

Meta-Complexity Theoretic Approach to Complexity Theory

Shuichi Hirahara

National Institute of Informatics



Meta-Complexity

➤ refers to the (meta-)complexity of problems asking for complexity.

Examples

- Minimum Circuit Size Problem (MCSP) [Kabanets & Cai '00]
≈ “the problem of computing the circuit complexity of a given function f ”
- Minimum Time-bounded Kolmogorov complexity Problem (MINKT) [Ko '91]
≈ “the problem of computing the time-bounded Kolmogorov complexity of a given string x ”

Recent Progress on Meta-Complexity

- Many papers have been published recently. For example:

[H. (FOCS'20)], [Liu & Pass (FOCS'20)], [Ilango (FOCS'20)]
[H. (CCC'20)], [Ilango (CCC'20)], [Saks & Santhanam (CCC'20)],
[Ilango, Loff, Oliveira (CCC'20)], [Kabanets-Koroth-Lu-Myrisiotis-Oliveira (CCC'20)]
[H. (STOC'20)], [Chen-Jin-Williams (STOC'20)]
[H. (ITCS'20)], [Santhaman (ITCS'20)], [Ilango (ITCS'20)],
[Chen-H.-Oliveira-Pich-Rajgopal-Santhanam (ITCS'20)]

...

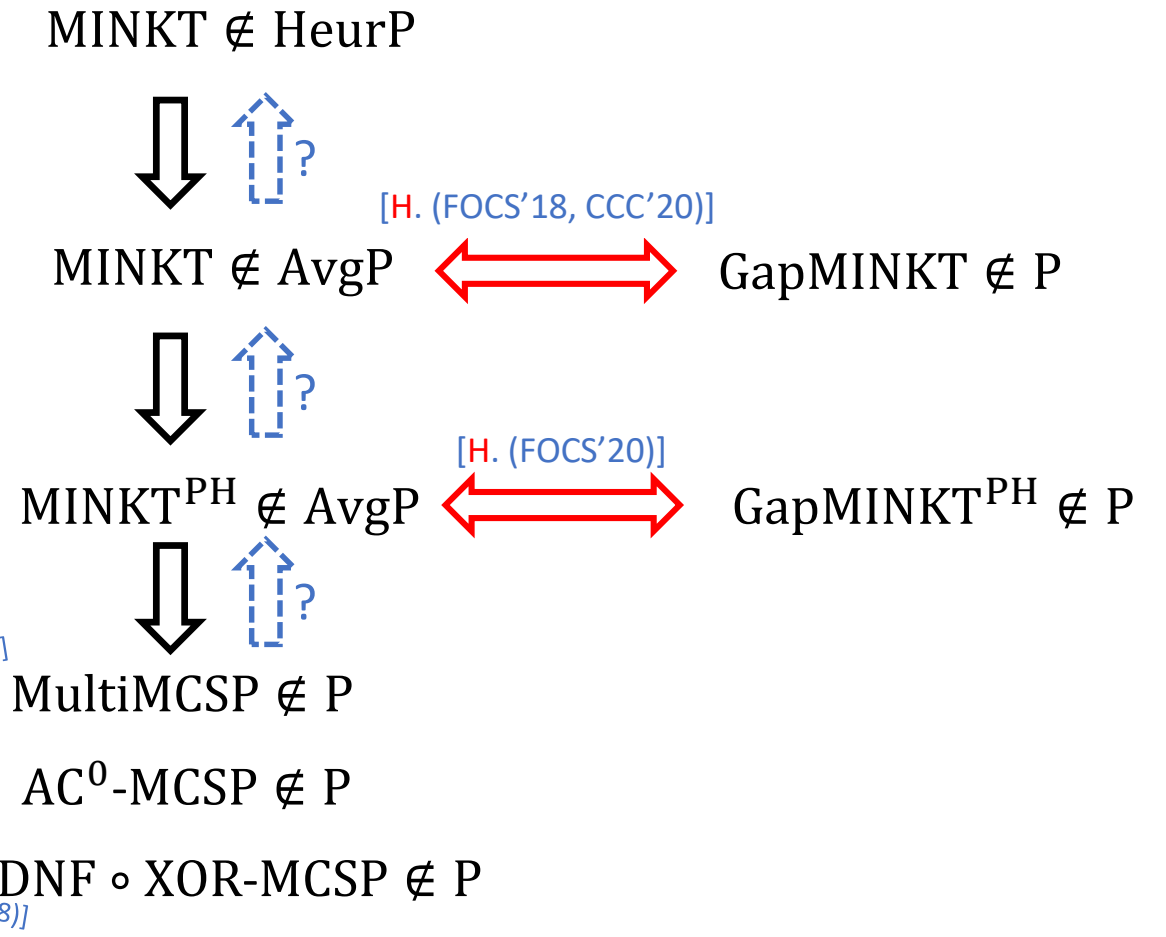
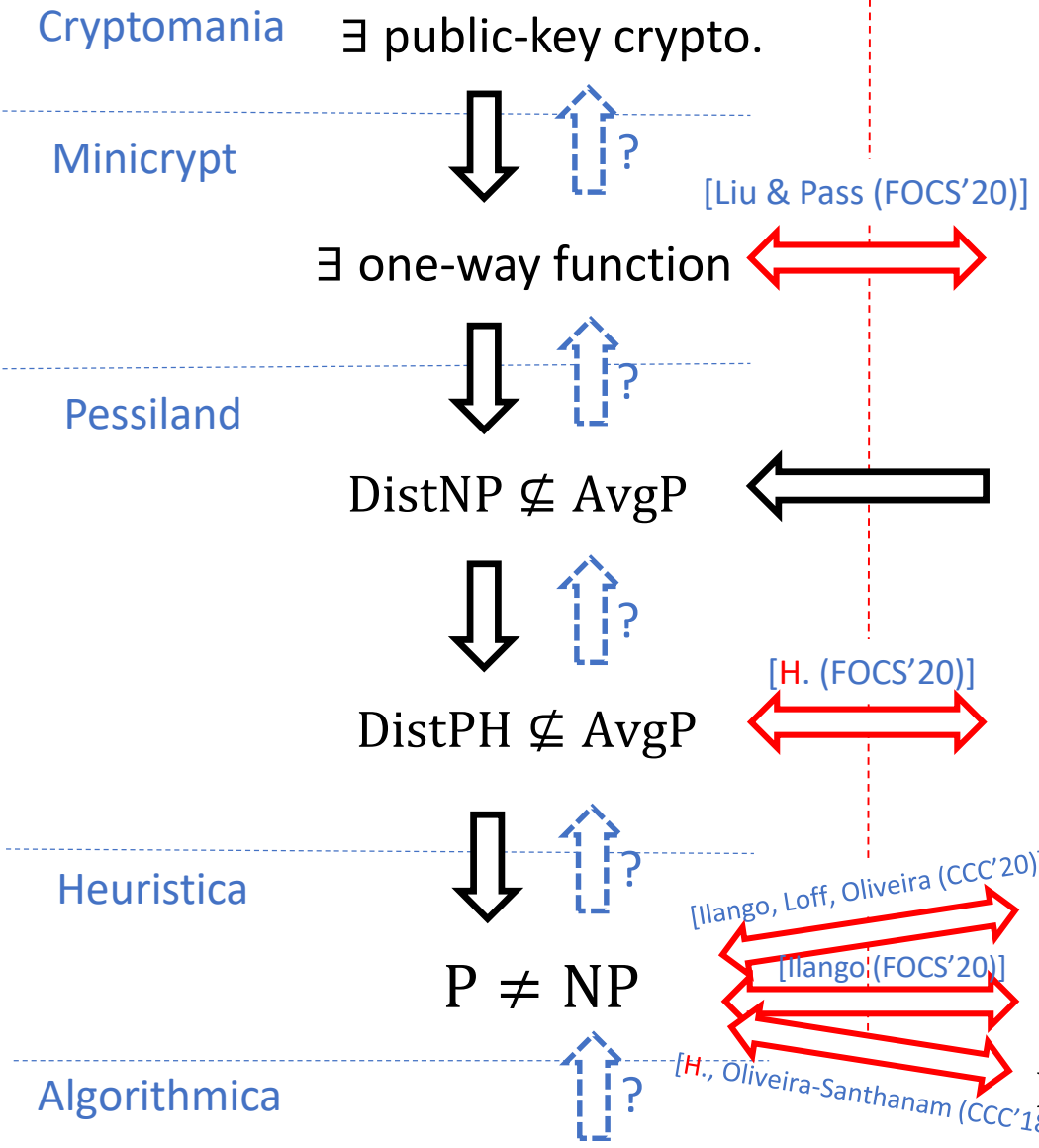
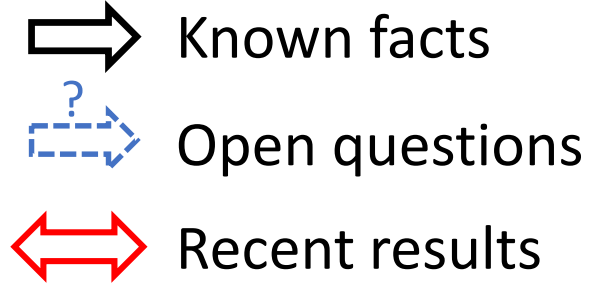
Today's Plan

- Focus on average-case complexity, meta-complexity, and Impagliazzo's five worlds.
- Try to convey high-level ideas and might ignore technical details.

(E.g., BPP vs. P; quasi-poly-time vs. poly-time)

Impagliazzo's Five Worlds

Meta-Complexity Worlds



Impagliazzo's five worlds and **Minimum Circuit Size Problem**

Impagliazzo's five worlds

Cryptomania

Minicrypt

Pessiland

Heuristica

$P \neq NP$

Algorithmica

$P = NP$

[Impagliazzo '95]

Classified five possible worlds
consistent with our current knowledge.

Impagliazzo's five worlds

Cryptomania

Minicrypt

Pessiland

Heuristica

$P \neq NP$

Algorithmica

$P = NP$

[Impagliazzo '95]

Classified five possible worlds
consistent with our current knowledge.



Easy to solve NP problems



No secure cryptography

Impagliazzo's five worlds

[Impagliazzo '95]

Classified five possible worlds
consistent with our current knowledge.

Cryptomania

\exists public-key crypto.

Minicrypt

\exists one-way function & \nexists public-key crypto.

Pessiland

$\text{DistNP} \not\subseteq \text{AvgP}$ & \nexists one-way function

Heuristica

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

Algorithmica

$P = \text{NP}$

Impagliazzo's five worlds

[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

Cryptomania

\exists public-key crypto.

Minicrypt

\exists one-way function & \nexists public-key crypto.

Pessiland

$\text{DistNP} \not\subseteq \text{AvgP}$ & \nexists one-way function

Heuristica

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

Algorithmica

$P = \text{NP}$



Easy to solve NP on average



Hard to solve NP in the worst-case

Impagliazzo's five worlds

[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

Cryptomania

\exists public-key crypto.



Secure public-key crypto exists



Cannot solve some NP problem

Minicrypt

\exists one-way function

&

\nexists public-key crypto.

Pessimism

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

&

\nexists one-way function

Heuristica

$P \neq \text{NP}$

&

$\text{DistNP} \subseteq \text{AvgP}$

Algorithmica

$P = \text{NP}$

Impagliazzo's five worlds

[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

Cryptomania

\exists public-key crypto.

Minicrypt

The Ultimate Goal of Complexity Theory

To determine which world corresponds to ours!
(in particular, to resolve the conjecture that our world is Cryptomania.)

Heuristica

$P \neq NP$

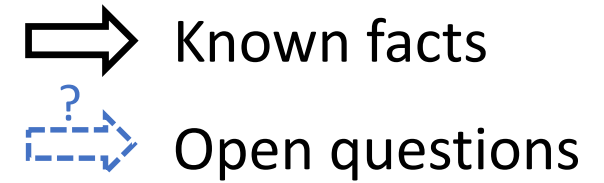
&

$\text{DistNP} \subseteq \text{AvgP}$

Algorithmica

$P = NP$

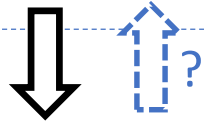
Known Facts and Open Questions



Cryptomania

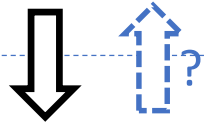
\exists public-key crypto.

Minicrypt



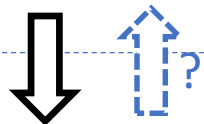
\exists one-way function

Pessiland



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

Heuristica

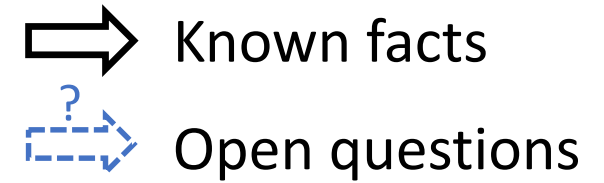


$P \neq \text{NP}$

Algorithmica



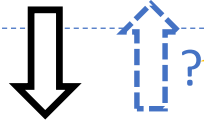
Towards Cryptomania



Cryptomania

∃ public-key crypto.

Minicrypt

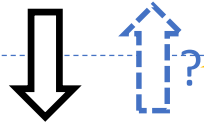


Open Question

Can we exclude Minicrypt from possible worlds?

∃ one-way function

Pessiland

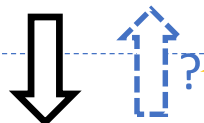


Open Question

Can we exclude Pessiland from possible worlds?

DistNP $\not\subseteq$ AvgP

Heuristica



Open Question

Can we exclude Heuristica from possible worlds?

P \neq NP

Algorithmica



Open Question

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

Proving all the implications



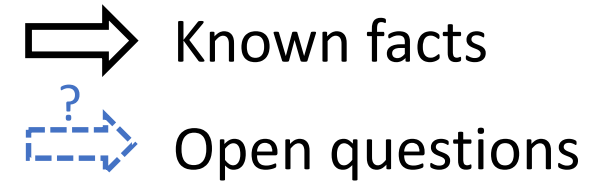
Our world is Cryptomania

Proving a implication





Excluding a world

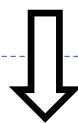

Limits of Current Proof Techniques





Cryptomania
 \exists public-key crypto.

Minicrypt
 

\exists one-way function


Pessiland
 

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

Heuristica
 

$P \neq NP$

Algorithmica

 : a barrier result
 Certain proof techniques are not sufficient to resolve the question.

Relativization barrier [Baker-Gill-Solovey '75]



Algebrization barrier [Aaronson & Wigderson '09]

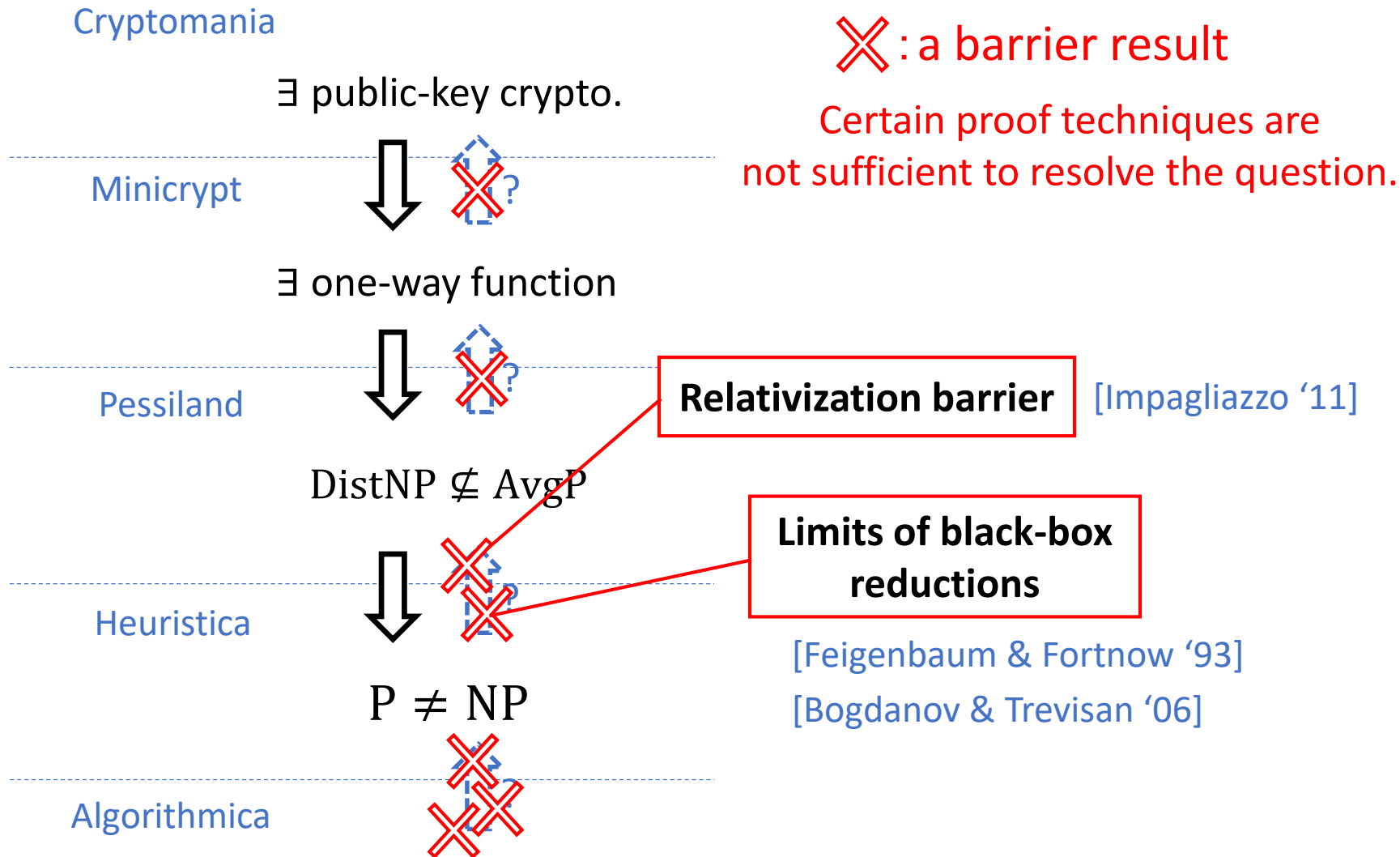
Natural proof barrier [Razborov & Rudich '97]

Proving all the implications
 \Leftrightarrow
 Our world is Cryptomania

Proving a implication
 \Leftrightarrow
 Excluding a world

Limits of Current Proof Techniques

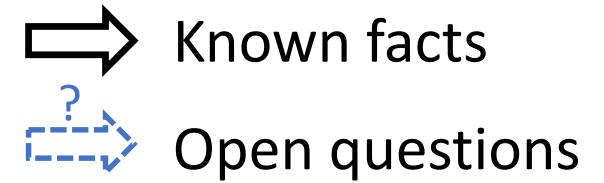
 Known facts
 Open questions



Proving all the implications
 \Leftrightarrow
 Our world is Cryptomania

Proving a implication
 \Leftrightarrow
 Excluding a world

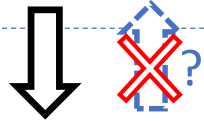
Approach: Meta-Complexity



Cryptomania

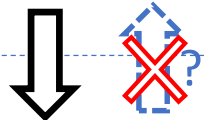
\exists public-key crypto.

Minicrypt



\exists one-way function

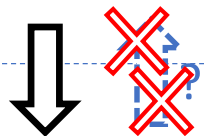
Pessiland



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

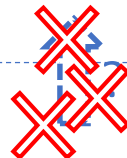
$\text{MCSP} \notin \text{P}$

Heuristica



$\text{P} \neq \text{NP}$

Algorithmica



Proving all the implications
 \Leftrightarrow
 Our world is Cryptomania

Proving a implication
 \Leftrightarrow
 Excluding a world

Minimum Circuit Size Problem (MCSP)

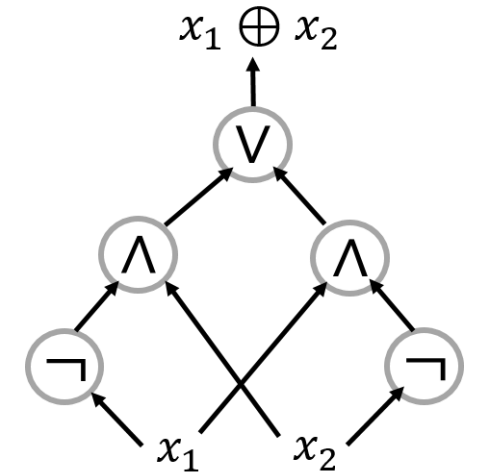
(informal) [Kabanets & Cai '00]

Input

- The truth table of a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$

Output

The minimum size of a circuit computing f



Example

$\text{truthtable}(\oplus_2) = 0110$

$\text{size}(\oplus_2) = 3$

MCSP = “the problem of **computing** the **circuit complexity** of f ”

- A representative example of **meta-complexity**-theoretic problems

Minimum Circuit Size Problem (MCSP)

[Kabanets & Cai '00]

Input

- The truth table of a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$
- A size parameter $s \in \mathbb{N}$

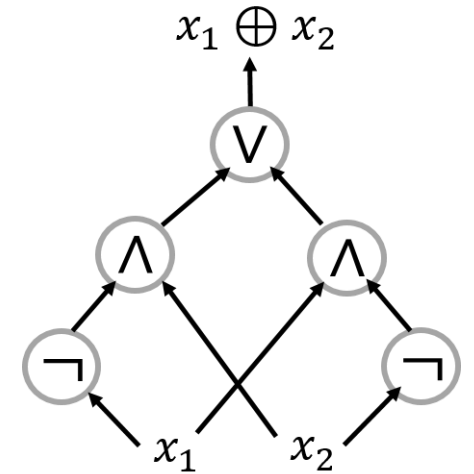
Example

$\text{truthtable}(\oplus_2) = 0110$

Output

Is the minimum size of a circuit computing f $\leq s$?

$\text{size}(\oplus_2) = 3$



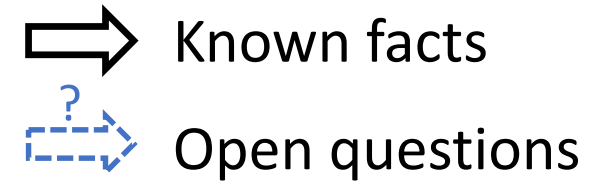
MCSP = “the problem of **computing** the **circuit complexity** of f ”

- A representative example of **meta-complexity**-theoretic problems

Fact: **MCSP** \in **NP**

Open: **NP**-hardness of **MCSP**

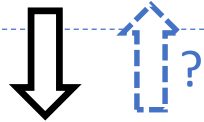
Relationships between the five worlds



Cryptomania

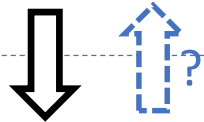
\exists public-key crypto.

Minicrypt



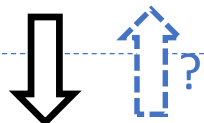
\exists one-way function

Pessiland



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

Heuristica



$P \neq NP$

Algorithmica



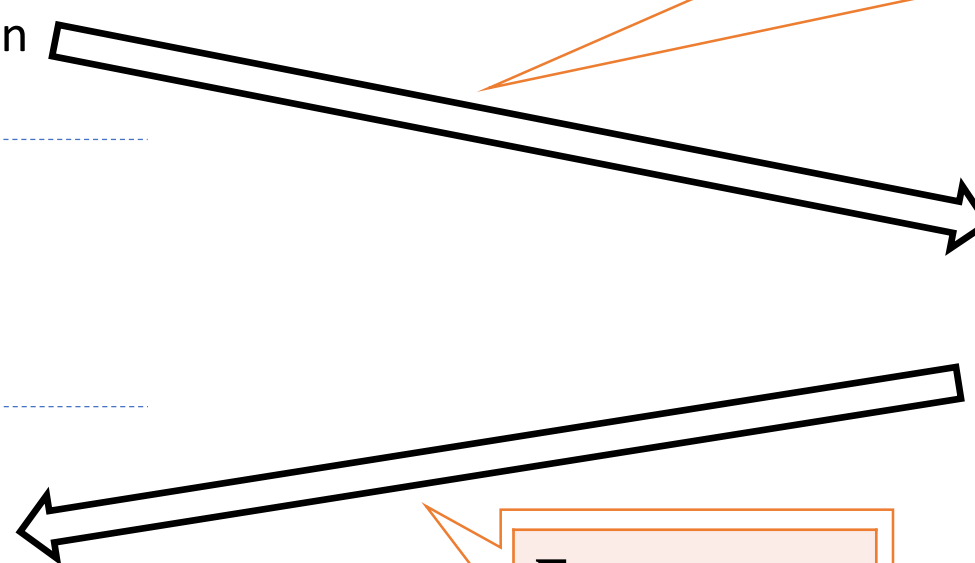
Theorem [RR97, HILL99, ABKvMR06]

\exists OWF implies $\text{MCSP} \notin \text{BPP}$.



$\text{MCSP} \notin P$

Fact

$\text{MCSP} \in \text{NP}$



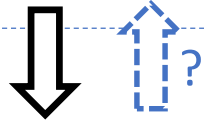
Relationships between the five worlds

 Known facts
 Open questions

Cryptomania

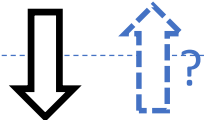
\exists public-key crypto.

Minicrypt



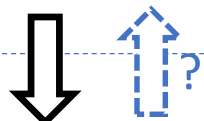
\exists one-way function

Pessiland



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

Heuristica



$P \neq NP$

Algorithmica



Theorem [RR97, HILL99, ABKvMR06]

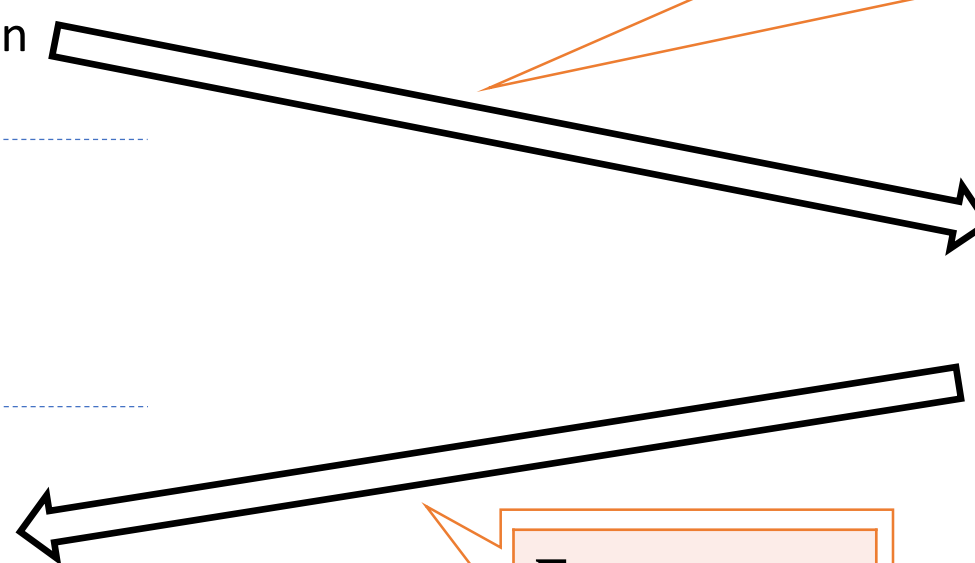
\exists OWF implies $\text{GapMCSP} \notin \text{BPP}$.

$\text{GapMCSP} \notin P$

Fact

$\text{MCSP} \in \text{NP}$

Gap: An approximation version



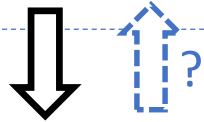
Worst- and average-case equivalence

⇒ Known facts
⇨ Open questions

Cryptomania

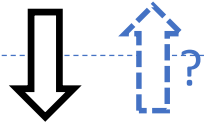
∃ public-key crypto.

Minicrypt



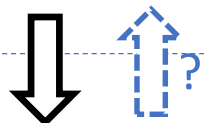
∃ one-way function

Pessiland



DistNP $\not\subseteq$ AvgP

Heuristica



P \neq NP

Algorithmica





Theorem [H. (FOCS'18)]

Worst- and average-case complexities of GapMCSP are equivalent.

GapMCSP \notin P

Gap: An approximation version

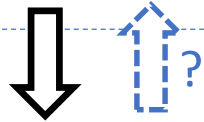
Worst- and average-case equivalence

 Known facts
 Open questions

Cryptomania

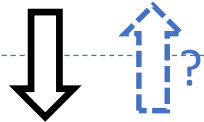
\exists public-key crypto.

Minicrypt

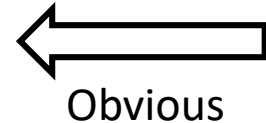


\exists one-way function

Pessiland



DistNP $\not\subseteq$ AvgP

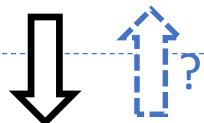


MCSPP \notin AvgP



GapMCSPP \notin P

Heuristica



P \neq NP

Algorithmica



Theorem [H. (FOCS'18)]
 Worst- and average-case complexities of GapMCSPP are equivalent.

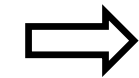

AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version

* More precisely, $(\text{MCSPP}[2^{\epsilon n}], \mathcal{U}) \notin \text{AvgBPP} (\exists \epsilon > 0) \Leftrightarrow \text{GapMCSPP} \notin \text{prBPP}$.

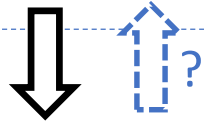
Overcoming limits of black-box reductions

 Known facts
 Open questions

Cryptomania

\exists public-key crypto.

Minicrypt

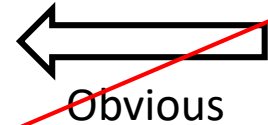


\exists This overcomes limits of black-box reductions!

Theorem [H. (FOCS'18)]
 Worst- and average-case complexities of GapMCSP are equivalent.

Pessiland

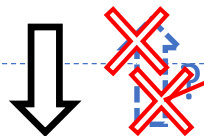
DistNP $\not\subseteq$ AvgP



MCSP \notin AvgP

GapMCSP \notin P

Heuristica



P \neq NP

Algorithmica

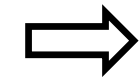



AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version

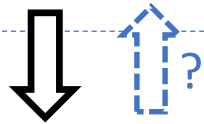
Overcoming limits of black-box reductions

 Known facts
 Open questions

Cryptomania

\exists public-key crypto.

Minicrypt



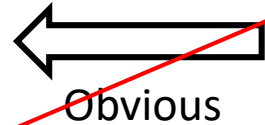
\exists This overcomes limits of black-box reductions!

Theorem [H. (FOCS'18)]

Worst- and average-case complexities of GapMCSP are equivalent.

Pessiland

DistNP $\not\subseteq$ AvgP

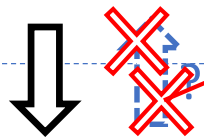


MCSP \notin AvgP

GapMCSP \notin P

Shown by non-black-box reductions that rely on efficiency of oracle.

Heuristica



(A special case of) **Theorem** [Bogdanov & Trevisan '06]

Algo

If there is a (black-box) randomized nonadaptive reduction from GapMCSP to DistNP, then GapMCSP \in coNP/poly.

(unlikely!)

AvgP = Average-Case Poly-time = Errorless Heuristics

$(L, \mathcal{D}) \in \text{AvgP} \stackrel{\text{def}}{\iff} \exists \text{ alg. } A \text{ such that}$

1. $A(x) = L(x)$ for every x , and
2. $\mathbb{E}_{x \sim \mathcal{D}_n} [t_A(x)^\epsilon] = O(n)$ for some $\epsilon > 0$,

where $t_A(x)$ denotes the running time of A on input x .

Equivalently:

$(L, \mathcal{D}) \in \text{AvgP} \stackrel{\text{def}}{\iff} \exists \text{ alg. } A \text{ such that}$

1. $A(x, \delta) \in \{L(x), \perp\}$ for every x ,
2. $\Pr_{x \sim \mathcal{D}_n} [A(x, \delta) = \perp] \leq \delta$, and
3. $t_A(x, \delta) \leq \text{poly}(n/\delta)$.

A New Approach Towards Excluding Heuristica

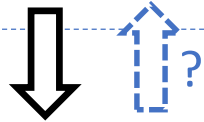
⇒ Known facts

⇌? Open questions

Cryptomania

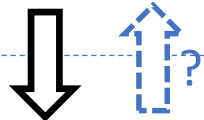
∃ public-key crypto.

Minicrypt

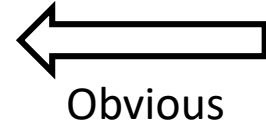


∃ one-way function

Pessiland



DistNP $\not\subseteq$ AvgP



MCSP \notin AvgP



GapMCSP \notin P

Corollary of “⇌”
If GapMCSP is NP-hard,
then Heuristica is excluded.

Open Question
Can we exclude Heuristica?



P \neq NP

Algorithmica



Open Question
Is GapMCSP NP-hard?

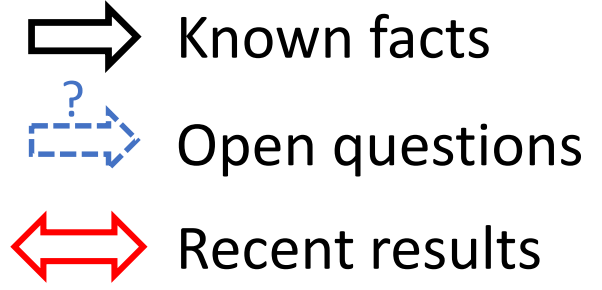
AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version

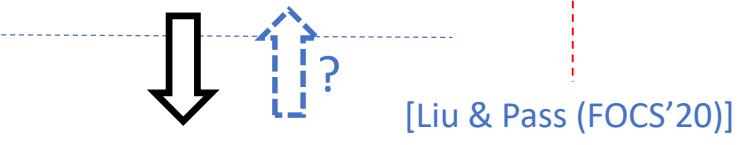
Impagliazzo's Five Worlds

Meta-Complexity Worlds



Cryptomania \exists public-key crypto.

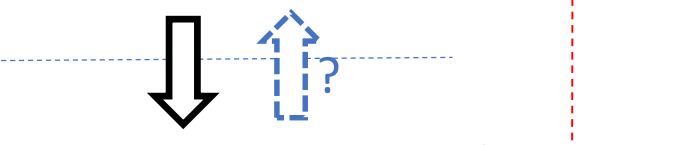
Minicrypt



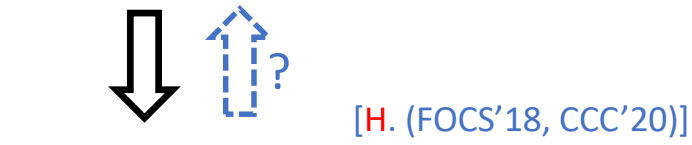
\exists one-way function

MINKT \notin HeurP

Pessiland



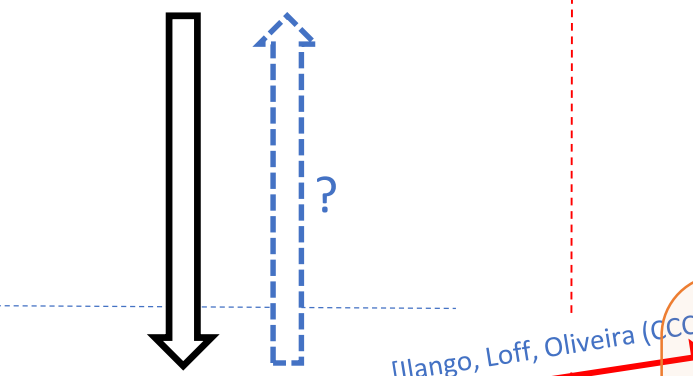
DistNP $\not\subseteq$ AvgP



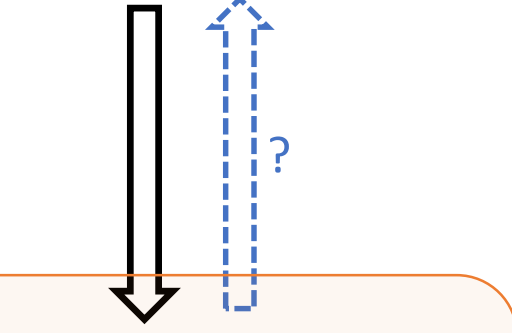
MCSP \notin AvgP

⇔ GapMCSP \notin P

Heuristica



P \neq NP



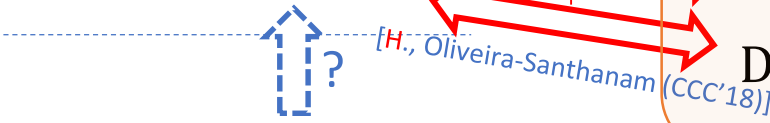
MultiMCSP \notin P

AC⁰-MCSP \notin P

DNF \circ XOR-MCSP \notin P

NP-complete problems

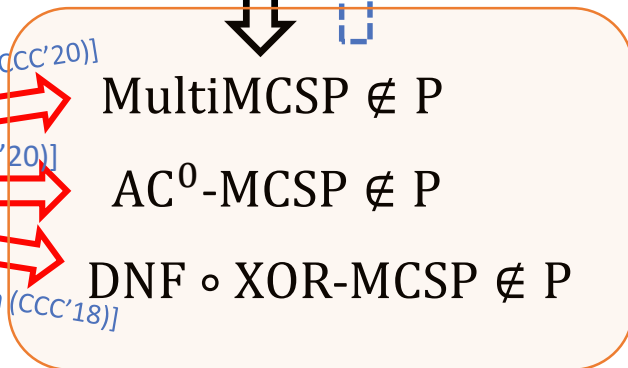
Algorithmica



[Ilango, Loff, Oliveira (CCC'20)]

[Ilango (FOCS'20)]

[H., Oliveira-Sadhanam (CCC'18)]



Recent Progress on NP-hardness of MCSP

Towards excluding Heuristica

\mathcal{C} -MCSP for a restricted circuit class \mathcal{C}

- A natural approach to make progress toward NP-hardness of MCSP:

To restrict ourselves to a circuit class \mathcal{C} such as $\mathcal{C} \in \{\text{DNF}, \text{AC}^0, \dots\}$.

Definition (\mathcal{C} -MCSP)

Given $f: \{0,1\}^n \rightarrow \{0,1\}$ and $s \in \mathbb{N}$,
is there a \mathcal{C} -circuit of size at most s computing f ?

NP-hardness of DNF-MCSP

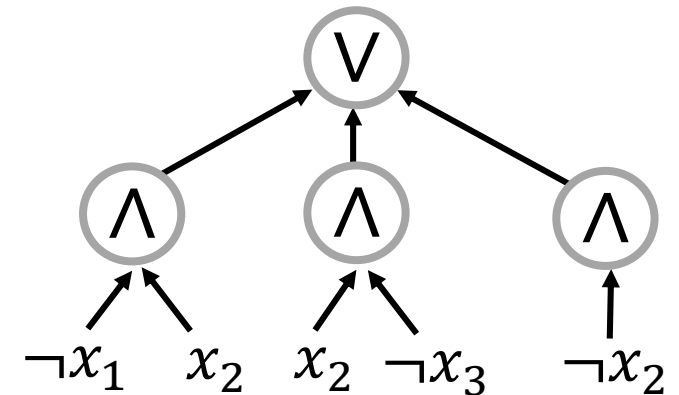
- Nearly 40 years ago, Masek proved NP-hardness of DNF-MCSP.

Theorem [Masek (1978 or 1979, unpublished)]

DNF-MCSP is NP-hard.

Examples of DNF formula

$$\varphi = (\neg x_1 \wedge x_2) \vee (x_2 \wedge \neg x_3) \vee \neg x_2$$



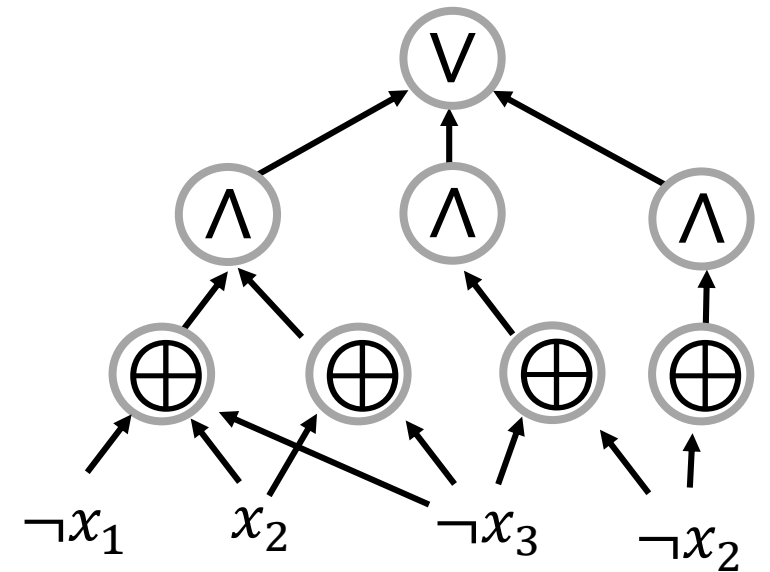
NP-hardness of (DNF \circ XOR)-MCSP

- We were able to extend DNF formulas to DNF \circ XOR formulas.

Theorem [H., Oliveira & Santhanam (CCC'18)]

(DNF \circ XOR)-MCSP is NP-hard.

A DNF \circ XOR formula



Recent Progress: NP-hardness of AC^0 -MCSP

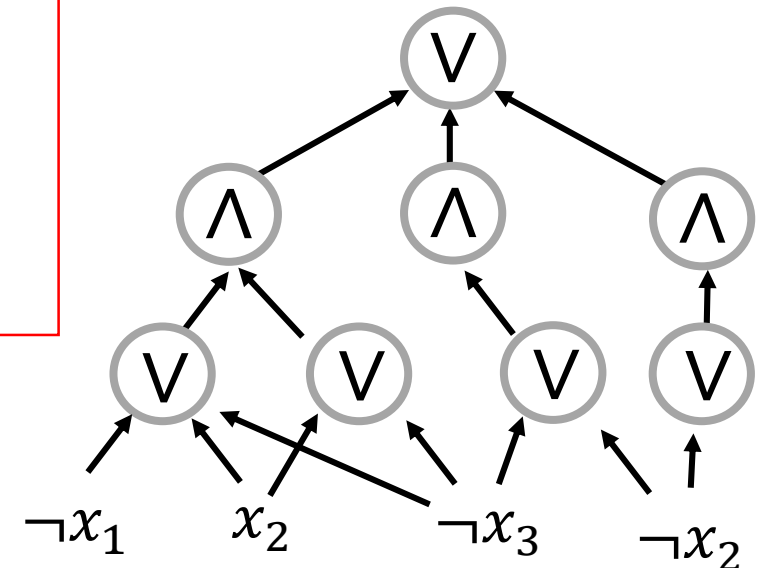
- [Rahul Ilango] extended the frontier to depth- d AC^0 formulas for any constant $d \geq 2$.

(cf. talk on June 18 in Oxford-Warwick complexity meeting.)

Theorem [Ilango (FOCS'20)]

For any constant $d \geq 2$,
Depth- d - AC^0 -MCSP is NP-hard
(under randomized quasi-polynomial-time reductions).

An AC^0 formula



Recent Progress: NP-hardness of Multi-MCSP

Theorem [Ilango-Loff-Oliveira (CCC'20)]

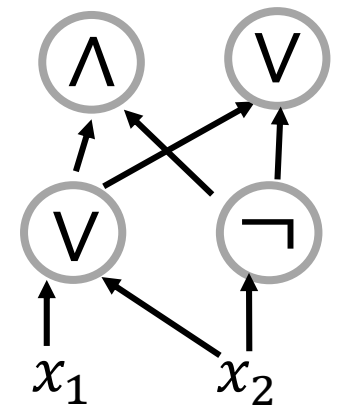
Multi-MCSP is NP-hard
(under randomized reductions).

Definition (Multi-MCSP)

Given a function $f: \{0,1\}^n \rightarrow \{0,1\}^m$ and a size parameter s ,
is there a **multi-output** circuit of size s computing f ?

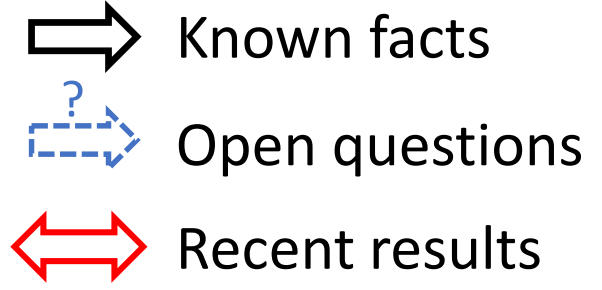
Key Idea: Instead of restricting a circuit class,
try to restrict the structure of a circuit by specifying the m -bit output!

A **multi-output** circuit



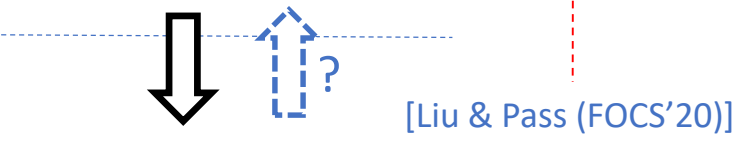
Impagliazzo's Five Worlds

Meta-Complexity Worlds



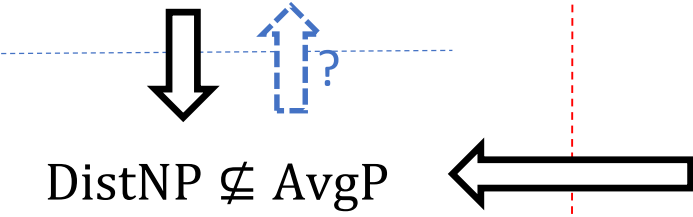
Cryptomania \exists public-key crypto.

Minicrypt

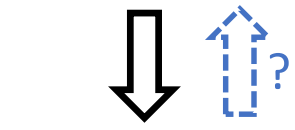


\exists one-way function

Pessiland



MINKT \notin HeurP



Relativization barrier [Impagliazzo '11] [Ko '91]

MCSP \notin AvgP \leftrightarrow GapMCSP \notin P

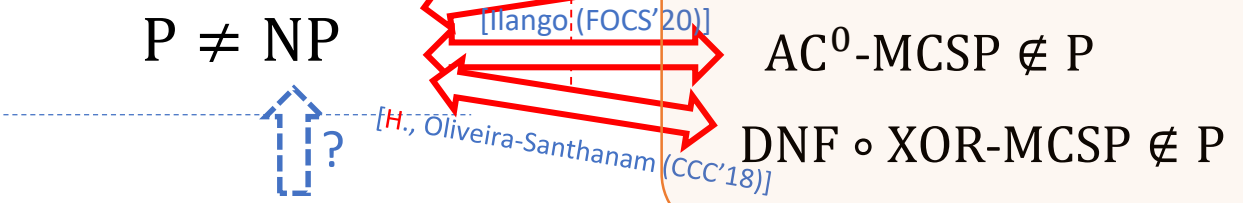
Heuristica



Open Question

- What's the difference between Multi-MCSP and MCSP?
- Non-relativizing proof techniques?

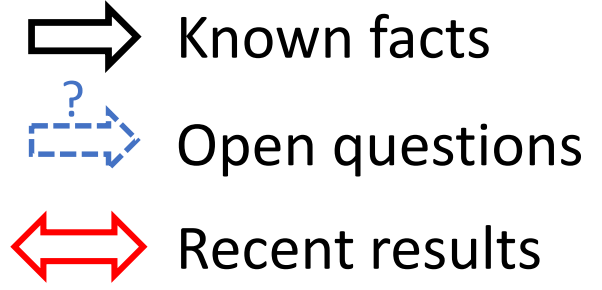
Algorithmica



NP-complete problems

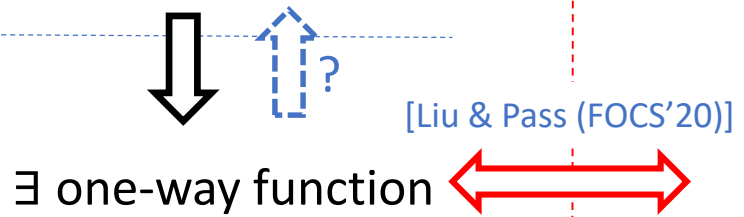
Impagliazzo's Five Worlds

Meta-Complexity Worlds

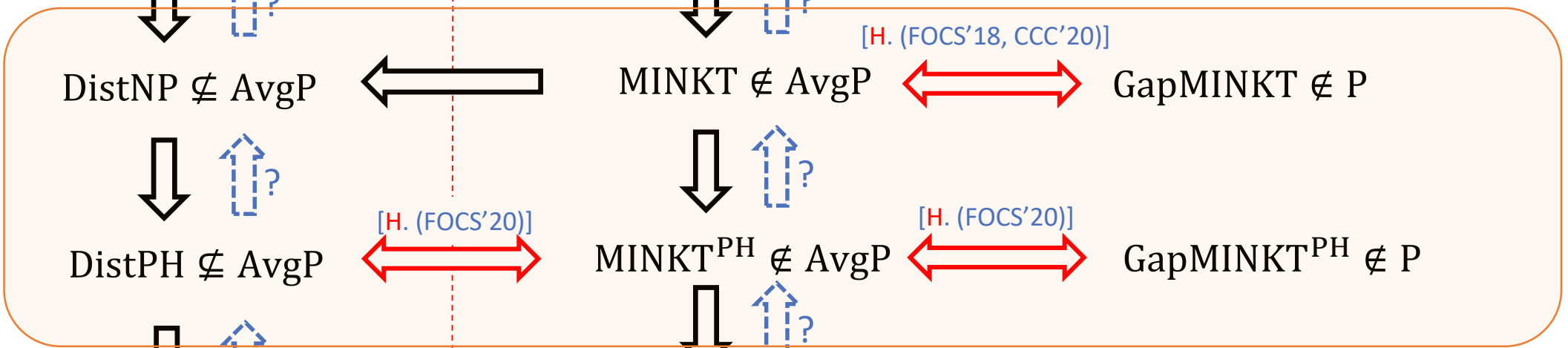


Cryptomania \exists public-key crypto.

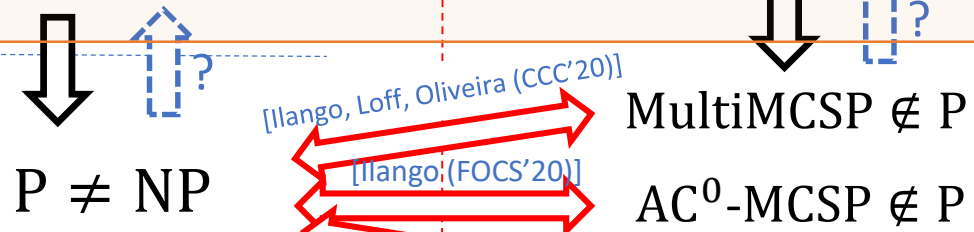
Minicrypt



Pessiland



Heuristica



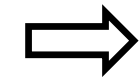

Algorithmica



Average-Case Complexity versus Meta-Complexity

Towards better understanding of average-case complexity

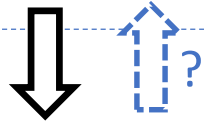
Can we prove the converse?

 Known facts
 Open questions

Cryptomania

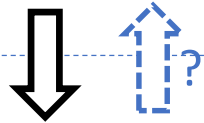
\exists public-key crypto.

Minicrypt

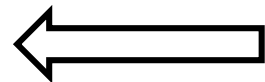


\exists one-way function

Pessiland



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

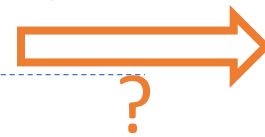
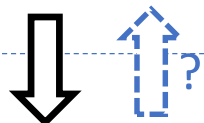


$\text{MCSP} \notin \text{AvgP}$



$\text{GapMCSP} \notin \text{P}$

Heuristica



$\text{P} \neq \text{NP}$

Algorithmica



Theorem [H. (FOCS'18)]

Worst- and average-case complexities of GapMCSP are equivalent.

AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version

MINKT

(Minimum Time-bounded Kolmogorov Complexity Problem) [Ko '91]

Input

- A binary string $x \in \{0,1\}^*$
- A time bound 1^t (in unary)

Output

$K^t(x)$ (t -time-bounded Kolmogorov complexity)

$K^t(x) :=$ the minimum size of a program M that outputs x in time t .

Example

$$x = 1^n$$

$$K^t(x) = \log n + O(1) \quad \leftarrow \text{print "1" } \times n$$

$$x = 1010111010101101$$

$$K^t(x) \geq n - 1 \text{ with probability } \geq \frac{1}{2}.$$

MINKT = “the problem of **computing** the time-bounded **Kolmogorov complexity** of x ”

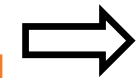

Cf. **MCSP** = “the problem of **computing** the **circuit complexity** of f ”

➤ **meta-complexity** theoretic problems.

Fact: **MINKT** \in **NP**

Open: **NP-hardness** of **MINKT**

MINKT versus MCSP

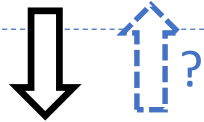
 Known facts
 Open questions

Theorem [H. (FOCS'18, CCC'20)]
 Worst- and average-case complexities of GapMINKT are equivalent.

Cryptomania

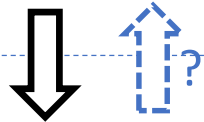
\exists public-key crypto.

Minicrypt



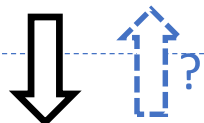
\exists one-way function \implies MINKT \notin AvgP \iff^* GapMINKT \notin P

Pessiland



DistNP $\not\subseteq$ AvgP \longleftarrow MCSP \notin AvgP \iff^* GapMCSP \notin P

Heuristica



P \neq NP

GapMINKT: a $O(\log t|x|)$ -additive approximation of $K^t(x)$

Algorithmica

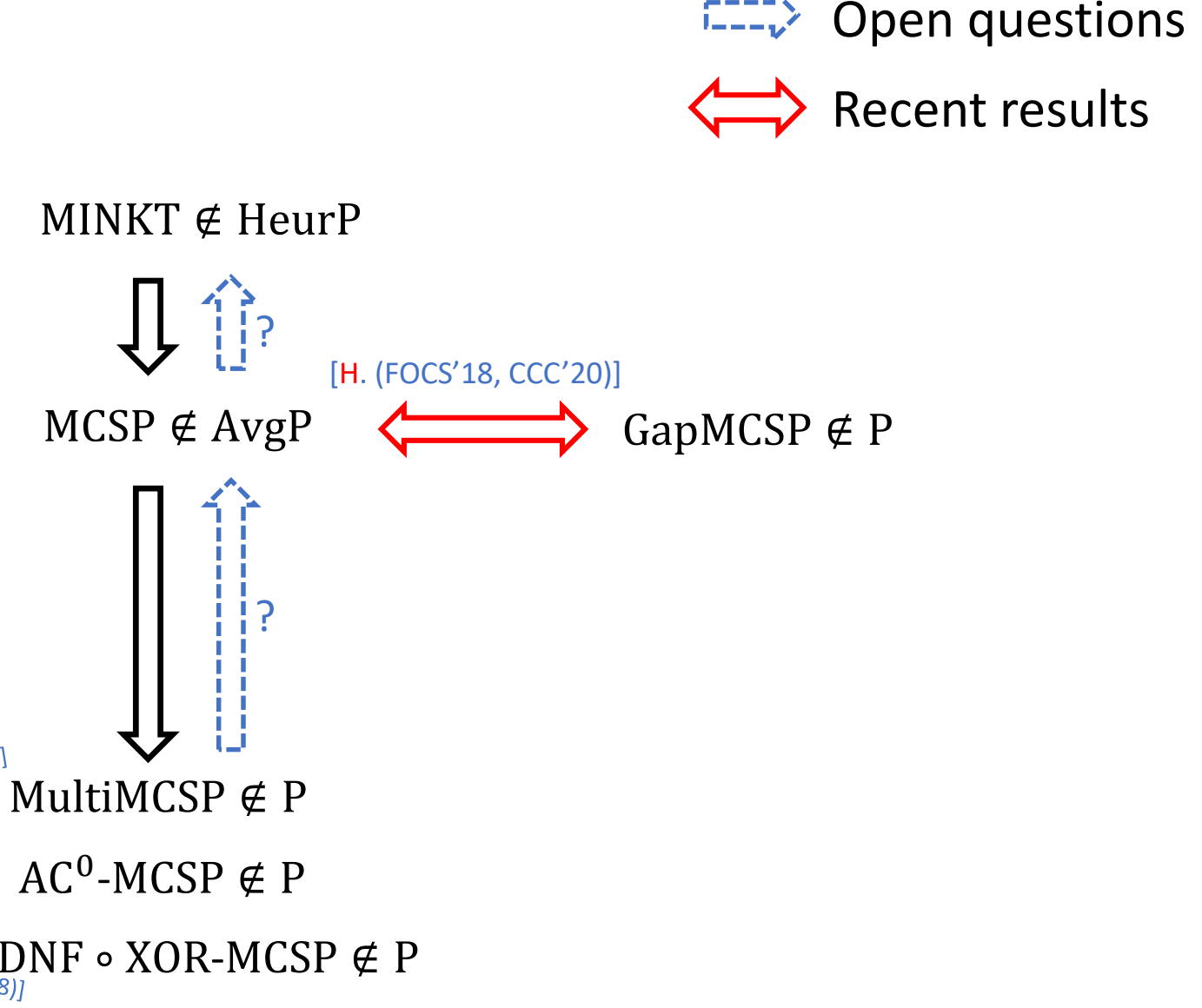
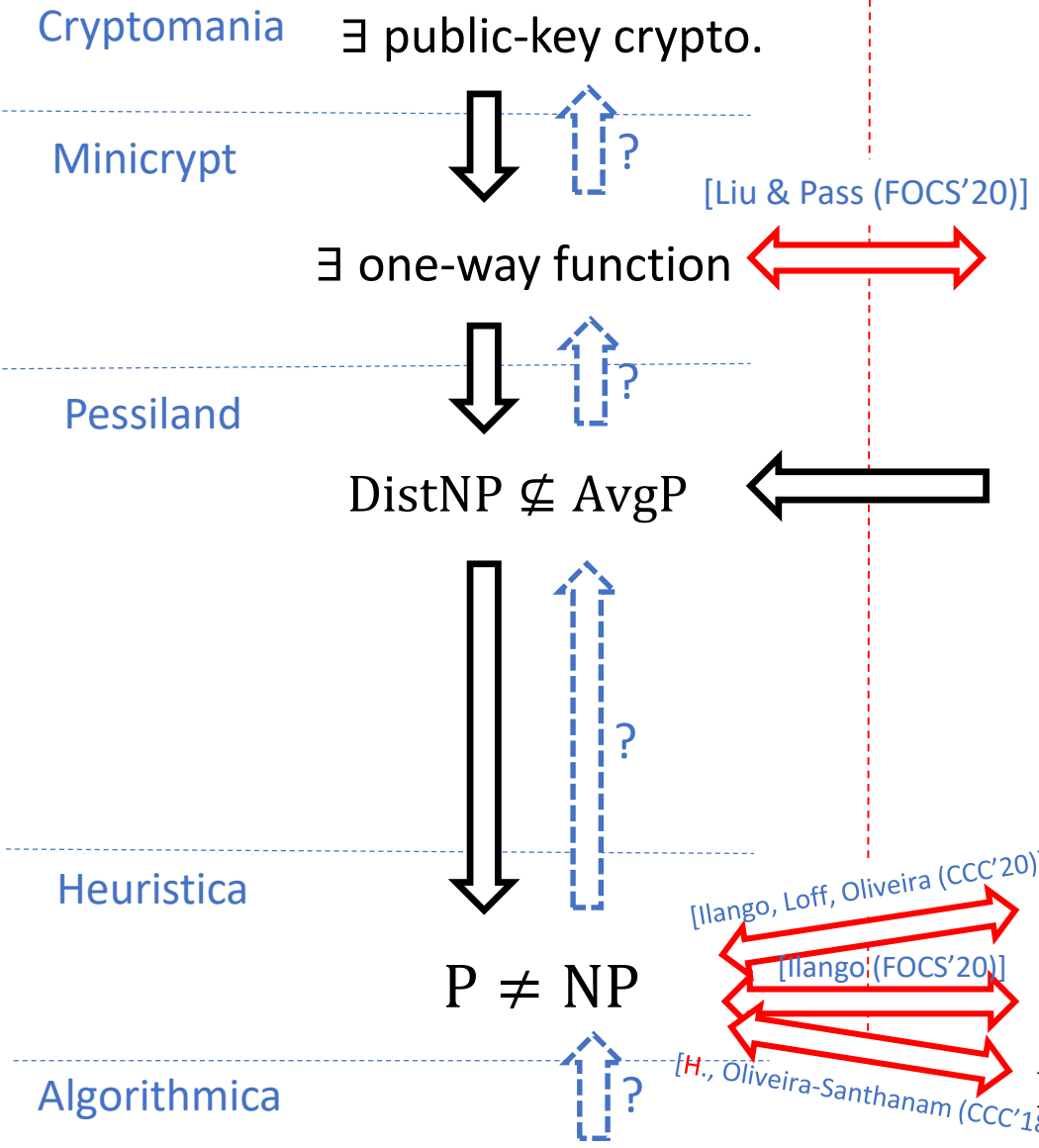
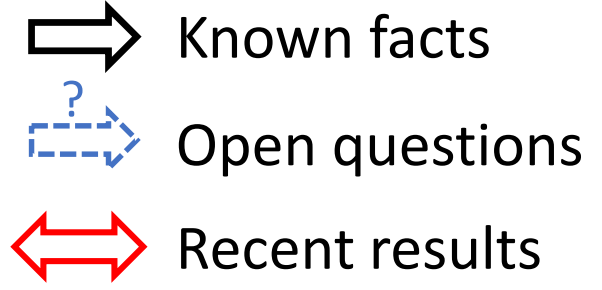


GapMCSP: a $|f|^{1-\epsilon}$ -factor approximation of $\text{size}(f)$

*Assuming the existence of complexity-theoretic PRG (for derandomization).

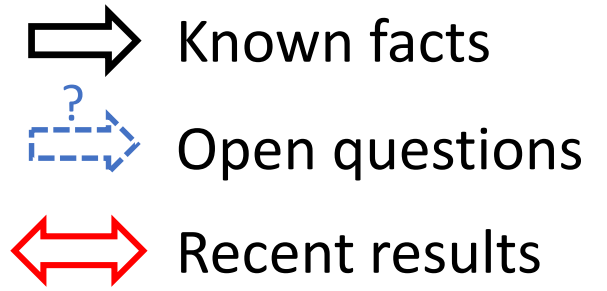
Impagliazzo's Five Worlds

Meta-Complexity Worlds



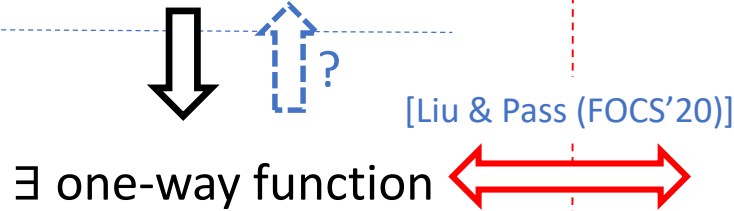
Impagliazzo's Five Worlds

Meta-Complexity Worlds



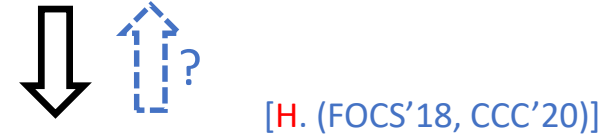
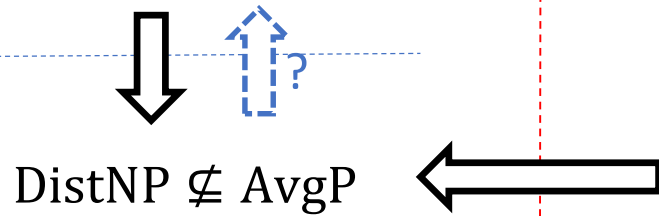
Cryptomania \exists public-key crypto.

Minicrypt



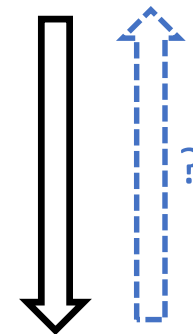
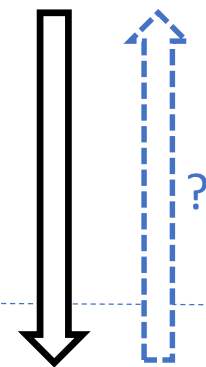
MINKT \notin HeurP

Pessiland



MINKT \notin AvgP ⇔ GapMINKT \notin P

Heuristica



MultiMCSP \notin P

[Ilango, Loff, Oliveira (CCC'20)]

AC⁰-MCSP \notin P

[Ilango (FOCS'20)]

Algorithmica

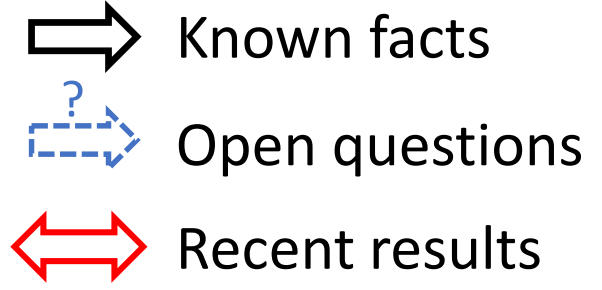


DNF \circ XOR-MCSP \notin P

[H., Oliveira-Sadhanam (CCC'18)]

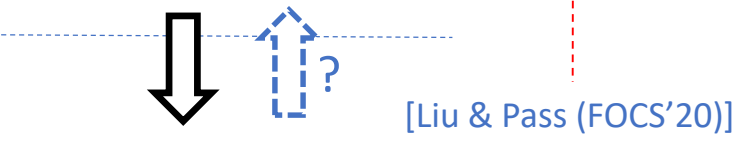
Impagliazzo's Five Worlds

Meta-Complexity Worlds



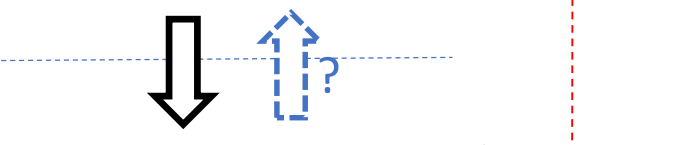
Cryptomania \exists public-key crypto.

Minicrypt



\exists one-way function

Pessiland



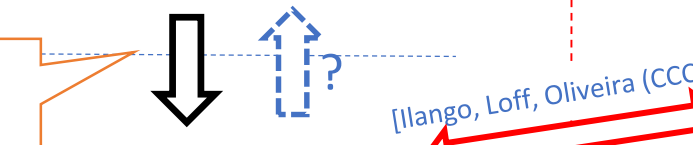
$\text{DistNP} \not\subseteq \text{AvgP}$

PH: polynomial-time hierarchy



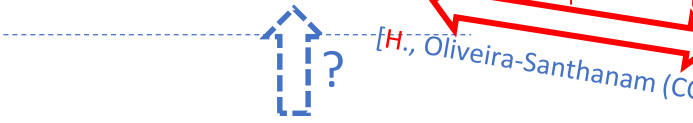
$\text{DistPH} \not\subseteq \text{AvgP}$

$P = NP \Leftrightarrow P = PH$

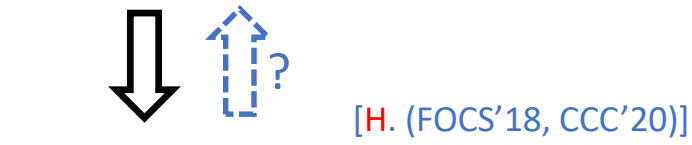


$P \neq NP$

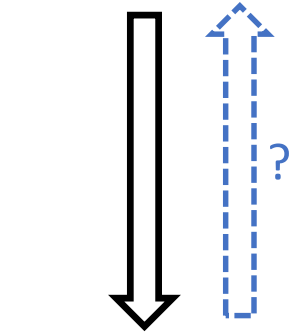
Algorithmica



$\text{MINKT} \notin \text{HeurP}$



$\text{MINKT} \notin \text{AvgP} \Leftrightarrow \text{GapMINKT} \notin P$



$\text{MultiMCSP} \notin P$

$\text{AC}^0\text{-MCSP} \notin P$

$\text{DNF} \circ \text{XOR-MCSP} \notin P$

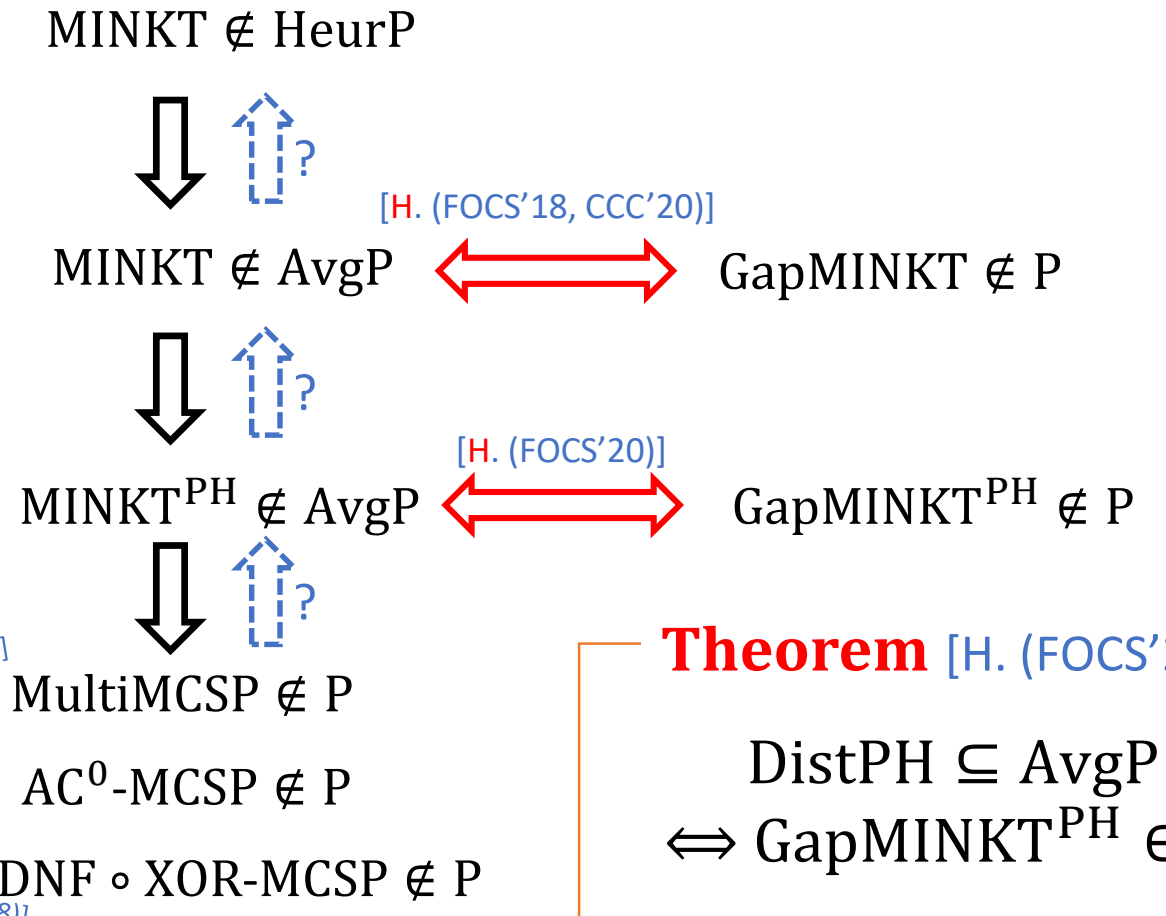
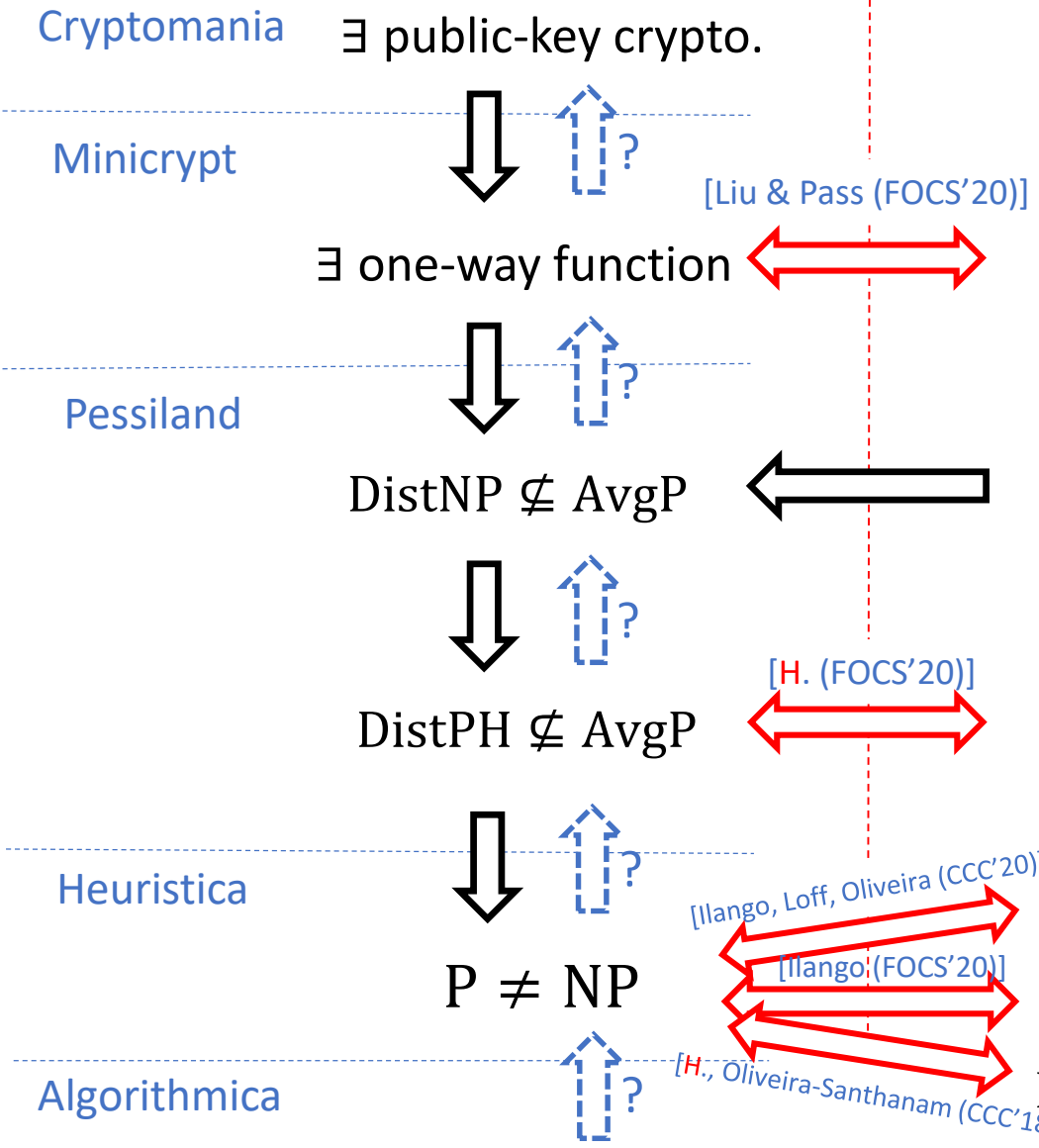
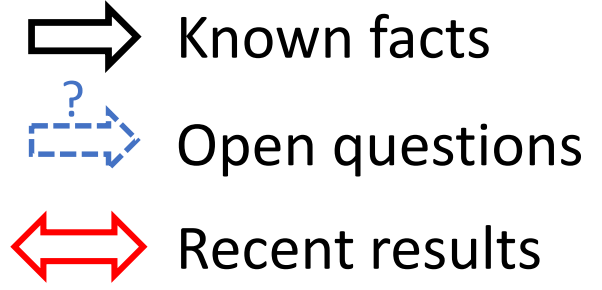
[Ilango, Loff, Oliveira (CCC'20)]

[Ilango (FOCS'20)]

[H., Oliveira-Santhanam (CCC'18)]

Impagliazzo's Five Worlds

Meta-Complexity Worlds



Theorem [H. (FOCS'20)]

DistPH \subseteq AvgP
 \Leftrightarrow GapMINKT^{PH} \in P

Average-Case Complexity

Meta-Complexity Worlds

Worst-Case
Meta-Complexity

Σ_k SAT: A Σ_k^p -complete problem

GapMINKT $^{\Sigma_k$ SAT} $\in P$ ($\forall k \in \mathbb{N}$)

GapMINKT $^A \in P$ for any $A \in PH$.



DistPH \subseteq AvgP $\xleftrightarrow{[H. (FOCS'20)]}$

MINKT $^{PH} \in$ AvgP $\xleftrightarrow{[H. (FOCS'20)]}$

GapMINKT $^{PH} \in P$

Theorem [H. (FOCS'20)]
DistPH \subseteq AvgP
 \Leftrightarrow GapMINKT $^{PH} \in P$

Average-Case Complexity

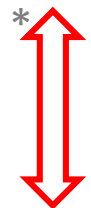
$$\text{DistPH} \subseteq \text{Avg}_{1-1/\text{poly}(n)}^1 \text{P}$$



$$\text{DistPH} \subseteq \text{Avg}_{1-1/\text{poly}(n)} \text{P}$$



$$\text{DistPH} \subseteq \text{AvgP}$$

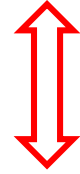


\nexists PH-computable
hitting set generator
secure against P

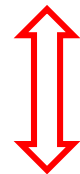


Meta-Complexity Worlds

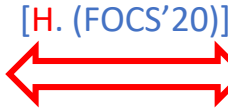
$$\text{coMINKT}^{\text{PH}} \in \text{Avg}_{1-1/\text{poly}(n)}^1 \text{P}$$



$$\text{MINKT}^{\text{PH}} \in \text{Avg}_{1-1/\text{poly}(n)} \text{P}$$



$$\text{MINKT}^{\text{PH}} \in \text{AvgP}$$



Worst-Case Meta-Complexity

One-sided-error heuristic
that succeeds
with prob. $\geq 1/\text{poly}(n)$

Errorless heuristic
that succeeds with
prob. $\geq 1/\text{poly}(n)$ ($\forall k \in \mathbb{N}$)



$$\text{GapMINKT}^{\text{PH}} \in \text{P}$$

Theorem [H. (FOCS'20)]

$$\text{DistPH} \subseteq \text{AvgP} \\ \Leftrightarrow \text{GapMINKT}^{\text{PH}} \in \text{P}$$

*Under the assumption that $\text{P} = \text{ZPP}$

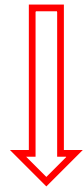
Average-Case Complexity

PH is easy on
a $1/\text{poly}(n)$ -fraction
of inputs

$$\text{DistPH} \subseteq \text{Avg}_{1-1/\text{poly}(n)}\text{P}$$

PH is easy on
most inputs

$$\text{DistPH} \subseteq \text{AvgP}$$



Meta-Complexity Worlds

Corollary [H. (FOCS'20)]

Errorless hardness
amplification for PH
(for **deterministic** algorithms)

Worst-Case Meta-Complexity

$$\text{GapMINKT}^{\text{PH}} \in \text{P}$$

Average-Case Complexity

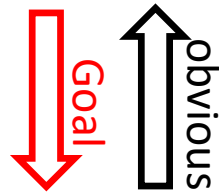
Corollary [H. (FOCS'20)]

Errorless hardness amplification for PH
(for **deterministic** algorithms)

Meta-Complexity Worlds

Worst-Case Meta-Complexity

$\text{DistPH} \subseteq \text{Avg}_{1-1/\text{poly}(n)}\text{P}$



$\text{DistPH} \subseteq \text{AvgP}$

$\text{MINKT}^{\text{PH}} \in \text{NP}^{\text{PH}} = \text{PH}$

$\text{MINKT}^{\text{PH}} \in \text{Avg}_{1-1/\text{poly}(n)}\text{P}$

Based on non-black-box worst-to-average-case reductions and build on [H. (FOCS'18, CCC'20)]

$\text{GapMINKT}^{\text{PH}} \in \text{P}$

Based on unexpected hardness results for Kolmogorov complexity and build on [H. (ITCS'20, STOC'20)]

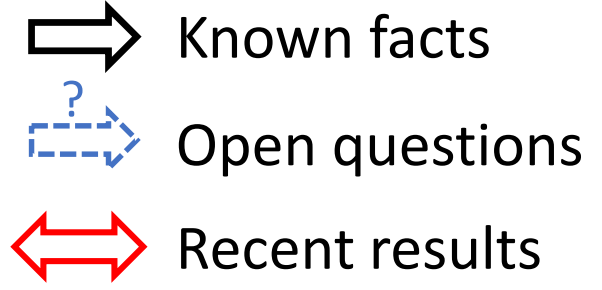
This is an **average-case-to-worst-case** reduction and not an **average-case-to-average-case** reduction.

➤ Meta-complexity appears essential!

- The proof goes through **meta-complexity worlds** (despite that the theorem is purely **average-case complexity-theoretic**).

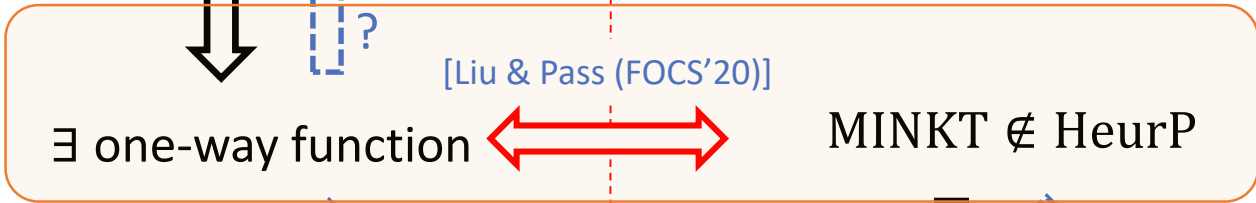
Impagliazzo's Five Worlds

Meta-Complexity Worlds

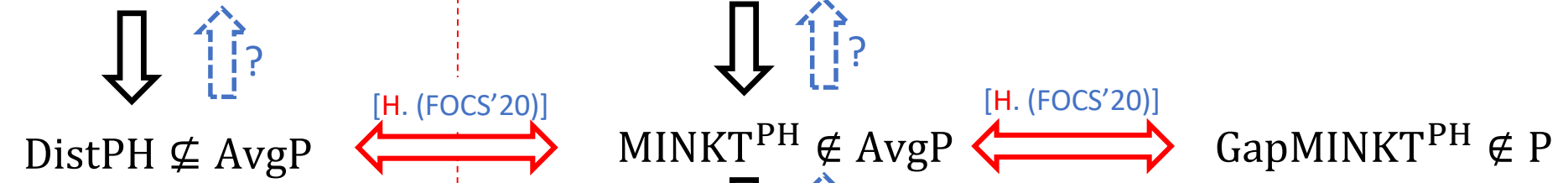
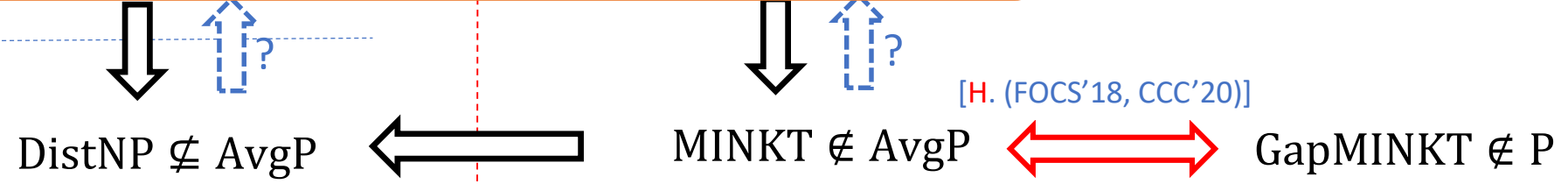


Cryptomania \exists public-key crypto.

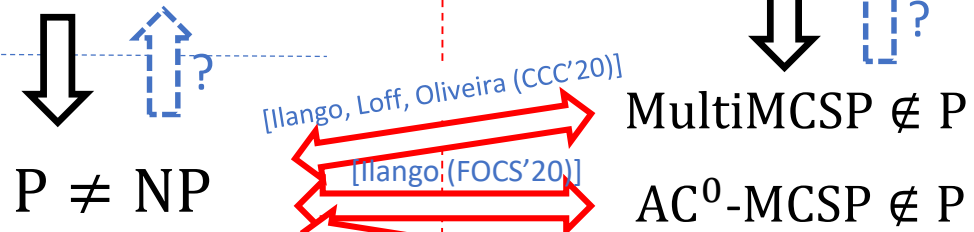
Minicrypt



Pessiland



Heuristica



Algorithmica

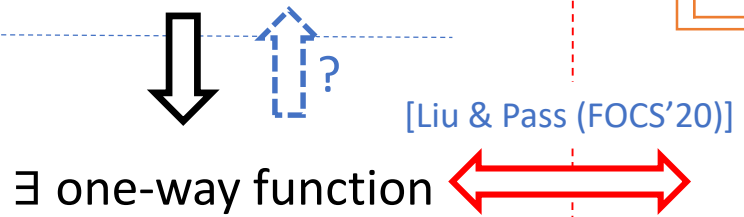


Impagliazzo's Five Worlds

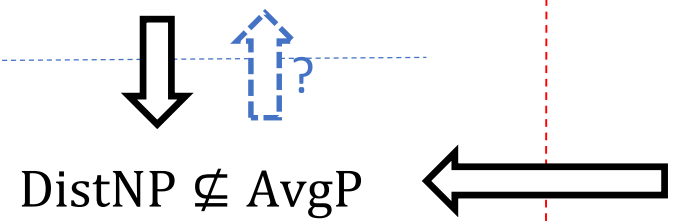
Theorem [Liu & Pass (FOCS'20)]
 \exists one-way function if and only if
 MINKT is hard for **two-sided-error** average-case algorithms.

Cryptomania \exists public-key crypto.

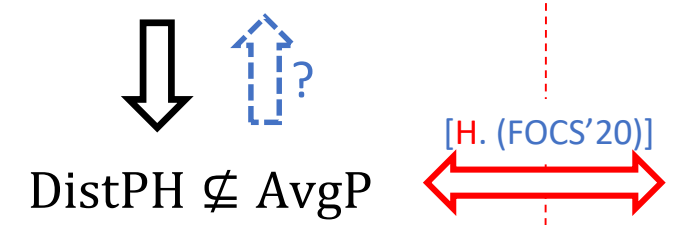
Minicrypt



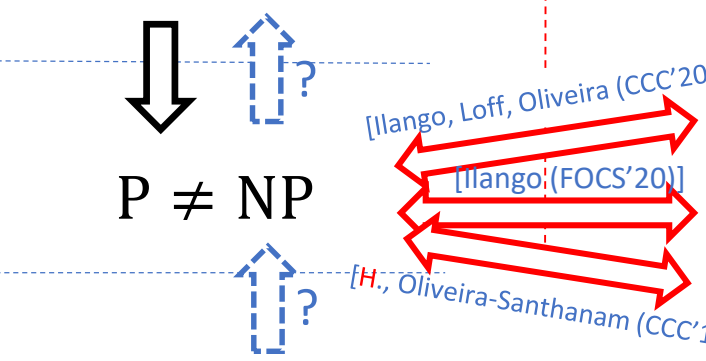
Pessiland



Heuristica



Algorithmica



MINKT \notin HeurP

MINKT \notin AvgP \iff GapMINKT \notin P

MINKT^{PH} \notin AvgP \iff GapMINKT^{PH} \notin P

MultiMCSP \notin P

AC⁰-MCSP \notin P

DNF \circ XOR-MCSP \notin P

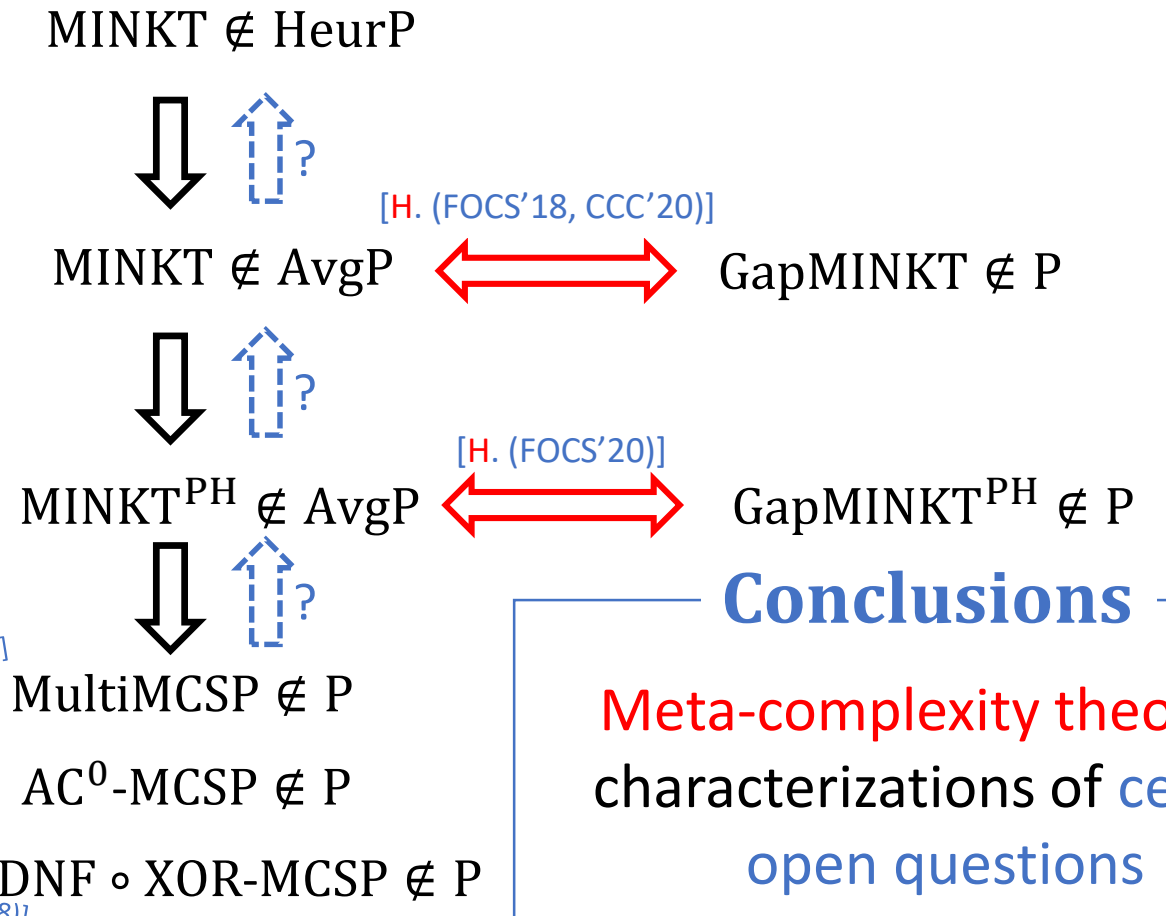
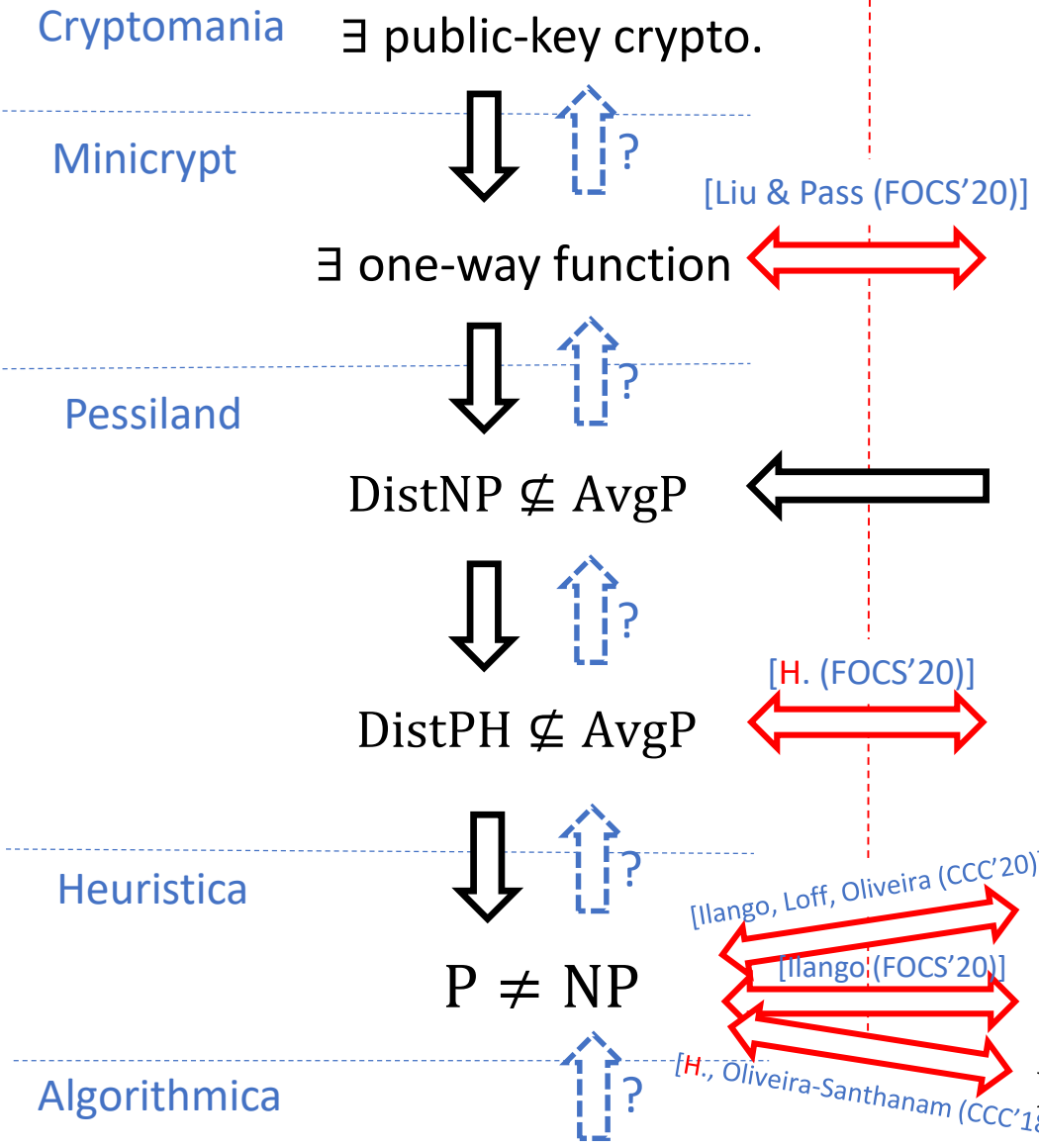
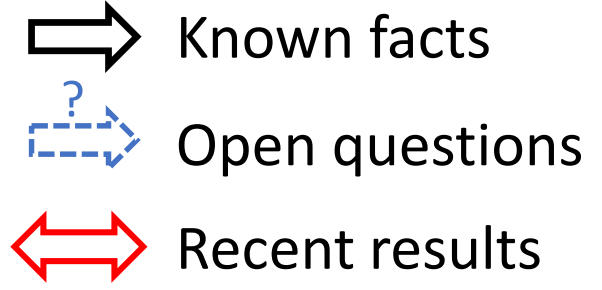
Open Question

- Is there a difference between errorless and **two-sided-error** average-case notions for MINKT?

Recent results

Impagliazzo's Five Worlds

Meta-Complexity Worlds



Conclusions

Meta-complexity theoretic characterizations of central open questions

Summary

- Recent results provide **meta-complexity-theoretic** characterizations of **central open questions in complexity theory**.
- A **meta-complexity view** is useful (and appears promising):
E.g., A **hardness amplification theorem** for PH via **meta-complexity** [H. (FOCS'20)]
- **Open**: Does $\text{GapMINKT} \in \text{P}$ imply $\text{DistNP} \subseteq \text{AvgP}$?
This implies a hardness amplification theorem for NP [H. (FOCS'20)]
- Questions or comments?