公開

（事後評価・研究者用）

研　究　報　告　書

「安全な暗号の確立に向けた回路最小化問題の計算困難性の解析」

研究期間: 2019 年 4 月～2021 年 3 月
研究者番号: 50227
研 究 者: 平原　秀一

1. 研究のねらい

情報通信技術は現代の社会にとって必要不可欠になっており、通信の秘密は公開鍵暗号方式と呼ばれる暗号技術によって守られている。一方で、その安全性は未だ数学的に証明されていない。本研究の究極的な目標は、計算量理論に裏付けされた**絶対的に**安全な暗号の存在を示すことである。残念ながら現在の暗号は**相対的な**安全性に基づいている。例えば、現在広く使われている RSA 暗号などの安全性は「素因数分解を効率的に解けない」といった証明されていない経験的な仮定に基づいており、真に安全とは限らない。

しかしながら、前述の目標を達成するためには計算量理論（計算複雑性理論）における超難問である P≠NP 予想を解決する必要がある。**NP** とは効率的に証拠の正しさを検証できる問題全体のことで、**P** とは効率的に計算できる問題全体のことである。P≠NP 予想は効率的に正しさを検証できるが、効率的に計算することはできない問題の存在を問う未解決問題であり、暗号の安全性に深く関わっている。この未解決問題はミレニアム懸賞の問題のひとつで 100 万ドルの懸賞金がかけられているが、現状では残念ながら解決への道筋がたっていない。さらに悪いことに、公開鍵暗号の安全性は P≠NP 予想を解決するだけでは不十分であり、P≠NP 予想の平均時計算量の一般化である$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$予想などを解決しなければならない。

そこで本研究では、「回路最小化問題（Minimum Circuit Size Problem; MCSP）」および「時間制限付きコルモゴロフ記述量問題（MINKT）」と呼ばれる、計算量理論において中心的な問題の計算困難性を解明することを目指す。これらの問題は「メタ計算問題」と呼ばれる問題群で、どのくらい計算するのが難しいか未解決である。ACT-I 本期間において、メタ計算問題は$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$予想に深く関連していることが明らかになった。本 ACT-I 加速フェーズでは、メタ計算問題の計算困難性を解明することにより、絶対的に安全な暗号の構築に資することを目指す。

2. 研究成果

（1）概要

本研究における最も重要な成果として、平均時計算量に対して「メタ計算量」を用いた新しい解析手法を開発し、NP の平均時計算量に関する長年の未解決問題を解決することに成功した。以下に用語の説明と詳細を述べる。

平均時計算量とは、最悪時計算量に対する概念である。通常アルゴリズムの性能は最悪時計算量に対して行われることが多い。すなわち、アルゴリズムにとって最悪な入力における計算時間のことを**最悪時計算量**と呼ぶ。最悪時計算量は、現実的には現れないような入力も考慮していることから、非現実的な計算時間の解析になることがある。対して、平均時計算量とは、ランダムに生成された入力におけるアルゴリズムの期待計算時間のことであ

り、より現実的な状況に即している。特に、暗号の安全性を議論するためには、平均時計算量の概念は不可欠である。

計算量理論の主要な未解決問題の一つとして、NP の最悪時計算量の困難性の仮定（例えば P≠NP）から NP の平均時計算量の困難性（例えばDistNP ⊄ AvgP; 平均時計算量の意味での P≠NP）を証明する、というものがある。この未解決問題を解決することは、安全な暗号を構築するための重要な一歩である。しかしながら、中心的未解決問題であるがゆえ、なぜ現在の証明手法では解決できないか、ということに関して多くの研究がなされてきた。特に「相対化のバリア」、「ブラックボックス帰着の限界」、「困難性増幅の不可能性」という三つのバリアを同時に突破するような新しい証明手法が必要であるということが知られている。

ACT-I 本期間および ACT-I 加速フェーズの集大成となる成果として、とある強い最悪時計算量の仮定（$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right)$）に基づいて NP の平均時計算量の困難性（$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$）を証明した。これを証明するためには「ブラックボックス帰着の限界」、「困難性増幅の不可能性」という二つのバリアを突破する必要があることが知られており、長年の未解決問題であった。本研究では、メタ計算量に基づく新しい証明手法を開発し、それら二つのバリアを突破し未解決問題を解決することに成功した。

ACT-I 本期間においては、ブラックボックス帰着の限界を世界で初めて突破する成果を得ていた。本加速フェーズでは、メタ計算量に基づく証明手法を開発することにより、さらに困難性増幅の不可能性のバリアを突破することに成功した。この新しい証明手法は、時間制限付きコルモゴロフ記述量問題の解析（成果 1, 2, 3, 4 および本期間の成果）に基づいている。成果 1 および 2 は理論計算機科学の二大トップ会議である FOCS 2020, STOC 2020 にそれぞれ採択された。

（2）詳細

以下ではメタ計算量および成果 1, 2, 3 について詳細な説明を与える。

計算量とは、計算問題を計算するために必要な資源（計算時間やメモリ、回路サイズなど）のことである。例えば素因数分解を解くための時間計算量は非常に大きいと予想されている。**メタ計算量**とは、「計算量を問う計算問題の計算量」のことである。例えば、回路最小化問題は「ブール値関数$f: \{0,1\}^n \to \{0,1\}$を**計算**する最小サイズの回路を**計算**せよ」という問題である。「計算」というものを二つ異なるレベルで考えていることから、回路最小化問題を解くためにかかる計算量はメタ計算量と呼ばれる。同様に、時間制限付きコルモゴロフ記述量問題とは、「文字列$x \in \{0,1\}^*$と時間制限tが与えられたときに、t時間以内でxを計算する最小のプログラムを計算せよ」という問題である。

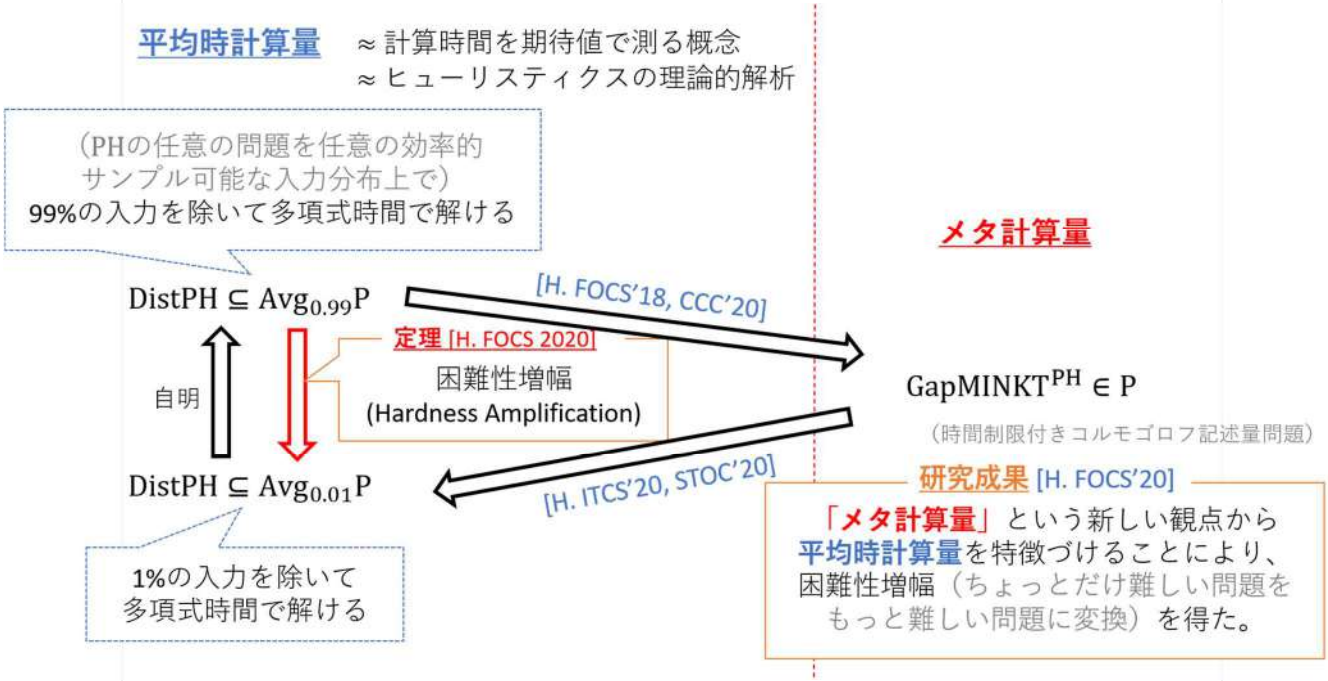
回路最小化問題や時間制限付きコルモゴロフ記述量問題は、NP に属する問題であることは簡単にわかる。しかし、どのくらい計算が難しいかということに関してはよくわかっていない。Allender ら（STACS'04, CiE'12）は、コルモゴロフ記述量問題の計算困難性はある種の証明手法（非適応的ブラックボックス帰着など）では証明できない、ということを予想した。

成果 2, 3：Allender の予想の否定的解決

STOC’20 および ITCS’20 の成果では、Allender らの予想を否定的に解決することに成功した。具体的には、NP の平均時計算量版である DistNP を解くことよりも、一般化された時間制限付きコルモゴロフ記述量問題$\mathrm{MINKT}^{\mathrm{NP}}$の方が計算困難である、ということを証明した。

成果 1: メタ計算量による平均時計算量の新しい解釈とその応用

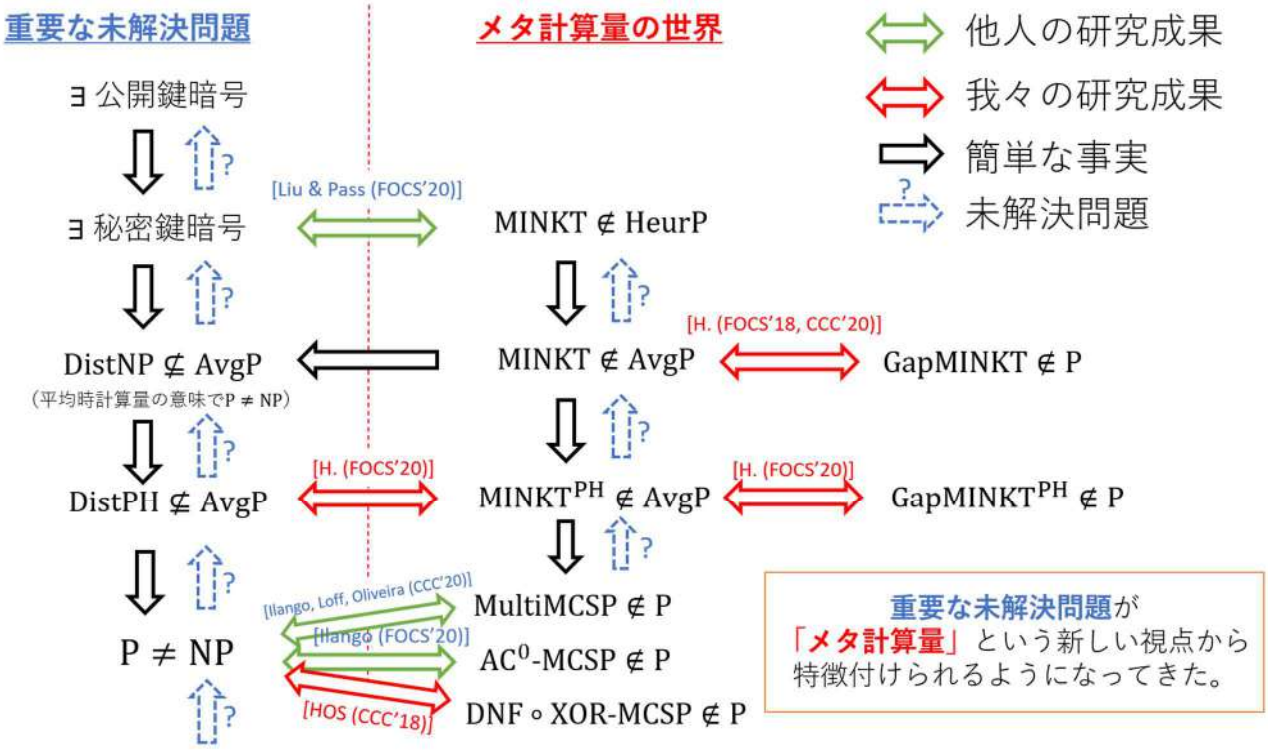
FOCS’20 の成果では、前述の成果 1,2 および成果 4 などに基づいて、メタ計算量による平均時計算量の新しい解析手法を開発した。具体的には、NP の一般化として PH という計算量クラスがある。PH の**平均時計算量**を$\mathrm{GapMINKT}^{\mathrm{PH}}$というある種の時間制限付きコルモゴロフ記述量問題の**最悪時計算量**を用いて特徴付けを与えた。この成果により、平均時計算量という解析しにくく捉えがたいものを、最悪時計算量というより解析のしやすいものに置き換えることが可能になった。特に、特徴づけの系のとして、PH に対する**困難性増幅**を証明することに成功した。困難性増幅とは、少し難しい計算問題をより難しい問題に変換することである。これはメタ計算問題$\mathrm{GapMINKT}^{\mathrm{PH}}$を経由することによって、以下の図のように証明している。



この研究成果は ACT-I 本期間における成果(FOCS’18)、成果 4(CCC’20)および成果 2, 3(STOC’20, ITCS’20)において開発した時間制限付きコルモゴロフ記述量問題を解析する証明手法に基づいている。

3.　今後の展開

近年、世界的にもメタ計算量の重要性が認知されてきており、重要な成果が得られてきた。下図に我々の研究成果と他の研究チームによって得られた研究成果を図示する。



図の左側に図示しているものは、計算量理論における中心的未解決問題である。これら重要な未解決問題が、メタ計算量という概念によって特徴付けが得られるようになってきた。これらの特徴付けは「メタ計算量」という新しい視点を与えており、この新しい視点により計算量理論がさらに発展していくことが見込まれる。

今後は、JST さきがけ「数学と情報科学で解き明かす多様な対象の数理構造と活用」領域において「メタな視点に基づく計算量理論の新展開」として、メタ計算量に基づく手法をさらに推し進めていくことを目指す。

4.　自己評価

時間制限付きコルモゴロフ記述量問題に関して新しい証明手法を開発し、それによって平均時計算量のメタ計算量による解析手法という新しい証明手法を開発した。特に、NP の平均時計算量に関する長年の未解決問題を解決することができたことから、予想以上に研究に進展があったといえる。

5. 主な研究成果リスト

(1)論文(原著論文)発表

1. Shuichi Hirahara. “Characterizing Average-Case Complexity of PH by Worst-Case Meta-Complexity.” 61th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2020). 50-60
2. Shuichi Hirahara. “Unexpected hardness results for Kolmogorov complexity under uniform reductions.” 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2020). 1038-1051
3. Shuichi Hirahara. “Unexpected Power of Random Strings.” 11th Annual Innovations in Theoretical Computer Science (ITCS 2020). 41:1-41:13
4. Shuichi Hirahara. “Non-Disjoint Promise Problems from Meta-Computational View of Pseudorandom Generator Constructions.” 35th Computational Complexity Conference (CCC 2020), 20:1-20:47
5. Shuichi Hirahara, Nobutaka Shimizu “Nearly Optimal Average-Case Complexity of Counting Bicliques Under SETH.” ACM-SIAM Symposium on Discrete Algorithms (SODA 2021).

(2)特許出願

研究期間累積件数:0 件

(3)その他の成果(主要な学会発表、受賞、著作物、プレスリリース等)

6. Shuichi Hirahara, “Non-black-box Worst-case to Average-case Reductions within NP” Highlights of Algorithms (HALG 2019), 招待講演
7. 平原 秀一, “メタ計算量の近年の進展について” 離散数学とその応用研究集会 (JCCA 2020), 招待講演