公開

（事後評価・研究者用）

研　究　報　告　書

「制限された回路の最小化問題と回路下界の研究」

研究期間：平成 30 年 10 月～平成 31 年 3 月
研究者番号：５０１５２
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。すなわち、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（計算の複雑さの理論）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、後述の図に示す通り、計算量理論における 4 つの中心的な未解決問題を解決する必要がある。

そこで本研究では、「回路最小化問題（Minimum Circuit Size Problem; MCSP）」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により、計算量理論全体に貢献することを目指す。回路最小化問題とは、入力としてブール値関数$f:\{0,1\}^n \to \{0,1\}$の真理値表が与えられたとき、その関数fを計算するような最小のゲート数をもつ論理回路を求めるような問題である。この問題の研究の歴史は 1950 年代ごろまで遡ると言われているが、計算の困難性については未だによくわかっていない。回路最小化問題は前述の 4 つの中心的な未解決問題に深く関連している計算問題であり、この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ができると予想できる。そこで、回路最小化問題が NP 完全かどうか（＝他の多くの自然な最適化問題と同様に難しい問題かどうか）という特に重要な未解決問題の解決に向けて、本研究では制限された回路を最小化する問題に着目し研究を行う。特に回路の深さを 3 に制限した場合の回路最小化問題の計算困難性を解析することを目指す。

2．　研究成果

（1）概要

本研究の研究成果として、以下の二つの重要な成果を得た。

<u>成果①【ブラックボックス帰着の限界突破】</u>

回路最小化問題について、最悪時計算量（＝アルゴリズムの最も時間のかかる入力

において、計算時間を計る）と平均時計算量（＝入力がランダムに生成されたときにアルゴリズムの平均計算時間を計る）が等しくなることを証明した。つまり、回路最小化問題がある一つの入力で計算困難ならば、多くの入力でも計算困難であることを証明した。

この成果は、前述の 4 つの中心的な未解決問題の一つである「NP 問題について平均時計算量と最悪時計算量は等しいか」という問いに、新しいアプローチを与えていると見なすことができる。具体的には、回路最小化問題が NP 完全であることを証明しさえすれば、我々の成果と組み合わせることにより、前述の未解決問題を解決することができる。特に回路最小化問題の計算困難性の解析が、絶対的に安全な暗号の構築に実際に資することを証明した。

さらにこの成果が重要な点は、既存の証明技法の限界を突破している新しい手法に基づいていることである。具体的には、平均時計算量と最悪時計算量の同値性を証明するためには、ブラックボックス帰着と呼ばれる証明手法では解決できないことが知られていた。本研究の証明技法はブラックボックス帰着ではない証明手法に基づいており、特にその限界を世界で初めて突破することに成功した。

本成果は国際的に高く評価されており、理論計算機科学のトップ会議 FOCS'18 に採択および日本人初となる Machtey Award（最優秀学生論文賞）を受賞した。

成果②【深さ 3 段の回路クラスに対する回路最小化問題の NP 完全性の解決】

回路の深さを制限したとき、深さ 2 段の回路クラスに対する回路最小化問題については、Masek が 1979 年に NP 完全性を解決していたが、それをより表現能力の高い回路クラスについて拡張することは約 40 年間未解決であった。本研究ではこの未解決問題を解決し、OR-AND-XOR という深さ 3 段の回路クラスに対する回路最小化問題が NP 完全であることを証明した。本成果は計算量理論のトップ会議 CCC'18 に採択された。

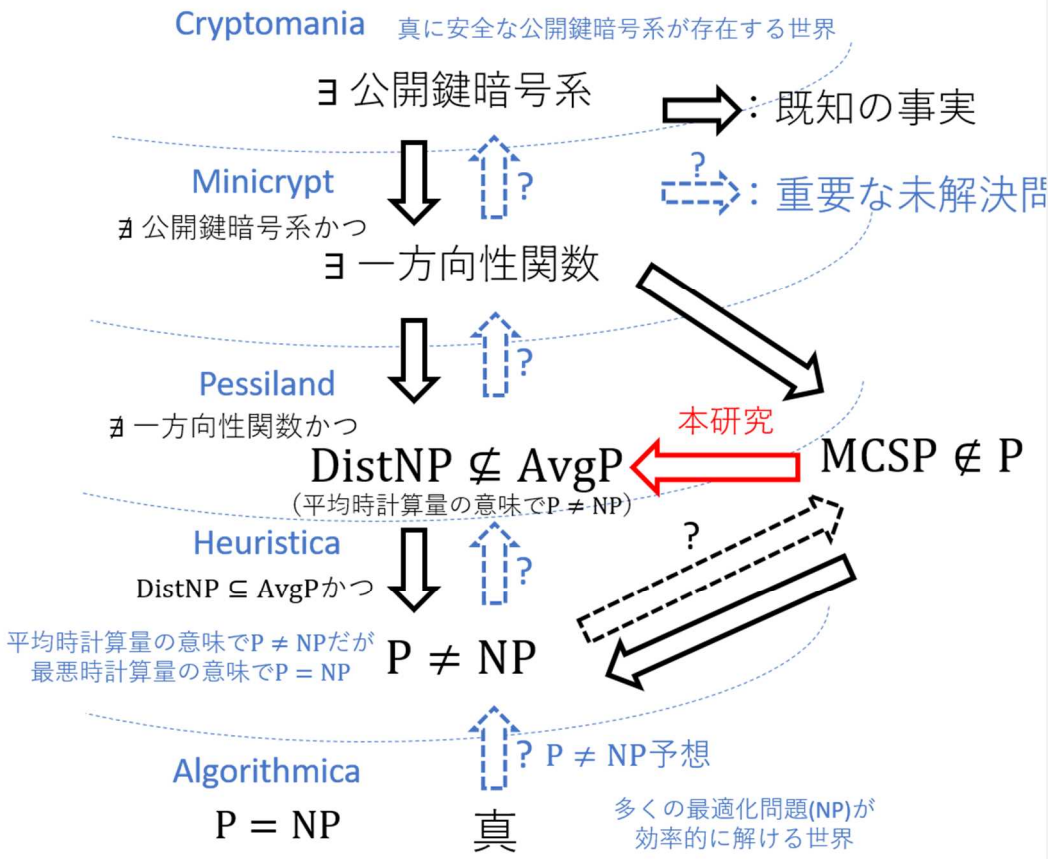
（2）詳細

成果①【ブラックボックス帰着の限界突破】

安全な公開鍵暗号系を構築するためには、P≠NP を証明するだけでは不十分である。実際、「P≠NP」は最悪時計算量（＝アルゴリズムが最も悪い振る舞いをするような入力における計算時間を計る）に基づいて定式化されているが、安全な公開鍵暗号方式を構築するためには、**平均時計算量**の意味での計算困難性を解析する必要がある。つまり、ランダムに秘密鍵を生成したときに、効率的な敵対者が「暗号を破る」という問題を効率的に解けないようにしなくてはならない。

このように「公開鍵暗号系の存在」と「P≠NP」には大きな隔たりがある。平均時計算量や暗号に関する Russell Impagliazzo のサーベイ論文において、この隔たりは明確に解説されている。彼は計算量理論の現在の知識と一貫性のある 5 つのありうる世界（Algorithmica, Heuristica, Pessiland, Minicrypt, Cryptomania）を提案した。これら 5 つの可能世界のうち、ちょうど一つが我々の世界に対応している。例えば Algorithmica と呼ばれる世界は P=NP であるような世界のことを言う。この世界では

安全な暗号を構築することはできない。一方で、Cryptomania という世界は安全な公開鍵暗号が存在する世界である。多くの研究者はこの世界に住んでいると予想しているが、数学的には未解決である。計算量理論の究極的な目標は、どれが我々の真の世界に対応しているかを明らかにすることにある。特に「我々の世界は Cryptomania である」という予想を解決することで、数学的に裏付けされた公開鍵暗号系の存在を証明することが究極的な目標である。



これらの重要な未解決問題に関して、例えば「公開鍵暗号系が存在する ならば P≠NP」などは知られている（上図の黒い矢印に対応する）。その逆を示すことが計算量理論における 4 つの中心的な未解決問題である（青い矢印「?」に対応する）。例えば一番下の矢印は P≠NP 予想に対応しており、これを証明できれば Algorithmica を可能世界から除外することができる。下から二番目の矢印は前述の「NP 問題について平均時計算量と最悪時計算量は等しいか」という未解決問題に対応しており、証明できれば Heuristica という中間の世界を除外することができる。同様に一つの矢印を除外するごとに一つの可能世界が除外され、最終的に 4 つの矢印をすべて証明することにより我々の世界が Cryptomania であると結論づけることができる。

しかしながら、上述の未解決問題は計算量理論における中心的な未解決問題であり、現在の証明手法には限界があることが知られている。例えば Heuristica を除外するためには、「相対化のバリア」と「ブラックボックス帰着の限界」という二つの証明手法

の限界を突破する必要があることが知られている。

本研究では、ブラックボックス帰着の限界を初めて突破することに成功した。具体的には、回路最小化問題がある一つの入力で計算困難（MCSP ∉ P）ならば、多くの入力でも計算困難であることを証明した（  ）。これは下から二番目の矢印「  」を示すための全く新しいアプローチを与えている。回路最小化問題の NP 完全性「  」を示すことができれば、我々の赤い矢印と組み合わせることによって青い矢印（＝Heuristica を除外）できる。

成果②【深さ 3 段の回路クラスに対する回路最小化問題の NP 完全性の解決】

もう一つの成果として、回路最小化問題の NP 完全性に関しても進展を与えることに成功した。、深さ 2 段の回路クラスに対する回路最小化問題については、Masek が 1979 年に NP 完全性を解決していたが、それをより表現能力の高い回路クラスについて拡張することは約 40 年間未解決であった。そして表現能力の高い回路クラスについて NP 完全性を示すことは、先行研究の論文において明確に述べられるなど、計算量理論のコミュニティの中で重要な未解決問題として明確に認識されていた。本研究ではその約 40 年来の未解決問題を解決することに成功した。具体的には、OR-AND-XOR 回路という深さ 3 段の回路クラスに着目した。これは一段目が OR,二段目が AND,三段目が XOR ゲートからなるような回路クラスである。このような制約の下で最小の回路を求めるような計算問題が NP 完全であることを証明した。

3. 今後の展開

以上二つの成果をまとめると、本研究の成果は計算量理論に次のような意味で貢献したといえる。計算量理論の究極的な目標である安全な公開鍵暗号の構築のためには、Cryptomania 以外の 4 つの可能世界を除外する必要がある。成果①では可能世界の一つである Heuristica を除外するための新しいアプローチとして、回路最小化問題の計算困難性（特に NP 完全性）を解析すればよいことを証明している。さらに成果②では、一般の回路最小化問題の NP 完全性を解決するための第一歩として、約 40 年来の未解決問題であった深さ 3 段の回路クラスに対する回路最小化問題の NP 完全性を解決することができた。

今後はこれらの研究をさらに推し進め、回路最小化問題を研究の軸としてさらに計算量理論を発展させていくことを目指す。特に、本研究の証明技術を用いて将来的には実用的な暗号が構築される可能性がある。

4. 自己評価

【研究目的の達成状況】

当初目標として掲げていた深さ 3 の回路最小化問題の計算困難性の解析は十分に達成することができた（成果②）。さらに成果①では、研究提案時に抱いていた「回路最小化問題の計算困難性を解析することが計算量理論にとって重要である」という直感を数学的に証明することに成功し、予想以上に研究に進展があったといえる。

【研究の進め方（研究実施体制及び研究費執行状況】
　研究費は主に共同研究のための旅費として使用した。特に成果②は ACT-I 予算により Oxford 大学を訪問したことによって得られたものである。

【研究成果の科学技術及び学術・産業・社会・文化への波及効果】
　本研究は学術、特に暗号の基礎となる計算量理論に対して大きな貢献をしたといえる。また、将来的には本研究で得られた証明技術を用いて、実用的な暗号が構成される可能性がある。

【研究課題の独創性・挑戦性】
　本研究課題は「数学的な裏付けのある絶対的に安全な暗号の構築」という非常に挑戦的な未解決問題に貢献するべく、回路最小化問題に着目するという独自のアイディアに基づくものである。

5.　主な研究成果リスト

（1）論文（原著論文）発表

成果①. Shuichi Hirahara. “Non-Black-Box Worst-Case to Average-Case Reductions within NP.” 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS), 247-258, Paris, France, October 7-9, 2018
成果②. Shuichi Hirahara, Igor Carboni Oliveira, Rahul Santhanam. “NP-hardness of Minimum Circuit Size Problem for OR-AND-MOD Circuits.” 33rd Computational Complexity Conference (CCC), 5:1-5:31, San Diego, CA, USA, June 22-24, 2018

（2）特許出願

研究期間累積件数：0 件

（2）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）

受賞

1. COMP-ELC 学生シンポジウム最優秀論文賞（2018/3/23）
2. 電子情報通信学会　2018 年度学術奨励賞（2019/3/21）
3. Machtey Award (Best Student Paper Award at FOCS'18)（2018/10/7）