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]

  $\approx$ "the problem of computing the circuit complexity of a given function f"

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

  $\approx$ "the problem of computing the time-bounded Kolmogorov complexity of a given string x"

Recent Progress on Meta-Complexity

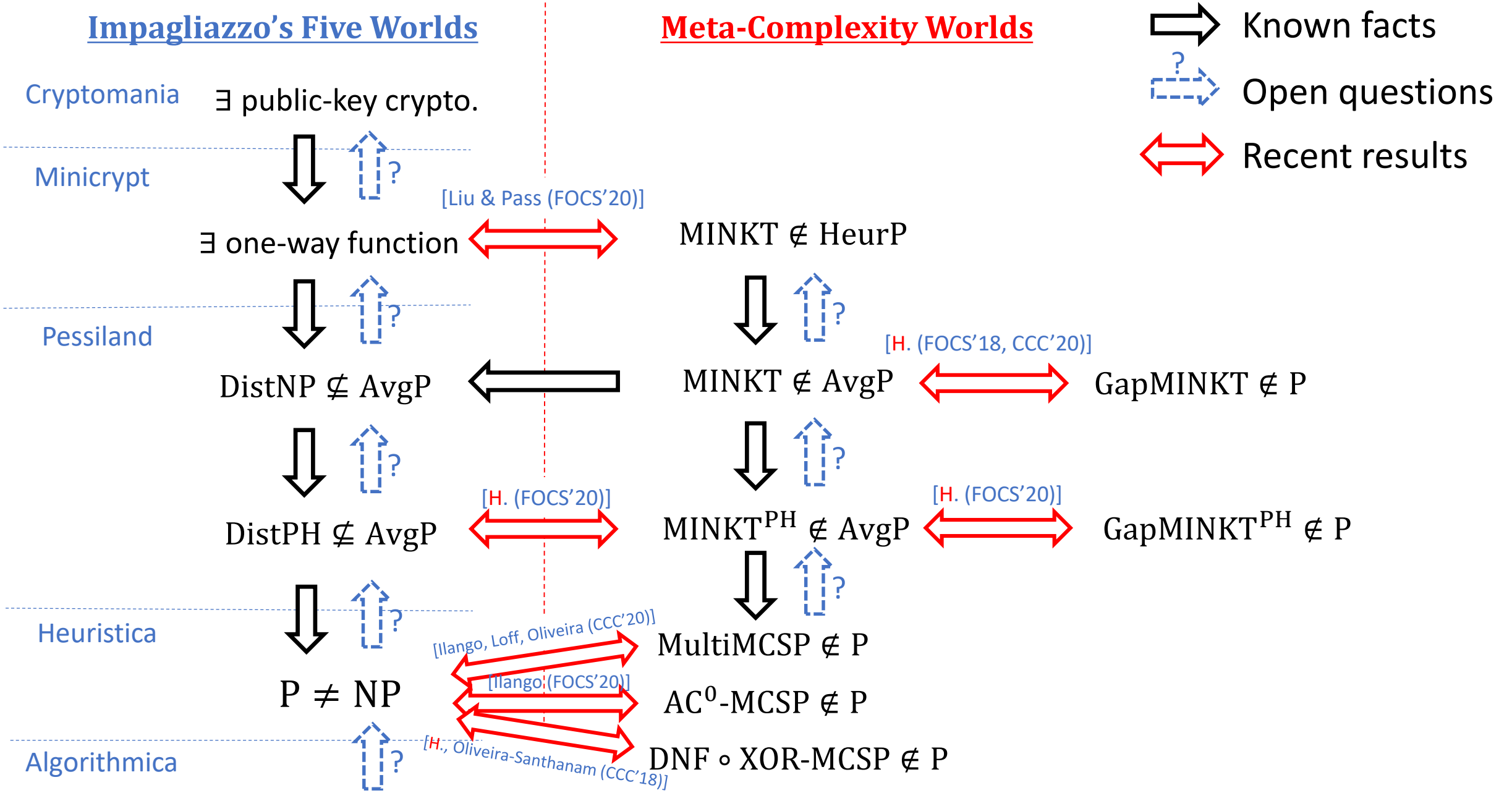
- Many papers have been published recently. For example:

  [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

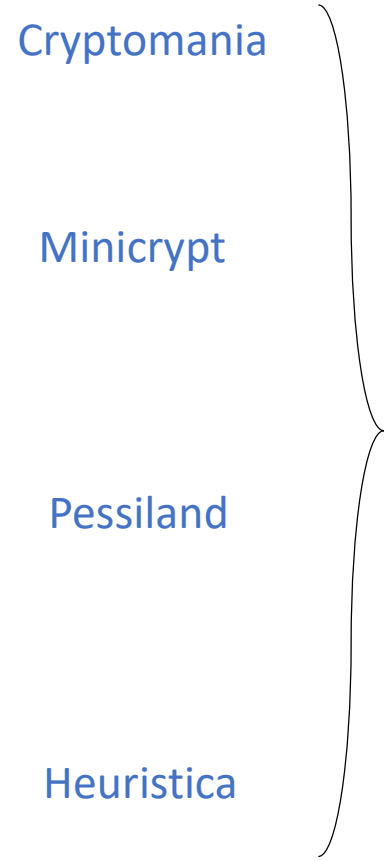
- Focus on average-case complexity, meta-complexity, and Impagliazzo's five worlds.
- Try to convey high-level ideas and might ignore technical details.

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


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
DistPH ∉ AvgP
[H. (FOCS'20)]
MINKT^PH ∉ AvgP
[H. (FOCS'20)]
GapMINKT^PH ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC^0-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica

Impagliazzo's five worlds and Minimum Circuit Size Problem

Impagliazzo's five worlds



$P \neq NP$

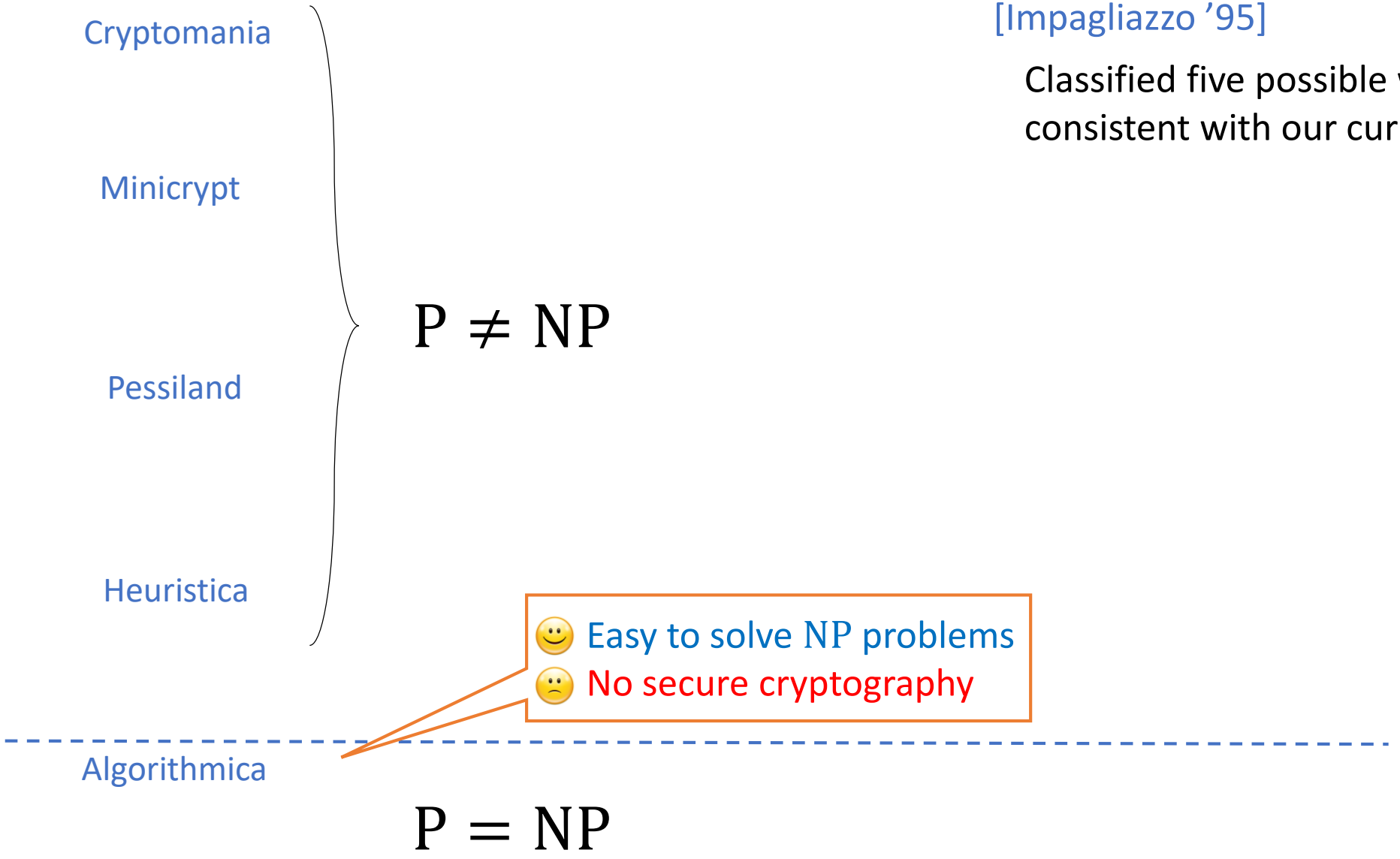
[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

Algorithmica

$P = NP$

Impagliazzo's five worlds



[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes

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

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

---

Heuristica

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

Algorithmica

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

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes

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

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

🙂 Easy to solve NP **on average**

😕 Hard to solve NP **in the worst-case**

Heuristica

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

Algorithmica

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

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes

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.

Pessiland

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

Heuristica

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

Algorithmica

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

The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes

Impagliazzo's five worlds

[Impagliazzo '95]

Classified five possible worlds consistent with our current knowledge.

Cryptomania

∃ 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

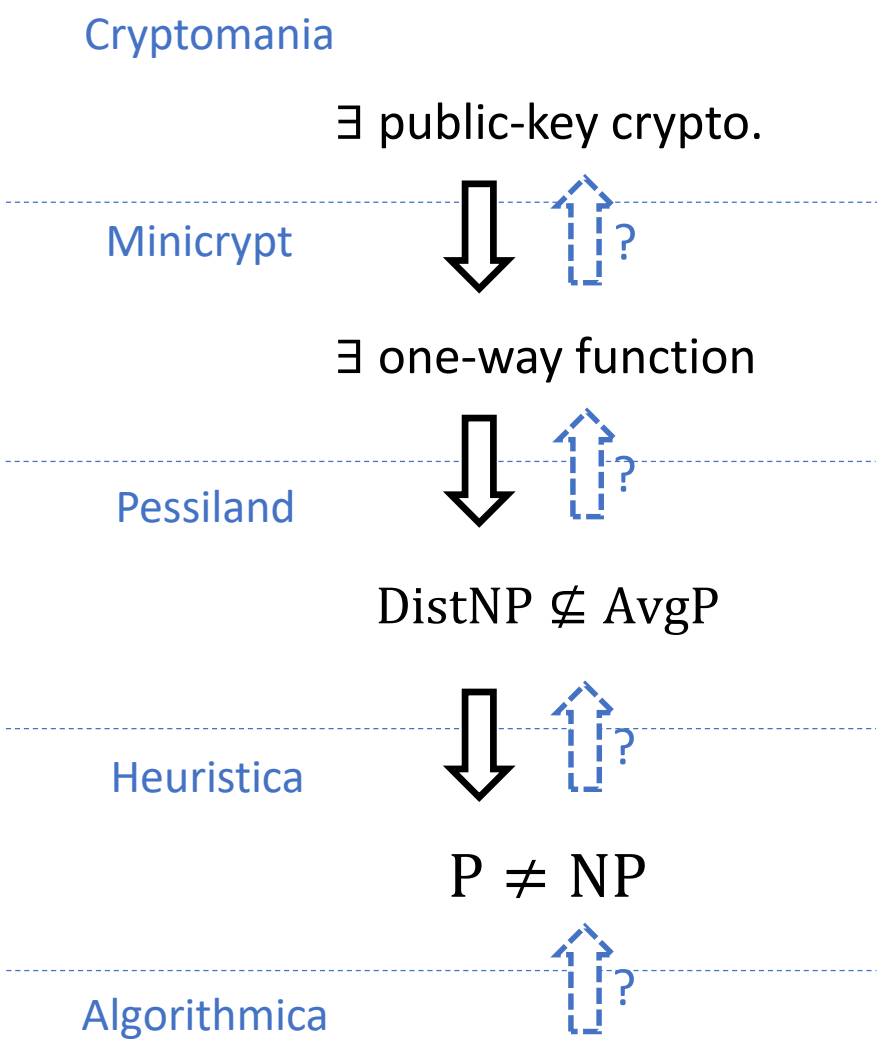
$P \neq NP$ & $DistNP \subseteq AvgP$

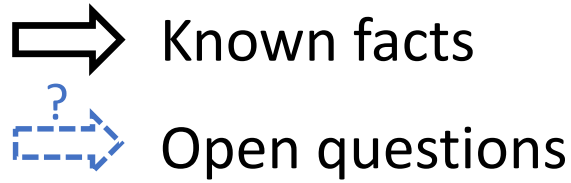
Algorithmica

$P = NP$

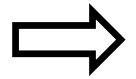
The icons are from https://commons.wikimedia.org/wiki/Category:Oxygen_icons_emotes

Known Facts and Open Questions





Towards Cryptomania



Known facts

Open questions

Cryptomania

∃ public-key crypto.

Minicrypt

Open Question

Can we exclude Minicrypto from possible worlds?

∃ one-way function

Pessiland

Open Question

Can we exclude Pessiland from possible worlds?

DistNP ⊄ AvgP

Heuristica

Open Question

Can we exclude Heuristica from possible worlds?

P ≠ NP

Algorithmica

Open Question

P ≠ NP (⟺ Can we exclude Algorithmica?)

Proving all the implications

⟺

Our world is Cryptomania

Proving a implication

⟺

Excluding a world

Limits of Current Proof Techniques


Known facts


Open questions

: a barrier result

Certain proof techniques are
not sufficient to resolve the question.

Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊈ AvgP

Heuristica

P ≠ NP

Algorithmica

Relativization barrier [Baker-Gill-Solovey '75]

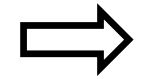
Algebrization barrier [Aaronson & Wigderson '09]

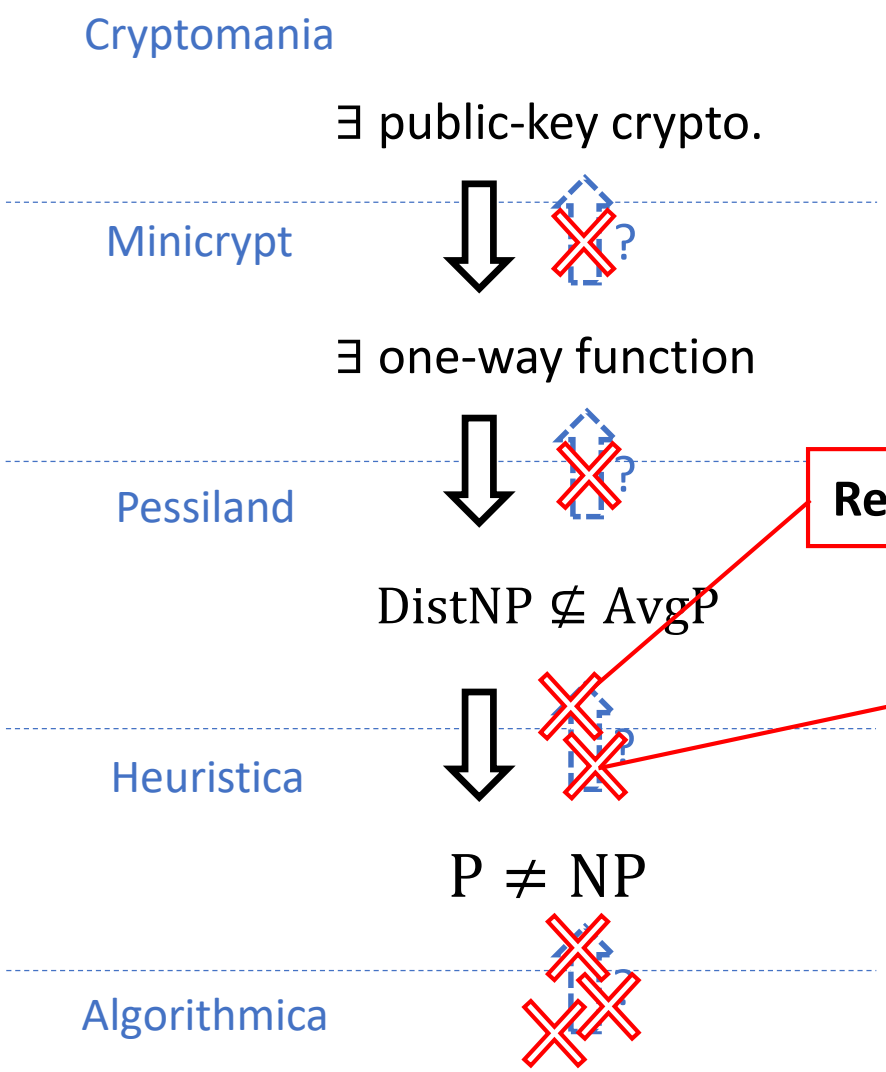
Natural proof barrier [Razborov & Rudich '97]

Proving all the implications
⇔
Our world is Cryptomania

Proving a implication
⇔
Excluding a world

Limits of Current Proof Techniques





: a barrier result

Certain proof techniques are
not sufficient to resolve the question.

Relativization barrier [Impagliazzo '11]

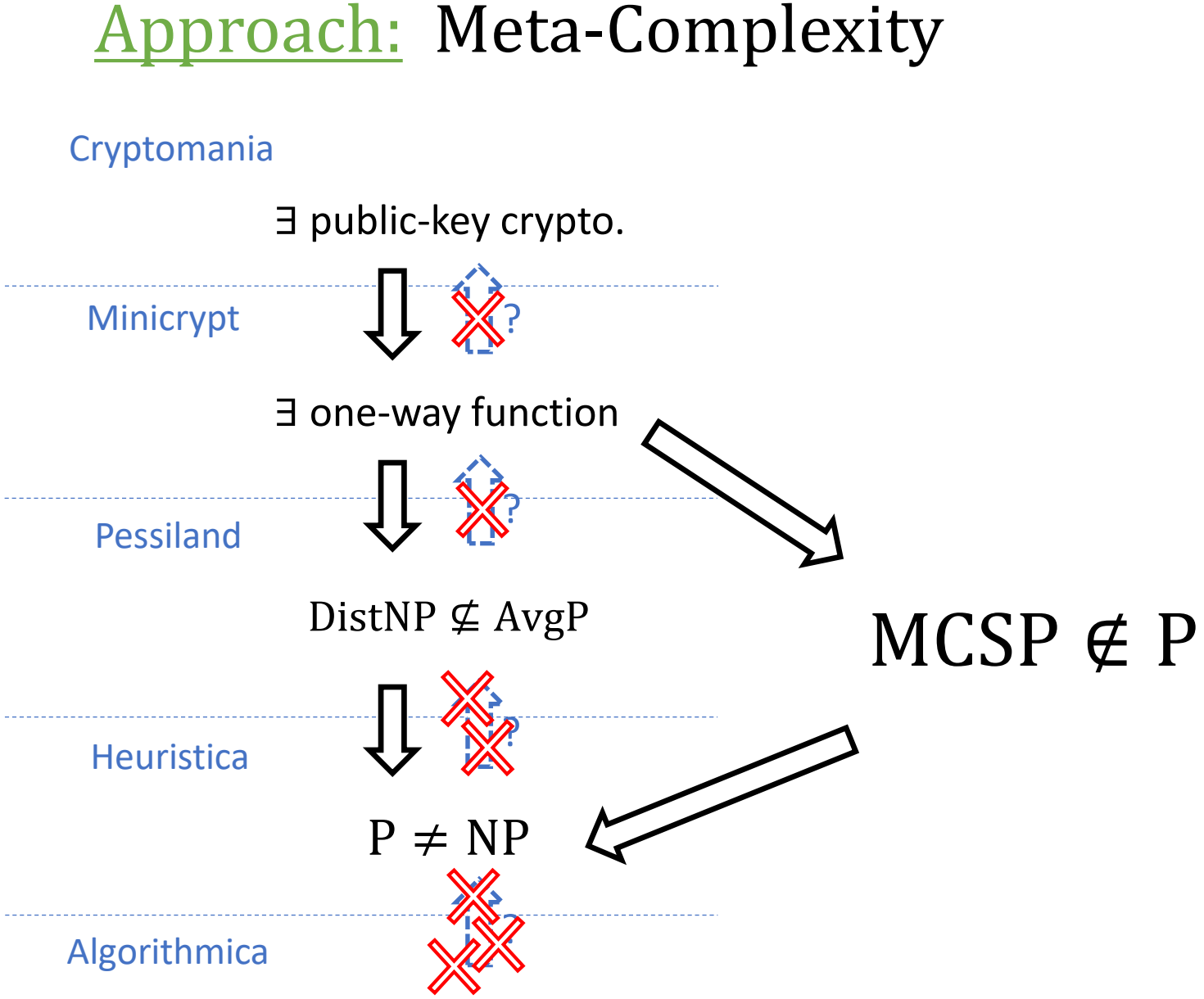
Limits of black-box reductions

[Feigenbaum & Fortnow '93]
[Bogdanov & Trevisan '06]

Proving all the implications
⇔
Our world is Cryptomania

Proving a implication
⇔
Excluding a world

Approach: Meta-Complexity



Proving all the implications
⇔
Our world is Cryptomania

Proving a implication
⇔
Excluding a world

Minimum Circuit Size Problem (MCSP)

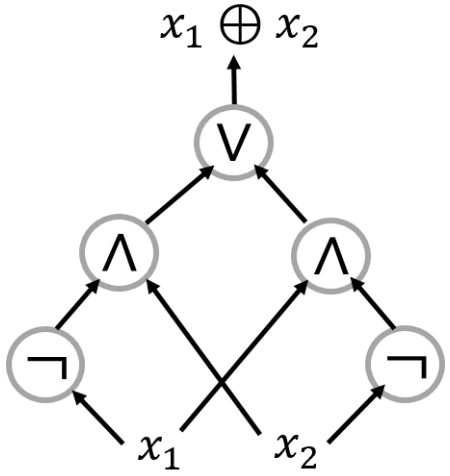
(informal) [Kabanets & Cai '00]

Input

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

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)

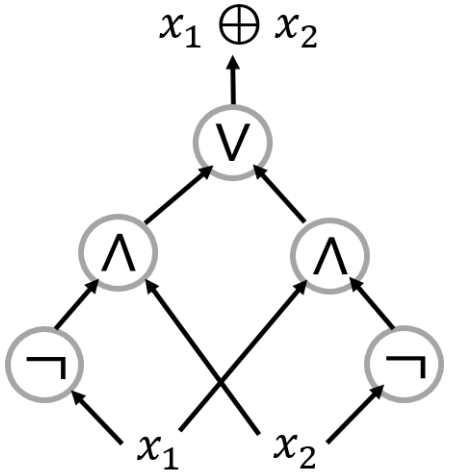
[Kabanets & Cai '00]

Input

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

Output

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



Example $\text{truthtable}(\oplus_2) = 0110$ $\text{size}(\oplus_2) = 3$

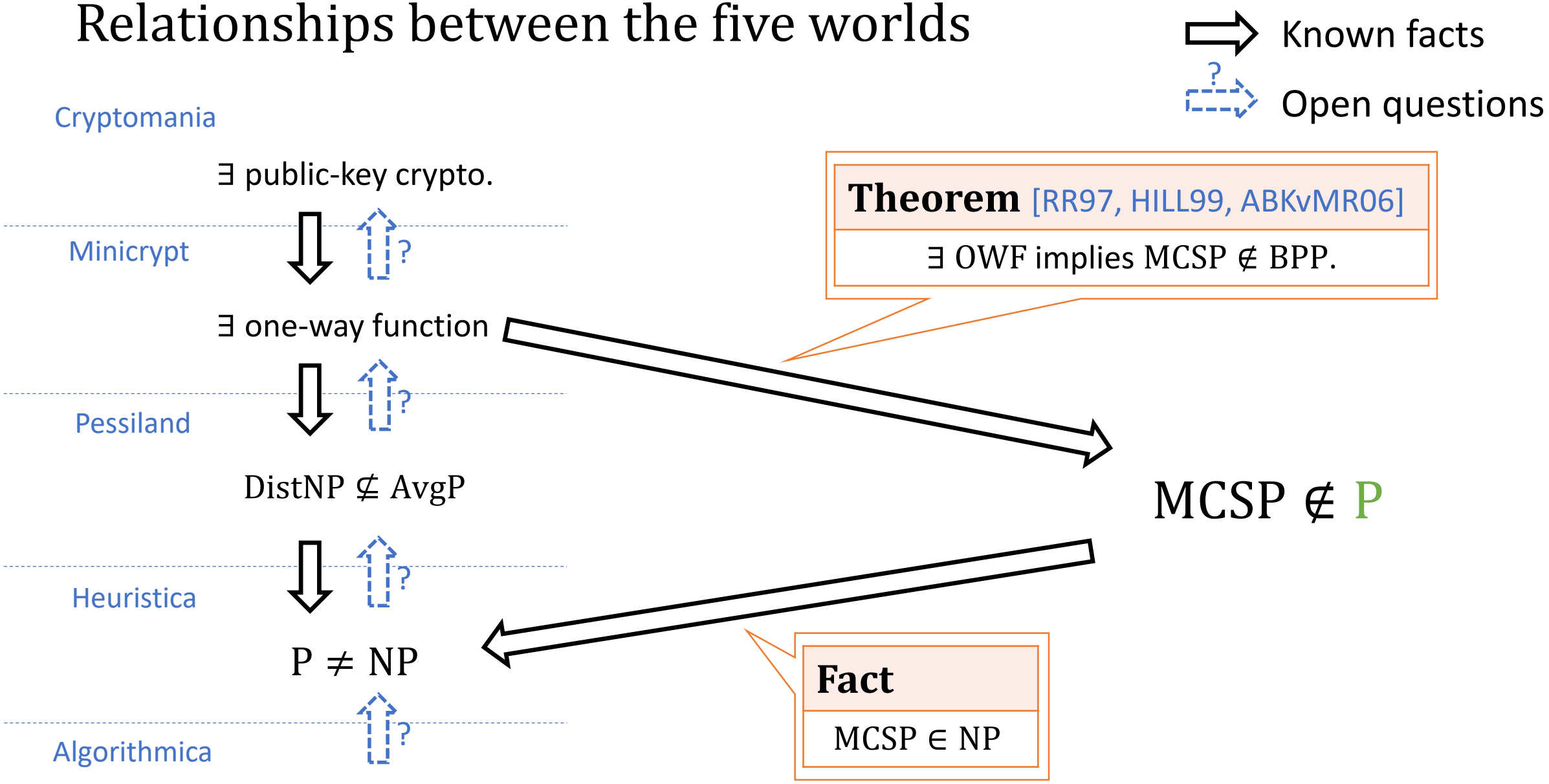
MCSP = "the problem of computing the circuit complexity of f"

- A representative example of meta-complexity-theoretic problems

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

Open: **NP**-hardness of MCSP

Relationships between the five worlds



Relationships between the five worlds

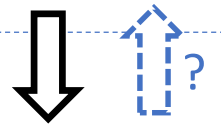
Known facts

Open questions

Cryptomania

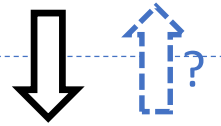
∃ public-key crypto.

Minicrypt



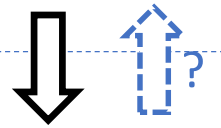
∃ one-way function

Pessiland



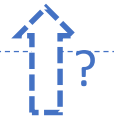
DistNP ⊈ AvgP

Heuristica



P ≠ NP

Algorithmica



Theorem [RR97, HILL99, ABKvMR06]

∃ OWF implies GapMCSP ⊈ BPP.

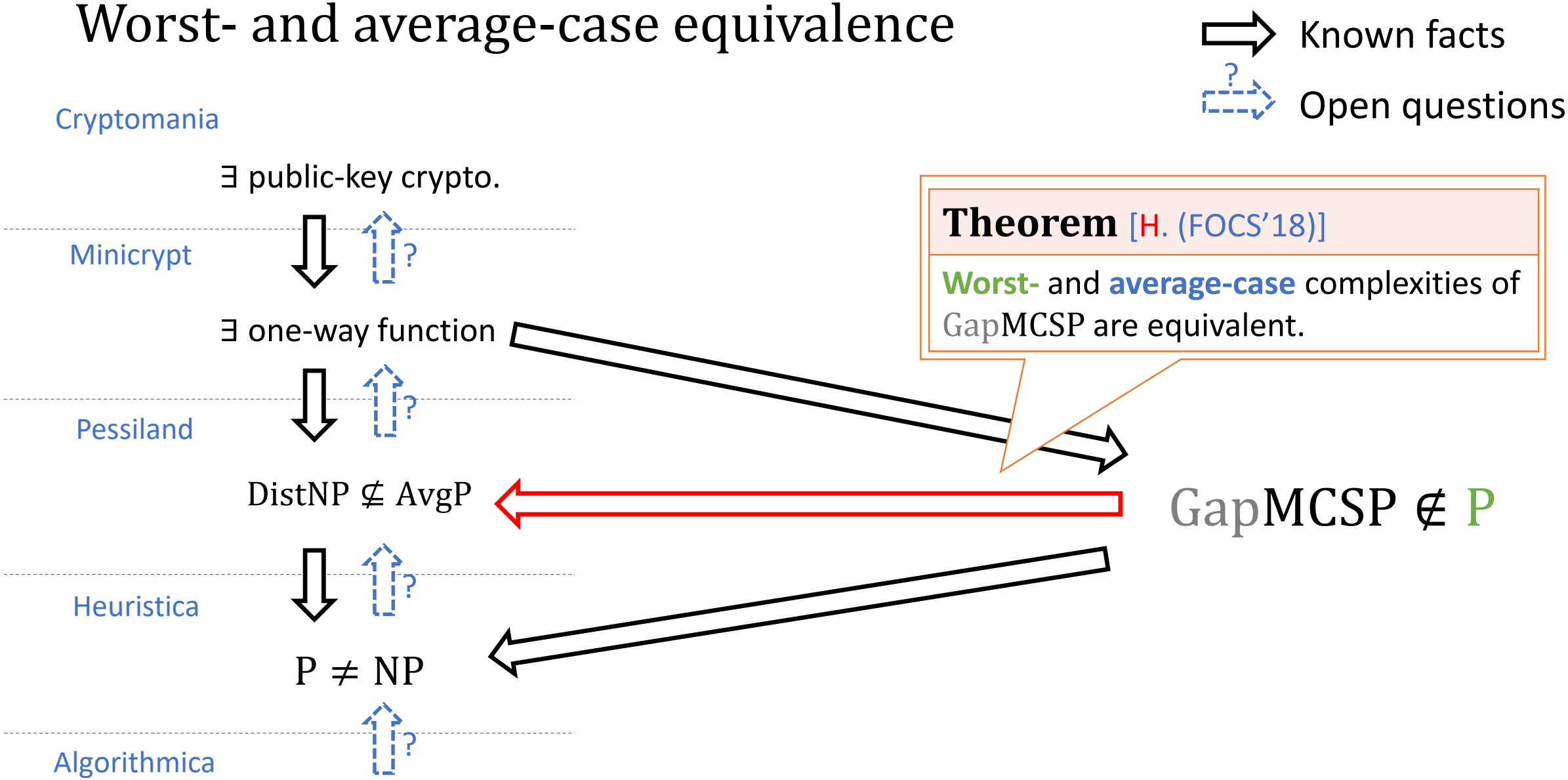
GapMCSP ⊈ P

Fact

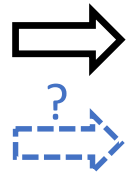
MCSP ∈ NP

Gap: An approximation version

Worst- and average-case equivalence



Worst- and average-case equivalence



Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊄ AvgP

Heuristica

P ≠ NP

Algorithmica

Obvious

MCSP ⊄ AvgP ⟺* GapMCSP ⊄ P

Theorem [H. (FOCS'18)]

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

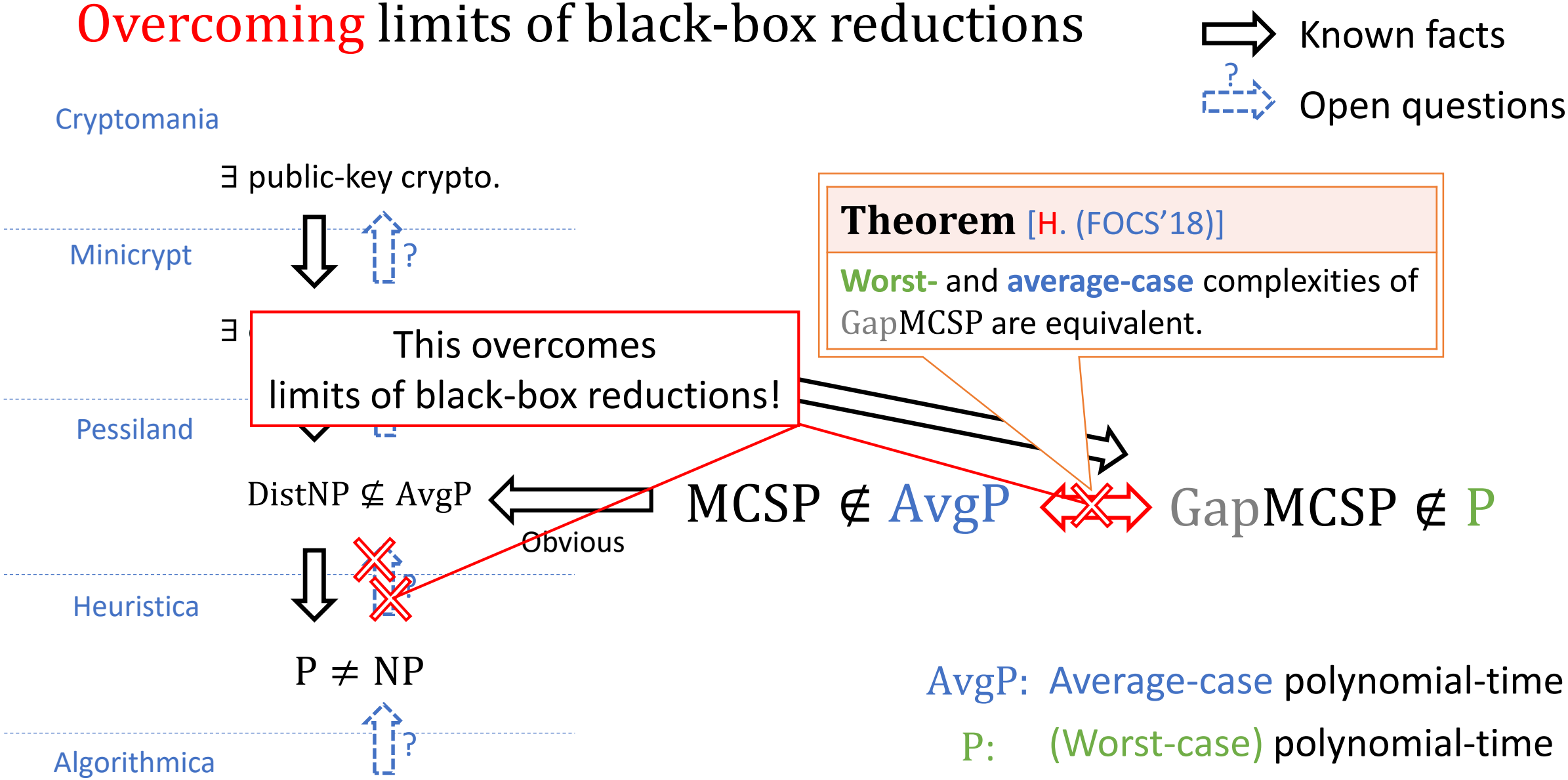
AvgP: Average-case polynomial-time

P: (Worst-case) polynomial-time

Gap: An approximation version

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

Overcoming limits of black-box reductions



Overcoming limits of black-box reductions

Known facts

Open questions

Cryptomania

∃ public-key crypto.

Minicrypt

∃

This overcomes limits of black-box reductions!

Pessiland

DistNP ⊄ AvgP

Obvious

MCSP ⊄ AvgP

GapMCSP ⊄ P

Heuristica

Algo

Theorem [H. (FOCS'18)]

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

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

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

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

(unlikely!)

AvgP = Average-Case Poly-time = Errorless Heuristics

$(L, \mathcal{D}) \in \text{AvgP} \overset{\text{def}}{\iff}$ $\exists$ alg. A 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:

$(L, \mathcal{D}) \in \text{AvgP} \overset{\text{def}}{\iff}$ $\exists$ alg. A 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 ⊄ AvgP

Obvious

MCSP ⊄ AvgP ⟺ GapMCSP ⊄ P

Corollary of "⟺"

If GapMCSP is NP-hard,
then Heuristica is excluded.

Open Question

Can we exclude Heuristica?

P ≠ NP

Algorithmica

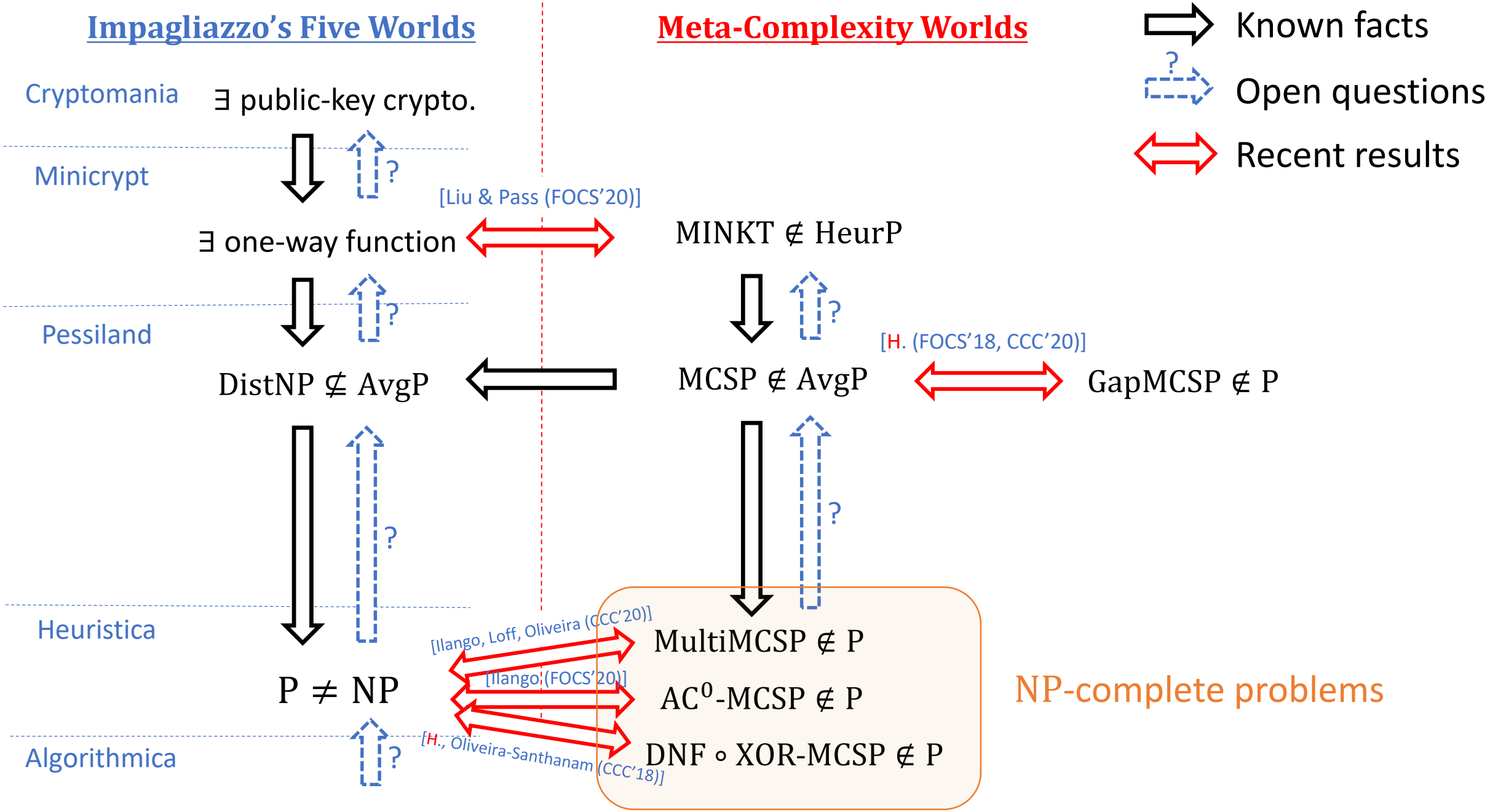
Open Question

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
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MCSP ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMCSP ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
[Ilango (FOCS'20)]
[H., Oliveira-Santhanam (CCC'18)]
MultiMCSP ∉ P
AC⁰-MCSP ∉ P
DNF ∘ XOR-MCSP ∉ P
NP-complete problems
Algorithmica

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 $\mathcal{C} \in \{\mathrm{DNF}, \mathrm{AC}^0, \dots\}$.

Definition ($\mathcal{C}$-MCSP)

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

NP-hardness of DNF-MCSP

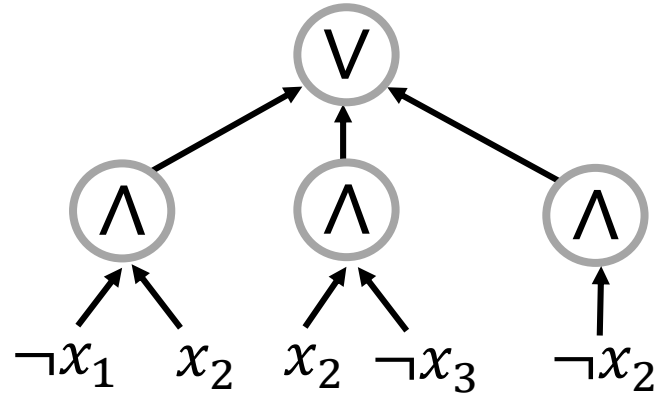
- Nearly 40 years ago, Masek proved NP-hardness of DNF-MCSP.

Theorem [Masek (1978 or 1979, unpublished)]

DNF-MCSP is NP-hard.

Examples of DNF formula

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



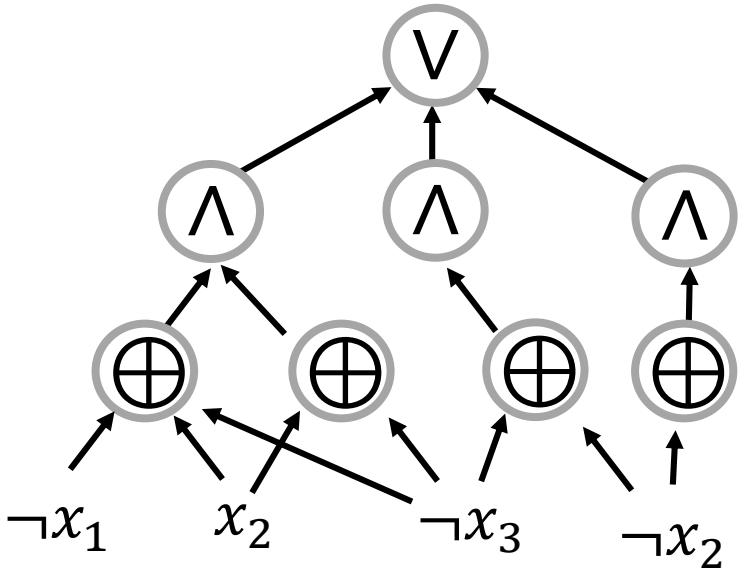
NP-hardness of $(\mathrm{DNF} \circ \mathrm{XOR})$-MCSP

- We were able to extend DNF formulas to $\mathrm{DNF} \circ \mathrm{XOR}$ formulas.

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

$(\mathrm{DNF} \circ \mathrm{XOR})$-MCSP is NP-hard.

A $\mathrm{DNF} \circ \mathrm{XOR}$ formula



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

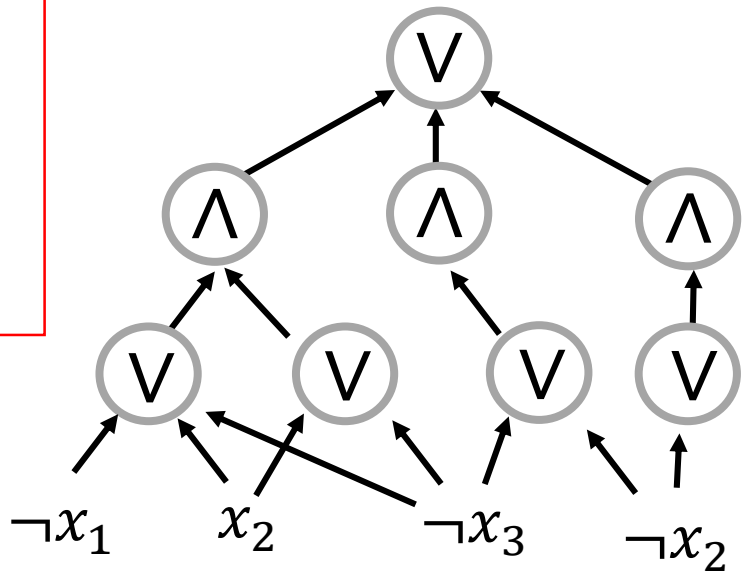
➢ [Rahul Ilango] extended the frontier to depth-d AC^0 formulas for any constant $d \geq 2$.

(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

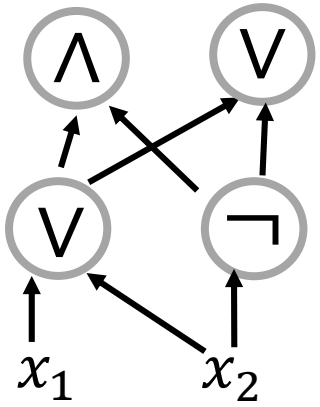
Theorem [Ilango-Loff-Oliveira (CCC'20)]

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

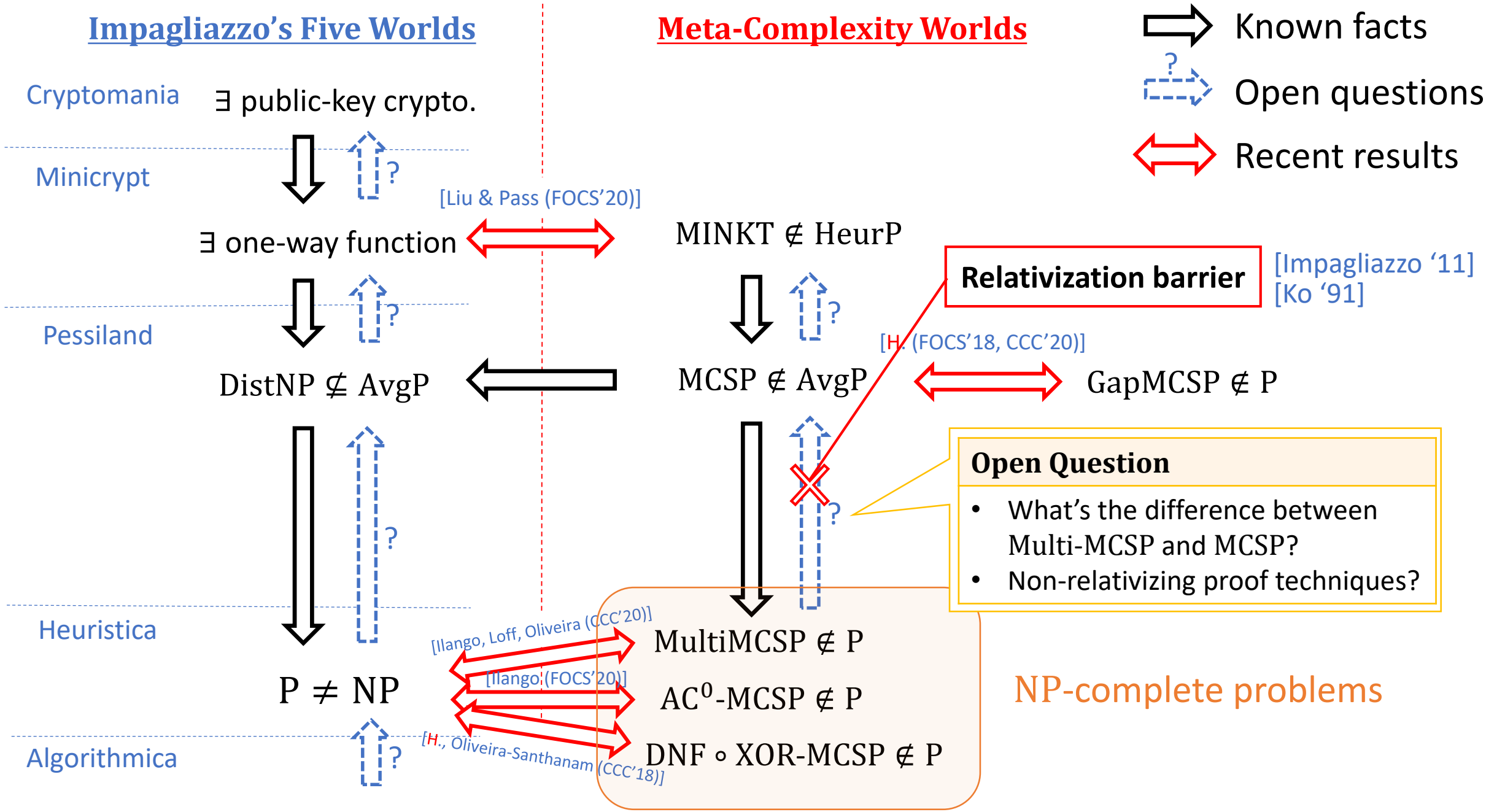
Definition (Multi-MCSP)

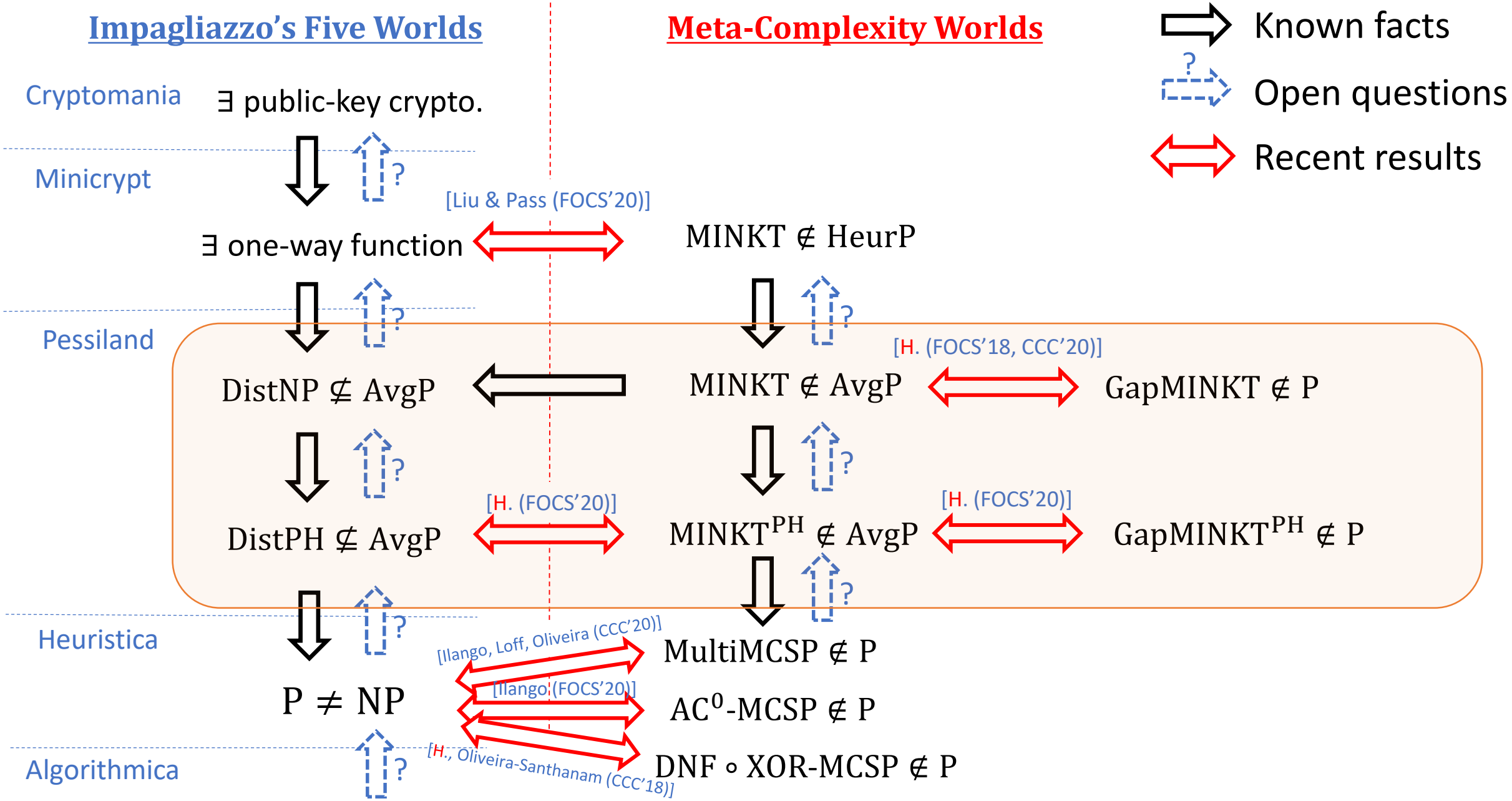
Given a function $f: \{0,1\}^n \to \{0,1\}^m$ and a size parameter s,
is there a multi-output circuit of size s computing f?

A multi-output circuit



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

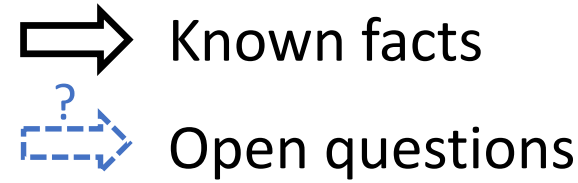

Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MCSP ∉ AvgP
Relativization barrier
[Impagliazzo '11]
[Ko '91]
[H. (FOCS'18, CCC'20)]
GapMCSP ∉ P
Open Question
What's the difference between Multi-MCSP and MCSP?
Non-relativizing proof techniques?
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
[Ilango (FOCS'20)]
[H., Oliveira-Santhanam (CCC'18)]
MultiMCSP ∉ P
AC⁰-MCSP ∉ P
DNF ∘ XOR-MCSP ∉ P
NP-complete problems
Algorithmica


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
DistPH ∉ AvgP
[H. (FOCS'20)]
MINKT^PH ∉ AvgP
[H. (FOCS'20)]
GapMINKT^PH ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC^0-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica

Average-Case Complexity versus Meta-Complexity

Towards better understanding of average-case complexity

Can we prove the converse?



Cryptomania

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊄ AvgP

Heuristica

P ≠ NP

Algorithmica

Theorem [H. (FOCS'18)]

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

$\mathrm{MCSP} \notin \mathrm{AvgP} \iff \mathrm{GapMCSP} \notin \mathrm{P}$

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

$\mathrm{K}^t(x)$ (t-time-bounded Kolmogorov complexity)

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

Example

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

$x = 1010111010101101$ $\quad \mathrm{K}^t(x) \geq n - 1$ with probability $\geq \frac{1}{2}$.

MINKT = "the problem of computing the time-bounded Kolmogorov complexity of x"

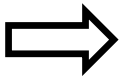
Cf. **MCSP** = "the problem of computing the circuit complexity of f"

➢ 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

∃ public-key crypto.

Minicrypt

∃ one-way function

Pessiland

DistNP ⊈ AvgP

Heuristica

P ≠ NP

Algorithmica

$\text{MINKT} \notin \text{AvgP} \overset{*}{\Longleftrightarrow} \text{GapMINKT} \notin \text{P}$

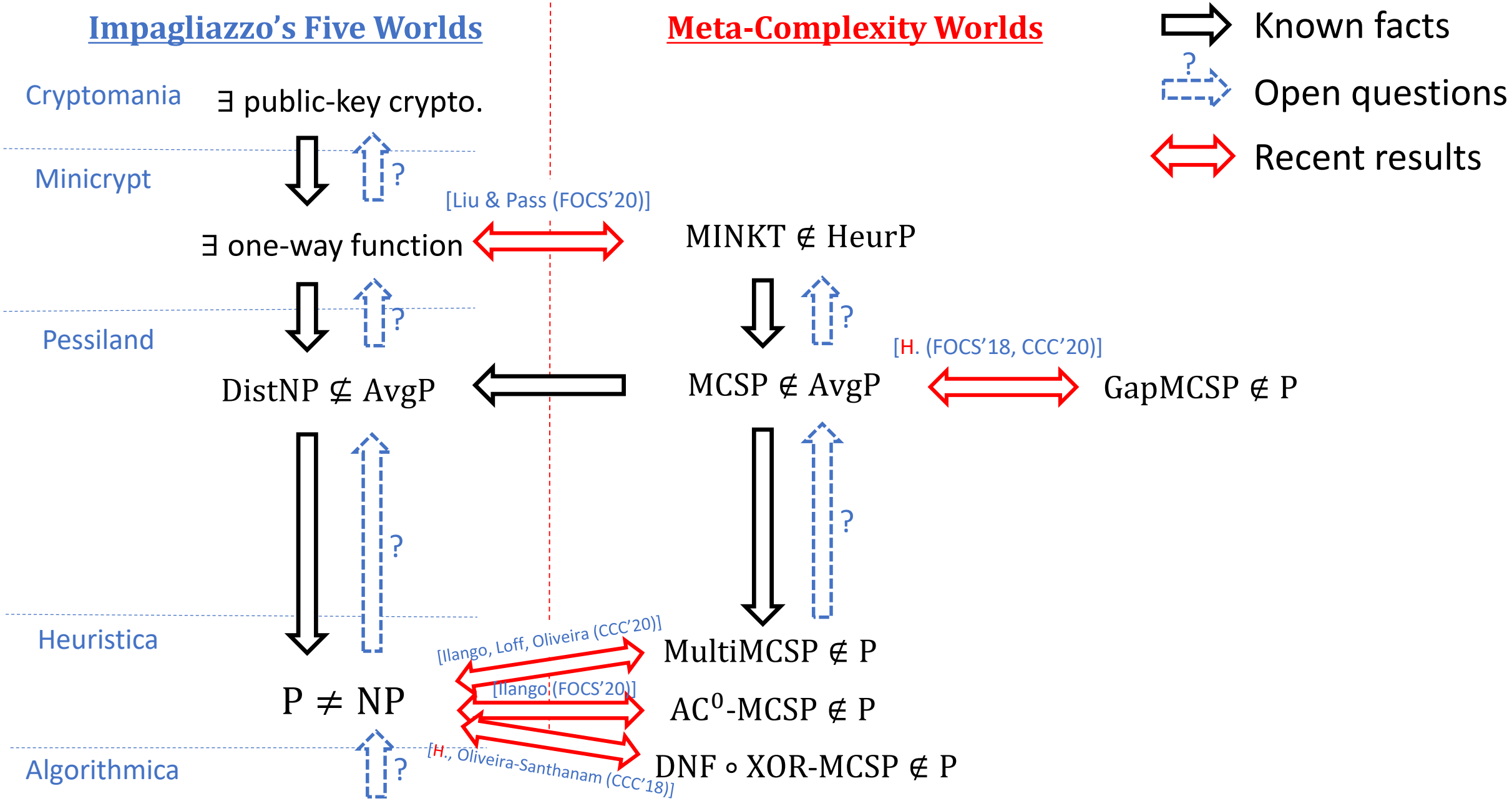
[H. & Santhanam '17]

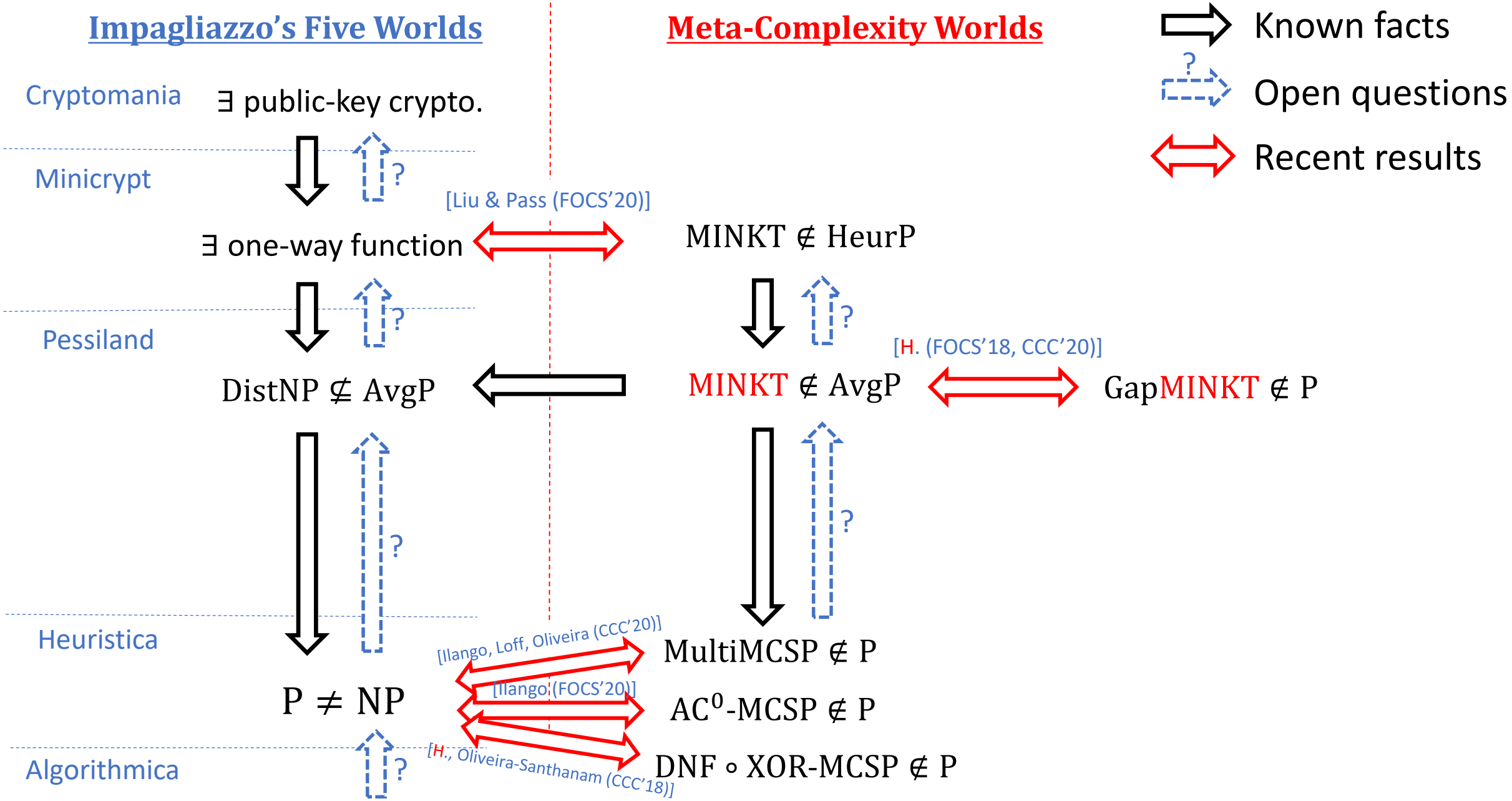
$\text{MCSP} \notin \text{AvgP} \overset{*}{\Longleftrightarrow} \text{GapMCSP} \notin \text{P}$

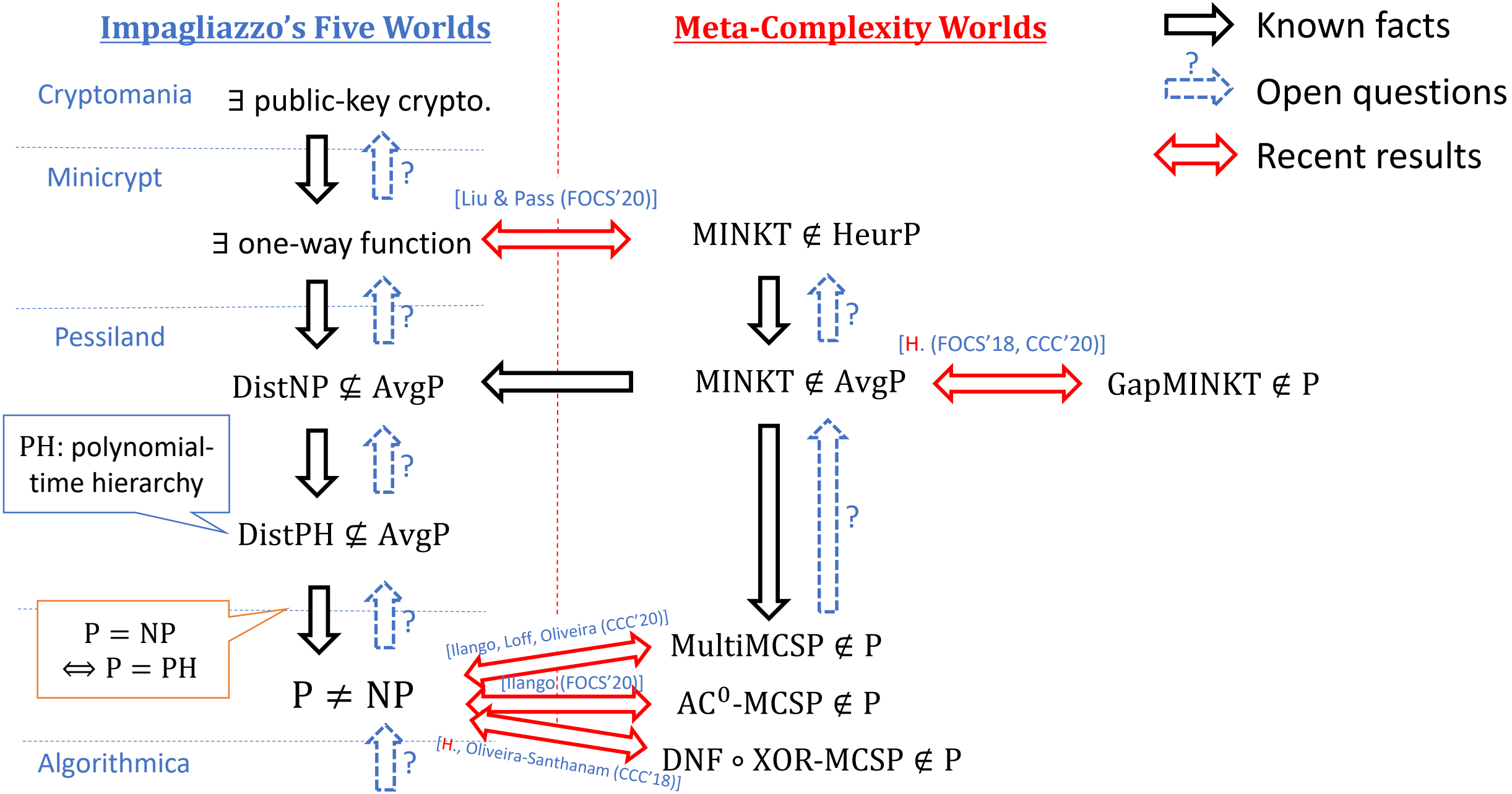
GapMINKT: a $O(\log t|x|)$-additive approximation of $\text{K}^t(x)$

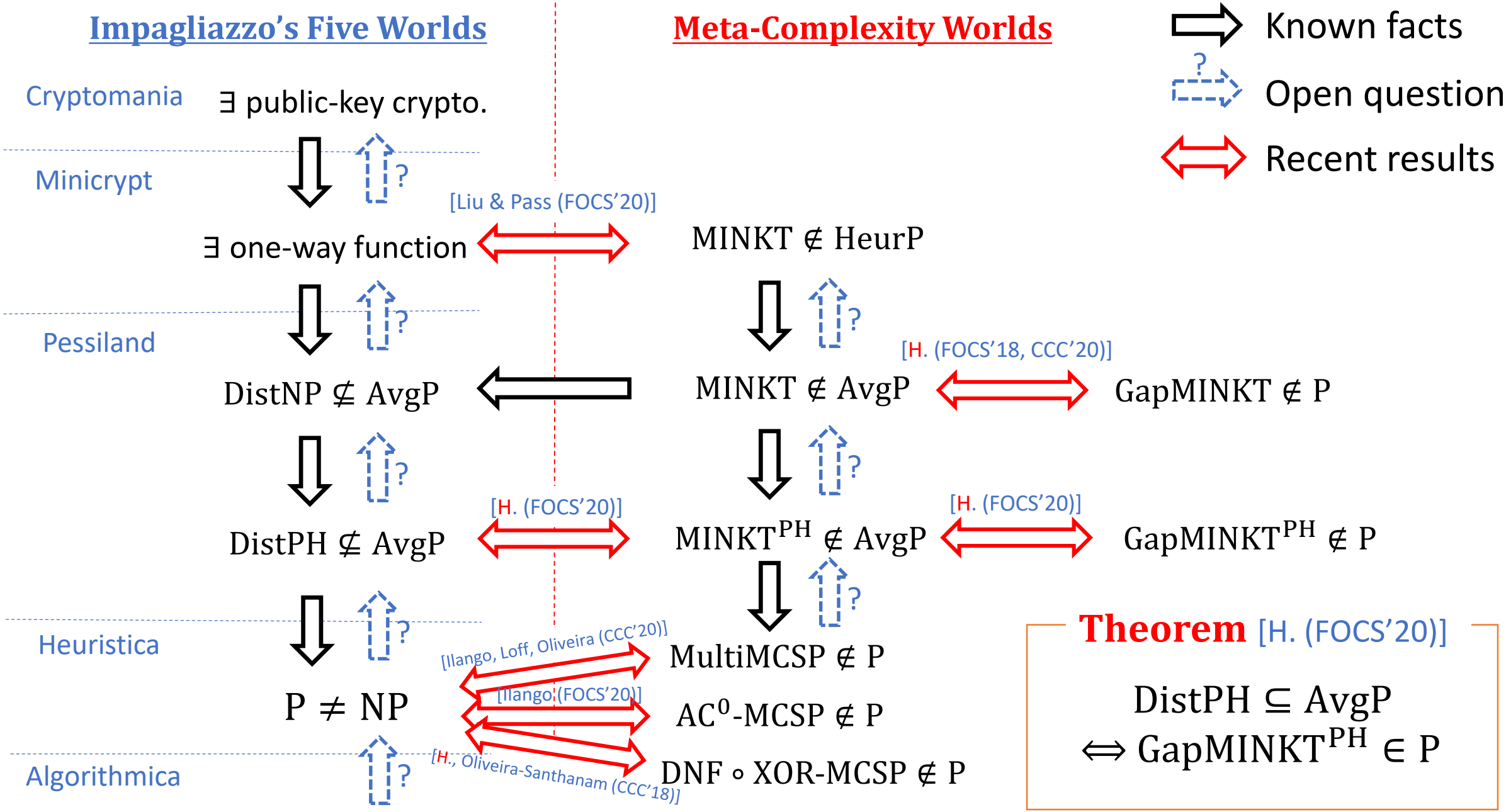
GapMCSP: a $|f|^{1-\epsilon}$-factor approximation of $\text{size}(f)$

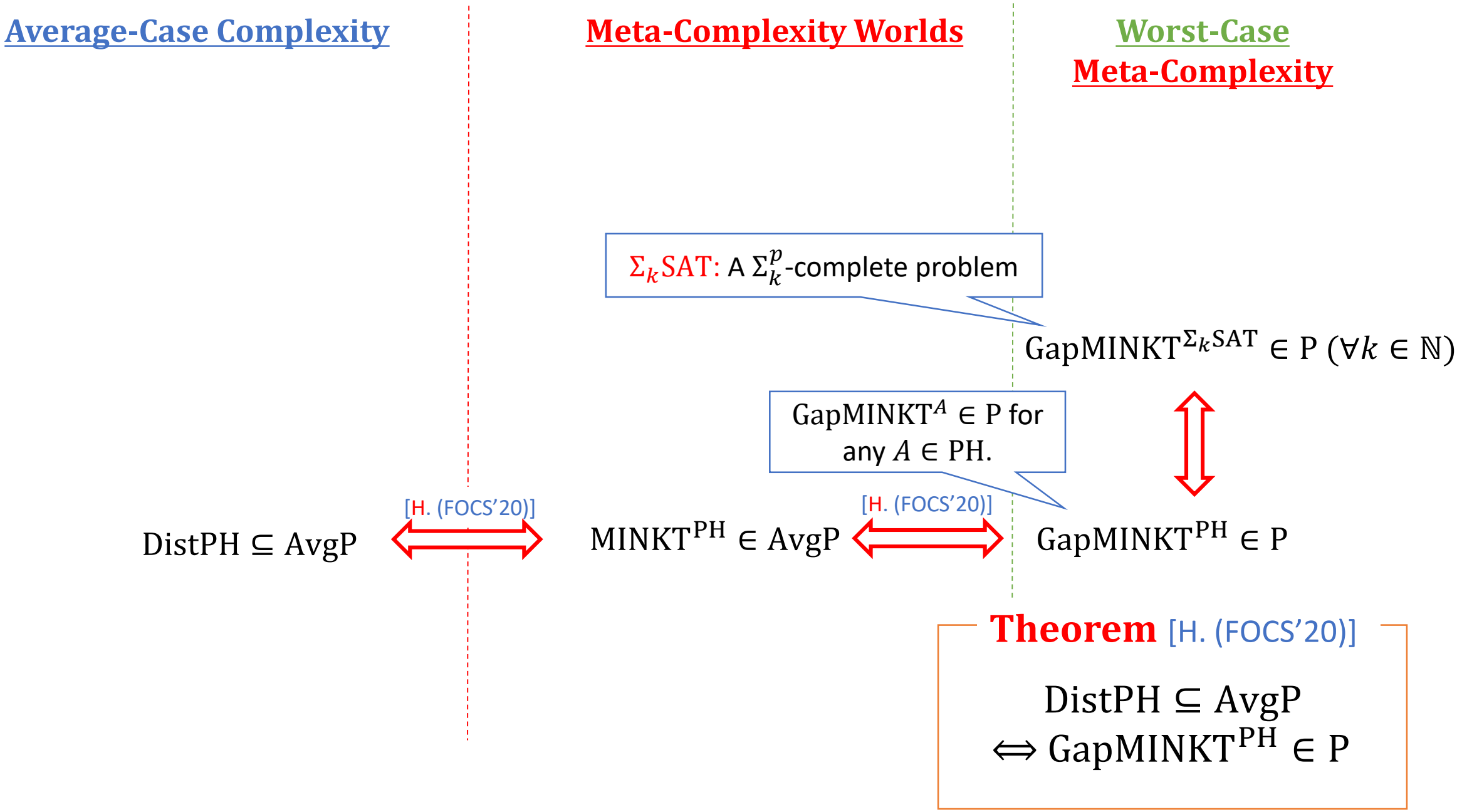
*Assuming the existence of complexity-theoretic PRG (for derandomization).

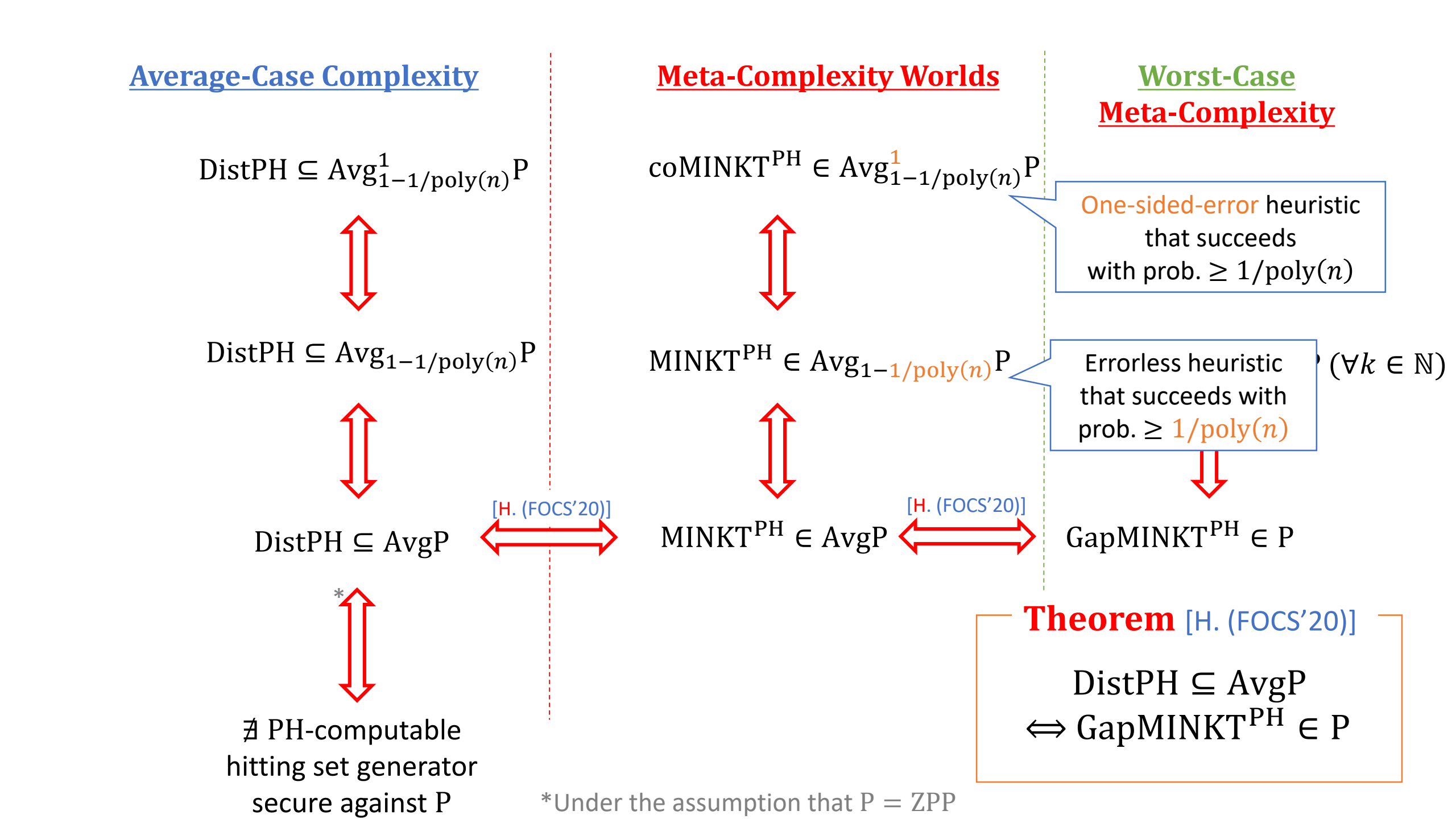

Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MCSP ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMCSP ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC⁰-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
[Ilango (FOCS'20)]
[H., Oliveira-Santhanam (CCC'18)]
MultiMCSP ∉ P
AC⁰-MCSP ∉ P
DNF ∘ XOR-MCSP ∉ P
Algorithmica


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
PH: polynomial-time hierarchy
DistPH ∉ AvgP
P = NP ⇔ P = PH
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC⁰-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
DistPH ∉ AvgP
[H. (FOCS'20)]
MINKT^PH ∉ AvgP
[H. (FOCS'20)]
GapMINKT^PH ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
[Ilango (FOCS'20)]
[H., Oliveira-Santhanam (CCC'18)]
MultiMCSP ∉ P
AC^0-MCSP ∉ P
DNF ∘ XOR-MCSP ∉ P
Algorithmica
Theorem [H. (FOCS'20)]
DistPH ⊆ AvgP
⇔ GapMINKT^PH ∈ P

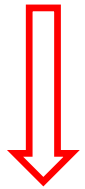

Average-Case Complexity
Meta-Complexity Worlds
Worst-Case Meta-Complexity
Σ_kSAT: A Σ_k^p-complete problem
$\mathrm{GapMINKT}^{\Sigma_k\mathrm{SAT}} \in \mathrm{P}\ (\forall k \in \mathbb{N})$
$\mathrm{GapMINKT}^{A} \in \mathrm{P}$ for any $A \in \mathrm{PH}$.
[H. (FOCS'20)]
[H. (FOCS'20)]
$\mathrm{DistPH} \subseteq \mathrm{AvgP}$
$\mathrm{MINKT}^{\mathrm{PH}} \in \mathrm{AvgP}$
$\mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$
Theorem [H. (FOCS'20)]
$\mathrm{DistPH} \subseteq \mathrm{AvgP}$
$\Leftrightarrow \mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$


Average-Case Complexity
Meta-Complexity Worlds
Worst-Case Meta-Complexity
$\mathrm{DistPH} \subseteq \mathrm{Avg}^{1}_{1-1/\mathrm{poly}(n)}\mathrm{P}$
$\mathrm{coMINKT}^{\mathrm{PH}} \in \mathrm{Avg}^{1}_{1-1/\mathrm{poly}(n)}\mathrm{P}$
One-sided-error heuristic that succeeds with prob. $\geq 1/\mathrm{poly}(n)$
$\mathrm{DistPH} \subseteq \mathrm{Avg}_{1-1/\mathrm{poly}(n)}\mathrm{P}$
$\mathrm{MINKT}^{\mathrm{PH}} \in \mathrm{Avg}_{1-1/\mathrm{poly}(n)}\mathrm{P}$
$(\forall k \in \mathbb{N})$
Errorless heuristic that succeeds with prob. $\geq 1/\mathrm{poly}(n)$
$\mathrm{DistPH} \subseteq \mathrm{AvgP}$
[H. (FOCS'20)]
$\mathrm{MINKT}^{\mathrm{PH}} \in \mathrm{AvgP}$
[H. (FOCS'20)]
$\mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$
*
$\nexists$ PH-computable hitting set generator secure against P
Theorem [H. (FOCS'20)]
$\mathrm{DistPH} \subseteq \mathrm{AvgP}$
$\Leftrightarrow \mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$
*Under the assumption that $\mathrm{P} = \mathrm{ZPP}$

Average-Case Complexity

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

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



PH is easy on most inputs

$\mathrm{DistPH} \subseteq \mathrm{AvgP}$

Meta-Complexity Worlds

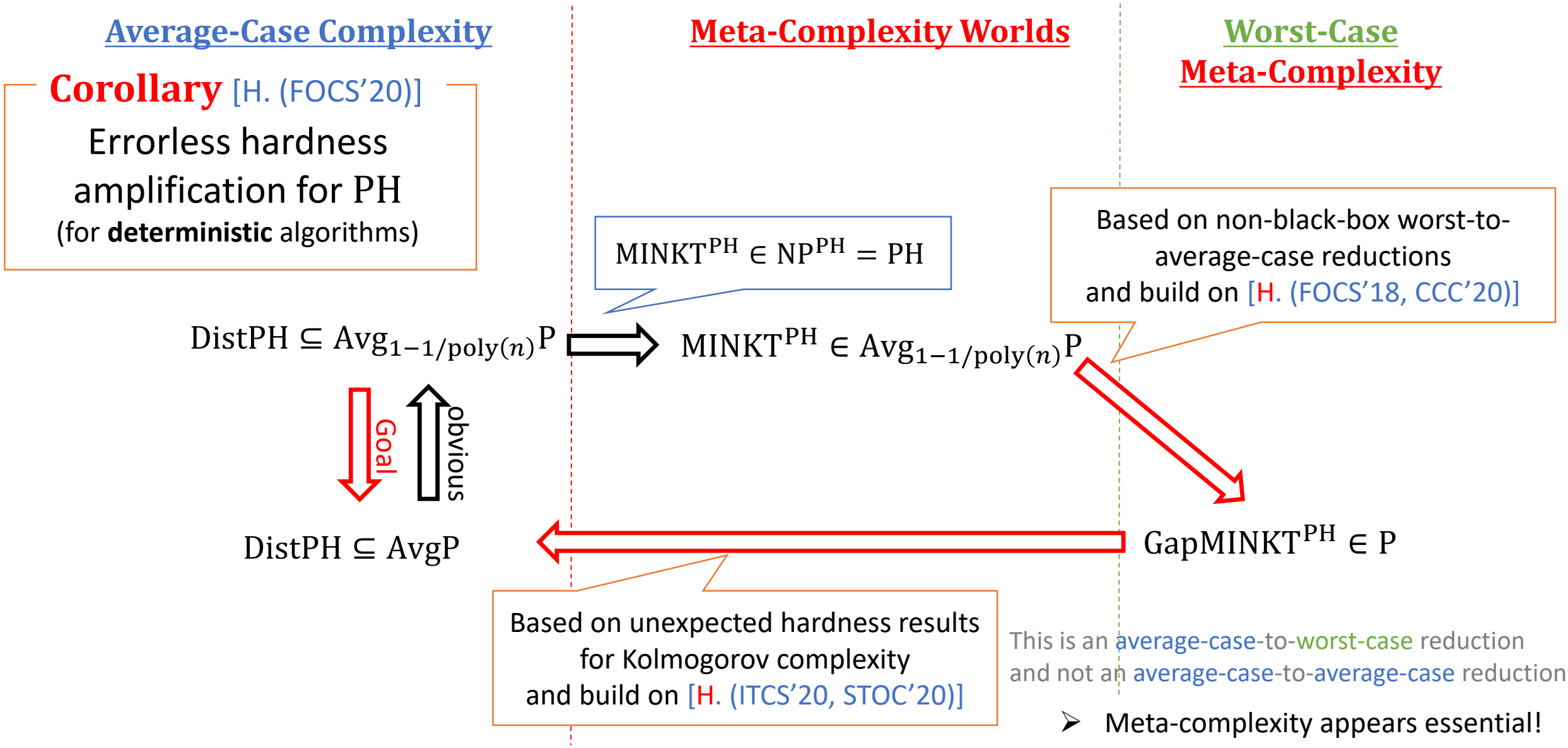
Corollary [H. (FOCS'20)]

Errorless hardness amplification for PH

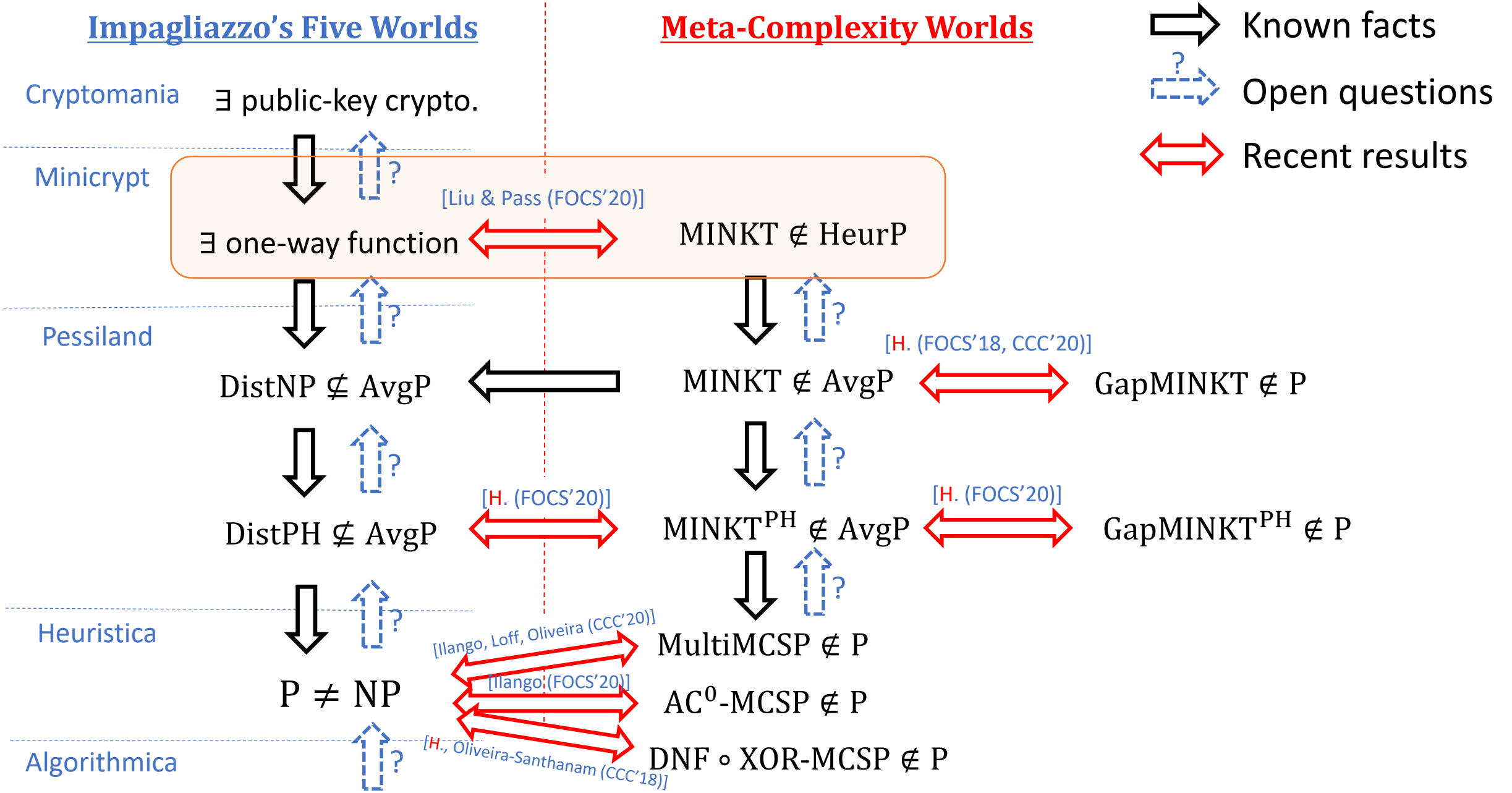
(for **deterministic** algorithms)

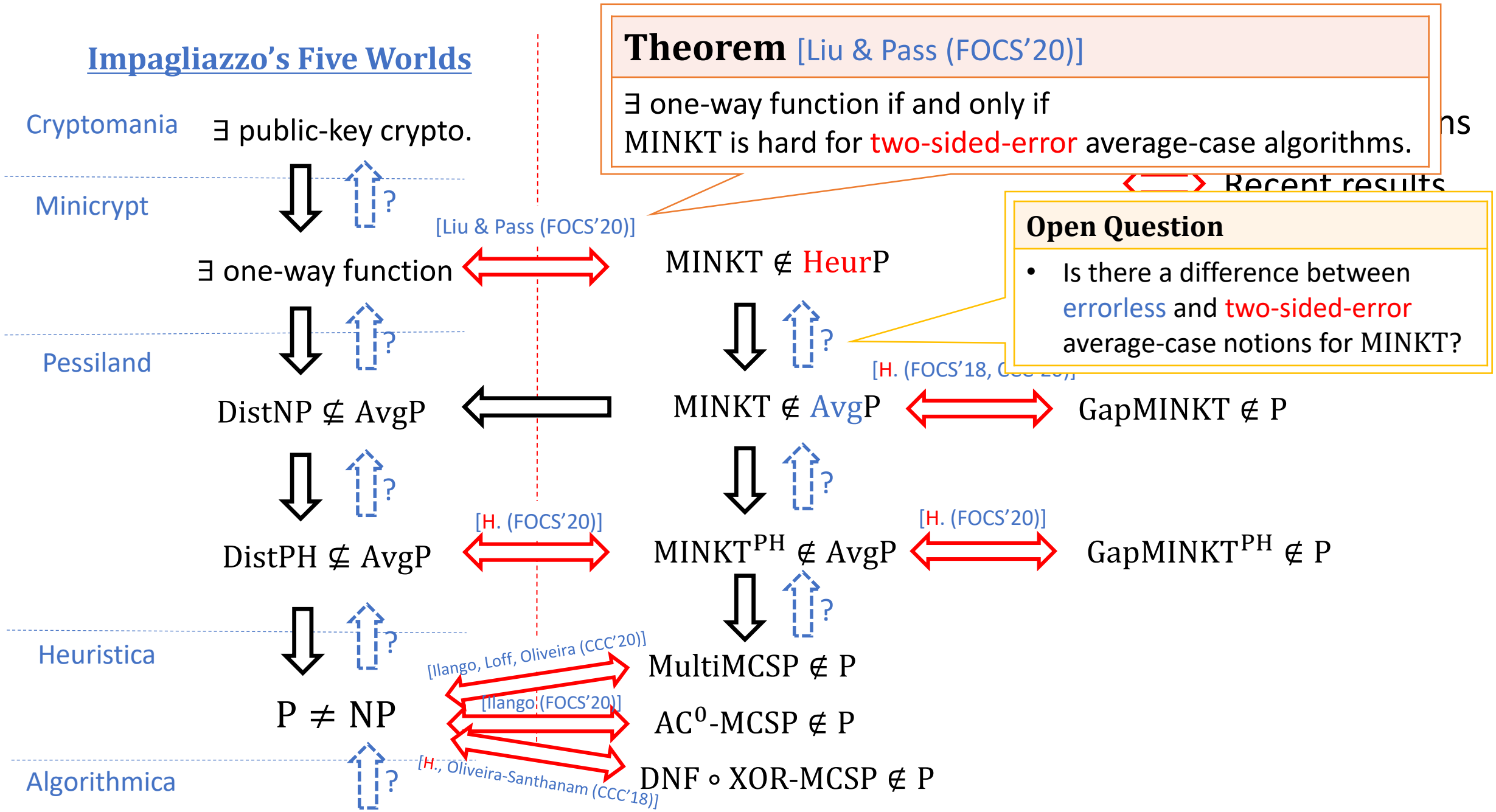
Worst-Case Meta-Complexity

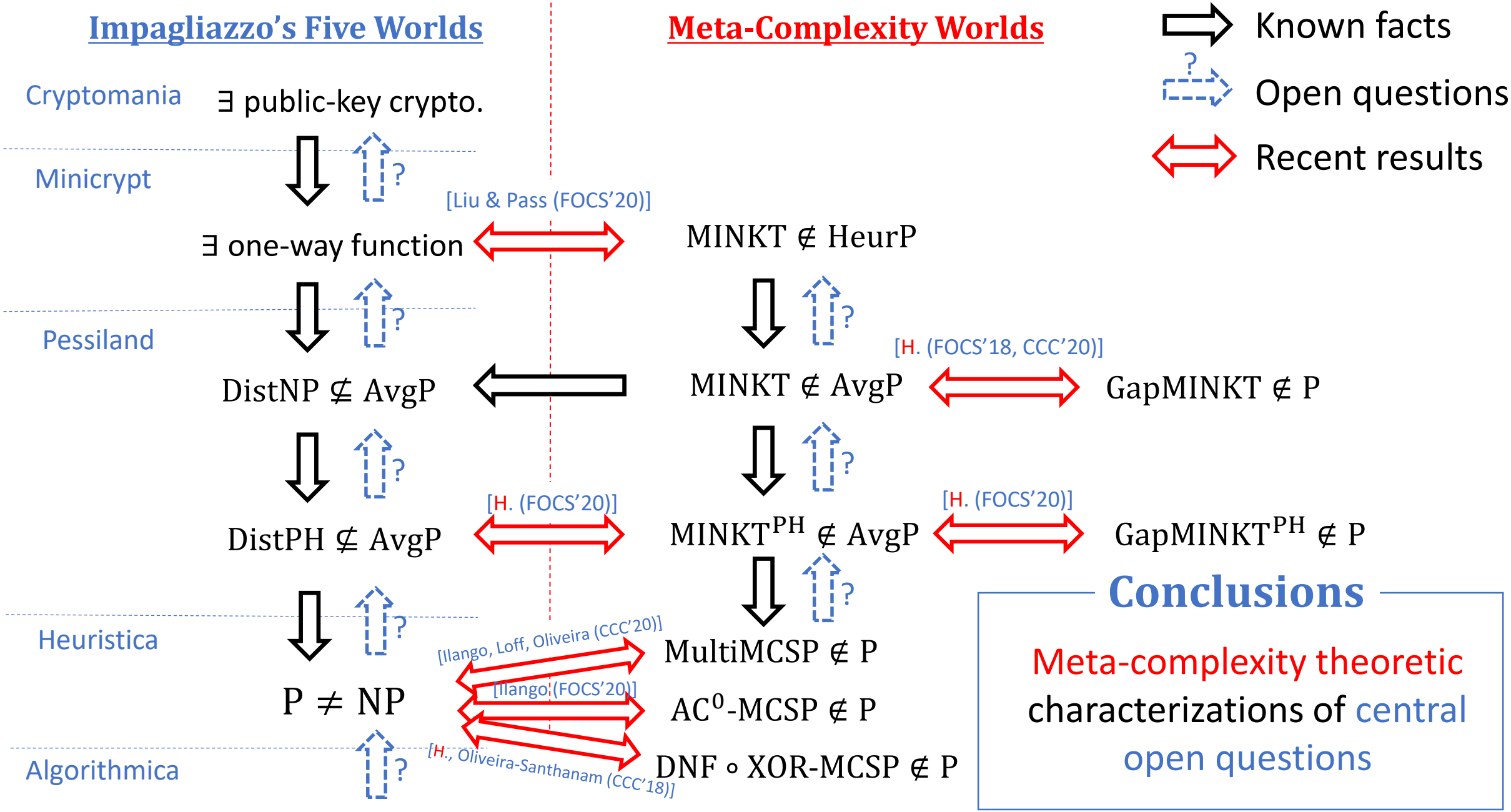
$\mathrm{GapMINKT}^{\mathrm{PH}} \in \mathrm{P}$



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


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
[Liu & Pass (FOCS'20)]
∃ one-way function
MINKT ∉ HeurP
Pessiland
[H. (FOCS'18, CCC'20)]
DistNP ∉ AvgP
MINKT ∉ AvgP
GapMINKT ∉ P
[H. (FOCS'20)]
[H. (FOCS'20)]
DistPH ∉ AvgP
MINKT^PH ∉ AvgP
GapMINKT^PH ∉ P
Heuristica
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
P ≠ NP
AC^0-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica


Impagliazzo's Five Worlds
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
Pessiland
DistNP ⊄ AvgP
DistPH ⊄ AvgP
Heuristica
P ≠ NP
Algorithmica
?
Theorem [Liu & Pass (FOCS'20)]
∃ one-way function if and only if
MINKT is hard for two-sided-error average-case algorithms.
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Open Question
• Is there a difference between errorless and two-sided-error average-case notions for MINKT?
[H. (FOCS'18,
MINKT ∉ AvgP
GapMINKT ∉ P
[H. (FOCS'20)]
MINKT^PH ∉ AvgP
[H. (FOCS'20)]
GapMINKT^PH ∉ P
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC^0-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P


Impagliazzo's Five Worlds
Meta-Complexity Worlds
Known facts
Open questions
Recent results
Cryptomania
∃ public-key crypto.
Minicrypt
∃ one-way function
[Liu & Pass (FOCS'20)]
MINKT ∉ HeurP
Pessiland
DistNP ∉ AvgP
MINKT ∉ AvgP
[H. (FOCS'18, CCC'20)]
GapMINKT ∉ P
DistPH ∉ AvgP
[H. (FOCS'20)]
MINKT^PH ∉ AvgP
[H. (FOCS'20)]
GapMINKT^PH ∉ P
Heuristica
P ≠ NP
[Ilango, Loff, Oliveira (CCC'20)]
MultiMCSP ∉ P
[Ilango (FOCS'20)]
AC^0-MCSP ∉ P
[H., Oliveira-Santhanam (CCC'18)]
DNF ∘ XOR-MCSP ∉ P
Algorithmica
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 $\mathrm{GapMINKT} \in \mathrm{P}$ imply $\mathrm{DistNP} \subseteq \mathrm{AvgP}$?

  This implies a hardness amplification theorem for NP [H. (FOCS'20)]

- Questions or comments?