あなたの身の回りの暗号は大丈夫？

計算量理論と暗号の世界

平原　秀一

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

計算量理論： 計算困難性の追求

（計算複雑性理論とも）

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

  様々な問題を解く計算方法を考案

- **計算量理論**

  ある問題の計算が難しいことを証明

  暗号理論の基礎となる理論。

- **暗号理論**

⋮

⋮

計算量理論の中心的未解決問題

P ≠ NP予想

- ７つあるミレニアム懸賞問題のひとつ
- 解決には１００万ドルの懸賞金が懸けられている
- 数学全般・社会全体に大きな影響を与えうる

（参考）ミレニアム懸賞問題

クレイ数学研究所によって２０００年に発表された、１００万ドルの懸賞金がかけられている問題。

1. ヤン–ミルズ方程式と質量ギャップ問題
2. リーマン予想
3. **P ≠ NP予想**
4. ナビエ–ストークス方程式の解の存在と滑らかさ
5. ホッジ予想
6. ポアンカレ予想（グレゴリー・ペレルマンにより解決済）
7. バーチ・スウィンナートン＝ダイアー予想

目次

1. 暗号理論の基礎（秘密鍵暗号、公開鍵暗号、RSA暗号）
2. 多項式時間と指数時間の違い
3. P ≠ NP予想と暗号

通信の安全性

私のパスワードは
「abcXYZ」です。

「abcXYZ」

利用者

銀行

盗聴者

悪い人にパスワードが
盗聴されてしまうかも…

シーザー暗号 — 単純な暗号の例

ユリウス・カエサル
（英語読みではジュリアス・シーザー）
紀元前１００年頃～紀元前４４年

- 暗号の歴史は少なくとも紀元前にさかのぼる

- カエサルは秘密を伝える際に、各文字を
アルファベット３文字分ずらして暗号化したと言われている。

例：

$$A \mapsto D$$
$$HELLO \mapsto KHOOR$$

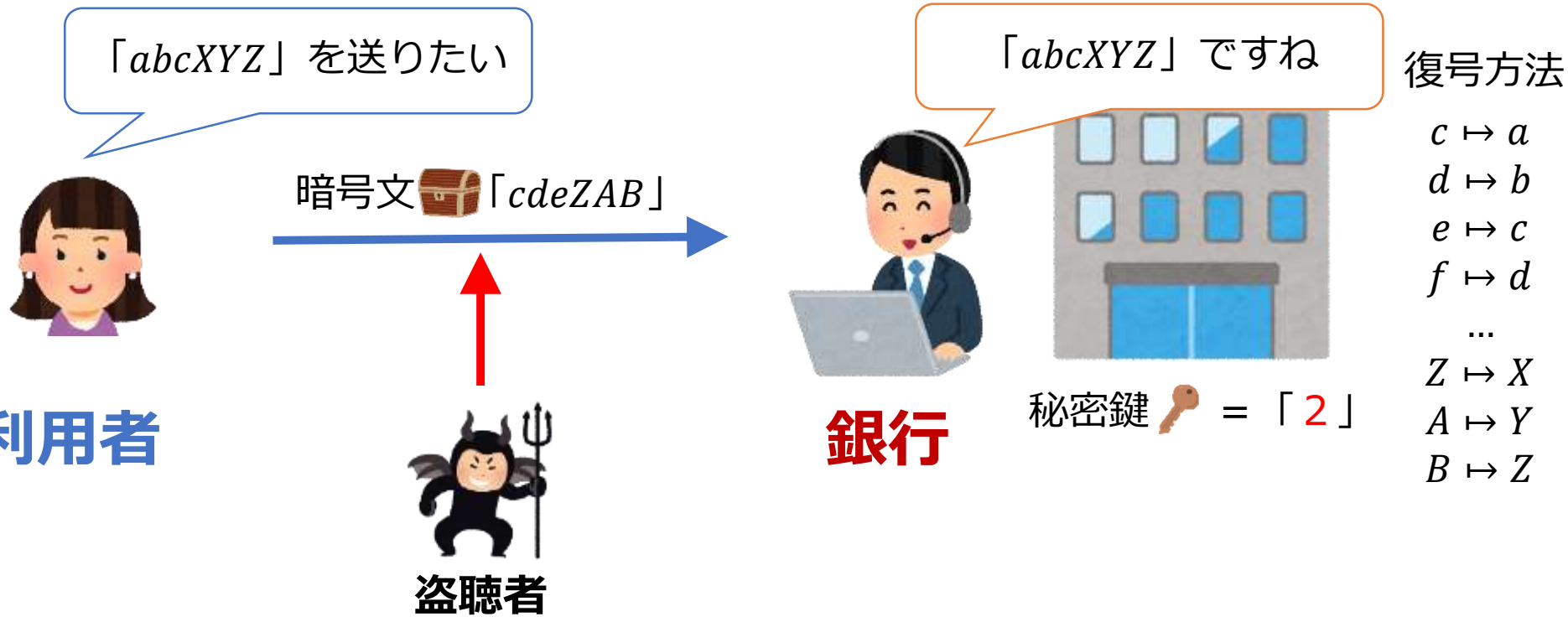
画像出展: https://ja.wikipedia.org/wiki/ガイウス・ユリウス・カエサル

秘密鍵暗号方式（シーザー暗号を例に）

秘密鍵 🔑 =「2」

2文字分ずらす

$a \mapsto c$
$b \mapsto d$
$c \mapsto e$
$d \mapsto f$
…
$X \mapsto Z$
$Y \mapsto A$
$Z \mapsto B$



復号方法

$c \mapsto a$
$d \mapsto b$
$e \mapsto c$
$f \mapsto d$
…
$Z \mapsto X$
$A \mapsto Y$
$B \mapsto Z$

問題点

1. 頻度分析などで容易に暗号を解読できてしまう。 ← 現在ではAES暗号などのより優れた秘密鍵暗号方式がある
2. 事前に「秘密鍵🔑」を共有しておく必要がある。 ← 公開鍵暗号方式なら事前に鍵の共有が不要！

公開鍵暗号方式

事前に秘密鍵の共有が不要！

秘密鍵　解読するための鍵

公開鍵　暗号化するための鍵

を使ってメッセージを
暗号化して送信

公開鍵「011010」を使って
暗号化してください

公開鍵

暗号文

利用者

秘密鍵 を使って
暗号文 を解読できる

銀行

？？？

盗聴者

公開鍵暗号方式の安全性

暗号文 は秘密鍵 をもつ人だけが解読できる

RSA暗号 — 公開鍵暗号の代表例

- 1977年にRivest, Shamir, Adlemanによって開発された。
- 最も広く用いられている公開鍵暗号方式の一つ。
- RSA暗号の安全性は素因数分解の計算困難性に基づく。

（大きい桁数の）素因数分解が現実的な時間では解けない
という**予想**が正しいときに限り安全

一方向性関数 — 暗号の重要となる要素

一方向性関数とは

順方向は容易に計算できるが、
逆方向の計算は効率的に計算できない関数のこと。

例： 掛け算

入力

$$863 \times 941$$

掛け算

解

$$812083$$

一方向性関数 — 暗号の重要となる要素

一方向性関数とは

順方向は容易に計算できるが、
逆方向の計算は効率的に計算できない関数のこと。

例： 掛け算

解

863×941

（素因数）　（素因数）

掛け算 →

← **素因数分解**

入力

812083

一方向性関数 — 暗号の重要となる要素

一方向性関数とは

順方向は容易に計算できるが、
逆方向の計算は効率的に計算できない関数のこと。

例： 掛け算

掛け算などを計算して暗号化する

解 

863×941

（素因数）（素因数）

掛け算 →

← **素因数分解**

入力 

812083

現実的な時間では
計算できない！

解読するには素因数分解を計算する必要がある
（秘密鍵  を知る必要がある）

目次

1. 暗号理論の基礎
2. 多項式時間と指数時間の違い
3. P ≠ NP予想と暗号

掛け算を計算するのにかかる時間は？

$$
\begin{array}{r}
863 \\
\times\ 941 \\
\hline
863 \\
3452 \\
7767 \\
\hline
812083
\end{array}
$$

問　3桁×3桁の掛け算をするためには
1桁×1桁の掛け算を何回する必要があるか？

$1\times3,\ 1\times6,\ 1\times8$
$4\times3,\ 4\times6,\ 4\times8$
$9\times3,\ 9\times6,\ 9\times8$

答　9回

一般に、m桁×m桁の掛け算は
m^2くらいの「手間」がかかる。

- このような計算時間（$m^2, m^3, \ldots$）のことを**多項式時間**と呼ぶ。

素因数分解を計算するのにかかる時間は？

試し割り法

812083を素因数分解したい。

余り

2で割り算をしてみる：$812083 = 406041 \times 2 + 1$

3で割り算をしてみる：$812083 = 270694 \times 3 + 1$

4で割り算をしてみる：$812083 = 203020 \times 4 + 3$

⋮

863で割り算をしてみる：$812083 = 863 \times 941 + 0$

割り切れる

⟹ 素因数がわかる

3桁の素因数を見つけるのに約1000回の「手間」がかかる！

より一般に、m桁の素因数を見つけるのに約10^m回の「手間」がかかる。

- このような計算時間（$2^m, 10^m, \ldots$）のことを**指数時間**と呼ぶ。

多項式時間と指数時間の違い

$1\mathrm{G}$（ギガ） $= 10^{9}$
1μ（マイクロ） $= 10^{-6}$
$1n$（ナノ） $= 10^{-9}$

- 現在のCPUの性能は $1\mathrm{GHz}$～$5\mathrm{GHz}$ 程度。
  - つまり、１秒間あたり１０億回～５０億回程度の演算ができる。

桁数m	3	30	300
筆算の計算時間 (m^2)			
試し割り法の計算時間 (10^m)			

- 大きい桁数の素因数分解を試し割り法で計算すると、
  現実的な時間では解けない。

掛け算と素因数分解の計算時間の差

筆算を使えば約m^2時間
（多項式時間）で計算できる。

掛け算などを計算して暗号化する

入力 

掛け算

解

863×941 ⇒ 812083

⇐

素因数分解

現実的な時間では
計算できない！

解読するには素因数分解を計算する必要がある
（秘密鍵  を知る必要がある）

試し割り法だと約10^m時間
（指数時間）かかってしまう。

掛け算と素因数分解の計算時間の差

筆算を使えば約m^2時間
（多項式時間）で計算できる。

掛け算などを計算して暗号化する

入力 

掛け算

解

863×941 ⇒ 812083

⇐

素因数分解

現実的な時間では
計算できない！

解読するには素因数分解を計算する必要がある
（秘密鍵  を知る必要がある）

試し割り法だと約10^m時間
（指数時間）かかってしまう。

- 盗聴者  は試し割り法よりも高速な計算方法を使うかもしれない！

素因数分解を解くアルゴリズム

- 様々な計算方法（アルゴリズム）が提案されている。

  例：ポラード・ロー素因数分解法、$p-1$法、数体ふるい法、などなど

- しかし、素因数分解を計算する多項式時間アルゴリズムは知られていない。

- 多くの研究者はそのようなアルゴリズムは存在しないだろうと予想している。
  - このことから、RSA暗号は安全だと予想されている。
  - **P** ≠ **NP予想**は、この予想の一般化

目次

1. 暗号理論の基礎
2. 多項式時間と指数時間の違い
3. P ≠ NP予想と暗号

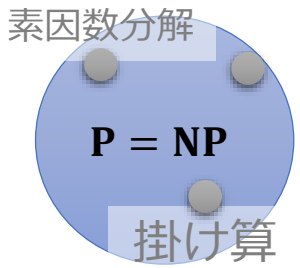
P ≠ NP予想 — 数学の超難問

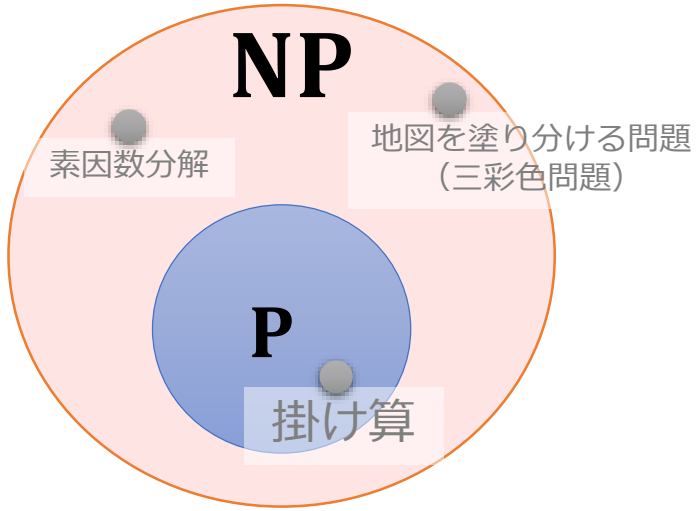
P = { 多項式時間で計算できる問題全体 }　　例： 掛け算 ∈ **P**

NP = { 多項式時間で解の正しさを検証できる問題全体 }

例：素因数分解 ∈ **NP**, 掛け算 ∈ **NP**

P = NP　or　**P ≠ NP**





P ≠ NP予想 — 数学の超難問

P ＝ { 多項式時間で計算できる問題全体 }　　例： 掛け算 ∈ **P**

NP ＝ { 多項式時間で**解の正しさを検証できる**問題全体 }

例：素因数分解 ∈ **NP**, 掛け算 ∈ **NP**

≒ テストの答案を素早く採点できる

素因数分解の理解度テスト

テスト問題①

812083

を素因数分解せよ.

（正しいとは限らない）解

（生徒１の回答）863×941

（生徒２の回答）800×900

P ≠ NP予想

「解の正しさを簡単に検証できるが、
多項式時間では計算できない問題が存在するであろう」

$\mathbf{P} \neq \mathbf{NP}$予想と暗号の関係

数学の証明を高速
に見つけられる

$\mathbf{P} = \mathbf{NP}$ or $\mathbf{P} \neq \mathbf{NP}$

☺ 任意のNPの問題が
効率的に解ける

☹ どのような公開鍵暗号でも
効率的に解読可能

☹ 効率的に解けないNPの問題が存在する

☺ 安全な暗号が存在する（？）

Impagliazzoの５つの可能世界

Russell Impagliazzo

我々の知識と一貫性の
ある世界を5つに分類

Cryptomania

Minicrypt

Pessiland

Heuristica

$P \neq NP$

Algorithmica

$P = NP$

画像出展：https://www.simonsfoundation.org/people/russell-impagliazzo/

Impagliazzoの５つの可能世界

Russell Impagliazzo

我々の知識と一貫性の
ある世界を5つに分類

Cryptomania

Minicrypt

Pessiland

Heuristica

$$P \neq NP$$

任意のNPの最適化問題が
高速に解ける。
数学者が不要になる。
安全な暗号は作れない。

Algorithmica

$$P = NP$$

画像出展：https://www.simonsfoundation.org/people/russell-impagliazzo/

Impagliazzoの５つの可能世界

Russell Impagliazzo

我々の知識と一貫性のある世界を5つに分類

Cryptomania

$\exists$ 公開鍵暗号

Minicrypt

$\exists$ 秘密鍵暗号 & $\nexists$ 公開鍵暗号

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$
（平均時計算量の意味で$\mathrm{P} \neq \mathrm{NP}$）
& $\nexists$ 秘密鍵暗号

Heuristica

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

Algorithmica

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

画像出展：https://www.simonsfoundation.org/people/russell-impagliazzo/

Impagliazzoの５つの可能世界

Russell Impagliazzo

Cryptomania

$\exists$ 公開鍵暗号

☹難しい問題が存在するが、
☺安全な公開鍵暗号系が
存在する。

Minicrypt

$\exists$ 秘密鍵暗号 & $\nexists$ 公開鍵暗号

Pessiland

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$
（平均時計算量の意味で$\mathrm{P} \neq \mathrm{NP}$）
& $\nexists$ 秘密鍵暗号

Heuristica

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

Algorithmica

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

画像出展：https://www.simonsfoundation.org/people/russell-impagliazzo/

Impagliazzoの５つの可能世界

Russell Impagliazzo

Cryptomania

ョ 公開鍵暗号

我々の知識と一貫性の
ある世界を5つに分類

Minicrypt

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。）

Heuristica

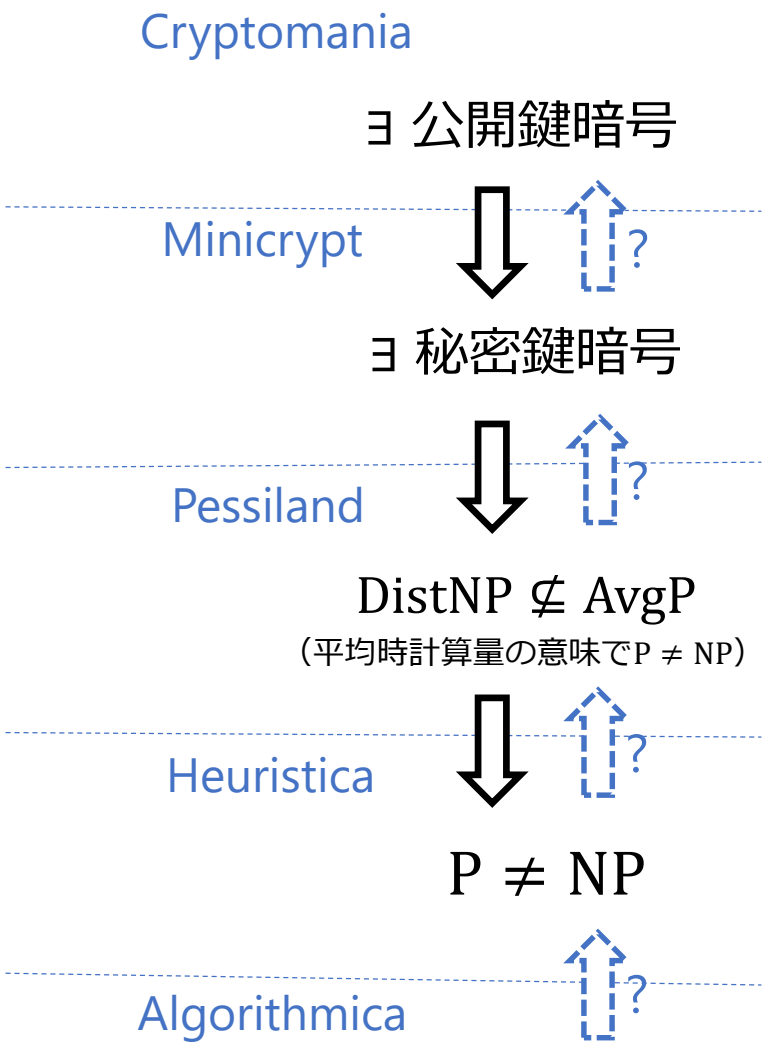
$P \neq NP$ & $DistNP \subseteq AvgP$

Algorithmica

$P = NP$

画像出展：https://www.simonsfoundation.org/people/russell-impagliazzo/

既知の事実と未解決問題



⇨：既知の事実

?⇢：重要な未解決問題

公開鍵暗号構築への道

⇨：既知の事実

?⇢：重要な未解決問題

Cryptomania

∋ 公開鍵暗号

Minicrypt ⇩ ?⇧

重要な未解決問題

Minicryptを除外できるか？

∋ 秘密鍵暗号

Pessiland ⇩ ?⇧

重要な未解決問題

Pessilandを除外できるか？

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

（平均時計算量の意味で$\mathrm{P} \neq \mathrm{NP}$）

Heuristica ⇩ ?⇧

重要な未解決問題

Heuristicaを除外できるか？

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica ?⇧

重要な未解決問題

$\mathrm{P} \neq \mathrm{NP}$予想（Algorithmicaを除外できるか？）

全ての矢印を証明

⇔

我々の世界はCryptomania！

１つの矢印を証明

⇔

１つの可能世界を除外

現在の証明手法の限界

⇨：既知の事実

⇢?：重要な未解決問題

Cryptomania

∋ 公開鍵暗号

Minicrypt ⇩ ⇢?

∋ 秘密鍵暗号

Pessiland ⇩ ⇢?

$\mathrm{DistNP} \not\subseteq \mathrm{AvgP}$

（平均時計算量の意味で$\mathrm{P} \neq \mathrm{NP}$）

Heuristica ⇩

$\mathrm{P} \neq \mathrm{NP}$

Algorithmica ⇢?

╳：理論的な障害

ある種の証明手法では
その未解決問題を解決できない

相対化のバリア

代数化のバリア

自然な証明のバリア

全ての矢印を証明
⇔
我々の世界はCryptomania！

１つの矢印を証明
⇔
１つの可能世界を除外

現在の証明手法の限界

⇨：既知の事実

?⇢：重要な未解決問題

Cryptomania

∃ 公開鍵暗号

Minicrypt ⇩ ?

∃ 秘密鍵暗号

Pessiland ⇩ ?

DistNP ⊈ AvgP

（平均時計算量の意味でP ≠ NP）

Heuristica ⇩

P ≠ NP

Algorithmica

相対化のバリア

ブラックボックス帰着の限界

✕：理論的な障害

ある種の証明手法では
その未解決問題を解決できない

全ての矢印を証明
⇔
我々の世界はCryptomania！

１つの矢印を証明
⇔
１つの可能世界を除外

着眼点：回路最小化問題（MCSP）

⇨：既知の事実

⇢：重要な未解決問題

Cryptomania

∃ 公開鍵暗号

Minicrypt

∃ 秘密鍵暗号

Pessiland

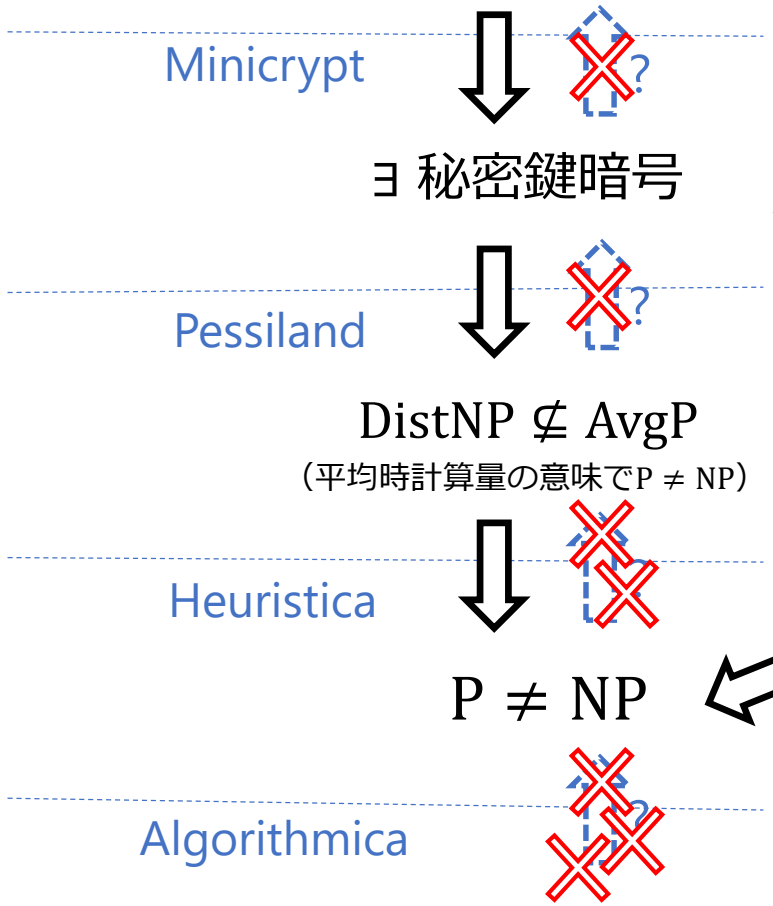
DistNP ⊄ AvgP

（平均時計算量の意味でP ≠ NP）

Heuristica

P ≠ NP

Algorithmica



✕：理論的な障害

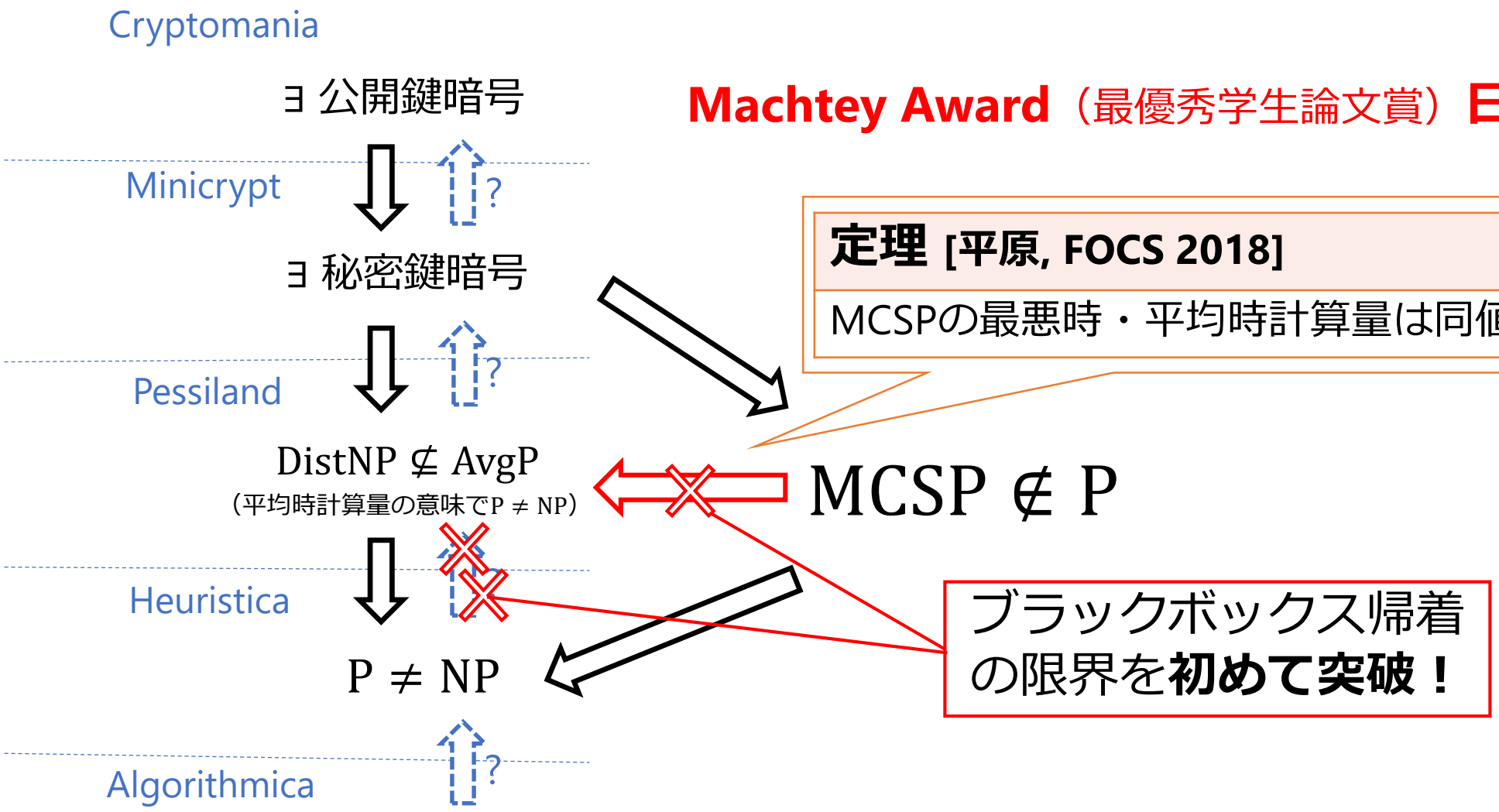
ある種の証明手法では
その未解決問題を解決できない

MCSP ⊄ P

全ての矢印を証明
⇔
我々の世界はCryptomania！

１つの矢印を証明
⇔
１つの可能世界を除外

最近の研究成果：ブラックボックス帰着の**限界突破**



Machtey Award（最優秀学生論文賞）**日本人初受賞！**

まとめ

- 計算量理論：効率的な計算の限界を追求する学問。

  安全な暗号 ⇔ 盗聴者がどのような計算方法を用いても解読できない。

- 中心的未解決問題：$P \neq NP$予想
  - 真に安全な公開鍵暗号を構成するための第一歩

安全だと予想されているが、
まだ証明されていない。

あなたの身の回りの暗号は大丈夫？

計算量理論と暗号の世界

真に安全な暗号を構築することに
貢献する理論

平原　秀一

人 情報・システム研究機構
報学研究所
ute of Informatics

研究系・助教

国立情報学研究所　市民講座