量子コンピュータの出現に対抗し得る公開鍵暗号の研究

総務省 戦略的情報通信研究開発推進制度 (SCOPE) 平成 20 年度採択課題
ICT イノベーション創出型研究開発　ICT 安心・安全技術

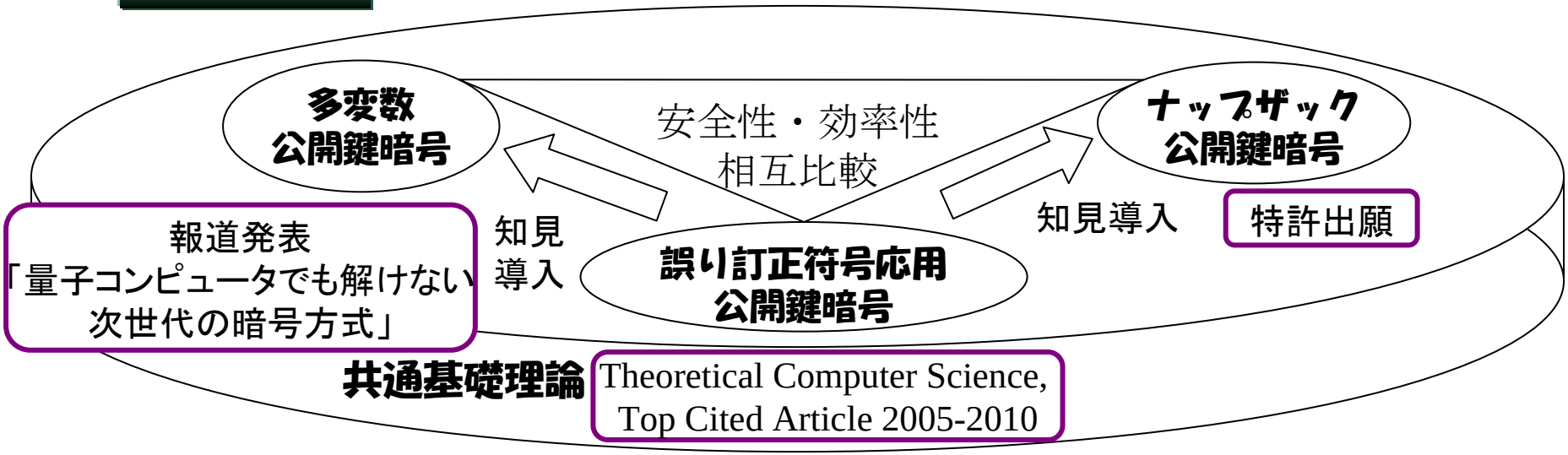
新世代公開鍵暗号技術と情報セキュリティに関する研究開発

研究目的

量子コンピュータが暗号解読に利用され、RSA暗号や楕円暗号が破られる想定外の危機が到来しても、盗聴や改ざんから新世代ネットワークの情報・データを保護できる公開鍵暗号技術の確立

研究概要・研究成果

NP完全問題を一方向性関数として利用
有力候補として下記の3暗号について研究



社会的意義

SoMoCS時代の基盤構築；機密、個人情報漏洩、相手認証
先進的な理論構築、実用的な技術開発における貢献

本研究開発による成果数

- 査読付き論文数　　53件（海外分：46件）
  - 当初目標　　27件
- 口頭発表数　　111件（海外分：7件）
  - 当初目標　　45件

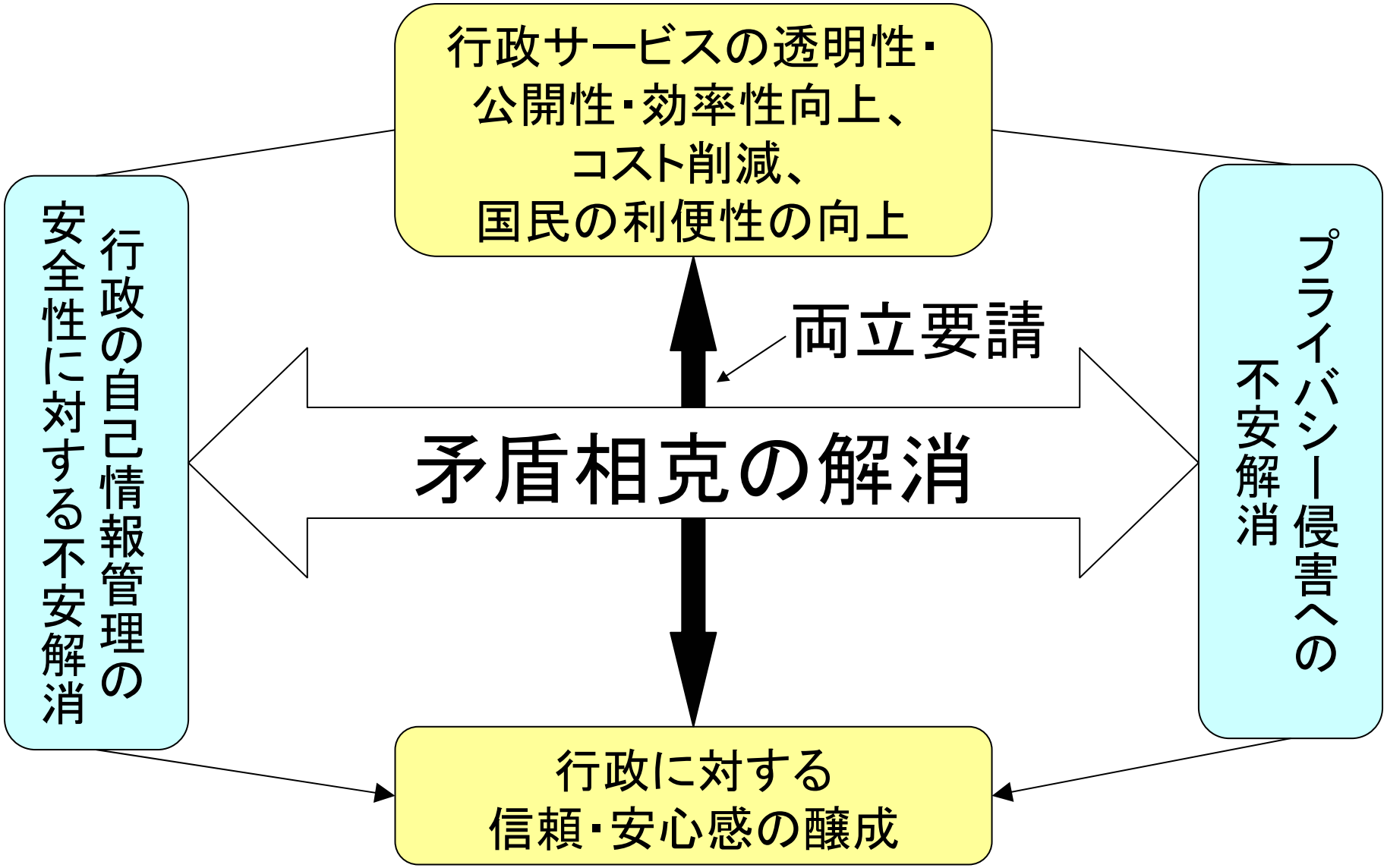

行政サービスの透明性・
公開性・効率性向上、
コスト削減、
国民の利便性の向上
両立要請
矛盾相克の解消
行政の自己情報管理の
安全性に対する不安解消
プライバシー侵害への
不安解消
行政に対する
信頼・安心感の醸成

図　電子行政サービス

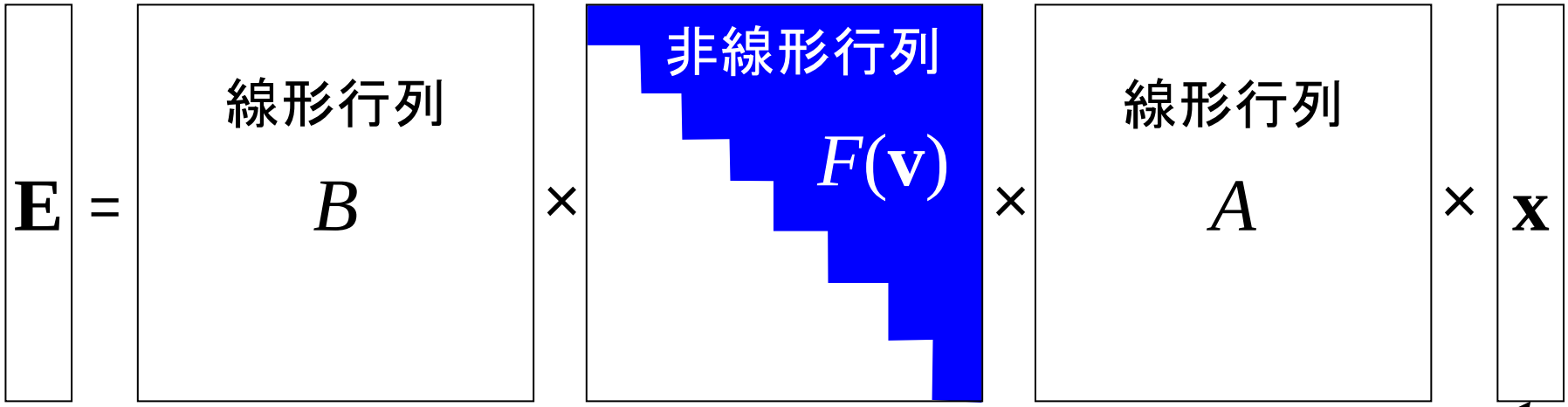
日本発祥の多変数公開鍵暗号

1980年代　松本・今井（MI暗号）、辻井

1990年代　笠原・境，STS暗号

海外は　Post量子以降活発

公開鍵



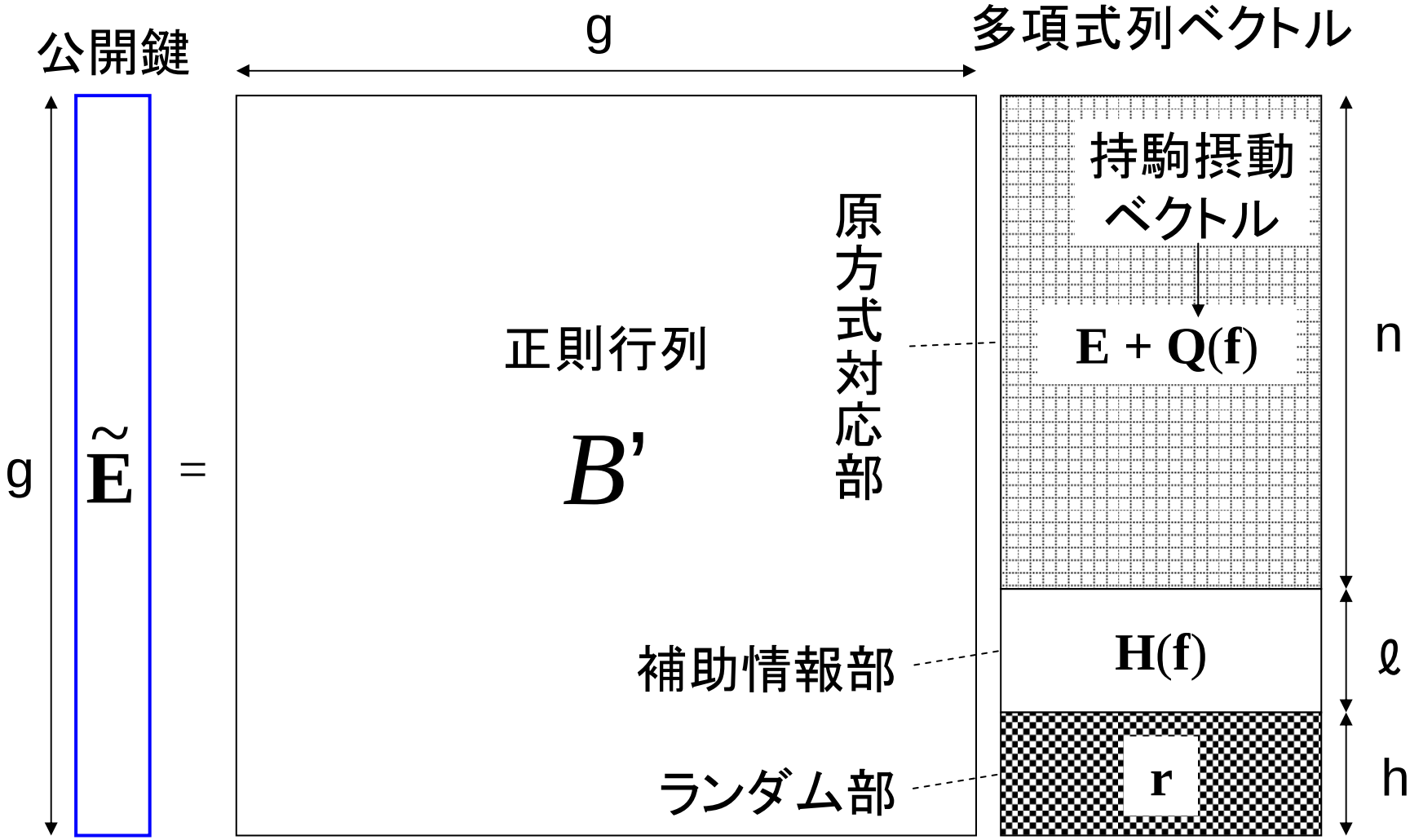
$$\mathbf{E} = B\mathbf{w} \qquad \mathbf{w} = F(\mathbf{v})\mathbf{v} \qquad \mathbf{v} = A\mathbf{x}$$

平文変数ベクトル

秘密鍵：$B, F(\mathbf{v}), A$

組織暗号という概念とそのSTS多変数公開鍵による実現、
医療・介護ネットワークなどへの応用

SCOPE 成果：非線形持駒摂動ベクトル方式



Fujita, Tadaki, and Tsujii: "Nonlinear piece in hand perturbation vector method for enhancing security of multivariate public key cryptosystems," PQCrypto 2008

SCOPE 成果：役割交代型署名 (Hidden Pair of Bijection)

全変数の集合を u と v という半分ずつに分ける

$$F_1(u) + F_2(v) +$$ u 変数と v 変数の積の線形結合

u, v それぞれについての全単射 (STS/Matsumoto-Imai)

- 署名するときは，u 変数か v 変数のどちらかに 0 を代入する．
  すると，0 を代入した変数を含む項は全て 0 になり，
  もう一方の変数についての全単射となる．これを解いて署名する．
- 通常，余分な変数に 1 通りの値しか代入しない方式では，
  署名の張る線形空間の次元が小さくなるため
  変数集合の分け方が解る．しかし変数の選び方を複数取れる
  ようにしたことでこの脆弱性は修正できた．

SCOPE 成果：役割交代型署名・署名の方法

v 変数に **0** を代入した場合

$$\boxed{F_1(u)} + \boxed{\mathbf{0}} + \boxed{\mathbf{0}}$$

u 変数に **0** を代入した場合

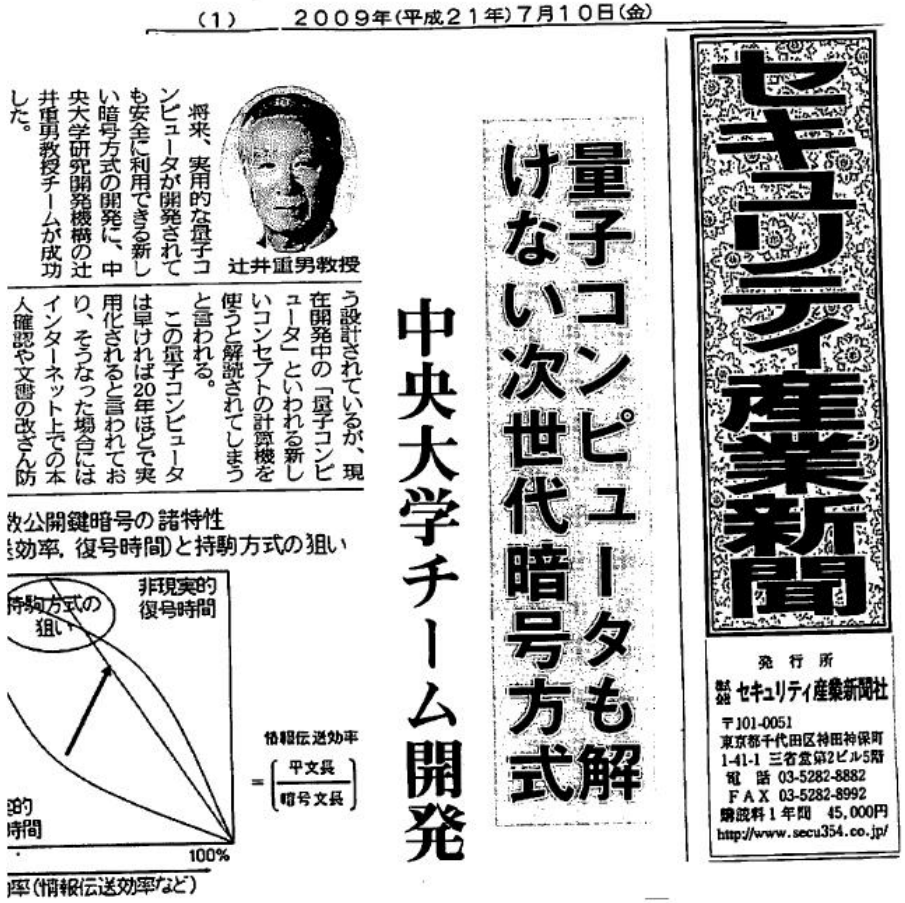
$$\boxed{\mathbf{0}} + \boxed{F_2(v)} + \boxed{\mathbf{0}}$$

- どちらの変数に 0 を代入したかは署名者以外は解らない.
- 全単射を組み合わせた方式なので，必ず1回で署名できる.
  既存の MPKC 署名方式では 1 回で署名できるとは保証されない.
- 既存の MPKC 署名方式 (UOV 方式) と比べて
  (署名長：文書長) の値が小さい (データ効率が良い)

Gotaishi and Tsujii: “Hidden Pair of Bijection signature scheme,” Cryptology ePrint Archive, Report 2011/353, July 2011.

多変数公開鍵暗号に関する SCOPE 成果発表

- PPS 方式（セキュリティ産業新聞 2009年7月10日号）
  - Piece in hand（持駒）
  - PMI
  - STS
- 国際会議発表
  - PQCrypto 2008, 2010
  - ISITA 2010
- 論文誌掲載
  - 電子情報通信学会
  - 日本応用数理学会


（1） 2009年(平成21年)7月10日(金)

セキュリティ産業新聞

量子コンピュータも解けない次世代暗号方式

中央大学チーム開発

辻井重男教授

将来、実用的な量子コンピュータが開発されても安全に利用できる新しい暗号方式の開発に、中央大学研究開発機構の辻井重男教授チームが成功した。

う設計されているが、現在開発中の「量子コンピュータ」といわれる新しいコンセプトの計算機を使うと解読されてしまうと言われる。

この量子コンピュータは早ければ20年ほどで実用化されると言われており、そうなった場合にはインターネット上での本人確認や文書の改ざん防

次公開鍵暗号の諸特性
送効率，復号時間）と持駒方式の狙い

持駒方式の狙い

非現実的復号時間

100%

情報伝送効率 = 平文長 / 暗号文長

率（情報伝送効率など）

発行所
セキュリティ産業新聞社
〒101-0051
東京都千代田区神田神保町
1-41-1 三省堂第2ビル5階
電話 03-5282-8882
FAX 03-5282-8992
購読料1年間 45,000円
http://www.secu354.co.jp/

Tsujii, Tadaki, Gotaishi, Fujita, and Kasahara: "Proposal of PPS multivariate public key cryptosystems," Cryptology ePrint Archive, Report 2009/264, June 2009.

部分和問題（ナップザック問題の一例）

品物 1: 容積 c_1

品物 2:
容積 c_2

品物 5:
容積 c_5

品物 3:
容積 c_3

品物 6:
容積 c_6

品物 4:
容積 c_4

品物 7:
容積 c_7

…

品物 n-1:
容積 c_{n-1}

品物 n:
容積 c_n

ナップザックを
ちょうど満たすように
品物の組み合わせを
求めよ

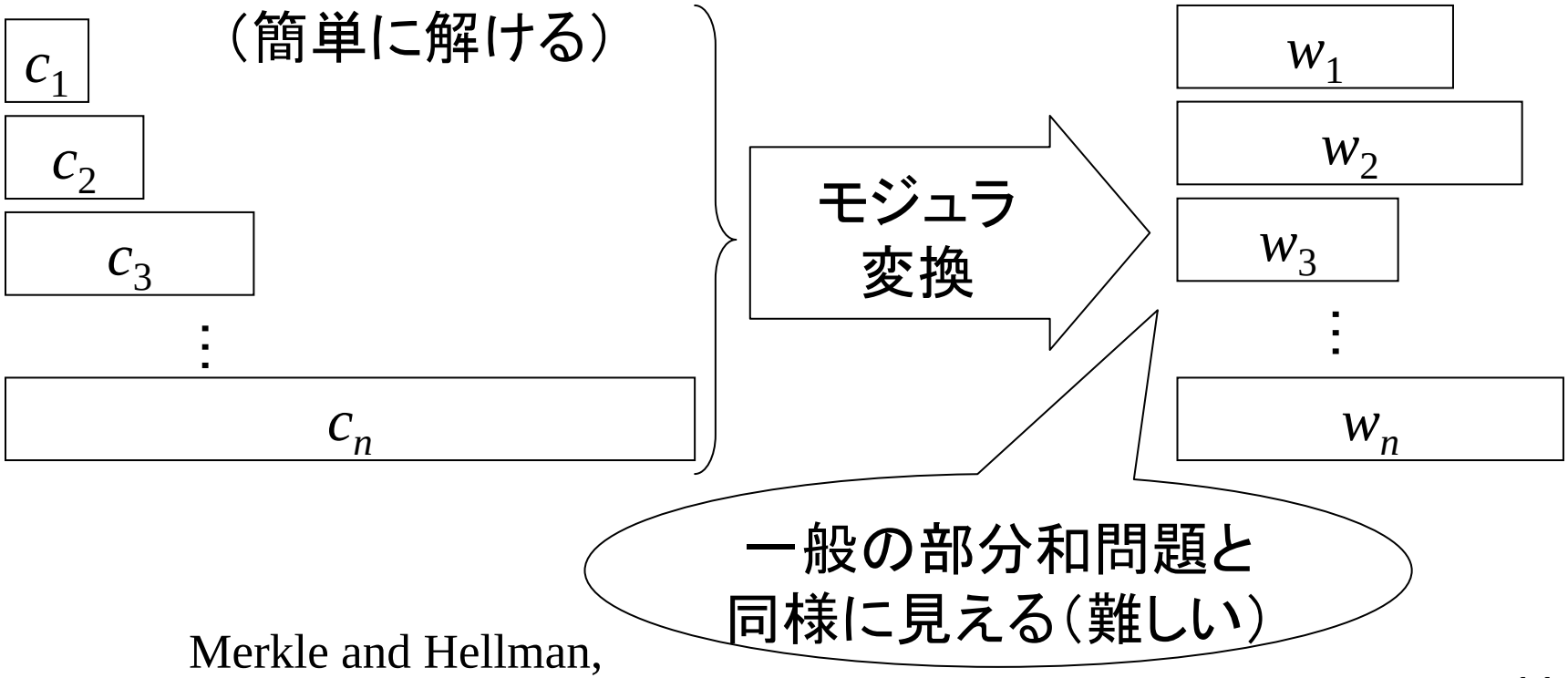
ナップザック: 容量 C

ナップザック公開鍵暗号

秘密鍵：$c_1, \ldots, c_n$

公開鍵：$w_1, \ldots, w_n$

超増加列をなすように構成
（簡単に解ける）



Merkle and Hellman,
"Hiding information and signatures in trapdoor knapsacks," 1978.

SCOPE 成果：乱数列を用いた ナップザック公開鍵暗号の新しい構成法

- 数論の基本定理（中国人の剰余定理）を用いて，
  従来の秘密鍵に乱数列を合成することにより，
  従来の攻撃法に対して安全なナップザック暗号の構成法を提案．

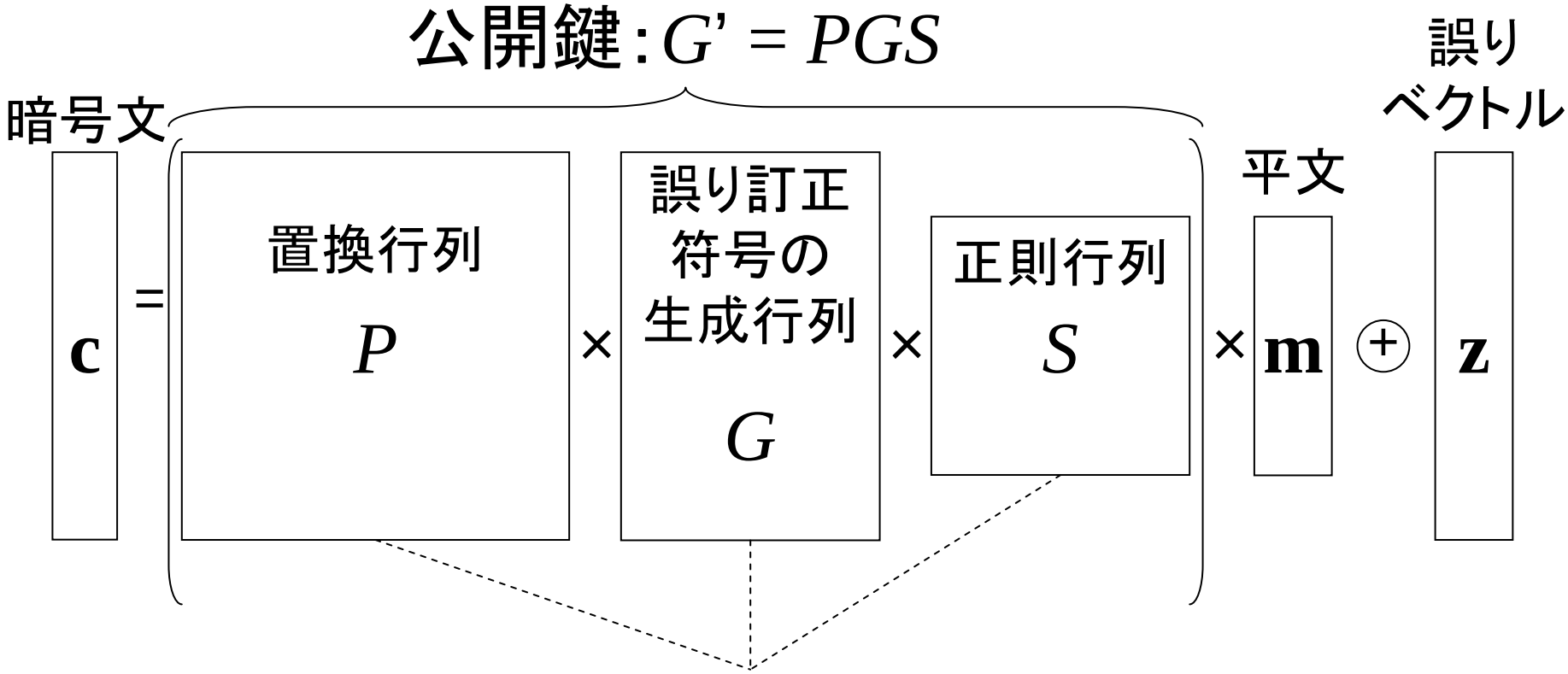
- 従来の攻撃法への安全性について
  - 公開鍵を乱数と区別することが難しいため，Shamir の攻撃（公開鍵から秘密鍵を求める攻撃）に対して安全．
  - 密度の高いナップザック暗号を設計できるため，
    低密度攻撃（暗号文から平文を求める攻撃）に対して安全．

Murakami, “A new construction of knapsack PKC by using a random sequence,” IEEE GLOBECOM2009

ナップザック暗号に関する SCOPE 成果発表

- 特許出願
  - 複数のナップザックを用いるナップザック暗号（特願2009-285093）
  - 高密度ナップザック暗号（特願2009-105254）
  - 低密度ナップザック暗号（特願2009-179664）
- 国際会議発表
  - ISITA2008, 2010, ICCIT2008, 2009, ICIS2009, IEEE GLOBECOM 2009
- 論文誌掲載
  - 日本応用数理学会

誤り訂正符号応用公開鍵暗号



McEliece,
"A public-key cryptosystem based on algebraic coding theory," 1978.

従来方式とSCOPE 提案方式との比較

従来代表方式：McEliece PKC

- Goppa符号応用 ⇒ 符号化率 1 未満
- 符号化率 $\rho \cong 0.5$ ⇒ ディジタル署名困難
- 誤り付加率 $\varepsilon \cong 0.05$ ⇒ 小さな値であり、安全性が十分でない

SCOPE 提案方式：K(IX)SE(1)PKC

- 完全符号応用 ⇒ 符号化率 1 実現
- 符号化率 $\rho = 1.0$ ⇒ ディジタル署名容易
- 誤り付加率 $\varepsilon = 0.125$ ⇒ 大きな値であり、安全性が高い

M. Kasahara, "A Construction of New Class of Linear Multivariate Public Key Cryptosystem Constructed Based on Error Correcting Codes," Technical Report of IEICE, ISEC 2009-135(2010-03).

誤り訂正符号応用公開鍵暗号に関する SCOPE 成果発表

- 学会発表
  - 情報理論とその応用シンポジウム (SITA)
  - 暗号と情報セキュリティシンポジウム (SCIS)
  - 日本応用数理学会 2009 年度年会

- 研究会発表
  - ISEC 研究会

他の暗号方式（多変数公開鍵暗号、
ナップザック公開鍵暗号）への知見の導入

SCOPE 成果:
計算可能性の理論における一方向性関数

一方向性関数は、計算量理論に基づく現代暗号理論で、本質的な役割を果たす。

本研究では、計算量理論ではなく、計算可能性の理論において一方向性関数と考えることが出来る概念を発見した。

この一方向性は、チェイティンの停止確率Ωの二進展開と、万能チューリングマシンUの停止問題との間のチューリング同値性を、精密化することにより得られるものである。

SCOPE 成果：計算可能性的一方向性関数
全く新しい耐量子コンピュータ暗号への展開

この一方向性関数を用いると、計算量的ではなく、計算可能性的に安全な暗号プロトコルを構成することが可能になると期待される。

量子コンピュータでも、計算不可能な関数は計算することが出来ない。従って、このような暗号プロトコルに対し、量子コンピュータは全く歯が立たない。

計算可能性の理論における一方向性関数の発見は、本SCOPE研究開発が成し遂げた世界初の成果であり、今後発展が期待される。

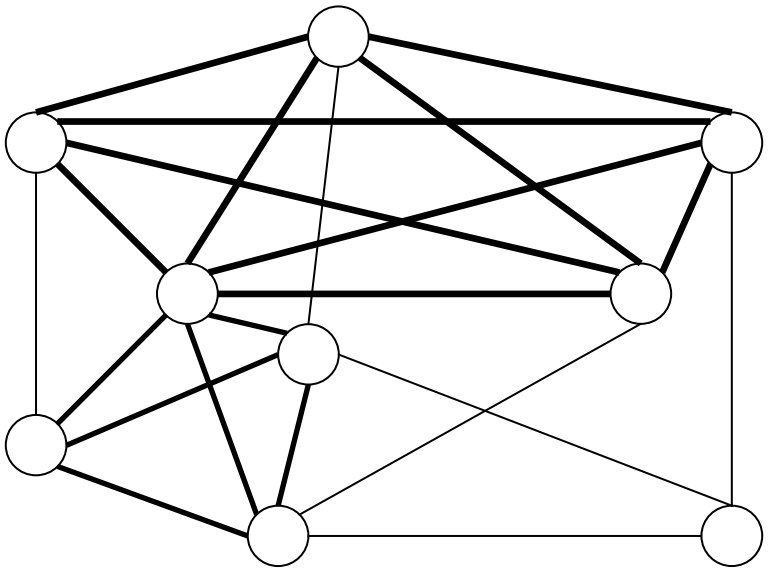
アルゴリズム基礎に関する SCOPE 成果発表

- 国際会議発表 (Lecture Notes in Computer Science Series)
  - K. Tadaki: "A new representation of Chaitin Ω number based on compressible strings," UC2010.
  - K. Tadaki: "Partial randomness and dimension of recursively enumerable reals," MFCS 2009.
  - K. Tadaki: "Chaitin Ω numbers and halting problems," CiE 2009.
  - K. Tadaki: "Fixed point theorems on partial randomness," LFCS'09.

- 論文誌掲載
  - K. Tadaki: "A statistical mechanical interpretation of algorithmic information theory: Total statistical mechanical interpretation based on physical argument," Journal of Physics: Conference Series (JPCS).

- 只木孝太郎: アルゴリズム的情報理論の統計力学的解釈, 特集 ランダムネスを捕まえる. 数学セミナー, 2011年2月号.

最大クリーク問題



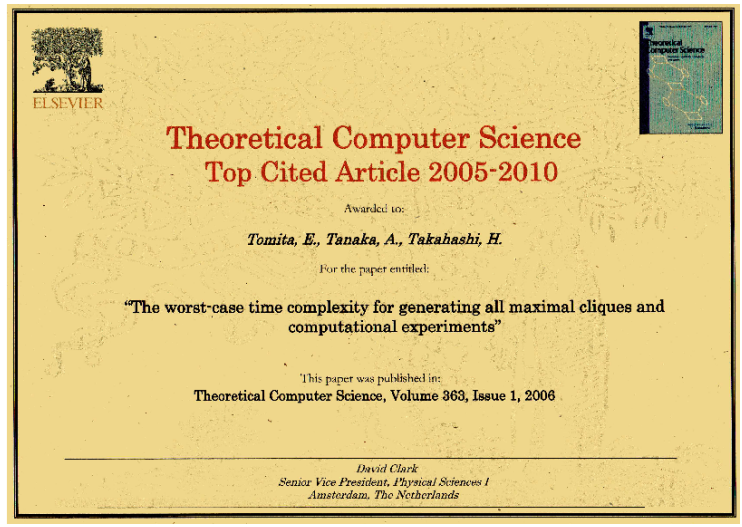
グラフ中のクリーク
（任意の二頂点間に
辺があるような頂点集合）
の中で最大のものを見つけよ

最大クリーク問題は、典型的な NP 困難問題であり、
かつ多くの重要な応用を持つ。

Matsunaga, Yonemori, Tomita, and Muramatsu: “Clique-based data mining for related genes in a biomedical database,” BMC Bioinformatics 2009.

NP 完全型暗号方式に関する SCOPE 成果発表

- 受賞
  - Theoretical Computer Science Top Cited Article 2005-2010



- 出版後約 8 ヶ月で 2,500 件以上のダウンロード.　他の賞の 10 倍の高ダウンロード数.
  - Tomita, Akutsu, and Matsunaga, "Efficient algorithms for finding maximum and maximal cliques: Effective tools for bioinformatics," in "Biomedical Engineering, Trends in Electronics, Communications and Software," 2011.（招待論文）

- 3rd of Most viewed articles in past 30 days: BMC Bioinformatics in July 2009
  - Matsunaga, Yonemori, Tomita, and Muramatsu: "Clique-based data mining for related genes in a biomedical database,"

最後に

- SoMoCS時代の基盤技術として、再び重要性が認識され始めた暗号技術（認証・署名、秘匿）へ貢献したい。

- 機密漏洩（認証・秘匿）
- プライバシー保護VS活用（電子行政・医療介護など）

- 本研究開発課題を掲載したホームページ
- http://www2.chuo-u.ac.jp/kikoh/scope/chuo-crypt-scope-index.html

- SCOPE 研究開発課題終了後の研究成果

  http://c-faculty.chuo-u.ac.jp/~rfujita/pqc.html

関係各位に感謝します。有難うございました。