真に安全な情報通信社会に向けて

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

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　平原 秀一

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**（ある問題が効率的に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

素数 p, q ⇄ $n = p \times q$
（掛け算：効率的に計算できる／素因数分解：計算に時間がかかる（と予想されている））


正規の利用者


盗聴者


Shorの量子アルゴリズム (1994)

➢ 量子コンピュータで効率的に解読できる

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

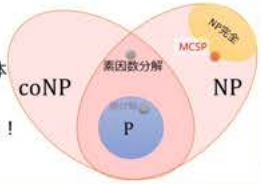
⇒ そしてそれらの開発者は世界を掌握できてしまう！

➢ **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の五つの可能世界

➢ 実はP ≠ NPを示すだけでは、暗号を構築するのには不十分

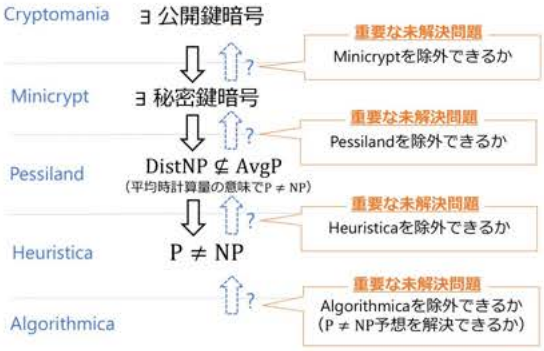
Russell Impagliazzo

- 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

Algorithmica	Heuristica	Pessiland	Minicrypt	Cryptomania
	☺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。
P = NP	**DistNP ⊆ AvgP** **P ≠ NP**	**∄ 秘密鍵暗号** **DistNP ⊄ AvgP**	**∄ 公開鍵暗号** **∃ 秘密鍵暗号**	**∃ 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。）



3. 我々の研究成果

➢ なぜ重要な未解決問題を解決することは難しいのか？

✕：理論的な障壁　既存の証明の技法には限界があり、重要な未解決問題を解決できない。

➢ ACT-I本期間では、回路最小化問題という問題を考えることにより、「ブラックボックス帰着の限界」を初めて突破する成果を得た。

➢ ACT-I加速フェーズでは平均時計算量に関する**長年の未解決問題**を解決！

加速フェーズの主要成果 [H. (STOC'21)]

$$\mathrm{UP} \not\subseteq \mathrm{DTIME}\left(2^{o(n)}\right) \Longrightarrow \mathrm{DistNP} \not\subseteq \mathrm{AvgP}$$

UP（素因数分解など）が最悪時計算量の意味で指数的に難しい（$2^{o(n)}$時間では計算できない）

NPが平均時計算量の意味で難しい

➢ 「ブラックボックス帰着」や「困難性増幅」と呼ばれる証明手法では証明できない、ということが知られていた。[Boganov-Trevisan'06] [Viola'05]
（「相対化のバリア」が適用できるかどうかは未解決）

➢ **メタ計算量理論**に基づく証明手法により、同時に突破することに成功！

4. 平均時計算量とメタ計算量

➢ 最悪時計算量と平均時計算量

- アルゴリズムAの計算時間は**最悪時計算量**によって評価されることが多い。

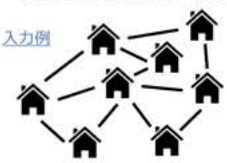
  $\max_x t_A(x)$　（$t_A(x)$: 入力xにおけるアルゴリズムAの計算時間）

  ...しかし、現実的な状況では最悪な入力が現れるとは限らない。

- アルゴリズムAの（入力分布μにおける）の**平均時計算時間**とは、計算時間の期待値 $\mathbb{E}_{x\sim\mu}[t_A(x)]$ のこと。

  暗号の安全性を議論するためには平均時計算量が重要！

- 例：ハミルトン路問題（NP完全問題）


入力例

問　任意の場所からスタートして、全ての家をちょうど一度だけ通るような経路は存在するだろうか？

➢ この問題はP ≠ NP予想の下で最悪時計算量の意味で効率的に解けない。
ハミルトン路問題 ∉ P

➢ 一方で、50%の確率で道を作るような入力（ランダムグラフ）では平均時計算量の意味で効率的に解けることが知られている。
(ハミルトン路問題, $\mathcal{U}$) ∈ AvgP

➢ 証明技法：メタ計算量

メタ計算問題の例
- 回路最小化問題 =「ブール値関数$f:\{0,1\}^n \to \{0,1\}$を**計算**する最小の回路を**計算**せよ」
- コルモゴロフ記述量問題（MINKT）=「文字列$x \in \{0,1\}^n$を**計算**する最小のプログラムを**計算**せよ」

- **平均時計算量**を**最悪時メタ計算量**（MINKT）の概念で特徴づけることにより証明。