真に安全な暗号の構成を目指して

制限された回路の最小化問題と回路下界の研究

平原 秀一

東京大学 THE UNIVERSITY OF TOKYO 情報理工学系研究科 博士課程 → NII 大学共同利用機関法人 情報・システム研究機構 国立情報学研究所 National Institute of Informatics 情報学プリンシプル研究系 助教

1. 究極的な目標：安全な暗号

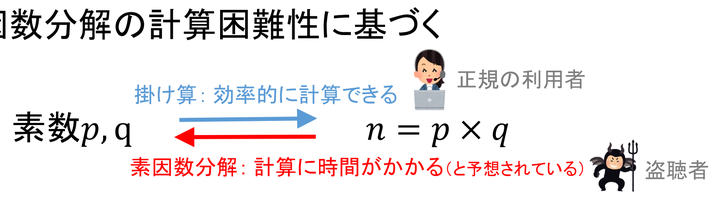
情報科学
- 理論計算機科学（数学を使って計算を解析する）
  - アルゴリズム論：様々な問題が計算できることを追求
  - **計算量理論**：ある問題が計算できないことを追求
- ⋮

➢ 公開鍵暗号方式 ・ 現代の情報通信社会の通信の秘密を守る基盤技術

しかし… **真に安全な暗号**が存在するかどうかは未解決！

例：RSA暗号方式

➢ 素因数分解の計算困難性に基づく



➢ 量子コンピュータで効率的に解読できる　Shorの量子アルゴリズム (1994)

現代の暗号方式の安全性が崩壊するシナリオ

① （大規模な）量子コンピュータの実現

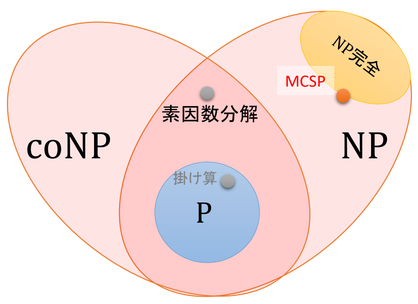
② （P = NPを示すような）革新的なアルゴリズムの開発

⟹ そしてそれらの開発者は世界を掌握できてしまう！

➢ **P ≠ NP予想** ・ ミレニアム懸賞金問題の一つ （賞金100万ドル）

P　効率的に計算できる問題全体

NP　効率的に解の正しさを検証できる問題全体
多くの自然な最適化問題を含む



もしP = NPだとすると、全ての暗号を破れてしまう！

2. Impagliazzoの5つの可能世界

➢ 実はP ≠ NPを示すだけでは、暗号を構築するのには不十分　Impagliazzo (1995)

- 平均計算量（＝入力がランダムに生成されたときの計算時間）を解析する必要がある
- 現在の計算量理論の知識と一貫性のある世界を5つに分類

😃 任意のNPの最適化問題が高速に解けるが、
😰 安全な暗号は作れない。

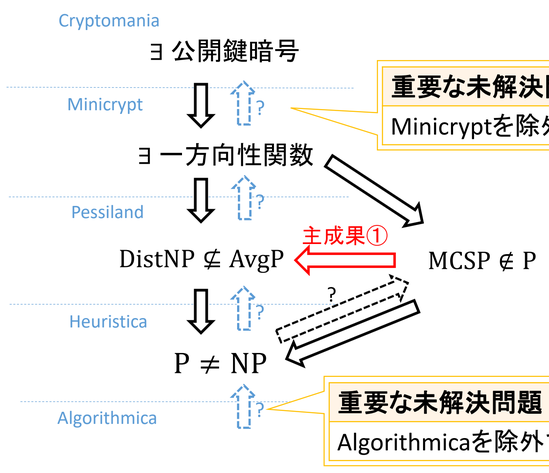
😰 最悪計算量の意味でP ≠ NPだが、
😃 平均計算量の意味でP = NP

😰 最適化問題は解けないが、
😃 安全な公開鍵暗号系が存在する。

Algorithmica	Heuristica	Pessiland	Minicrypt	Cryptomania
P = NP	**DistNP ⊆ AvgP** **P ≠ NP**	∄ 一方向性関数 **DistNP ⊈ AvgP**	∄ 公開鍵暗号 ∃ 一方向性関数	∃ 公開鍵暗号

計算量理論の究極的な使命

我々の世界がどの世界であるかを決定すること！
（特に、Cryptomaniaであるという予想を解決し、絶対的に安全な暗号を確立すること。）



- 1つの矢印を証明 ⇔ 1つの可能世界を除外
- 4つ全ての矢印を証明 ⇔ 我々の世界はCryptomania！

➢ 理論的な障害

既知の証明手法ではこれらの未解決問題を解決できない

（例）Heuristicaを除外するためには次の2つの障害を突破するような証明手法が必要となる。

※ ブラックボックス帰着の限界
※ 相対化のバリア

3. 回路最小化問題 (MCSP)

我々の着眼点：MCSPという中心的な計算問題を解析する

➢ 回路最小化問題（Minimum Circuit Size Problem; MCSP）

- 関数を計算する最小の論理回路を求める計算問題

入力

関数$f:\{0,1\}^n \to \{0,1\}$の真理値表

（入力例）

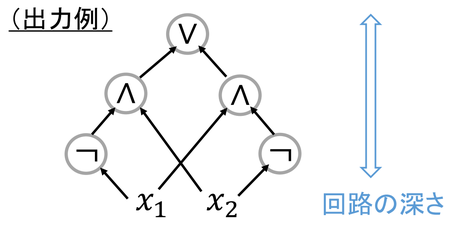
$f =$

x_1	x_2	x_1 xor x_2
0	0	0
0	1	1
1	0	1
1	1	0

出力

関数fを計算する最小のゲート数の論理回路

（出力例）



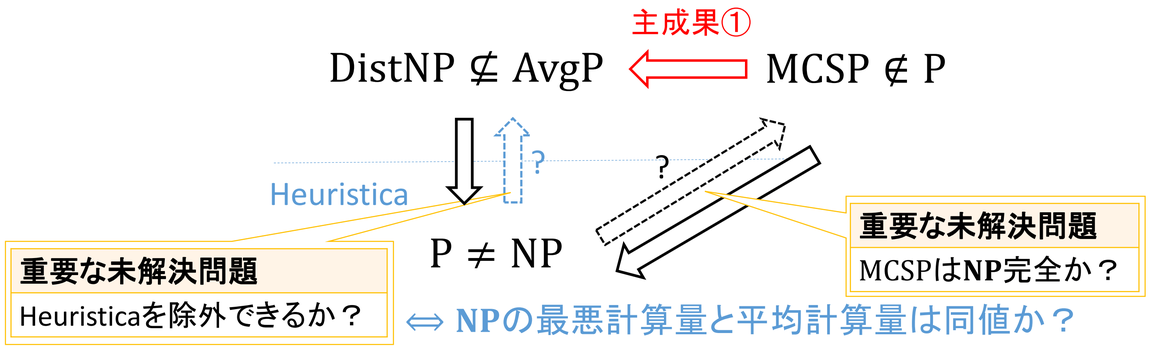
- ハードウェアの設計で自然に現れる基礎的な問題

重要な未解決問題

MCSPは**NP**完全か？
（＝ **NP**の中で最も難しい問題か？）

成果①　**NP**完全性が解決できれば可能世界を一つ除外できる

成果②　制限された場合にNP完全性を解決！（約40年来の未解決問題）



⇔ **NP**の最悪計算量と平均計算量は同値か？

主成果①　(Hirahara, FOCS'18)

MCSPの最悪計算量と平均計算量は同値

➢ 非ブラックボックス帰着手法を開発することにより、ブラックボックス帰着の限界を世界で初めて突破！

Machtey Award（FOCS'18, 最優秀学生論文賞）受賞　（日本人初）

➢ Heuristicaを除外するための新しいアプローチ

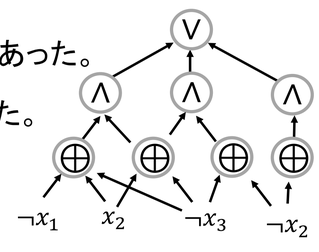
MCSPの**NP**完全性「?」を解決すれば十分！

Masek（1979年）　深さ2段に制限した場合の回路最小化問題のNP完全性を解決
OR-AND回路（＝DNF式）

➢ しかし、それを深さ3段以上に拡張することは約40年間未解決であった。

➢ さらにその未解決問題を解決することの重要性が認識されていた。

"Thus an **important open question** is to resolve the NP-hardness of … function minimization results above for classes that are stronger than DNF."
（Allender, Hellerstein, McCabe, Pitassi, and Saks (2008)の論文より引用）



主成果②　(Hirahara-Oliveira-Santhanam, CCC'18)

OR-AND-XOR回路最小化問題はNP完全

ある種の深さ3段の回路について、回路最小化問題のNP完全性を解決！

本研究の貢献のまとめ

究極的な目標：

絶対的に安全な暗号の確立

⇧ 新しい知見

Heuristicaを除外

主成果① ⇧ 初めてブラックボックス帰着の限界を突破

一般の回路最小化問題のNP完全性

⇧ 第一ステップとして

深さ3段に制限された回路最小化問題のNP完全性を解決！ **主成果②**

Masekの結果以来約40年間未解決だった