{E} \not\subseteq \mathrm{ioSIZE}(2^{o(n)})$) [H. FOCS'18]

  $\nexists\, \mathrm{OWF} \Leftrightarrow (\mathrm{MINKT}, \mathcal{U}) \in$ HeurBPP [Liu-Pass FOCS'20]
- We propose a conjecture sufficient for resolving this open question:

Meta-Complexity Padding Conjecture (informal)

$\mathrm{K}^{\mathrm{poly}}$ is reducible to $\mathrm{dK}^{\mathrm{poly}}$ via an approximation-preserving padding reduction R.

$R: x \mapsto (y, \mathcal{D}, s)$

$s > 100 \cdot n$

Yes: $\mathrm{K}^{\mathrm{poly}(|x|)}(x) \le n^{0.01}$ → $\mathrm{dK}^{\mathrm{poly}}(y|\mathcal{D}) \le s$

No: $\mathrm{K}(x) \ge n - 3$ → $\mathrm{dK}^{\mathrm{poly}}(y|\mathcal{D}) > 1.1 \cdot s$

Consequences of the Padding Conjecture

Theorem (informal)

Under the Meta-Complexity Padding Conjecture,
the following are equivalent:

- There exists a one-way function.
- $\mathrm{GapMCSP} \notin \mathrm{BPP}$ (with a very large gap)
- $\mathrm{GapMrKP} \notin \mathrm{BPP}$ ($\mathrm{rK}^{\mathrm{t}}(x)$: a randomized variant of $\mathrm{K}^{\mathrm{t}}(x)$)
  (with a somewhat small gap)
- There exists a hitting set generator.

Proposition: If ∃ OWF secure against $\mathrm{P/poly}$, then Meta-Complexity Conjecture is true.

Paddability of Meta-complexity Problems

- Formula-MCSP is paddable via an approximation-preserving reduction:
  - The KRW (Karchmer-Raz-Wigderson) conjecture:

$$\mathrm{L}(f \diamond g) \approx \mathrm{L}(f) \cdot \mathrm{L}(g)$$

$f \diamond g(x_1, \ldots, x_n) \coloneqq f\big(g(x_1), \ldots, g(x_n)\big)$: block-wise composition

  - The KRW conjecture for $g = \bigoplus_m$ is resolved [Hastad'98].

$$\mathrm{L}(f \diamond \bigoplus_m) \approx \mathrm{L}(f) \cdot m^2.$$

- Open: Can we get a similar padding reduction for MCSP?

Open Questions

- Are meta-complexity problems paddable?

- Can we get a similar characterization using MINcKT (conditional time-bounded Kolmogorov complexity)?

  [Huang-Ilango-Ren'23]: MINcKT is NP-hard if iO exists.

  It suffices to show MINcKT is NP-hard if OWF exists.