Computer Security Symposium 2024
22-25 October 2024

暗号の安全性解析に向けた グレブナー基底の計算量理論の定式化

工藤 桃成[1,a)]　横山 和弘[2]

概要：多変数多項式系を解くための主要な方法にグレブナー基底計算があり，多変数多項式暗号をはじめとした公開鍵暗号に対する攻撃としても利用される．しかし，グレブナー基底の計算量評価は理論的に非常に難しい問題であるため，暗号分野の先行研究においては数学的な正確さを欠く（あるいは誤った）議論がなされていることも少なくない．本稿では，そのような議論がなされてきた事例として半正則性と求解次数に着目し，数学的に正確かつ厳密な定式化を行う．その上で，半正則な非斉次多項式列に対する求解次数の上界を評価し，グレブナー基底の計算量評価式を正しい形で与える．さらに，従来の半正則性の定義を拡張することで，よりタイトな計算量評価式が得られたので，これについても紹介し，暗号の安全性解析への応用可能性を議論する．

Formulation of the complexity theory on Gröbner basis computation with the view toward to cryptanalysis

Momonari Kudo[1,a)]　Kazuhiro Yokoyama[2]

Abstract: Gröbner basis computation is a typical tool for solving multivariate polynomial systems, and it is applied to constructing effective attacks against public key cryptosystems. However, it is theoretically quite difficult to estimate the complexity of Gröbner basis computation, which has caused mathematically inaccurate (or incorrect) discussions in the cryptographic literature. In this paper, we focus on semi-regularity and solving degree, and formulate them in a mathematically accurate and precise way. Then we estimate an upper bound on solving degree for semi-regular inhomogeneous polynomial sequences, and present formulae to measure the complexity of the Gröbner basis computation for such a sequence. Furthermore, we obtain a tighter bound on the complexity by extending the notion of semi-regular, and finally discuss applications of our theoretical results to analyzing cryptanalysis.

1. はじめに

多変数多項式系を解くための主要な方法に Gröbner 基底計算があり，多変数多項式暗号をはじめとした公開鍵暗号に対する攻撃としても利用される．しかし，Gröbner 基底の計算量評価は理論的に非常に難しい問題であるため，先行研究においては数学的な正確さを欠く（あるいは誤った）議論がなされていることも少なくない．実際，その計算量評価において重要な役割を果たす「正則性次数」，「半正則性」，「求解次数」などの概念には複数の定義が存在し，混同されてきた．他にも，入力多項式系が斉次の場合にしか適用できない主張を，非斉次の場合に（適切な仮定を課すことなく）流用してしまっている先行研究も存在する．

本稿では，上記に挙げた半正則性と求解次数に関して，複数ある定義を数学的に正確かつ厳密な形で与える（3 – 4 節）．特に，乱立する求解次数については，それらの大小関係や一致する条件などの基本的性質を示す（4.3 小節後半および 4.4 小節）とともに，講演者による正則性次数に関して線形な上界評価を紹介する（定理 5.1.1）．また，その上界評価に基づいて，半正則な非斉次多項式列に対す

[1] 福岡工業大学情報工学部情報通信工学科
Department of Information and Communication Engineering, Fukuoka Institute of Technology
[2] 立教大学理学部数学科
Department of Mathematics, Rikkyo University
[a)] m-kudo@fit.ac.jp

る Gröbner 基底の計算量評価式を正しい形で与える（系 5.1.2，5.3 小節）．さらに，暗号分野で仮定されうる「入力多項式列が半正則ではないが半正則である場合と同様の計算挙動になる」という条件について，従来の半正則性の定義を拡張することで理論的な定式化が得られたので，これについても紹介し，暗号の安全性解析への応用可能性を議論する（5.2 – 5.3 小節）．紙数の都合上，原著論文の参照を省くこともあるが，その場合 [21] や [29] を参照されたい．

2. 準備

以下, K を体, $R = K[x_1, \ldots, x_n]$ を K 上の n 変数多項式環とし, $\prec$ を R 上の項順序とする．元 $f \in R$ に対し, その総次数を $\deg(f)$（または単に $\deg f$）と表す．y を新たな変数とし，$f \in R \setminus \{0\}$ に対し，$f^h := y^{\deg(f)} f(x_1/y, \ldots, x_n/y) \in R[y]$ を f の斉次化という．また，$f_1, \ldots, f_m \in R$ と取るときは，それらの総次数をそれぞれ $d_1, \ldots, d_m$ とする．各 f_i が斉次のとき集合 $\{f_1, \ldots, f_m\}$ は斉次であるといい，そうでないとき非斉次であるという．可換環 A とその部分集合 S に対し，$\langle S \rangle_A$ は S で生成される A のイデアルを表し，A が明らかである場合は単に $\langle S \rangle$ と書く．R のイデアルは零イデアルでないもののみ考える．

2.1 Gröbner 基底

R において，$x_1^{\alpha_1} \cdots x_n^{\alpha_n}$（$\alpha_i$ は非負整数）の形の元を単項式といい，単項式に $K \setminus \{0\}$ の元を乗じたものを項という．元 $f \in R \setminus \{0\}$ に現れる単項式のうち，$\prec$ に関して最大となる単項式を f の**先頭単項式**といい $\mathrm{LM}_\prec(f)$ で表す．f における $\mathrm{LM}_\prec(f)$ の係数を f の**先頭係数**といい $\mathrm{LC}_\prec(f)$ と表す．また，$\mathrm{LT}_\prec(f) = \mathrm{LC}_\prec(f) \cdot \mathrm{LM}_\prec(f)$ を f の**先頭項**という．部分集合 $S \subset R \setminus \{0\}$ に対し $\mathrm{LT}_\prec(S) := \{\mathrm{LT}_\prec(f) : f \in S\}$ と定義し，$\mathrm{LM}_\prec(S)$ についても同様に定義する．元 $f, g \in R \setminus \{0\}$ に対し，f の項 t が $\mathrm{LT}_\prec(g)$ で割り切れるとき，$r := f - (t/\mathrm{LT}_\prec(g))g$ を f の g による単項簡約といい，r を求めることを f を g で単項簡約するという．有限集合 $F \subset R \setminus \{0\}$ に対し，f を F のいずれかの元で単項簡約することを繰り返せば，有限回の操作の後, r は F のどの元でも単項簡約できなくなる．このときの r を，f の F による**正規形（normal form）**と呼び，$\mathrm{NF}_{\prec,F}(f)$ と書く．また，$\mathrm{NF}_{\prec,F}(f) = 0$ のとき, f は F に関して 0-簡約であるという．元 $f, g \in R \setminus \{0\}$ に対して，$t = \mathrm{LCM}(\mathrm{LM}_\prec(f), \mathrm{LM}_\prec(g))$ とおくとき，$S_\prec(f, g) := (t/\mathrm{LT}_\prec(f)) \cdot f - (t/\mathrm{LT}_\prec(g)) \cdot g$ を **S-多項式**という．以上の準備のもと，次が成り立つ：

定理 2.1.1 ([5]) R のイデアル I に対し次が成り立つ：

(1) 有限集合 $G \subset I$ が存在して, $\langle \mathrm{LT}_\prec(G) \rangle_R = \langle \mathrm{LT}_\prec(I) \rangle_R$ を満たす（よって G は I を生成する）．このときの G を $\prec$ に関するイデアル I の **Gröbner 基底**と呼ぶ．

(2) 有限集合 $G \subset I$ について，次は全て同値である：

(2a) G は $\prec$ に関する I の Gröbner 基底である．

(2b) $f \in I$ ならば $\mathrm{NF}_{\prec,G}(f) = 0$ である．

(2c) $I = \langle G \rangle$ が成り立ち，かつ，任意の $f, g \in G$ に対し $\mathrm{NF}_{\prec,G}(S_\prec(f, g)) = 0$ となる．

定理 2.1.1 (2c) より，R のイデアル I の生成元からなる有限集合 F を入力として，$\prec$ に関する I の Gröbner 基底を計算するアルゴリズム（Buchberger アルゴリズム）が直ちに導かれる．具体的には，集合 G，P の初期値をそれぞれ F，$\{\{f, g\} : f, g \in F\}$ とし，次の手続きを繰り返す：

- $\{f, g\} \in P$ を選び $P \leftarrow P \setminus \{\{f, g\}\}$ と更新した後，$r := \mathrm{NF}_{\prec,G}(S_\prec(f, g)) \neq 0$ なら $G \leftarrow G \cup \{r\}$ と更新．

アルゴリズムの実行中における P の各元 $\{f, g\}$ (i.e., 簡約すべき S-多項式に対応する多項式ペア) は **S ペア**と呼ばれる．また，G は常に I を生成し，これは**中間基底**と呼ばれる．$\mathrm{NF}_{\prec,G}(S_\prec(f, g))$ を計算することなく $\mathrm{NF}_{\prec,G}(S_\prec(f, g)) = 0$ であることを事前に検知する判定法も知られている．

定理 2.1.1 (1) の条件 $\langle \mathrm{LT}_\prec(G) \rangle_R = \langle \mathrm{LT}_\prec(I) \rangle_R$ を満たす最小の G であって, 各元の先頭係数が 1 であるものを, $\prec$ に関する I の**簡約 Gröbner 基底**と呼ぶ．簡約 Gröbner 基底は $\prec$ と I により一意的に存在し，$\prec$ に関する I の Gröbner 基底の中から不要な元を取り除いて得られる．

2.2 Gröbner 基底の計算方法

Buchberger による定理 2.1.1 に基づいて，これまでに多くの Gröbner 基底計算アルゴリズムが提案されており，例えば F_4 [13]，F_5 [14]，Hilbert driven などがある．もし F が非斉次であって，イデアル $\langle F \rangle$ が零次元（すなわち K の代数閉包 $\overline{K}$ 上での零点が高々有限個）の場合，ある項順序 $\prec_1$ に関する $\langle F \rangle$ の Gröbner 基底が求まれば，別の項順序 $\prec_2$ に関する $\langle F \rangle$ の Gröbner 基底を，線形代数計算（FGLM 基底変換 [15]）により効率的に計算できると期待される．よって，特定の項順序（上記でいうところの $\prec_1$）について $\langle F \rangle$ の Gröbner 基底を高速に計算できるかが問題である．よく知られているように，総次数を優先して比較する次数付き項順序（特に次数付き逆辞書式順序）の場合は，他の項順序の場合よりも比較的高速に $\langle F \rangle$ の Gröbner 基底を計算できて，かつ計算量評価に適する，と考えられている（このことは F が斉次の場合も同様である）．そこで本稿では $\prec$ が次数付き項順序の場合を考える．

F_4 や F_5 等の，Buchberger アルゴリズムを基にしたアルゴリズムでは，S ペアを選択・収集する方法や S-多項式の正規系計算が，アルゴリズム全体の効率性に大きく影響する．我々がいま対象としている次数付き項順序においては，そのような方法として，**正規戦略（normal strategy）**を採用し，S ペアの収集と S-多項式の簡約を繰り返すのが最も効率的だと考えられている．具体的には，その時点で保持している（未処理の）S ペア $\{f, g\}$ たちのうち，総次数 $\deg \mathrm{LCM}(\mathrm{LM}_\prec(f), \mathrm{LM}_\prec(g))$ の値 d が最小となるものを

Algorithm 1 正規戦略 F_4 アルゴリズム [13]（簡易版）

```
G ← {f_1, ..., f_m}                                   ▷ 入力多項式集合
P ← {{f_i, f_j} : 1 ≤ i < j ≤ m}
while P ≠ ∅ do
    d ← min{deg LCM(LM_≺(f), LM_≺(g)) : {f, g} ∈ P}
    P_d ← {{f, g} ∈ P : deg LCM(LM_≺(f), LM_≺(g)) = d}
    P ← P ∖ P_d
    L ← Reduction(Left(P_d) ∪ Right(P_d), G)
    for r ∈ L with LM_≺(r) ∉ ⟨LM_≺(G)⟩ do
        P ← P ∪ {{g, r} : g ∈ G}, G ← G ∪ {r}
    end for
end while
return G                                   ▷ 出力多項式集合（Gröbner 基底）
```

収集し，それらに対応する S-多項式を中間基底 G で簡約する，というステップを繰り返す．本稿では，正規戦略により Gröbner 基底を計算するアルゴリズムを**正規戦略アルゴリズム**と呼ぶ．正規戦略アルゴリズムの各ステップにおける $\deg \mathrm{LCM}(\mathrm{LM}_\prec(f), \mathrm{LM}_\prec(g))$ の最小値 d は **step degree** と呼ばれる．

正規戦略アルゴリズムの具体例として，正規戦略を適用した F_4 アルゴリズム（簡易版）を Algorithm 1 に示す．内部関数 Left，Right，および Reduction の詳細は [13] を参照とするが，このうち特に Reduction は Macaulay 行列（4.2 小節で定義）を高速に行簡約することで複数の S-多項式の正規形を同時に求める．Algorithm 1 の場合，4 行目の d が step degree である（[13] では記号 d を **while**-loop のカウンタに用いているが，本稿では step degree に用いている）．

2.3 Hilbert 級数, 正則性次数

以下では，M を有限生成次数付き R-加群とする．各 $d \in \mathbb{Z}$ に対し，M の次数 d の斉次部分を M_d と書く．各 M_d は有限次元 K-線形空間であることに注意する．

定義 2.3.1 関数 $\mathrm{HF}_M : \mathbb{Z} \to \mathbb{Z}_{\geq 0}\ ;\ d \mapsto \dim_K M_d$ を M 上の **Hilbert 関数**という．また，級数 $\mathrm{HS}_M(z) := \sum_{d\in\mathbb{Z}} \mathrm{HF}_M(d) z^d$ を M 上の **Hilbert 級数**という．

定義 2.3.2 M が **Artin 的**であるとは，ある整数 d_0 が存在して，$d \geq d_0$ を満たす任意の整数 d に対して $M_d = 0$ となるときをいう．任意の $d < 0$ に対して $M_d = 0$ の場合，M が Artin 的であることは $\mathrm{HS}_M(z)$ が多項式となることに同値である．

定義 2.3.3 (Def. 4 of [2], Def. 4 of [3]) $f_1, \ldots, f_m$ が全て斉次のとき，斉次多項式集合 $F = \{f_1, \ldots, f_m\} \subset R$ の**正則性次数**を，$R/\langle F\rangle$ が Artin 的の場合は

$$d_{\mathrm{reg}}(F) := \min\{d \in \mathbb{Z}_{\geq 0} : R_d = \langle F\rangle_d\} = \deg(\mathrm{HS}_{R/\langle F\rangle}) + 1$$

と定義し，そうでない場合は $d_{\mathrm{reg}}(F) := \infty$ で定義する．

正則性次数と可換代数的な不変量（Castelnuovo-Mumford 正則量など）との関係については [7] を参照とする．

注意 2.3.4 $K = \mathbb{F}_q$（元数 q の有限体）の場合，正則性次数には異なる定義がある（cf. [12]）：$B := R/\langle x_1^q, \ldots, x_n^q\rangle$ とし，斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ の B^m への像を $\overline{\boldsymbol{F}}$ と表すとき，$\overline{\boldsymbol{F}}$ 上の Koszul 複体の 1 次ホモロジー群を用いて定義される（詳細は [7] の Sect. 4 を参照）．この定義による正則性次数は first fall degree とも呼ばれる．

次の定理 2.3.5 は代数幾何学ではよく知られた事実である（証明は例えば [9] の Prop. 3.3.7 を参照）：

定理 2.3.5 $R = K[x_1, \ldots, x_n]$ の斉次イデアル I に対し，R/I が Artin 的であることは，K の代数閉包 $\overline{K}$ 上の射影的零点集合 $V_{\overline{K}}(I)$ が空であることに同値である．

3. 多項式列の半正則性

本節では多項式列が半正則であることの定義を復習する．斉次多項式列の半正則性には，以下に述べる Bardet らによる定義（3.1 節），Pardue による定義（3.2 節），の 2 種類があり，後者の方がより強い条件で定義される．記号は 2 節冒頭で述べたものと同様とする．

3.1 Bardet らによる定義：暗号学的半正則性

本小節を通して，$f_1, \ldots, f_m \in R \setminus K$ をそれぞれ総次数 $d_1, \ldots, d_m$ の斉次多項式とする．まず，斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ の d-正則性を定義する．

定義 3.1.1 (Def. 3 of [2], Def. 1 & Thm. 1 of [11]) d は自然数で $d \geq \max\{d_i : 1 \leq i \leq m\}$ を満たすとする．斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が **d-正則**であるとは，次の同値条件を満たすときをいう：

(1) 任意の $i \in \{1, \ldots, m\}$，および $d_i \leq t < d$ を満たす任意の自然数 t に対して，f_i 倍により定義される K-線形写像 $(R/\langle f_1, \ldots, f_{i-1}\rangle)_{t-d_i} \to (R/\langle f_1, \ldots, f_{i-1}\rangle)_t$ が単射である．

(2) $\mathrm{HS}_{R/\langle f_1,\ldots,f_m\rangle}(z) \equiv \frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n} \pmod{z^d}$.

(3) $\boldsymbol{F}$ 上の Koszul 複体（cf. Def. 7.6.6 of [17]）を $K_\bullet$ とするとき，その 1 次ホモロジー群 $H_1(K_\bullet)$ に関して $H_1(K_\bullet)_{\leq d-1} = 0$ が成り立つ．ここで $H_1(K_\bullet)_{\leq d-1}$ は，$H_1(K_\bullet)$ を自然に次数付き R-加群とみたときの，次数 $d-1$ 以下の斉次部分全ての直和である．

次に，Bardet らによる半正則性の定義を述べる．この定義による半正則列は，後に Bigdeli ら [4] によって暗号学的半正則列と名付けられた．本稿ではこれを踏襲する．

定義 3.1.2 (Def. 5 of [2], Def. 5 & Prop. 6 of [3]) 1 次以上の斉次多項式のなす列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が**暗号学的半正則（cryptographic semi-regular）**であるとは，次の同値条件を満たすときをいう：

(1) $F = \{f_1, \ldots, f_m\}$ の正則性次数 $D := d_{\mathrm{reg}}(F)$ に対して，$\boldsymbol{F}$ は D-正則である（すなわち $d = D$ に対し定義 3.1.1 に述べた同値条件が満たされる）．

(2) 等式 $\mathrm{HS}_{R/\langle f_1,\ldots,f_m\rangle}(z) = \left[\frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n}\right]$ が成り立つ．ここで $[\cdot]$ は非正係数をもつ最小次数項での打ち切り

（そのような項の次数以上の項は 0 とみなす）を表す．

定義 3.1.1，定義 3.1.2 の各項の同値性の証明については，[11] の Thm. 1，Prop. 1 をそれぞれ参照せよ．定義 3.1.1，定義 3.1.2 の条件 (2) から，斉次多項式列の d-正則性，暗号学的半正則性は実際には多項式の順序によらない．また，斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m)$ について，$\boldsymbol{F}$ が d-正則であればその任意の部分列も d-正則となるが（cf. Prop. 2 (a) of [11]），$\boldsymbol{F}$ が暗号学的半正則であってもその部分列が暗号学的半正則になるとは限らない．

注意 3.1.3　$m \leq n$ ならば，斉次多項式列 $\boldsymbol{F}$ が暗号学的半正則であることは，$\boldsymbol{F}$ が**正則**であることに同値である．ここで $\boldsymbol{F}$ が正則であるとは，$\mathrm{HS}_{R/\langle f_1,\ldots,f_m\rangle}(z) = \frac{\prod_{j=1}^{n}(1-z^{d_j})}{(1-z)^n}$ を満たすときをいい（同値な，そして定義 3.1.1 の条件 (1) に類似の定義として [17] の Def. 7.6.1 を参照），このとき $\boldsymbol{F}$ の任意の部分列も正則である．また，R の斉次元からなる正則列の長さは n 以下である（cf. Sect. 7.6 of [17]）．以上を踏まえると，暗号学的半正則列は正則列の過剰決定（$m > n$）な場合への拡張とみなせる．

注意 3.1.4　Fröberg [16] により，無限体上において斉次多項式列 $\boldsymbol{F}$ は generic に暗号学的半正則であることが予想されている（“generic” の定義は [24] を参照）．よく知られているように，予想は少なくとも $m \leq n$ であれば正しい．

3.2　Pardue による定義：半正則性

ここでは，Pardue [24] による斉次多項式列の半正則性の定義を述べる．

定義 3.2.1 (p. 581 of [24])　$f_1, \ldots, f_m \in R \setminus K$ を斉次元とする．斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が**半正則**であるとは，次の同値条件を満たすときをいう：

(1) 任意の $i \in \{1, \ldots, m\}$，および $d_i \leq t$ を満たす任意の自然数 t に対して，f_i 倍により定義される K-線形写像 $(R/\langle f_1, \ldots, f_{i-1}\rangle)_{t-d_i} \to (R/\langle f_1, \ldots, f_{i-1}\rangle)_t$ が maximal rank（すなわち単射または全射）である．

(2) $1 \leq i \leq m$ を満たす任意の自然数 i に対して等式 $\mathrm{HS}_{R/\langle f_1,\ldots,f_i\rangle}(z) = \left[\frac{\prod_{j=1}^{i}(1-z^{d_j})}{(1-z)^n}\right]$ が成り立つ．

注意 3.2.2　定義から明らかに，暗号学的半正則列は半正則列である．また，$m \leq n$ であれば正則，暗号学的半正則，半正則は全て同値となる．$m > n$ の場合に暗号学的半正則列が半正則列となるか否かは不明だが，Pardue は無限体上における「斉次多項式列が generic に暗号学的半正則であること」と「斉次多項式列が generic に半正則であること」の同値性，および Moreno-Socías 予想 [23] の主張はこれらよりも強いことを示している（cf. Thm. 2 of [24]）．

3.3　非斉次多項式列の半正則性

少なくとも 1 つ非斉次元を含む多項式列（**非斉次多項式列**または**アフィン多項式列**と呼ばれる）については，最大斉次部分のなす斉次多項式列により半正則性が定義される．

定義 3.3.1　非斉次多項式列 $\boldsymbol{F} := (f_1, \ldots, f_m) \in (R \setminus K)^m$ が暗号学的半正則（resp. 半正則）であるとは，斉次多項式列 $\boldsymbol{F}^{\mathrm{top}} := (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ が暗号学的半正則（resp. 半正則）であるときをいう．ここで $f \in R \setminus \{0\}$ に対し $f^{\mathrm{top}} := (f^h)|_{y=0}$ であり，これを f の**最大斉次部分**という．

注意 3.3.2　十分大きい体上で，$m > n$ の条件下で n 変数 m 本の非斉次多項式 $f_1, \ldots, f_m$ をランダム生成する場合，Fröberg 予想 [16] を仮定しても，「$\boldsymbol{F} = (f_1, \ldots, f_m)$ が半正則であり，同時に $F = \{f_1, \ldots, f_m\}$ が $\overline{K}$ 上で零点をもつこと」は起こりにくいと考えられる（詳細は [29] の注意 5 を参照）．このような状況が起こるのは，例えば，$f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}$ がランダムに生成され，一方で低次の項には‘従属性’がもたされるような場合である．

例えば，係数を独立一様ランダムに選ぶことで $g_1, \ldots, g_m \in R$ を生成し，点 $(a_1, \ldots, a_n) \in K^n$ を任意に選んだ後，各 $i \in \{1, \ldots, m\}$ に対して $c_i := g_i(a_1, \ldots, a_n)$，$f_i := g_i(x_1, \ldots, x_n) - c_i$ と定めれば，F は $\overline{K}$ 上で零点 $(a_1, \ldots, a_n)$ をもち，かつ高確率で $\boldsymbol{F}^{\mathrm{top}}$ は半正則になると期待できる．このような F に近しいものは，多変数多項式暗号の構成において現れ得る（cf. Sect. 2 of [19]）：$(g_1, \ldots, g_m)$ が公開鍵多項式列に対応し，暗号化方式（resp. 署名方式）の場合は $(a_1, \ldots, a_m)$，$(c_1, \ldots, c_m)$ がそれぞれ平文，暗号文（resp. 署名，平文）に対応する．公開鍵多項式列は係数を独立一様ランダムに選んで生成されるわけではないが，そのように生成されたと仮定して暗号の安全性解析がなされ，$\boldsymbol{F}$ が半正則性といった所望の性質を満たすと期待される．

4.　求解次数

本節では，求解次数の定義を分類した後，その評価に関する既存結果の一部を紹介する．記号は 2 節冒頭で述べたものと同様とし，$F = \{f_1, \ldots, f_m\}$ とする．また，$\prec$ を R 上の次数付き項順序とし，変数 $x_1, \ldots, x_n, y$ の中で y が最下位となるように $\prec$ を拡張して得られる $R[y]$ 上の次数付き項順序を $\prec^h$ と表す（詳細は [21] の Sect. A.2 を参照）．次数付き項順序 $\prec$ に関する $\langle F\rangle_R$ の簡約 Gröbner 基底に含まれる元の総次数の最大値を $\mathrm{max.GB.deg}_{\prec}(F)$ と書く（$\mathrm{max.GB.deg}_{\prec^h}(F^h)$ も同様に定義）．

求解次数は Gröbner 基底の計算量を評価する上で重要な役割を果たす特徴量であって，Ding-Schmidt の論文 [12] で初めて登場し，近年特に Gorla ら（cf. [4], [7], [8]）や著者（cf. [20], [21]）によって研究されてきた．ただし，求解次数には，以下に述べる 3 種類の定義が存在する．これらの定義は，先行研究において屡々混同されてきた．

4.1　Step degree を用いた定義（cf. p. 36 of [12]）

第一の定義として，2.2 小節で定義した正規戦略アルゴリズムを実行した際の step degree の最大値を**求解次数**

(solving degree) と呼ぶ．この定義による求解次数は，実行する正規戦略アルゴリズムを $\mathcal{A}$ としたとき，入力 F と項順序 $\prec$ にも依存するので，本稿では $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ と表す．

注意 4.1.1 [12] では，アルゴリズムの実行中に最も計算時間のかかる step degree を求解次数と呼んでいる箇所もあるが，そのように定義すると求解次数はアルゴリズムの実装方法にも依存し得るため，本稿では考えない．また，step degree を各ステップにおいて収集する S ペア $\{f,g\}$ の次数ではなく，対応する S-多項式の次数 $\deg S_{\prec}(f,g)$ と定義する場合，求解次数はアルゴリズムの実行全体において実際に生成された S-多項式の次数の最大値に他ならない（この定義は [26] や [27] などで採用されている）．

4.2 Macaulay 行列を用いた定義（cf. [7]）

第二の定義として，アルゴリズムに依存しない Macaulay 行列を用いるものを紹介する．ここで Macaulay 行列とは，係数体 K 上の行列であって，非空な有限集合 $S \subset R$ と次数付き項順序 $\prec$ に対して次のように定義される：$d = \max\{\deg(f) : f \in S\}$ とおき，R における d 次以下の単項式全体のなす集合を $\mathcal{T}_{\le d}$ とおいて，その元を $\prec$ に関して降順に並べて $\mathcal{T}_{\le d} = \{t_1, \dots, t_{\ell-1}, t_\ell = 1\}$ とする．S の元を任意に並べて $S = \{h_1, \dots, h_k\}$ とし，各元を $a_{i,j} \in K$ を用いて $h_i = \sum_{j=1}^{\ell} a_{i,j} t_j$ と表す．このとき，$k \times \ell$ 行列 $(a_{i,j})_{i,j}$ を $\prec$ に関する S の **Macaulay 行列**といい，$\mathrm{Mac}(S)$ と表す．Lazard [22] は，十分大きい d に対して $\mathcal{S}_{\le d}(F) := \{tf : f \in F,\ t \in \mathcal{T}_{\le d-\deg(f)}\}$ と定めると，$\mathrm{Mac}(\mathcal{S}_{\le d}(F))$ の行簡約階段形に対応する多項式集合 $B_{\le d}(F)$ の中に $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底が存在することを示した（この結果を基にしたアルゴリズムとして XL [10] が後に提案され，現在ではその様々な改良が存在する）．Caminata-Gorla [7] は，$B_{\le d}(F)$ が $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底となる最小の非負整数 d を，F の求解次数と定義した．本稿ではこの求解次数を $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ と表す．

4.3 Mutant を用いた定義（cf. [8]，[25]）

第二の定義では F のみで定まる Macaulay 行列 $\mathrm{Mac}(\mathcal{S}_{\le d}(F))$ を用いたが，$d = 1, 2, \dots$ と小さい順に F を逐次的に拡大して得られる Macauley 行列を用いた定義を紹介する．ただし，各 d における簡約では，$M := \mathrm{Mac}(\mathcal{S}_{\le d}(F))$，$B := B_{\le d}(F)$ とおいて，$\deg(f) < d$ を満たす多項式 $f \in B$ であって，$\mathrm{LM}_{\prec}(f)$ が M の行に対応する多項式の先頭単項式として現れないようなものが得られた場合，$B' := B \cup \{tf : t \in \mathcal{T}_{\le d-\deg(f)},\ tf \notin \mathrm{Span}_K(B)\}$ に対応する Macaulay 行列 $\mathrm{Mac}(B')$ を改めて M とおき，M を行簡約して得られる多項式集合を改めて B とおく．この操作を，上記のような f が得られなくなるまで繰り返して $\langle F\rangle_R$ の生成集合を拡張した後，拡張された生成集合が Gröbner 基底でなければ d を $d+1$ に置き換えて同様の操作を行う（詳細は [8] の Sect. 1 または [21] の Sect. 3 を参照）．以上の戦略は Mutant-XL [6] において既に用いられていたため，[25] では **mutant 戦略**と名付けられている．mutant 戦略によって $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底が得られる最小の d を求解次数と定義し，$\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ と表す．

定義から直ちに次の不等式

$$\max.\mathrm{GB.deg}_{\prec}(F) \le \mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \le \mathrm{sd}_{\prec}^{\mathrm{mac}}(F) \qquad (4.1)$$

が得られる．[8] において $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ に関する諸性質が調べられているので参照されたい．ただし [8] では $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ を表す記号として $\mathrm{sd}_{\prec}(F)$ が用いられている（我々の記号 $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$，$\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$，$\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ は [8] の記号 $\mathrm{sd}_{\prec}(F)$ を基にして区別のために新たに導入したものである）．

4.4 求解次数の評価と Gröbner 基底の計算量

入力 F が斉次なら，正規戦略アルゴリズム $\mathcal{A}$ に適切な設定を施すことで $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F) = \mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ となり，(4.1) において等号が成り立つ．従って，求解次数は，$\max.\mathrm{GB.deg}_{\prec}(F)$ を評価すればよい：$D_{\max} := \max.\mathrm{GB.deg}_{\prec}(F)$ とおくとき，$D_{\max} = O(n)$ であれば，$\langle F\rangle$ の Gröbner 基底の計算量は $\mathrm{Mac}(\mathcal{S}_{\le D_{\max}}(F))$ の行簡約の計算量 $O(m\binom{n+D_{\max}-1}{D_{\max}}^{\omega})$ となる（Sect. A.3 of [21]）．ここで $2 \le \omega < 3$ は行列積の指数である．$\prec$ が次数付き逆辞書式順序の場合，F に零次元性などを仮定することで，Lazard [22] による $\max.\mathrm{GB.deg}_{\prec}(F)$ の上界（**Macaulay 上界**）を適用できる．詳細は [29] の Sect. 3 を参照とする．

一方で F が非斉次の場合，(4.1) において等号が成立するとは限らない．また，$\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ と $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ の大小関係も不明であり，これらを評価するのは一般には難しい．しかし，F を変数 y で斉次化して考えることで，$\prec$ に関する F の Gröbner 基底の計算量を評価できる場合がある（特に $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ を上から評価できる）．実際，次が成り立つ：

- $\tilde{G}$ が $\prec^h$ に関する $\langle F^h\rangle_{R[y]}$ の Gröbner 基底であれば，$\tilde{G}$ の非斉次化 $\tilde{G}|_{y=1} = \{g(x_1, \dots, x_n, 1) : g \in \tilde{G}\}$ は $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底である．ここで $\prec^h$ は本節冒頭で定義した $R[y]$ 上の次数付き項順序である．

従って，$\tilde{G}$ の計算量を評価すれば十分であり，幾つかの仮定の下で F^h に Macaulay 上界を適用すればよい．実際，$\prec$ を次数付き逆辞書式順序として，$d_1 \ge \cdots \ge d_m$ の条件下で，$\dim_K R/\langle F\rangle < \infty$ かつ $R/\langle F^{\mathrm{top}}\rangle$ が Artin 的であれば，$\ell := \min\{m, n+1\}$ に対して次の Macaulay 上界：

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \le d_1 + \cdots + d_\ell - \ell + 1 \qquad (4.2)$$

が得られる．さらに，$\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ も (4.2) 右辺以下であることがわかる（詳細は [29] の Sect. 3 を参照）．

最後に，F が非斉次であり，かつ $R/\langle F^{\mathrm{top}}\rangle$ が Artin 的である場合に知られている既存結果を幾つか述べる．この場合，任意の次数付き項順序 $\prec$ に対して次が成り立つ：

$$\max.\mathrm{GB.deg}_{\prec}(F) \le d_{\mathrm{reg}}(F^{\mathrm{top}}) \qquad (4.3)$$

(cf. Rem. 15 of [7]). また，$d_{\mathrm{reg}}(F^{\mathrm{top}})$ と $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ はいずれも $\max.\mathrm{GB.deg}_{\prec}(F)$ 以上であるが，前者 2 つの値は（仮に $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ が半正則であっても）一致するとは限らない．実際，[4], [7], [8] に具体例が示されている．その他に，次のような求解次数の評価が知られている：

- [26], [27]：$K = \mathbb{F}_q$（位数 q の有限体）で，$\{x_i^q - x_i : 1 \le i \le n\} \subset F$ かつ $d_{\mathrm{reg}}(F^{\mathrm{top}}) \ge \max\{d_1, \ldots, d_m\}$ であれば，ある正規戦略アルゴリズム $\mathcal{A}$ に対して $\mathrm{sd}^{\mathcal{A}}_{\prec}(F) \le 2d_{\mathrm{reg}}(F^{\mathrm{top}}) - 1$，かつ $\mathcal{A}$ の実行中に計算される S-多項式の総次数は $2d_{\mathrm{reg}}(F^{\mathrm{top}}) - 2$ を超えない．
- [25]：$d_{\mathrm{reg}}(F^{\mathrm{top}}) \ge \max\{\deg(f) : f \in F\}$ であれば $\mathrm{sd}^{\mathrm{mut}}_{\prec}(F) \le d_{\mathrm{reg}}(F^{\mathrm{top}}) + 1$ が成り立つ．

5. 主結果

前節に引き続き，記号は 2 節冒頭で述べたものと同様とし，断らない限り $F = \{f_1, \ldots, f_m\}$ は非斉次とする．また，$\boldsymbol{F} = (f_1, \ldots, f_m)$ は暗号学的半正則であると仮定する．本節では，次数付き項順序 $\prec$ に関する $\langle F \rangle$ の Gröbner 基底の計算量を正確に評価する．また，2.3 小節で定義した正則性次数の概念を拡張し，幾つかの重要な性質を述べた後，それらの暗号の安全性解析への応用可能性を議論する．本節で述べる定理や命題の証明は紙数の都合上省略するので，[20], [21] を適宜参照されたい．

5.1 求解次数の上界および Gröbner 基底の計算量評価

まず，step degree を用いて定義される求解次数 $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$（4.1 小節参照）に対する正確な上界評価を与える（定理 5.1.1）．この定理は，斉次多項式列 $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ 上および $\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h)$ 上の Koszul 複体のホモロジーを構成するなどして証明される．

定理 5.1.1 (Thm. 3 of [21]) 非斉次多項式列 $\boldsymbol{F}$ は暗号学的半正則であるものとし，$D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ とおく．このとき，ある正規戦略アルゴリズム $\mathcal{A}$ が構成的に存在して $\mathrm{sd}^{\mathcal{A}}_{\prec}(F) \le 2D - 1$，かつ $\mathcal{A}$ の実行中に計算される S-多項式の総次数は $2D - 2$ を超えない．

定理 5.1.1 は 4.4 小節の最後に述べた Semaev-Tenti の結果（cf. [26], [27]）の暗号学的半正則列への拡張であり，仮定 $\{x_i^q - x_i : 1 \le i \le n\} \subset F$ および $D \ge \max\{d_1, \ldots, d_m\}$ が外れている．次の系 5.1.2 は定理 5.1.1 に基づくものであり，[26] の Thm. 3.65 と同様に証明できる：

系 5.1.2 定理 5.1.1 において，正規戦略アルゴリズム $\mathcal{A}$ の計算量オーダーは次式で上から評価される：

$$m\binom{n+D}{D}^{\omega} + \frac{1}{2}\binom{n+D}{D}^2\binom{n+D-1}{D-1}^2\binom{n+2D-2}{2D-2}.$$

もし $\mathcal{A}$ の実行中に 0-簡約が一度も起きないと仮定すると，$\mathcal{A}$ の計算量オーダーは次式で上から評価される：

$$m\binom{n+D}{D}^{\omega} + \binom{n+D-1}{D-1}^2\binom{n+2D-2}{2D-2}.$$

系 5.1.2 の評価式の第一項 $m\binom{n+D}{D}^{\omega}$ は，$\prec^h$ に関する $\langle F^h \rangle$ の簡約 Gröbner 基底における次数 D 以下の元全て（D-Gröbner 基底と呼ばれる）を求める計算量に等しい．

5.2 正則性次数の拡張による新しい計算量評価式

系 5.1.2 の評価式は最悪の評価であり，実用的にはよりタイトな評価が望まれる．ここでは，従来の正則性次数および半正則性の定義を拡張することで，より実用的な評価式を導く．以下では，$\prec$ は次数付き逆辞書式順序とする．

定義 5.2.1 (Def. 2.3.1 of [21]) 斉次イデアル $I \subset R$ の**一般化された正則性次数（generalized degree of regularity）** $\widetilde{d}_{\mathrm{reg}}(I)$ を次で定義する：ある d_0 が存在して，任意の $d \ge d_0$ に対して $\mathrm{HF}_{R/I}(d) = \mathrm{HF}_{R/I}(d_0)$ が成り立つとき，そのような d_0 の最小値を $\widetilde{d}_{\mathrm{reg}}(I)$ と定める．そのような d_0 が存在しないとき，$\widetilde{d}_{\mathrm{reg}}(I) = \infty$ と定める．なお，I が F で生成されるときは $\widetilde{d}_{\mathrm{reg}}(I)$ を $\widetilde{d}_{\mathrm{reg}}(F)$ と書く．

注意 5.2.2 定義 5.2.1 における d_0 の存在は，射影的零点集合 $V_{\overline{K}}(I)$ が有限であることに同値である（cf. Thm. 3.3.4 of [9]）．また，R/I が Artin 的であれば $\widetilde{d}_{\mathrm{reg}}(I) = d_{\mathrm{reg}}(I) < \infty$，さもなくば $\widetilde{d}_{\mathrm{reg}}(I) \le d_{\mathrm{reg}}(I) = \infty$ となる．

定理 5.2.3 (Prop. 2.3.4 of [21]) $f_1, \ldots, f_m \in R \setminus K$ は斉次とは限らないとする．もし『$R/\langle F^{\mathrm{top}} \rangle$ が Artin 的で，かつ $\boldsymbol{F}^{\mathrm{top}} = (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ が暗号学的半正則』（注意 3.3.2，5.3 小節で述べるようにこの仮定は暗号分野で重要である）であれば，$\widetilde{d}_{\mathrm{reg}}(F^h) \ge d_{\mathrm{reg}}(F^{\mathrm{top}}) - 1$ および

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h) \le \max\{d_{\mathrm{reg}}(F^{\mathrm{top}}), \widetilde{d}_{\mathrm{reg}}(F^h)\}$$

が成り立つ．さらに，$R[y]$ の単項式イデアル $\langle \mathrm{LM}_{\prec^h}(\langle F^h \rangle) \rangle$ が weakly reverse lexicographic（定義は [24] を参照）であれば，第二の不等式において等号が成り立つ．

注意 5.2.4 定理 5.2.3 において，各 $d \ge 0$ に対して $h_d := \mathrm{HF}_{R[y]/\langle F^h \rangle}(d)$ とおくとき，h_d は $d \le D-1$ において狭義単調増加する（Thm. 1 of [20]）．また $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$，$D' := \widetilde{d}_{\mathrm{reg}}(F^h)$ とするとき，$D' \ge D$ であることは

$$\cdots < h_{D-2} < h_{D-1} \ge h_D \ge \cdots \ge h_{D'} = h_{D'+1} = \cdots$$

に同値であり，$D' = D - 1$ であることは次に同値である：

$$\cdots < h_{D-2} < h_{D-1} = h_D = h_{D+1} = \cdots .$$

定義 5.2.5 (Def. 2.3.3 of [21]) $f_1, \ldots, f_m \in R \setminus K$ が全て斉次のとき，$\boldsymbol{F} = (f_1, \ldots, f_m)$ が**一般化された暗号学的半正則列（generalized cryptographic semi-regular sequence）**であるとは，$\boldsymbol{F}$ が $\widetilde{d}_{\mathrm{reg}}(F)$-正則のときをいう．$f_1, \ldots, f_m \in R$ のいずれかが非斉次である場合，$\boldsymbol{F}$ が一般化された暗号学的半正則列であるとは，$\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h)$

が一般化された暗号学的半正則列であるときをいう．

Fröberg 予想 [16]（cf. 注意 3.1.4）の類似として，我々は次の予想を提示する：

予想 5.2.6 (Conj. 4.3.4 of [21]) K（必要あれば代数閉包 $\overline{K}$ で考える）を無限体とし，$m \geq n$ とする．また，$F = \{f_1, \ldots, f_m\} \subset R \setminus K$ は非斉次，かつ，その $\overline{K}$ 上のアフィン零点集合は空でなく有限とする．このとき，与えられた K, n, m, $d_1, \ldots, d_m$ に対して，「$\boldsymbol{F} = (f_1, \ldots, f_m)$ が一般化された暗号学的半正則列である」という性質は generic に成り立つ（“generic” の定義は [24] を参照）．

Fröberg 予想と同様に，この予想は少なくとも $m = n$ の場合に正しいことが示される．

注意 5.2.7 予想 5.2.6 から，$K = \mathbb{F}_q$ かつ $m \geq n$ の場合に，$\overline{K}$ 上で少なくとも 1 つ零点をもつように，係数の “ほとんど” をランダムに選ぶことで構成された非斉次多項式集合 F（例えば注意 3.3.2 の第 2 段落で構成した F）に対して，$\boldsymbol{F} = (f_1, \ldots, f_m)$ は高確率で一般化された暗号学的半正則列になることが期待される．我々は実験的にも，このことを確認した（詳細は [21] の Sect. 4.3 を参照）．従って，注意 3.3.2 で述べたような，多変数多項式暗号における非斉次な公開鍵多項式列についても，一般化された暗号学的半正則列であることを期待できる．

以上の準備のもと，次が成り立つ：

定理 5.2.8 (Sect. 4.3 of [21]) $m \geq n$ とし，非斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m)$ に次の 2 条件：

(1) $\boldsymbol{F}^h$ は一般化された暗号学的半正則列，すなわち $\widetilde{d}_{\mathrm{reg}}(F^h)$-正則．

(2) $\boldsymbol{F}^{\mathrm{top}}$ は暗号学的半正則，すなわち $d_{\mathrm{reg}}(F^{\mathrm{top}})$-正則．

を仮定する．このとき，

$$D_{\mathrm{new}} := \begin{cases} \deg\left(\left[\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^{n+1}}\right]\right) + 1 & (m > n), \\ \sum_{i=1}^{n}(d_i - 1) + 1 & (m = n) \end{cases} \tag{5.1}$$

とおくと，$\max\{d_{\mathrm{reg}}(F^{\mathrm{top}}), \widetilde{d}_{\mathrm{reg}}(F^h)\} \leq D_{\mathrm{new}}$ である．従って定理 5.2.3 と 4.4 小節第一段落で述べたことから，F^h の $\prec^h$ に関する Gröbner 基底の（よって F の $\prec$ に関する Gröbner 基底の）計算量は $O\left(m\binom{n+D_{\mathrm{new}}}{D_{\mathrm{new}}}^{\omega}\right)$ となる．

注意 5.2.9 定理 5.2.8 において，もし $m = n+1$ なら，D_{new} は (4.2) 右辺の Macaulay 上界に等しい．

5.3 暗号の安全性解析への応用可能性

ここでは，5.1 – 5.2 小節の内容の，多変数多項式暗号の安全性解析への応用可能性を議論する．多変数多項式暗号の安全性は，多くの場合，有限体 $\mathbb{F}_q$ 上の 2 次多項式系の求解問題（MQ 問題）に帰着される（詳細は [19] を参照）．暗号化方式では $m \geq n$（overdetermined），署名方式では $m \leq n$（underdetermined）であるが，署名方式の場合も $\{x_i^q - x_i : 1 \leq i \leq n\}$ を F に付け加えることで overdetermined な多項式系が得られるので，$m \geq n$ の場合は非常に重要である．以下では，$m \geq n$ の場合に，次数付き項順序 $\prec$ に関する $\langle F \rangle$ の Gröbner 基底の計算量を評価する方法を述べる．なお，$n, m, d_1, \ldots, d_m$ が与えられたとき，D_{new} の値は (5.1) より容易に計算できる（$D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ についても定理 3.1.2 (2) から計算可能）．

● 一般の場合（$d_1 = \cdots = d_m = 2$ とも限らない）

暗号の分野（特に多変数多項式暗号の安全性解析）では，非斉次多項式列 $\boldsymbol{F}$ を暗号学的半正則と仮定した上で，

(1) 不等式 (4.3) に基づいて，F の求解次数を正則性次数 $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ で近似し（あるいは上から評価し），

(2) その上で，$\prec$ に関する $\langle F \rangle$ の Gröbner 基底の計算量オーダーを $\binom{n+D}{D}^{\omega}$ で見積もる（m が抜けている）

ことが多い（例えば [19] を参照）．これらは [3] の Prop. 6 (iv) に基づくが，「step degree が初めて D に達した後の計算量が無視できる」などの仮定が欠落している（実際，一般には無視できない）．特に (1) については，いま F が非斉次であるため，次数 D 未満の Gröbner 基底元が step degree $D+1$ 以上で求まる可能性があるので（このような現象は degree fall と呼ばれる），不等式 (4.3) のみから (1) を導くのは飛躍した議論である．従って，(1)，(2) をそのままの形で暗号の安全性解析に流用できるとは限らず，以下のような厳密かつ正確な議論が必要である．

- まず (1) に関して，$\boldsymbol{F}$ が暗号学的半正則であっても，F の求解次数と正則性次数 D とでは一般には前者が大きくなり，しかも乖離し得る（[4], [7], [8] の具体例を参照）．理論上，$\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ は $2D-1$ 以下（定理 5.1.1）であるので，この上界を用いるのが正確である．
- 次に (2) に関しては，F の求解次数 $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ の上界 $2D-1$ の下で，系 5.1.2 の計算量評価式を適用できる．

ただし，mutant 戦略を用いる場合は Salizzoni [25] の上界 $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq D+1$ を適用できて（4.4 小節），この場合の計算量評価式は [25] の Prop. 3.13 に記載の通りである．

実用上は，$\boldsymbol{F}$ が一般化された暗号学的半正則列であると仮定することで，定理 5.2.8 より $\boldsymbol{F}^h$ の求解次数 $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F^h)$ が D_{new} 以下となるため，計算量評価式 $O\left(m\binom{n+D_{\mathrm{new}}}{D_{\mathrm{new}}}^{\omega}\right)$ を適用できる．注意として，$m \gg n$ だと $D_{\mathrm{new}} \approx D$ となるので（[21] の Tables 1–4 参照），この場合は結果的にではあるが上記 (1) の近似が正当化される．

● $d_1 = \cdots = d_m = 2$ かつ $m = n+1$ の場合（cf. [28]）

この場合，$D = \lfloor (n+1)/2 \rfloor + 1$ であり（Thm. 4.1 of [4]），従って n が奇数（resp. 偶数）なら $2D - 1 = n + 2$（resp. $n+1$）となる．一方，$D_{\mathrm{new}} = n+2$ であり，もし $\boldsymbol{F}$ が一般化された暗号学的半正則列なら，$D' := \widetilde{d}_{\mathrm{reg}}(F^h)$ に対し

$$\mathrm{HS}_{R[y]/\langle F^h \rangle}(z) \equiv (1+z)^{n+1} \pmod{z^{D'}}$$

となる．特に n が偶数なら，$h_{D-1} = h_D$（よって y 倍により定義される K-線形写像 $(R[y]/\langle F^h \rangle)_{D-1} \to (R[y]/\langle F^h \rangle)_D$ は全単射）である．従って，[21] の Sect. 4.1 – 4.2 と同様の

議論により，F の Gröbner 基底計算において，step degree が初めて D に達する以前では degree fall は起きないことを証明できる（このことは，[28] の Sect. 3.3 における議論に対する，数学的に厳密な証明を与えたことになる）．

- **$\{f_1, \ldots, f_m\}$ が斉次である場合（e.g., [18]）**

多変数多項式暗号の中には，斉次な MQ 問題に安全性が帰着されるものがある．つまり，斉次な $F = \{f_1, \ldots, f_m\}$ に対する Gröbner 基底の計算量で安全性が評価される．この場合，$\boldsymbol{F}$ を暗号学的半正則列と仮定してしまうと，定理 2.3.5 により F は閉体 $\overline{K}$ 上で非自明な零点をもたない．このため，「$\boldsymbol{F}$ は暗号学的半正則ではないが，暗号学的半正則である場合と同様の計算挙動になる」と仮定することがある（例えば [18] の Sect. 4.2 および Table 4 を参照）．これは，Gröbner 基底が求まる step degree（すなわち求解次数）の直前までは，暗号学的半正則列の場合と同様に振舞うということであり，我々の言葉でいえば「$\boldsymbol{F}$ が $\widetilde{d}_{\mathrm{reg}}(F)$-正則（すなわち一般化された暗号学的半正則列）」ということになる．一般化された暗号学的半正則列では，定理 5.2.8 の上界 D_{new} および計算量評価式を適用できる．

謝辞　本研究は科学研究費基金（21K03377，23K12949）の助成を受けて行われました．

参考文献

[1] M. Bardet: Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie. PhD thesis, Université Paris IV, 2004.

[2] M. Bardet, J.-C. Faugére, and B. Salvy: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations (extended abstract). In: Proceedings of the International Conference on Polynomial System Solving, 71–74, 2004.

[3] M. Bardet, J.-C. Faugére, B. Salvy, and B.-Y. Yang: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proceedings of Eighth International Symposium on Effective Methods in Algebraic Geometry (MEGA 2005), 2005.

[4] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou: Semi-Regular Sequences and Other Random Systems of Equations. In: Women in Numbers Europe III, **24**, pp. 75–114, Springer, 2021.

[5] B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Innsbruck: Univ. Innsbruck, Mathematisches Institut (Diss.), 1965.

[6] J. A. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed: MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. In H. Handschuh, S. Lucks, B. Preneel, and P. Rogaway (eds), Symmetric Cryptography, Dagstuhl Seminar Proceedings, **9031**, pp. 1–7, Dagstuhl, Germany, 2009.

[7] A. Caminata and E. Gorla: Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra. In: Arithmetic of Finite Fields (Proc. of WAIFI 2020), LNCS, **12542**, pp. 3–36, Springer, 2021.

[8] A. Caminata and E. Gorla: Solving degree, last fall degree, and related invariants. J. Symb. Comp., **114**, 322–335, 2023.

[9] J. G. Capaverde: Gröbner bases: Degree bounds and generic ideals. PhD thesis, Clemson University, 2014.

[10] N. Courtois, A. Klimov, J. Patarin, and A. Shamir: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. EUROCRYPT 2000, LNCS, **1807**, pp. 392–407, Springer, 2000.

[11] C. Diem: Bounded regularity. Journal of Algebra, **423**, 1143–1160, 2015.

[12] J. Ding and D. Schmidt: Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields. In: M. Fischlin and S. Katzenbeisser (eds), Number Theory and Cryptography, LNCS, **8260**, pp. 34–49, Springer, Berlin, Heidelberg.

[13] J.-C., Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra, **139**, 61–88, 1999.

[14] J.-C., Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of ISSAC 2002, ACM Press, pp. 75–82, 2002.

[15] J.-C., Faugère, P. Gianni, D. Lazard, and T. Mora: Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symb. Comp., **16** (4), 329–344, 1993.

[16] R. Fröberg: An inequality for Hilbert series of graded algebras. Math. Scand., **56**, 117–144, 1985.

[17] G.-M. Greuerl and G. Pfister: A Sinular Introduction to Commutative Algebra. 2nd Edition, Springer, 2007.

[18] Y. Ikematsu and Rika Akiyama: Revisiting the security analysis of SNOVA. Proceedings of the 11th ACM Asia Public-Key Cryptography Workshop, pp. 54–61, 2024.

[19] Y. Ikematsu, S. Nakamura, and T. Takagi: Recent progress in the security evaluation of multivariate public key cryptography. IET Information Security, **17**, Issue 2, 210–226, 2022.

[20] M. Kudo and K. Yokoyama: On Hilbert-Poincaré series of affine semi-regular polynomial sequences and related Gröbner bases. In: T. Takagi et al. (eds), Mathematical Foundations for Post-Quantum Cryptography, Mathematics for Industry, 26 pages, Springer, to appear (arXiv:2401.07768).

[21] M. Kudo and K. Yokoyama: The solving degrees for computing Gröbner bases of affine semi-regular polynomial sequences. eprint/2024/528 or arXiv:2404.03530.

[22] D. Lazard: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer algebra (London, 1983), LNCS, **162**, pp. 146–156, Springer, Berlin, 1983.

[23] G. Moreno-Socías: Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

[24] K. Pardue: Generic sequences of polynomials. Journal of Algebra, **324.4**, 579–590, 2010.

[25] F. Salizzoni: An upper bound for the solving degree in terms of the degree of regularity. arXiv:2304.13485.

[26] I. Semaev and A. Tenti: Probabilistic analysis on Macaulay matrices over finite fields and complexity constructing Gröbner bases. J. Algebra, **565**, 651–674, 2021.

[27] A. Tenti: Sufficiently overdetermined random polynomial systems behave like semiregular ones. PhD Thesis, University of Bergen, 2019.

[28] 伊藤琢真, 黒川高司, 篠原直行, 内山成憲: Gröbner 基底計算における第二先頭単項式の有効性. SCIS2024, 2A2-3.

[29] 工藤桃成, 横山和弘: アフィン半正則な多項式列に付随する Hilbert 級数と関連する Gröbner 基底. RIMS 講究録, **2280**, 1–11, 2024.