Magma のグレブナ基底計算を利用した暗号解析
～多変数公開鍵暗号に対する代数攻撃～

2010年10月9日
研究集会「Magmaで広がる数学の世界」
九州大学大学院数理学研究院

藤田　亮　　中央大学研究開発機構

本研究は，総務省戦略的情報通信研究開発推進制度（SCOPE）による研究
「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」の成果の一つである.

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算

- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算
- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

問題

- 次の連立方程式を解きなさい

$$\begin{cases} 3x+6y+5z=2 \\ 5x+y+2z=4 \\ x+2y+z=6 \end{cases}$$

答え

- 次の連立方程式を解きなさい

$$\begin{cases} 3x+6y+5z=2 \\ 5x+y+2z=4 \\ x+2y+z=6 \end{cases}$$

$$x=6, \quad y=4, \quad z=6$$

答え

- 次の連立方程式を解きなさい

$$\begin{cases} 3x+6y+5z=2 \\ 5x+y+2z=4 \\ x+2y+z=6 \end{cases}$$

$$x=6, \quad y=4, \quad z=6$$

係数体：GF(7), $x, y, z \in \mathrm{GF}(7)$

問題

- 次の連立方程式を解きなさい

$$\begin{cases} 3x^2+xy+2xz+6y^2+4yz+5z^2+6x+4y+5z=3 \\ 6x^2+6xy+xz+3y^2+yz+3z^2+2x+y+4z=5 \\ 5x^2+2xy+3xz+3y^2+4yz+5z^2+6x+5y+z=3 \end{cases}$$

係数体:GF(7), $x, y, z \in \mathrm{GF}(7)$

準備

- 各式の右辺を 0 にする

$$\begin{cases} 3x^2+xy+2xz+6y^2+4yz+5z^2+6x+4y+5z+4=0 \\ 6x^2+6xy+xz+3y^2+yz+3z^2+2x+y+4z+2=0 \\ 5x^2+2xy+3xz+3y^2+4yz+5z^2+6x+5y+z+4=0 \end{cases}$$

係数体 : GF(7), $x, y, z \in \mathrm{GF}(7)$

解法の一例

(1)それぞれの式に x, y, z を掛けたものを付け足し，単項式の係数からなる行列をつくる

x^3	x^2y	x^2z	x^2	xy^2	xyz	xy	xz^2	xz	x	y^3	y^2z	y^2	yz^2	yz	y	z^3	z^2	z	1
[3	1	2	6	6	4	4	5	5	4	0	0	0	0	0	0	0	0	0	0]
[0	3	0	0	1	2	6	0	0	0	6	4	4	5	5	4	0	0	0	0]
[0	0	3	0	0	1	0	2	6	0	0	6	0	4	4	0	5	5	4	0]
[6	6	1	2	3	1	1	3	4	2	0	0	0	0	0	0	0	0	0	0]
[0	6	0	0	6	1	2	0	0	0	3	1	1	3	4	2	0	0	0	0]
[0	0	6	0	0	6	0	1	2	0	0	3	0	1	1	0	3	4	2	0]
[5	2	3	6	3	4	5	5	1	4	0	0	0	0	0	0	0	0	0	0]
[0	5	0	0	2	3	6	0	0	0	3	4	5	5	1	4	0	0	0	0]
[0	0	5	0	0	2	0	3	6	0	0	3	0	4	5	0	5	1	4	0]
[0	0	0	3	0	0	1	0	2	6	0	0	6	0	4	4	0	5	5	4]
[0	0	0	6	0	0	6	0	1	2	0	0	3	0	1	1	0	3	4	2]
[0	0	0	5	0	0	2	0	3	6	0	0	3	0	4	5	0	5	1	4]

解法の一例

(2) (1)の行列を掃き出す.

(3) 一変数多項式が得られたならば,

これを解き, その変数の値を得る.

変数を消し, 方程式を簡単化して, (1)に戻る

一変数多項式が得られない場合,

(1)に戻り, より次数の高い単項式,

例えば, xy, z^2, … などを

もとの式に掛けたものを付け足して並べる.

解法の一例

- この問題では，5 次以下の単項式を各式に掛けて並べた，(1)の行列を掃きだすと一変数方程式が得られる.

$$z^7 + 3z^6 + 5z^5 + 6z^3 + 3 = 0$$

$$z = 3$$

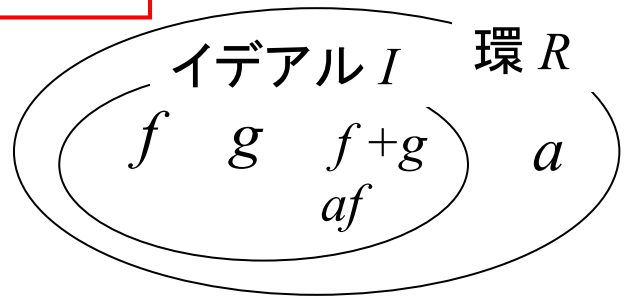
XL (eXtended Linearization) アルゴリズム
[Courtois-Klimov-Patarin-Shamir, EUROCRYPT 2000]

XL の方がグレブナ基底計算よりも冗長
[Ars-Faugère-Imai-Kawazoe-Sugita, ASIACRYPT 2004]

（両側）イデアルとは

可換環 R の部分集合で, 以下の1, 2をみたす I

1. $\forall f, g \in I \Rightarrow f + g \in I$
2. $\forall a \in R, \forall f \in I \Rightarrow af \in I$



イデアル I は, 以下の形で表現できる.

$$I = \langle f_1, \cdots, f_m \rangle = \{ g_1 f_1 + \cdots + g_m f_m \mid g_1, \ldots, g_m \in R \} \ (f_1, \ldots, f_m \in I)$$

$f_1, \ldots, f_m$:イデアル I を生成する基底

このような基底は一意でないが,
その中でも, グレブナ基底は「よい」性質を持つ.

「連立方程式が等価」とは

k : 任意の体, $f_i \in k[x_1,\ldots,x_n]$ $(i = 1,\ldots,s)$ として
V : アフィン多様体を以下のように定義

$$V(f_1,\ldots,f_s) = \left\{ \begin{array}{l} (a_1,\ldots,a_s) \in k^n \\ : \text{すべての} 1 \le i \le s \text{に対して } f_i(a_1,\ldots,a_s) = 0 \end{array} \right\}$$

（これは, 連立方程式 $f_1(x_1,\ldots,x_n) = \cdots = f_s(x_1,\ldots,x_n) = 0$ の解全体の集合）

命題　$f_1, \ldots, f_s$ と $g_1, \ldots, g_t$ が $k[x_1,\ldots,x_n]$ の同じイデアルの基底であるならば, $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$

同じイデアルの別の基底を探す限りにおいて,
それらの基底に対応する連立方程式は等価.

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算

- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

グレブナ基底計算を用いた求解

$$\begin{cases} 3x^2 + xy + 2xz + \cdots(\text{中略})\cdots + 5z + 4 = 0 \\ 6x^2 + 6xy + xz + \cdots(\text{中略})\cdots + 4z + 2 = 0 \\ 5x^2 + 2xy + 3xz + \cdots(\text{中略})\cdots + z + 4 = 0 \end{cases}$$

$$f_1 = 3x^2 + xy + 2xz + 6y^2 + 4yz + 5z^2 + 6x + 4y + 5z + 4$$

$$f_2 = 6x^2 + 6xy + xz + 3y^2 + yz + 3z^2 + 2x + y + 4z + 2$$

$$f_3 = 5x^2 + 2xy + 3xz + 3y^2 + 4yz + 5z^2 + 6x + 5y + z + 4$$

f_1, f_2, f_3 を基底とした多項式環イデアル I を考える

グレブナ基底計算を用いた求解

I のグレブナ基底(辞書式順序)を計算する

$$g_1 = x + 3y + 2z^6 + 2z^5 + 5z^4 + 3z^3 + 5z^2 + 4z,$$

$$g_2 = y^2 + 5z^5 + 3z^3 + z^2 + 2z + 3,$$

$$g_3 = yz + 4y + 5z^6 + 2z^5 + 3z^4 + 4z^3 + 2z^2 + 4z + 3,$$

$$g_4 = z^7 + 3z^6 + 5z^5 + 6z^3 + 3$$

三角形式になっており,
簡単に解ける

$$x = 0, \quad y = 4, \quad z = 3$$

または $\quad x = 3, \quad y = 3, \quad z = 3$

なぜ解けるのか

- 詳細について，本講演では，省略.
- グレブナ基底の理論に関しては，
  これまでに，数多くの文献が出ている.

- Cox, Little, and O'Shea,
  "Ideals, Varieties, and Algorithms," Springer, 2007 (3rd edition).
- 野呂, 横山, "グレブナー基底の計算 基礎篇,"
  東京大学出版会, 2003.
- Kreuzer and Robbiano,
  "Computational Commutative Algebra 2," Springer, 2005.
- 日比編, "グレブナー基底の現在," 数学書房, 2006.
- ...

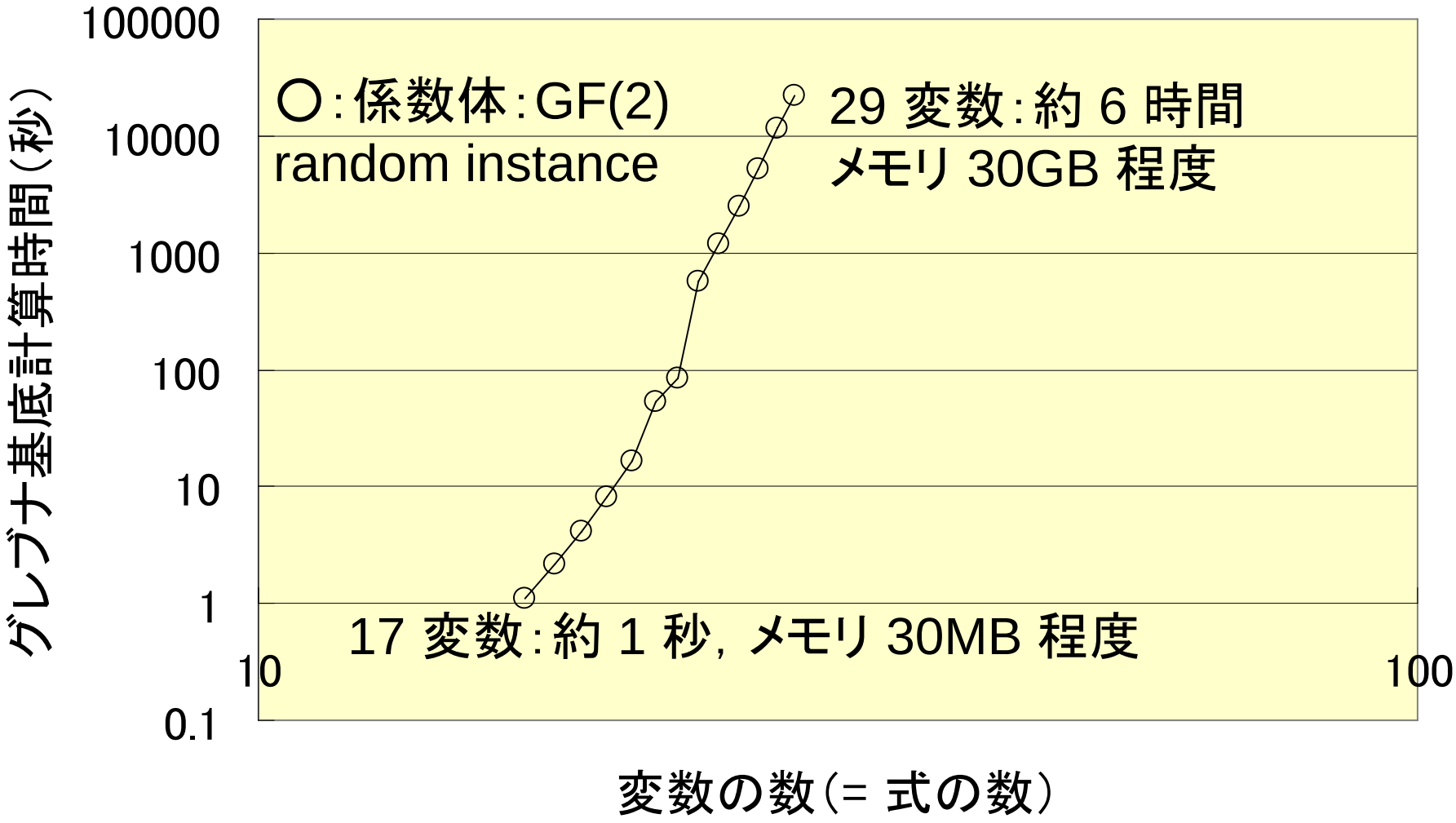
問題の困難性

- 有限体上の多変数非線形連立方程式の求解は NP 困難問題
  - Garey and Johnson, “Computers and Intractability: A Guide to the Theory of NP-Completeness,” Freeman, 1979.

- NP 困難問題は，量子コンピュータを用いても，解くことが困難であると，強く信じられている．

- ちなみに，イデアル所属判定問題は，さらに難しい（EXPSPACE 完全問題）

Magma のグレブナ基底計算時間



計算機実験環境(1)

- コンピュータ

  JCS(日本コンピューティングシステム)

  VC98220WSA-4U/T workstation
  - 2.80GHz AMD Opteron 8220 プロセッサ
  - 128GB RAM
- 数式処理ソフトウェア

  Magma V2.15-5
- グレブナ基底計算アルゴリズム

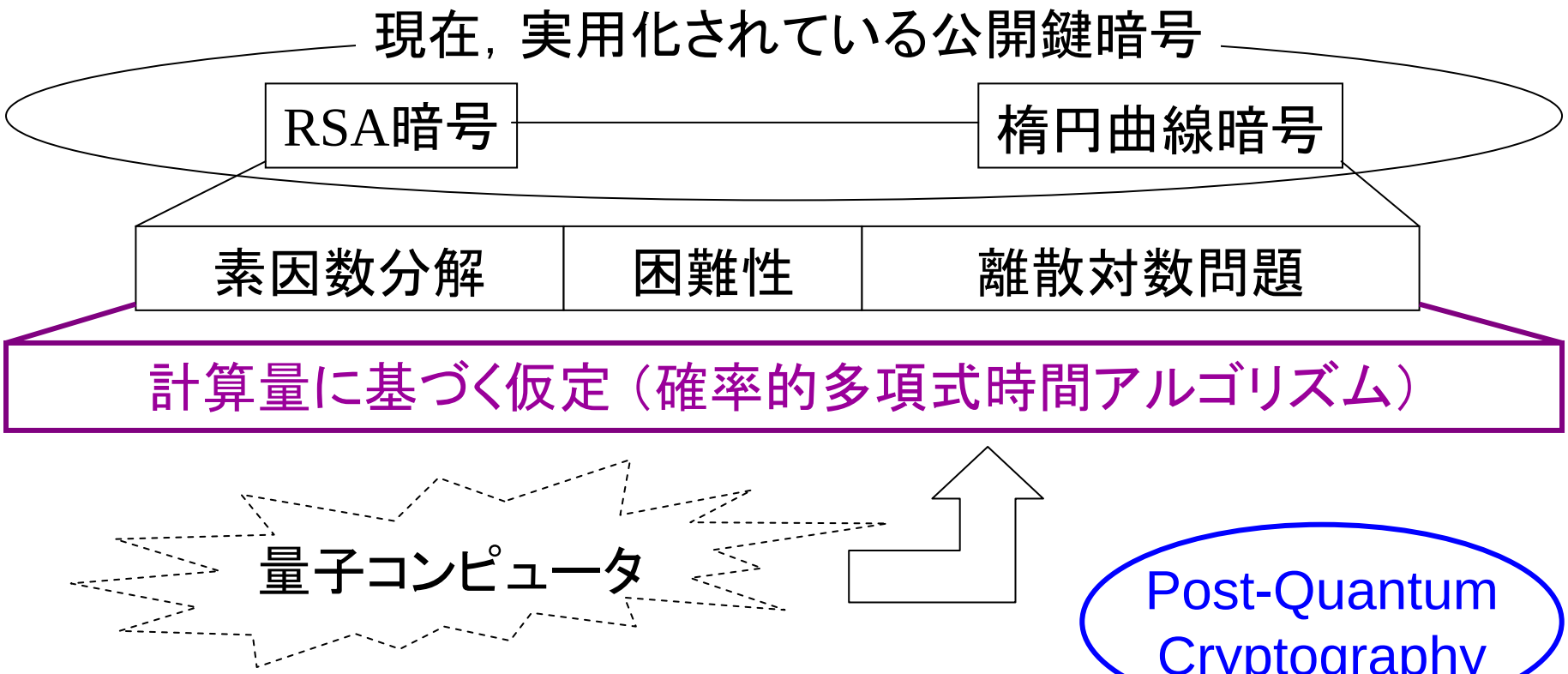
  F_4(Magma に実装されているもの)

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算

- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

(将来における)公開鍵暗号の危機



→異なる数学的困難性に基づく公開鍵暗号
（ex. 多変数公開鍵暗号）を開発しておく必要あり.

多変数公開鍵暗号とは

- 多変数非線形連立方程式の求解困難性に
  安全性の根拠を求めている公開鍵暗号
  （量子コンピュータに対抗し得る公開鍵暗号の候補の一つ）

- 暗号化，復号処理が高速
  …加算，乗算のみの単純な演算

- 鍵長は比較的長い（数 Kbit，数 Mbit）

  例：$SFLASH^{v3}$：112.3KB, QUARTZ：71KB（2000年ごろ）
  （参考）RSA 暗号：2048 bit, 楕円曲線暗号：200 bit 程度
  （2030 年前後まで安全と考えられている鍵長）

多変数公開鍵暗号に関する研究

暗号方式

MI（松本・今井他，1983, 1985, 1988）

順序解法（辻井他，1985, 1986）

核変換（一般化順序解法）（辻井他，1989）

1980年代，世界に先駆けて，
日本が発祥の公開鍵暗号方式

多変数公開鍵暗号に関する最近の研究

多種多様な方式，暗号解析手法が提案されており，
様々な文献に取り上げられている．

- Koblitz, “Algebraic Aspects of Cryptography,” Springer, 1998.
（林訳, “暗号の代数理論,” シュプリンガー・フェアラーク東京.）

- Ding, Gower, and Schmidt,
“Multivariate Public Key Cryptosystems,” Springer, 2006.

- 辻井, 笠原編著, “暗号理論と楕円曲線,” 森北出版, 2008.

- Bernstein, Buchmann, and Dahmen (editors),
“Post-Quantum Cryptography,” Springer, 2009.

多変数 2 次公開鍵暗号とは（1/5）

パラメータ：暗号系を構成する有限体の位数 q,
平文（ベクトル）の次元 n,
暗号文（ベクトル）の次元 m

$\mathbf{F}_q = \mathrm{GF}(q)$

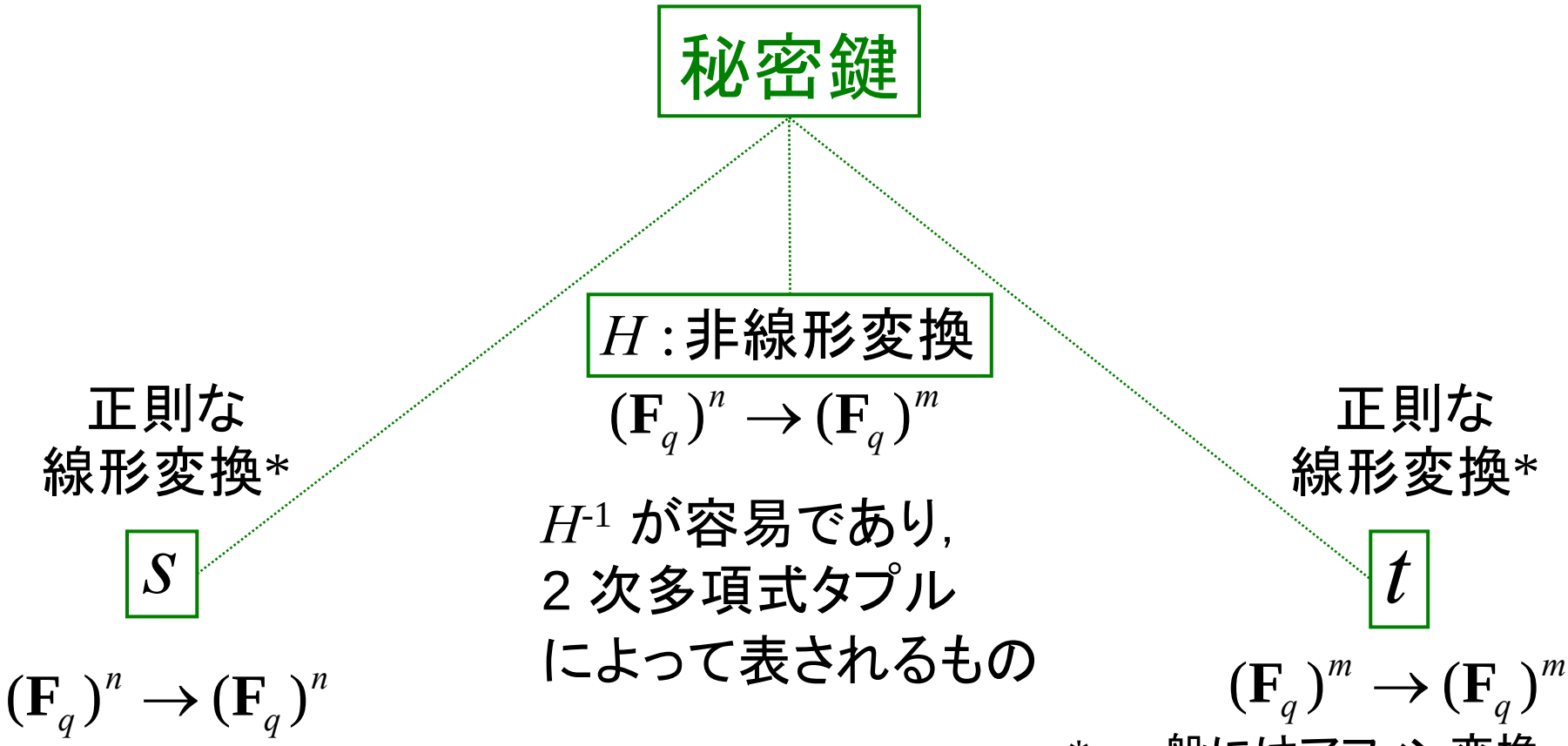
平文

$\mathbf{p} \in (\mathbf{F}_q)^n$

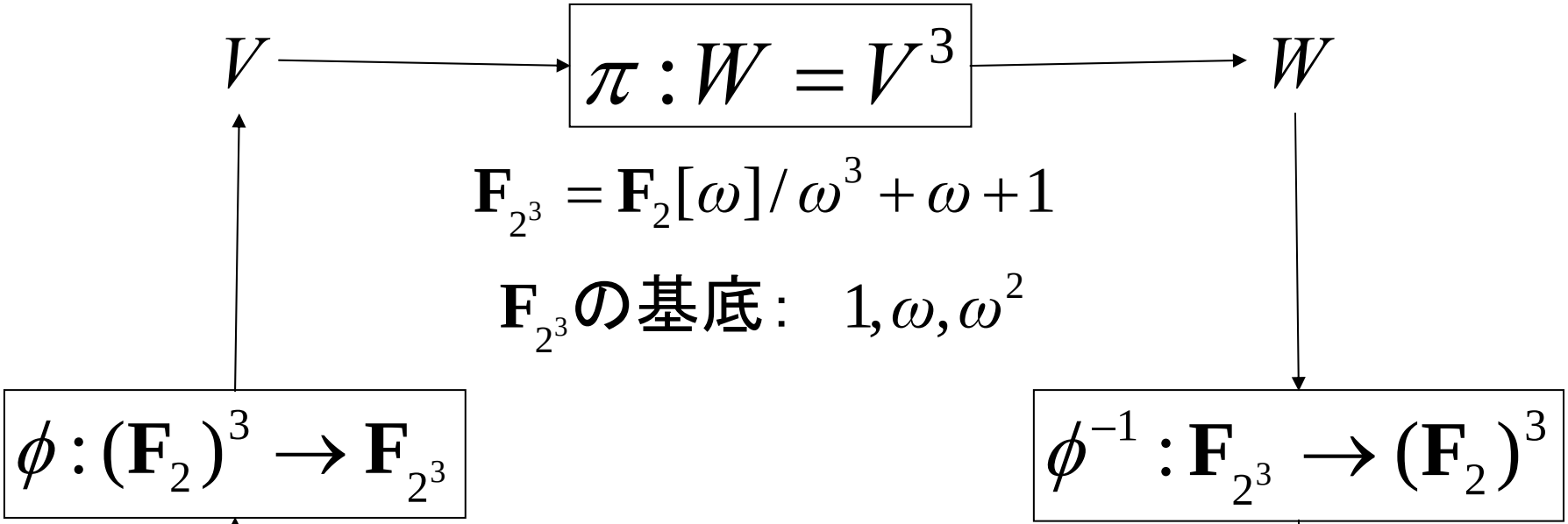
暗号文

$\mathbf{c} \in (\mathbf{F}_q)^m$

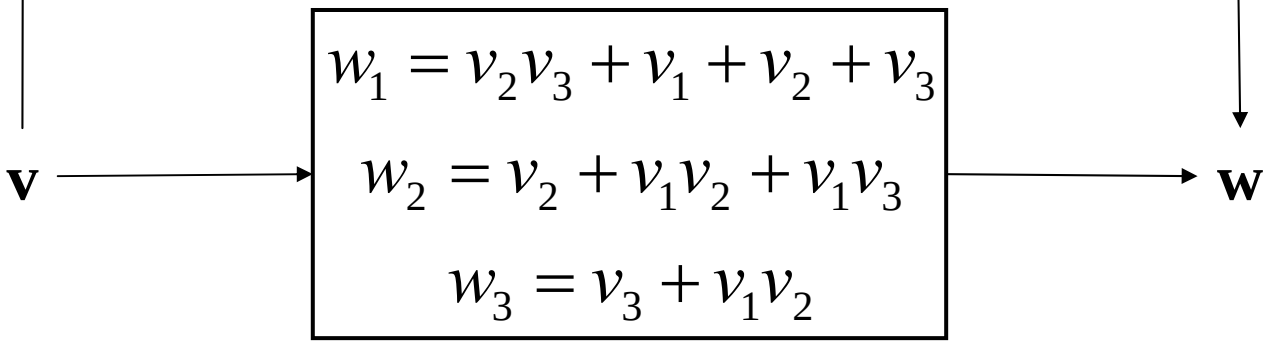
多変数 2 次公開鍵暗号とは(2/5)



一変数単項式表現（逆変換は容易）



多変数表現（逆変換は困難）



多変数 2 次公開鍵暗号とは(3/5)

$$\mathbf{F}_q[x_1, \ldots, x_n]^m$$

公開鍵: $E = t \circ H \circ s$:
多変数 2 次多項式(タプル)

正則な
線形変換

s

$(\mathbf{F}_q)^n \to (\mathbf{F}_q)^n$

H :非線形変換

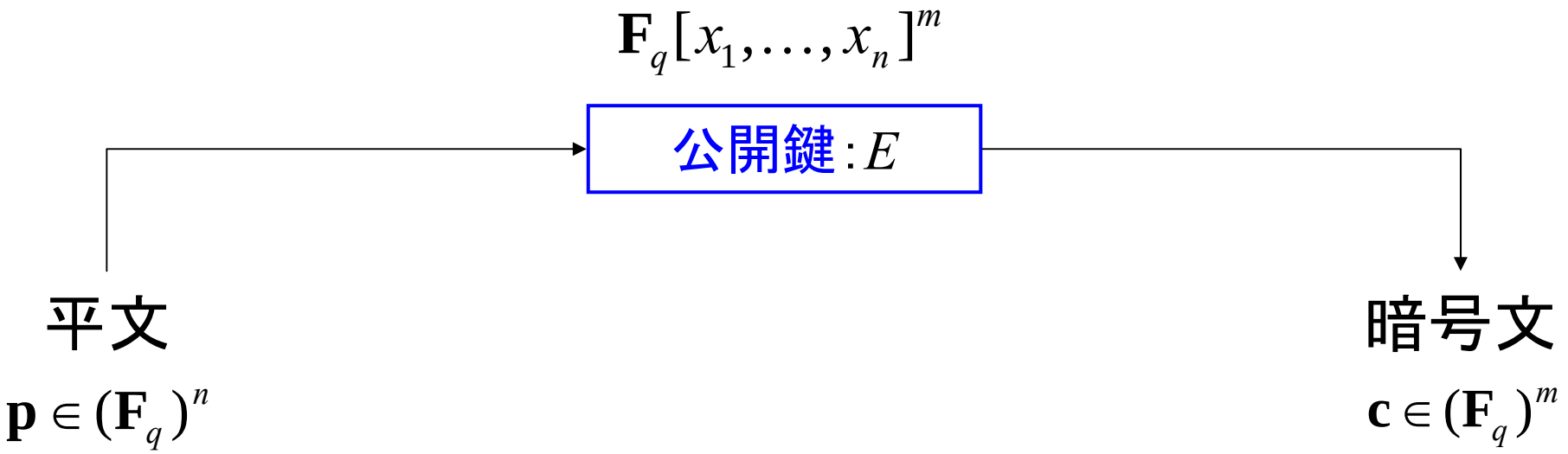
$(\mathbf{F}_q)^n \to (\mathbf{F}_q)^m$

正則な
線形変換

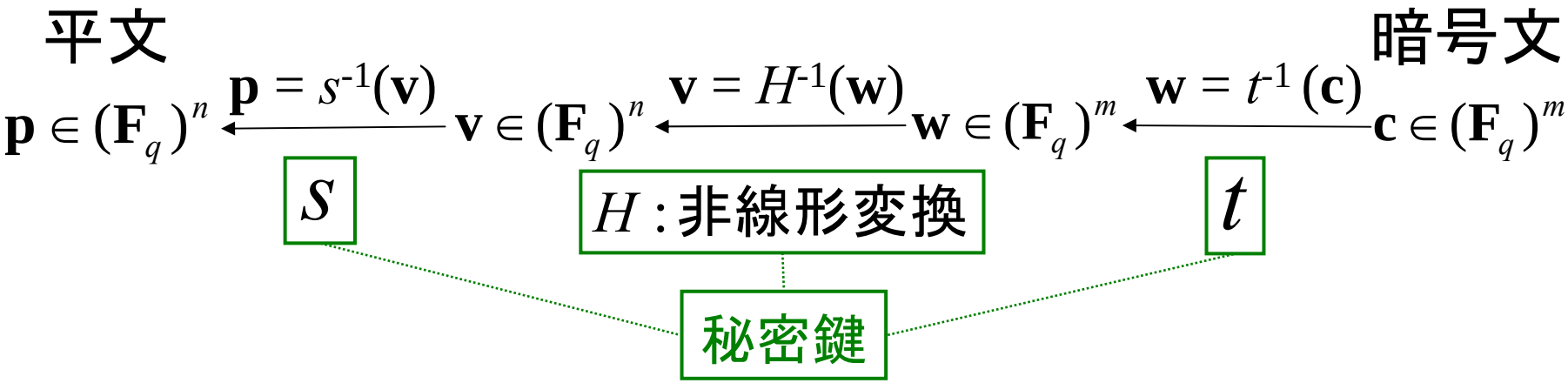
t

$(\mathbf{F}_q)^m \to (\mathbf{F}_q)^m$

多変数 2 次公開鍵暗号とは(4/5)

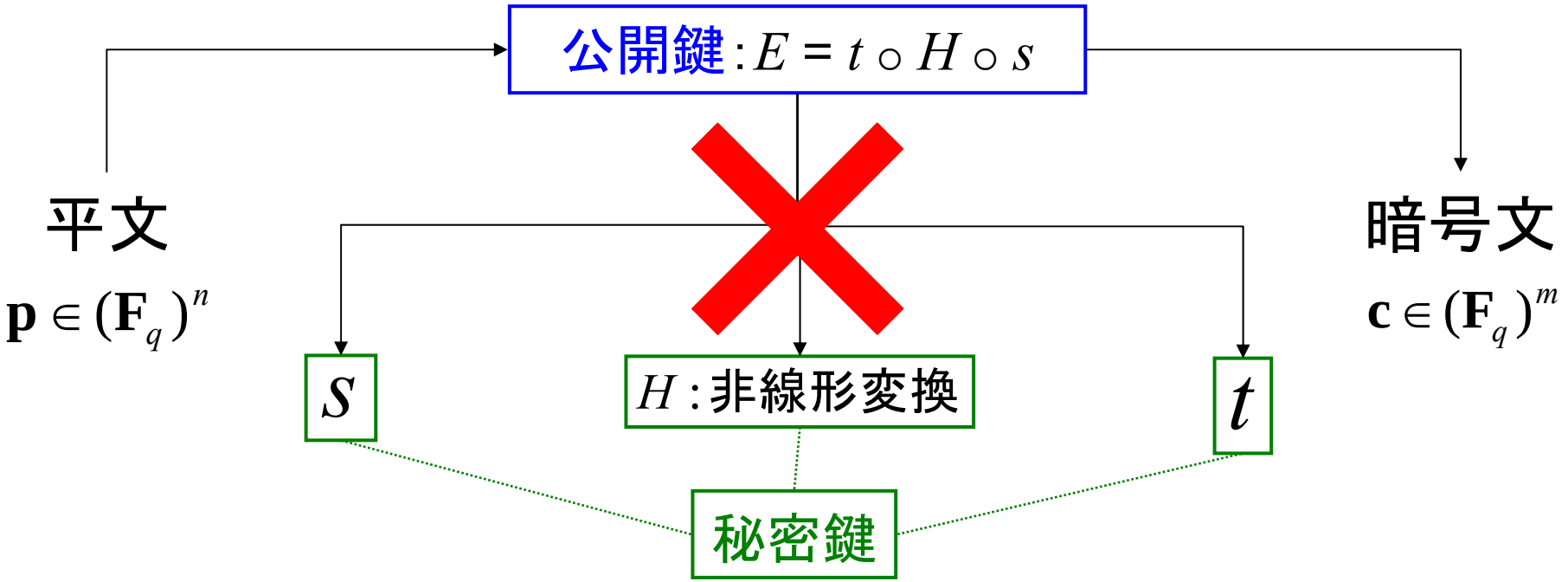


多変数 2 次公開鍵暗号とは(5/5)



多変数公開鍵暗号の安全性(1/2)

攻撃者が公開鍵を
秘密鍵に分解するのは困難



多変数公開鍵暗号の安全性(2/2)

攻撃者が E, $\mathbf{c}$ から
$\mathbf{p}$ を求めるのは困難

公開鍵 : E :
多変数多項式(タプル)

平文

$\mathbf{p} \in (\mathbf{F}_q)^n$

暗号文

$\mathbf{c} \in (\mathbf{F}_q)^m$

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算

- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

代数攻撃とは

攻撃者が，公開鍵 E と暗号文 **c** から
平文 **p** を得ようとする攻撃

公開鍵 : $E(\mathbf{x}) = (e_1(\mathbf{x}), \ldots, e_m(\mathbf{x}))^{\mathrm{T}}$

平文

暗号文
c

連立方程式

$$e_1(x_1, x_2, \cdots, x_n) = c_1$$
$$e_2(x_1, x_2, \cdots, x_n) = c_2$$
$$\vdots$$
$$e_m(x_1, x_2, \cdots, x_n) = c_m$$

XL アルゴリズム，グレブナ基底計算などにより，
この連立方程式を解く

連立方程式から
イデアルを構成

連立方程式

$$\begin{aligned} e_1(x_1, x_2, \cdots, x_n) &= c_1 \\ e_2(x_1, x_2, \cdots, x_n) &= c_2 \\ &\vdots \\ e_m(x_1, x_2, \cdots, x_n) &= c_m \end{aligned} \quad \Rightarrow \quad \begin{aligned} e_1(x_1, x_2, \cdots, x_n) - c_1 &= 0 \\ e_2(x_1, x_2, \cdots, x_n) - c_2 &= 0 \\ &\vdots \\ e_m(x_1, x_2, \cdots, x_n) - c_m &= 0 \end{aligned}$$

ここで，次のような多項式環イデアル I を考える．

$$I = \langle e_1(x_1, x_2, \cdots, x_n) - c_1, e_2(x_1, x_2, \cdots, x_n) - c_2, \cdots, e_m(x_1, x_2, \cdots, x_n) - c_m \rangle$$

$$I \subset P = \mathbf{F}_q[x_1, x_2, \ldots, x_n] \qquad P : \mathbf{F}_q \text{係数多項式環}$$

グレブナ基底計算による連立方程式の求解

$$I = \langle e_1(x_1, x_2, \cdots, x_n) - c_1, e_2(x_1, x_2, \cdots, x_n) - c_2, \cdots, e_m(x_1, x_2, \cdots, x_n) - c_m \rangle$$

このイデアル I のグレブナ基底 G を計算

$$G = \{x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n\}$$
$$I = \langle x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n \rangle$$

このとき平文 $\mathbf{x} = \mathbf{a} = (a_1, a_2, \cdots, a_n)^T$ （一意解）

$$G = \{1\}$$

（解なし）

一般の場合

$G = \{g_1, \ldots . g_t\}$

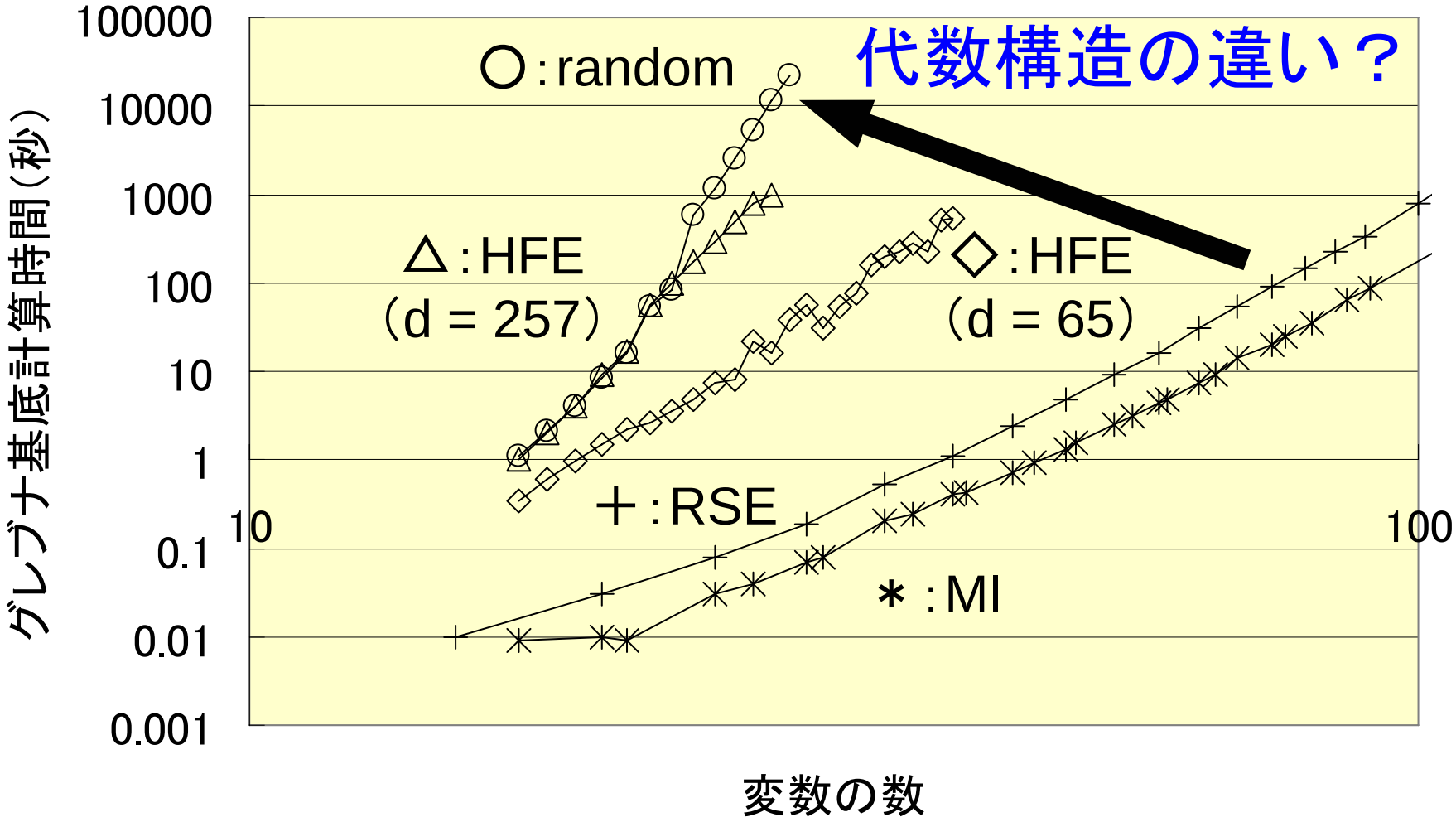
$g_i \in P$

解 : $V(g_1, \ldots . g_t)$

（複数の解）

V : アフィン多様体

「グレブナ基底攻撃」に対する安全性



代数攻撃の適用例

- HFE (Hidden Field Equation) に対する代数攻撃

  [Courtois-Daum-Felke, PKC 2003]

  [Faugère-Joux, CRYPTO 2003]

  [Granboulan-Joux-Stern, CRYPTO 2006]

  [Dubois-Gama, ASIACRYPT 2010, to appear]

- TRMC (Tractable Rational Map Cryptosystem) に対する代数攻撃

  [Joux-Kunz-Jacques-Muller-Ricordel, PKC 2005]

- TRMS (Tractable Rational Map Signature) に対する代数攻撃

  [Bettale-Faugère-Perret, AFRICACRYPT 2008]

代数攻撃の適用例

- MQQ (Multivariate Quadratic Quasigroups)
  に対する代数攻撃

  [Mohamed-Ding-Buchmann-Werner, CANS 2009]

  [Faugère-Gligoroski-Ødegård-Perret, CANS 2010, to appear]
- Dragon 型多変数公開鍵暗号に対する代数攻撃

  [Mohamed-Bulygin-Ding-Buchmann-Werner,
  CANS 2010, to appear]

代数攻撃の適用例(安全性解析)

- UOV (Unbalanced Oil and Vinegar) の安全性解析

  [Braeken-Wolf-Preneel, CT-RSA 2005]
- PMI (Perturbed Matsumoto-Imai) の安全性解析

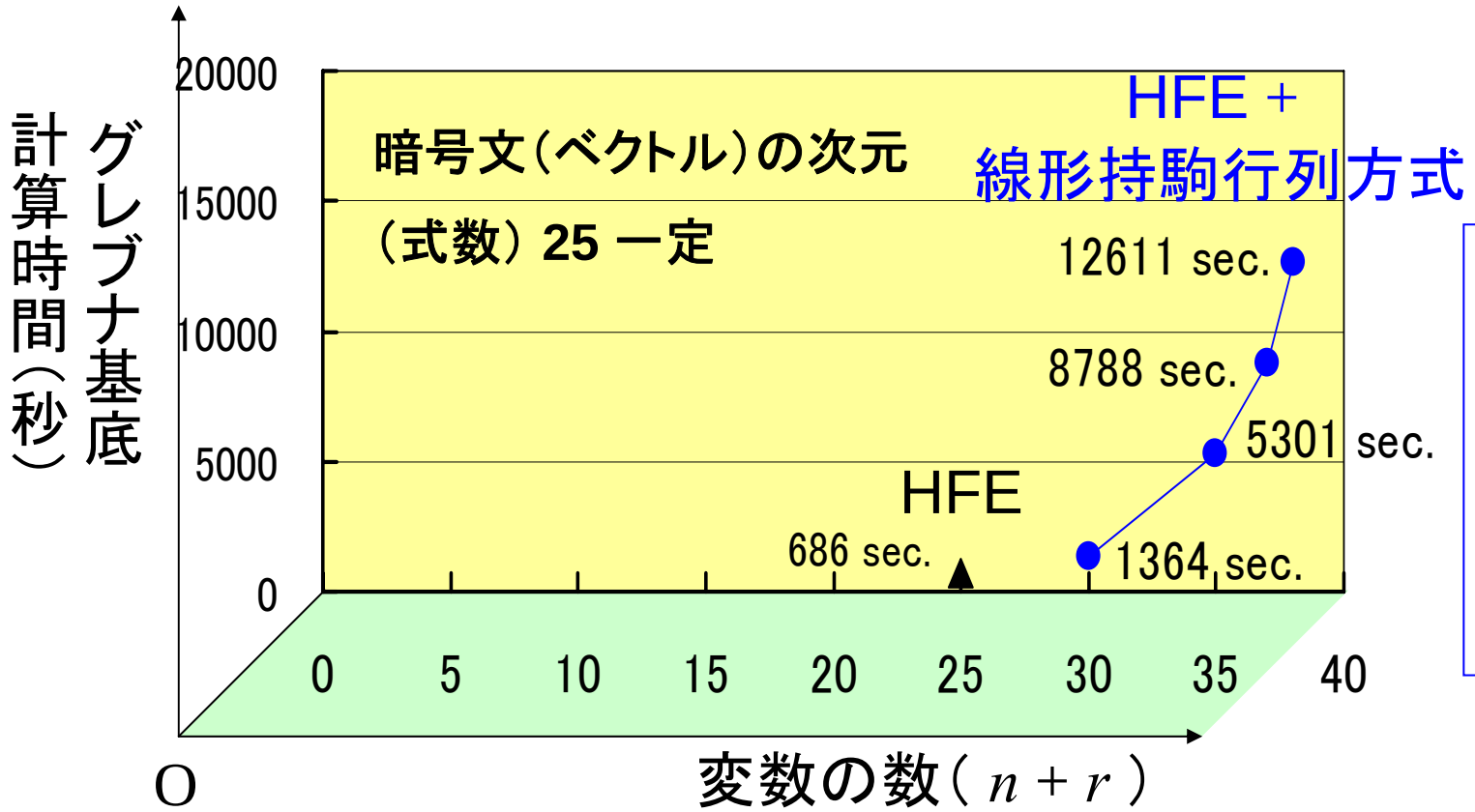
  [Ding-Gower-Schmidt-Wolf-Yin, IMA-CCC 2005]
- 線形持駒行列方式の安全性解析

  [Tsujii-Tadaki-Fujita, PQCrypto 2006]
- 非線形持駒摂動ベクトル方式の安全性解析

  [Fujita-Tadaki-Tsujii, PQCrypto 2008]
- rSTS 型多変数公開鍵暗号の安全性解析

  [Fujita, PQCrypto 2010, Recent Result Session]

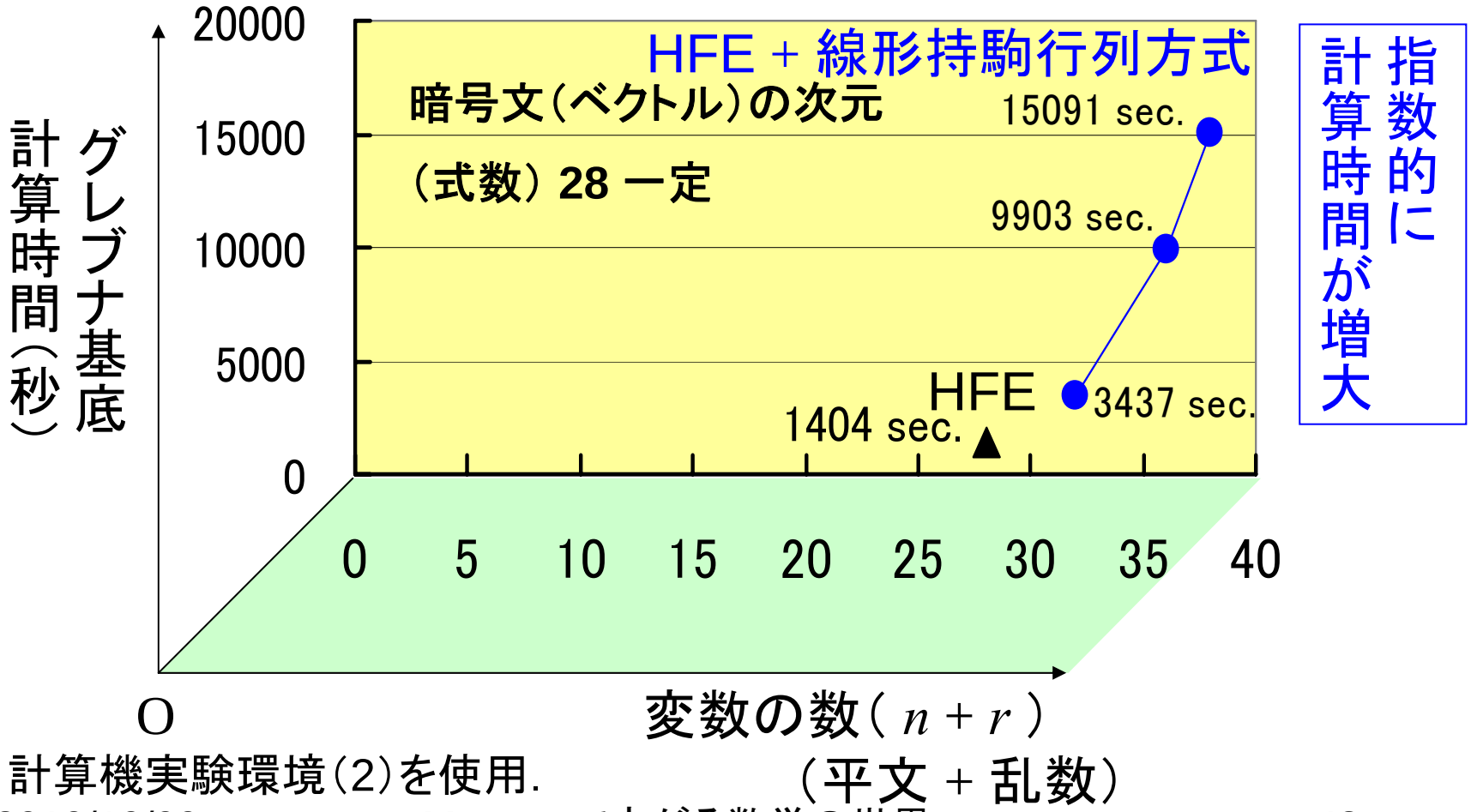
暗号解析のための
グレブナ基底計算時間の増大(式数:25)



指数的に計算時間が増大

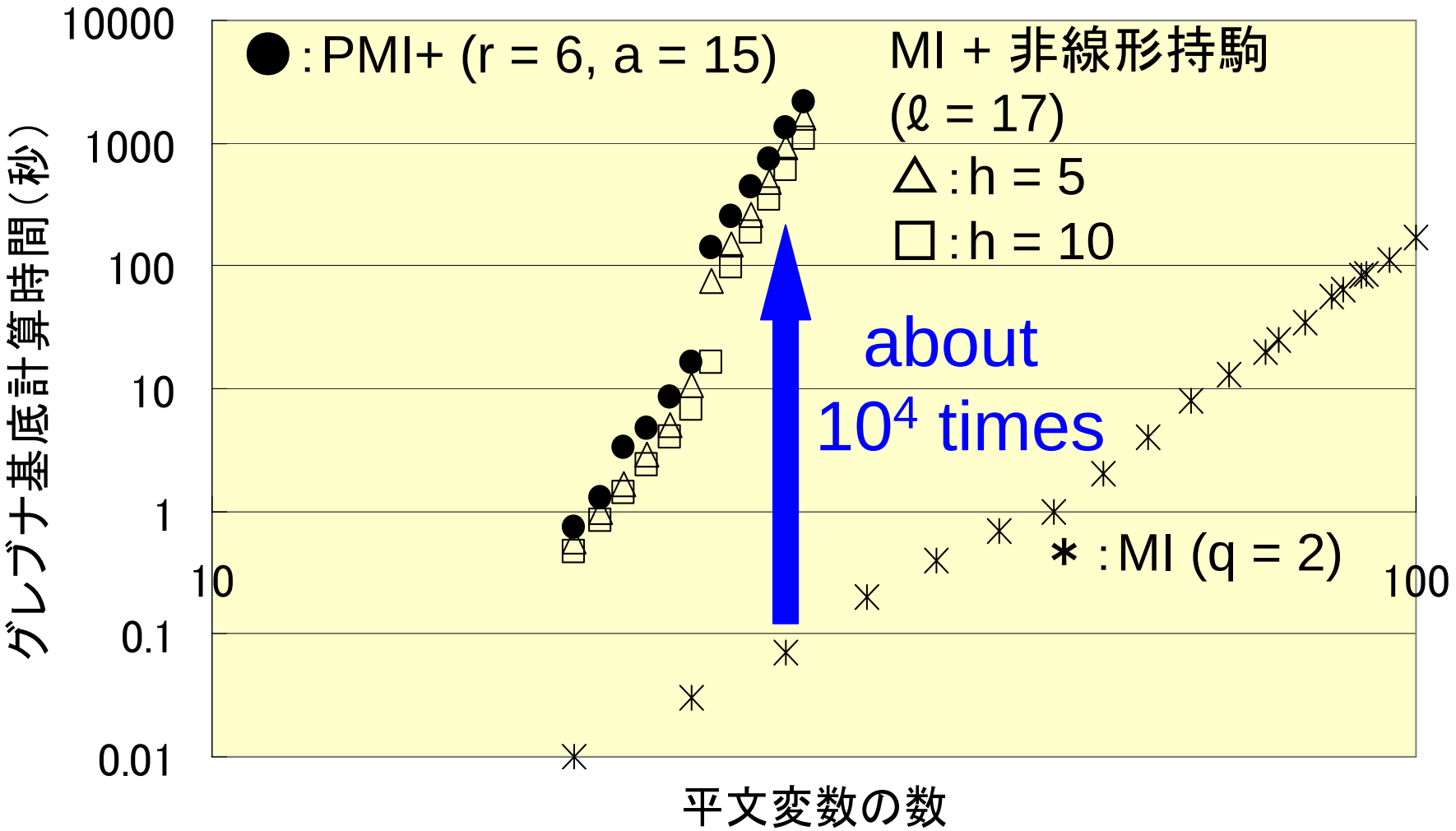
(注)計算機実験環境(2)を使用.

暗号解析のための
グレブナ基底計算時間の増大(式数:28)

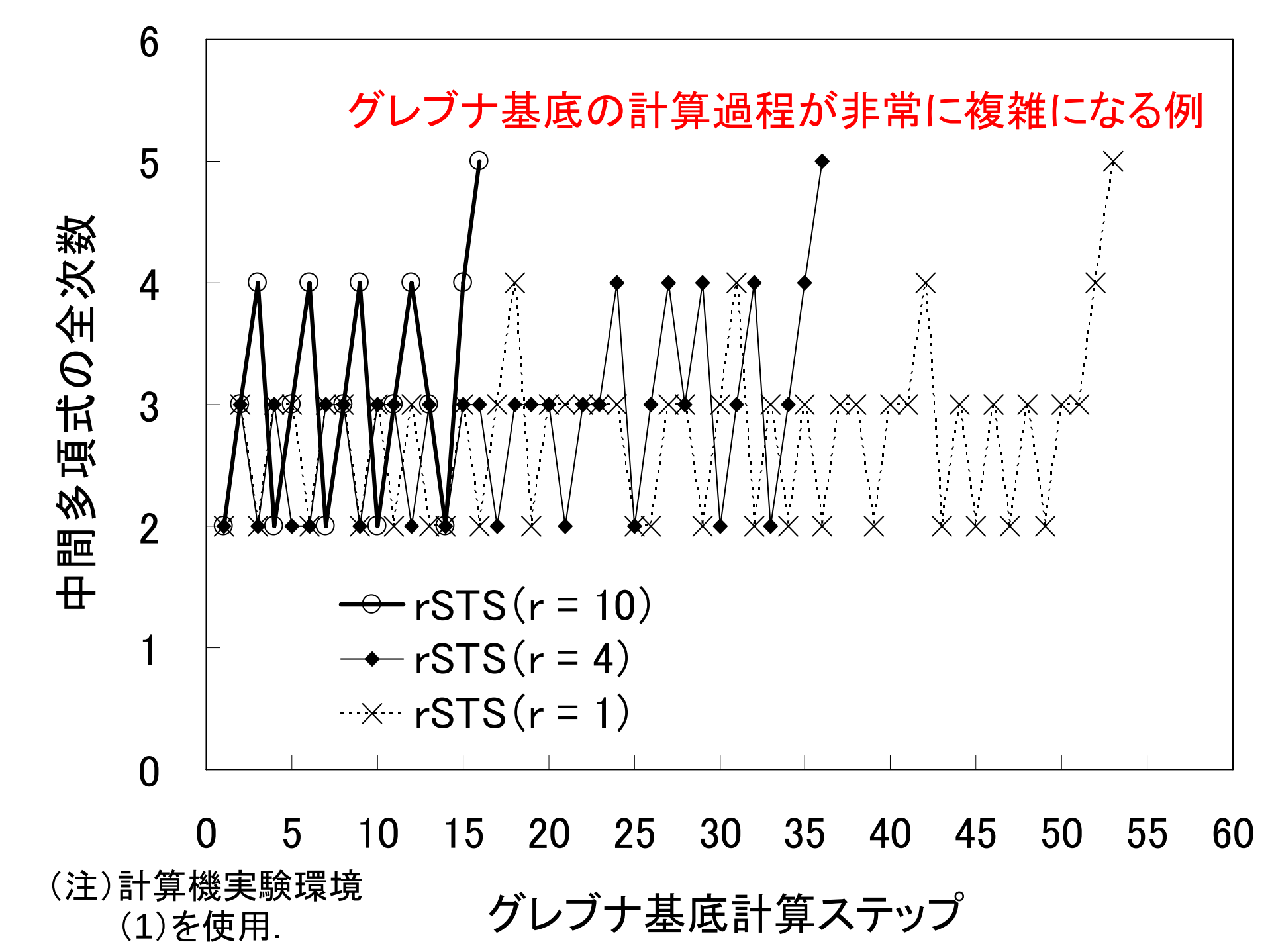


(注)計算機実験環境(2)を使用.

非線形持駒摂動ベクトル方式の安全性



（注）計算機実験環境（3）を使用.



(注)計算機実験環境
(1)を使用.

代数攻撃のためのアルゴリズム

- XL (eXtended Linearization)

  [Courtois-Klimov-Patarin-Shamir, EUROCRYPT 2000]

  GeometricXL [Murphy-Paterson, 2008]

- HXL (“Heuristic and Hybrid” XL)

  [Gotaishi-Tsujii, Inscrypt 2008 Special Track]

代数攻撃のためのアルゴリズム

- MXL (Mutant XL)

  [Ding-Buchmann-Mohamed-Mohamed-Weinmann, SCC 2008]

  MXL_2 [Mohamed-Mohamed-Ding-Buchmann, PQCrypto 2008]

  MXL_3 [Mohamed-Cabarcas-Ding-Buchmann-Bulygin, ICISC 2009]

  Magma の F4 アルゴリズムよりも
  高速に，少ないメモリ使用量で計算

代数攻撃のためのアルゴリズム

- CS (Characteristic Set) method
  - Ritt-Wu 法 [Ritt, 1950] [Wu, 1977]

- F_5 [Faugère, 2002]
  - 最新の結果では，Magma の F_4 と比較して
    数十倍から数百倍高速

- Zhuang-Zi [Ding-Gower-Schmidt, PQCrypto 2006]
  - Mutant Zhuang-Zi [Ding-Schmidt, PQCrypto 2010]

代数攻撃のためのアルゴリズム

- PET SNAKE

  (Parallel Elimination Technique
  Supporting Nice Algebraic Key Elimination)
  [Geiselmann-Matheis-Steinwandt, 2009]
  - MRHS (Multiple Right Hand Sides)

    [Raddum-Semaev, 2008]

- PolyBoRi (Polynomials over Boolean Rings)

  [Brickenstein-Dreyer, 2007]

Magma 以外の F_4 アルゴリズム実装

- Risa/Asir
  - 「F_4 風実装」(野呂正行教授(神戸大学))
- IPA-SMW [杉田-光成-渡辺, 2005]
  - ストリーム暗号 Toyocrypt 解読のために作られた
  - 係数体 GF(2) の場合に限られる
- Singular
  - Slimgb [Brickenstein, 2005]
- Maple
  - F_5 の方が, より高速
    (Faugère 教授(INRIA, パリ第 6 大学))

目次

- はじめに
  - 線形/非線形連立方程式の求解
- グレブナ基底計算

- 多変数公開鍵暗号
  - 多変数非線形連立方程式の求解困難性に基づく公開鍵暗号
- 代数攻撃
- おわりに

多変数公開鍵暗号研究の現状

- 多種多様な方式が提案されてきたが，
  ほとんどの方式が破られている

- 2003 年，SFLASH が
  NESSIE 推奨ディジタル署名に採択

- 2007 年，SFLASH に対する実用的な攻撃法が
  提案される

数学的構造，構成方法，
安全性に関して，今後，
多くの研究が必要

現在取り組んでいる研究課題

- 世界最強水準の，新しい多変数公開鍵暗号の提案
  （非常に難しい…）
- 他の種類の耐量子コンピュータ公開鍵暗号との
  安全性などに関する比較
- 多変数公開鍵暗号に対する攻撃手法に関する
  互いの関連性

数学的構造，構成方法，
安全性に関して，今後，
多くの研究が必要

付録

計算機実験環境(2)

- コンピュータ

  hp AlphaServer ES45 workstation
  - 1250MHz Alpha 21264 (EV68) プロセッサ
  - 32GB RAM
- 数式処理ソフトウェア

  Magma V2.12-14
- グレブナ基底計算アルゴリズム

  F_4 (Magma に実装されているもの)

計算機実験環境(3)

- コンピュータ

  PROSIDE edAEW416R2 workstation
  - 2.80GHz AMD Opteron Model 854 プロセッサ
  - 64GB RAM
- 数式処理ソフトウェア

  Magma V2.12-21
- グレブナ基底計算アルゴリズム

  F_4 (Magma に実装されているもの)

グレブナ基底とは：項順序（単項式順序）

多項式の各項を順序付ける.

例2　$f(x,y,z)=(x+y+z+1)^3$ を項順序に従って並べ替える.

1. 辞書式順序：いわゆる「辞書に載っている順」

$$x^3+3x^2y+3x^2z+3x^2+3xy^2+6xyz+6xy+3xz^2+6xz+3x$$
$$+y^3+3y^2z+3y^2+3yz^2+6yz+3y$$
$$+z^3+3z^2+3z$$
$$+1$$

2. 全次数辞書式順序：各項を次数の高い順に分け，それぞれの集合の中で辞書式順序で並べる.

$$x^3+3x^2y+3x^2z+3xy^2+6xyz+3xz^2+y^3+3y^2z+3yz^2+z^3$$
$$+3x^2+6xy+6xz+3y^2+6yz+3z^2$$
$$+3x+3y+3z$$
$$+1$$

グレブナ基底とは：項順序

3. 全次数逆辞書式順序（DRL; grevlex）

$$z^0y^0x^3 + 3z^0yx^2 + 3z^0y^2x + z^0y^3 + 3zy^0x^2 + 6zyx + 3zy^2 + 3z^2y^0x + 3z^2y + z^3$$
$$+3z^0y^0x^2 + 6z^0yx + 3z^0y^2 + 6zy^0x + 6zy + 3z^2$$
$$+3z^0y^0x + 3z^0y + 3z$$
$$+1$$

1.～3.のうち，3.（全次数逆辞書式）を用いると
多くの場合，もっとも速くグレブナ基底を計算できる．

主項：上に挙げたような，ある取り決めた順序に従い，
多項式を並べ替えるとき，最初に現れる項

$LT(f)$：$f \in R$ に対する f の主項（R：多項式環）

（LT: Leading Term）

グレブナ基底とは：多項式の除算

例3

割る順序を変えた

$$
\begin{array}{r|l}
y^2+z^2 & x^2 \\
x^2y+yz & 0 \\
z^3+xy & 0 \\
\hline
x^2y^2+xy & \leftarrow \text{多項式}: f \\
x^2y^2 \quad +x^2z^2 & \\
\hline
xy-x^2z^2 & \text{余り}: r \\
0 & \rightarrow \quad xy-x^2z^2
\end{array}
\qquad
\begin{array}{r|l}
x^2y+yz & y \\
y^2+z^2 & -z \\
z^3+xy & 1 \\
\hline
x^2y^2+xy & \\
x^2y^2 \quad +y^2z & \\
\hline
xy-y^2z & \\
-y^2z-z^3 & \\
\hline
xy \quad +z^3 & \\
xy \quad +z^3 & \\
\hline
0 &
\end{array}
$$

法：F

割り切れた

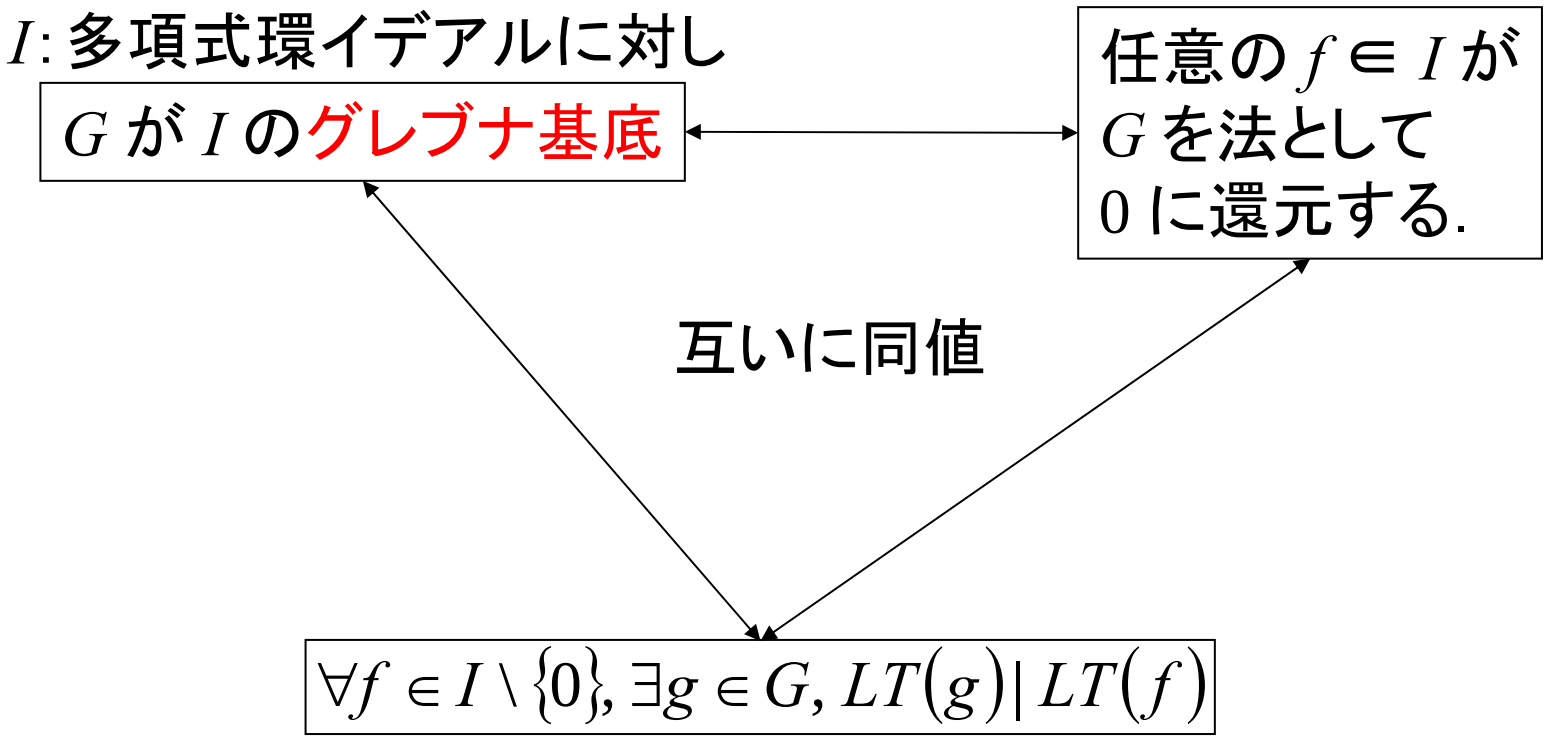
割る順序を変えると結果が異なる

F でなく，グレブナ基底 G で割れば，結果は一意となる．

= 多項式 f が，グレブナ基底 G を法として

余り r へと一意的に還元する．

グレブナ基底とは:グレブナ基底



グレブナ基底計算アルゴリズム :S多項式

$S(f, g)$: $f, g \in R$ に対する$\{f, g\}$の S 多項式

$$S(f,g) = \frac{L}{LT(f)} f - \frac{L}{LT(g)} g$$

L : f と g の主項の最小公倍式

G が I のグレブナ基底 ⇔ 同値 すべての $f, g \in G$ に対し, $S(f, g)$が G を法として 0 に還元する.

S多項式を使えば, ある多項式の集合が, グレブナ基底かどうか判定できる. →ブッフバーガーのアルゴリズム

ブッフバーガーのアルゴリズム

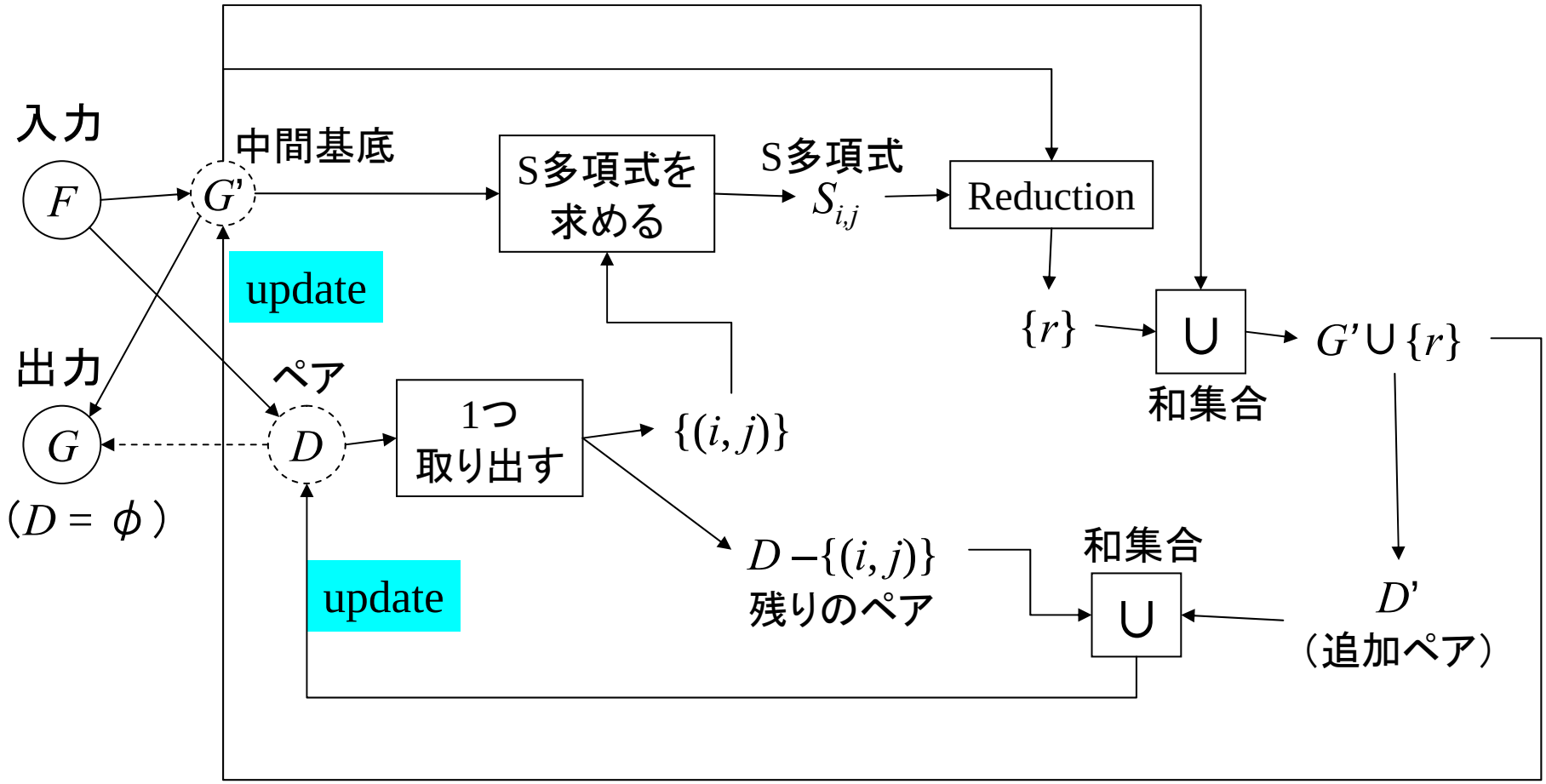
$I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$

Input : $F = \{f_1, \ldots, f_s\}$
Output : a Gröbner Basis G for I, with $F \subset G$
$G := F$
REPEAT
　　$G' := G$
　　FOR each pair $\{p,q\}$, $p \neq q$ in G' DO
　　　　S:=（$S(p,q)$ を G' を法として還元した結果）
　　　　IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$

非零である S に還元したら,
S を元の集合 G に付け加える.

このアルゴリズムは有限回のステップの後に停止する

Buchberger algorithm



アルゴリズムの改良

ブッフバーガーのアルゴリズムは，停止性こそ保証されているものの，冗長であり実用的でない．

→以下の方法が提案されている．

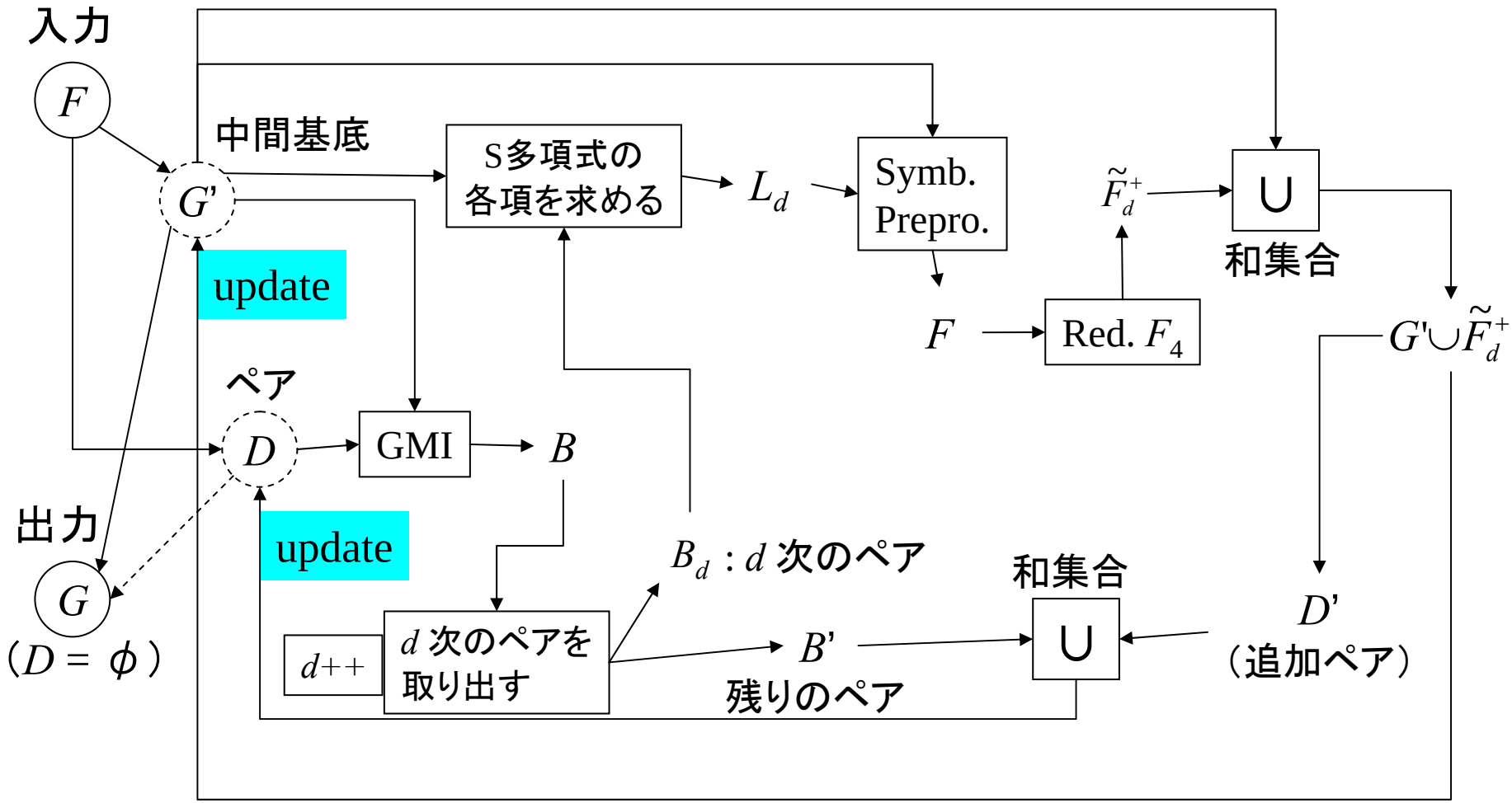
- 0 へ還元するかについてのテストが省ける S 多項式を検出する方法（Gebauer-Möller の方法）
- より効率的に S多項式を構成するペアを選択する方法（normal strategy, sugar strategy）

F_4アルゴリズム，F_5アルゴリズム

…より高速なグレブナ基底計算アルゴリズム

…多項式の除算を，行列の掃き出しによる並列処理で行う．

F_4 algorithm



GMI: Gebauer-Möller Installation　　Red.: Reduction

Symb. Prepro.: Symbolic Preprocessing

Field Polynomial の付加

イデアルの零点（アフィン多様体の元）を
有限体$\mathbf{F}_q$に限定したい（q が十分小さい場合）

= $\mathbf{F}_q$の代数的閉包にある零点を考えたくない.

→多項式環 $S_{q,n} = \mathbf{F}_q[x_1,\ldots,x_n]$ の代わりに,

その商環（剰余類環）

$$R_{q,n} = \mathbf{F}_q\left[x_1,\ldots,x_n\right]/\left\langle x_1^{\,q} - x_1,\ldots,x_n^{\,q} - x_n \right\rangle$$

を考える.

field polynomial

→イデアル $I \in S_{q,n}$ の基底として
field polynomial を付け加えて考える