Computer Security Symposium 2022
24 - 27 October 2022

UOV多項式系に対するHilbert級数について

池松 泰彦[1,a)]　清村 優太郎[2]　齋藤 恆和[2]

概要：UOV 署名方式は多変数多項式求解問題 (MQ 問題) を基にして構成される署名方式である．米国標準技術研究所 (NIST) が行っている耐量子計算機暗号 (PQC) 標準化プロジェクトのファイナリストであった Rainbow や最近提案された QR-UOV, MAYO などの構成の基盤となる非常に重要な方式である．一般に多変数多項式暗号 (MPKC) の安全性解析では, MQ 問題を解く計算量を解析する必要があるが, それは公開鍵からなる二次多項式系が生成するイデアルの Hilbert 級数と関係していることが知られている．この論文では, UOV に現れる多項式系が生成するイデアルの Hilbert 級数を考察する．特に, 実験により UOV 多項式系の Hilbert 級数の予測公式を導出し, MAYO の安全性解析への応用について考える．

キーワード：耐量子計算機暗号, 多変数多項式暗号, UOV, Hilbert 級数

Hilbert series for UOV polynomials

Yasuhiko Ikematsu[1,a)]　Yutaro Kiyomura[2]　Tsunekazu Saito[2]

Abstract: UOV is a signature scheme constructed based on the multivariate quadratic (MQ) problem. It is important since it is foundation of QR-UOV, MAYO, and Rainbow which is a finalist of NIST PQC standardization project. In general, to analyze the security of multivariate public key cryptosystems (MPKC), the complexity estimation of MQ problem is necessary. It is known that Hilbert series of the ideal generated by the public key of MPKC relates to such estimation. In this paper, we study Hilbert series of quadratic polynomials appeared in UOV. In particular, we guess the formula of the Hilbert series from some experimental results, and apply it to the security analysis of MAYO.

Keywords: Post-quantum cryptography, Multivariate public key cryptography, UOV, Hilbert series

1. はじめに

大規模な量子計算機の出現により, 既存の暗号技術が危殆化することが知られている．そのため, 量子計算機による攻撃に耐性のある暗号として耐量子計算機暗号 (PQC) [2] の研究開発が現在盛んに行われている．その中で, 米国標準技術研究所 (NIST) が行なっている PQC 標準化プロジェクト [19] が注目を集めており, 2022 年 7 月には第 3 ラウンドが終わり, 標準化される方式がいくつか選定された．このプロジェクトは継続しており, 今後もいくつかのラウンドを経て標準化方式がさらに選定されることになっている．

多変数多項式暗号 (MPKC) は二次方程式求解問題 (MQ 問題) を安全性の根拠とする暗号であり, 耐量子性を持つと考えられている．MPKC は 1980 年代の松本-今井方式 [18] をはじめとして, いくつもの方式が提案されてきた．特に, UOV 署名方式 [16] を多層化することで効率化を高めた Rainbow [9], [11] は NIST PQC 標準化プロジェクトにおいて第 3 ラウンドまで進出した方式としてこれまで注目を集めてきた．しかし, Beullens による simple attack [6] によって, 多層化に脆弱性があることがわかり, 標準化方式には選出されなかった．このことから現在, MPKC の分野では Rainbow のベースとなっている UOV 署名方式が再注目され, QR-UOV [15] や MAYO [5] といった多層化とは異なったアイデアに基づいた改良方式が提案され, その安全

[1] 九州大学マス・フォア・インダストリ研究所
Institute of Mathematics for Industry, Kyushu University
[2] NTT 社会情報研究所
NTT Social Informatics Laboratories
[a)] ikematsu@imi.kyushu-u.ac.jp

性解析が MPKC の分野の課題となっている.

UOV [16] の安全性解析で現れる主な攻撃は, 現在 direct attack, KS attack [17], reconciliation attack [12], intersection attack [4] の 4 つがある. 特に, direct attack は公開鍵とメッセージからなる二次方程式系を秘密鍵なしで解く MPKC における最も一般的な攻撃手法の一つである. その方程式系を解くためには, グレブナー基底アルゴリズム (F4 [13], F5 [14] など) や XL アルゴリズム [7] が使われる. 具体的には, ハイブリッドアプローチ [3] を使い, 変数の個数 n を多項式の個数 m 以下とした方程式系を解くことを試みる. 計算量評価は, それらが semi-regular system [1] になっていると仮定して行われる. その場合, semi-regular system が生成するイデアルの Hilbert 級数に現れる関数 $\frac{(1-t^2)^m}{(1-t)^n}$ を使い,, その関数の 0 以下の係数の最小次数を用いて計算量評価がなされる (詳しくは 2.2 を見よ).

このように, direct attack では, semi-regular system の生成するイデアルの Hilbert 級数が登場するが, これまでの研究で UOV 自体が生成するイデアルの Hilbert 級数については詳しく考えられてこなかった. そこでこの論文では, UOV の Hilbert 級数, もしくはより広く, UOV に現れる多項式 (UOV 多項式) の個数を通常の UOV より多くした場合に生成されるイデアルの Hilbert 級数がどのようになっているかを研究する. ここでは, 計算機実験を行い, その結果からそれらの Hilbert 級数の予測公式を導出する. さらに, その結果を使い UOV の変種である MAYO [5] に対する reconciliation attack [12] を詳しくみる.

この論文の構成は次の通りである. まず 2 章で UOV 署名方式やその安全性解析, 変種 MAYO について解説する. 次で, 3 章で Hilbert 級数の定義や semi-regular system について復習する. 4 章では, UOV に現れる多項式系が生成するイデアルの Hilbert 級数の計算機実験結果を考察し, 予測公式の導出を行う. 5 章では, その予測公式を使って MAYO の安全性解析に応用する. 最後に 6 章で, この論文の結論を述べる.

2. UOV 署名方式

ここでは, UOV 署名方式 [16] とその安全性解析について説明する. さらに, UOV の変種 MAYO [5] について説明する.

2.1 UOV の構成

$\mathbb{F}_q$ を位数 q の有限体とする. さらに, $v > o$ を二つの正の整数とする. このとき, $n = v + o$ とする. 二種類の変数の集合 $\mathbf{x}_v = (x_1, \ldots, x_v)$ と $\mathbf{x}_o = (x_{v+1}, \ldots, x_n)$ を用意し, $\mathbf{x} = (\mathbf{x}_v, \mathbf{x}_o)$ とおく. $\mathbf{x}_v$ の中の変数を vinegar 変数, $\mathbf{x}_o$ を oil 変数と呼ぶ. また, v を vinegar 次元, o を oil 次元と呼ぶことにする. UOV の鍵生成, 署名生成, 署名検証は次のように行われる.

鍵生成: 次のような形をとる n 変数 o 個の二次多項式系を一様ランダムにとる:

$$\begin{aligned} f_1(\mathbf{x}) = f_1(\mathbf{x}_v, \mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} a_{i,j}^{(1)} x_i x_j, \\ &\vdots \\ f_o(\mathbf{x}) = f_o(\mathbf{x}_v, \mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(o)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} a_{i,j}^{(o)} x_i x_j. \end{aligned} \tag{1}$$

ここで, 一様ランダムにとるとは, 各係数 $a_{i,j}^{(k)}$ を有限体 $\mathbb{F}_q$ から一様ランダムに選ぶことを意味する. この論文では, (1) のような形の二次多項式のことを UOV 多項式と呼ぶことにする. (1) の UOV 多項式からなる二次写像 $\mathcal{F} = (f_1, \ldots, f_o) : \mathbb{F}_q^n \to \mathbb{F}_q^o$ を UOV 署名方式の中心写像と呼ぶ. 可逆な線型写像 $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ を一様ランダムに選ぶことで, UOV の公開鍵は写像の合成によって $\mathcal{P} := \mathcal{F} \circ \mathcal{S} = (p_1, \ldots, p_o)$ で構成される. このとき, 秘密鍵は $\{\mathcal{F}, \mathcal{S}\}$ である.

署名生成: 与えられたメッセージ $\mathbf{m} = (m_1, \ldots, m_o) \in \mathbb{F}_q^o$ に対する署名 $\mathbf{s} \in \mathbb{F}_q^n$ は次のように生成される. まず, 一様ランダムに $\mathbf{c} = (c_1, \ldots, c_v) \in \mathbb{F}_q^v$ を選ぶ. 次に, $\mathbf{x}_v$ に $\mathbf{c}$ を代入することで得られる o 変数 o 個の線型方程式

$$f_1(\mathbf{c}, \mathbf{x}_o) = m_1, \cdots, f_o(\mathbf{c}, \mathbf{x}_o) = m_o,$$

の一つの解 $\mathbf{x}_o = \mathbf{d} \in \mathbb{F}_q^o$ を求める. もしその線型方程式に解が存在しなければ, 別の $\mathbf{c}$ を選び, 解が存在するまで行う. 最後に, $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{c}, \mathbf{d}) \in \mathbb{F}_q^n$ を計算すれば, この $\mathbf{s}$ が $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ の解であり, これがメッセージ $\mathbf{m}$ に対する署名となる.

署名検証: 検証は, 署名 $\mathbf{s}$ を公開鍵 $\mathcal{P}$ に代入し, $\mathcal{P}(\mathbf{s}) = \mathbf{m}$ が成り立てば受理し, そうでなければ拒否する.

2.2 UOV の安全性解析

UOV のパラメータを導出するためには, 主に 4 つの攻撃を考慮する必要がある: direct attack, KS attack [17], reconciliation attack [12], intersection attack [4]. ここでは, direct attack, KS attack, reconciliation attack の解説を行う.

Direct attack: この攻撃は, 与えられたメッセージ $\mathbf{m}$ に対する二次方程式系 $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ を秘密鍵なしで直接解いて署名を偽造する攻撃である.

そのような方程式系を解くためには, グレブナー基底アルゴリズム (例えば, F_4 [13], F_5 [14]) や XL アルゴリズム [7] が使われる. 方程式系 $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ は $n = v + o$ 変数 o 個の二次多項式系である. 攻撃を成功させるには解を一つ見つ

ければ良いので, $\mathbf{x}$ の中の $v\ (=n-o)$ 個の変数にランダムな値を代入して, o 変数 o 個の二次多項式系に縮小する. このとき, 得られる多項式系は semi-regular system [1] になると考えられる (定義は 3.2 で復習する). その求解は XL アルゴリズム [7] と Wiedemann アルゴリズム [20] とハイブリッドアプローチ [3] の組み合わせで行われ, 計算量は次の式で与えられる:

$$\min_{0\le k\le o} q^k \cdot 3\binom{o-k+D_{reg}}{D_{reg}}^2\binom{o-k}{2}.$$

ここで, $0\le k\le o$ はハイブリッドアプローチの中で固定される変数の個数であり, D_{reg} は多項式 $\frac{(1-t^2)^o}{(1-t)^{o-k}}$ における t^d の係数が 0 以下となる最小の整数 d を表す.

KS attack [17]: この攻撃は (1) にある多項式系 $f_1,\ldots,f_o$ の持つ特別な形を利用する攻撃である. 簡単のために, $\mathbb{F}_q$ の標数は奇数であるとする. 各 f_i は斉次二次多項式であるので, $n\times n$ 対称行列を使って次のように一意的に表現できる:

$$f_i(\mathbf{x}) = \begin{pmatrix}\mathbf{x}_v & \mathbf{x}_o\end{pmatrix}\cdot\begin{pmatrix}*_{v,v} & *_{v,o}\\ *_{o,v} & 0_{o,o}\end{pmatrix}\cdot\begin{pmatrix}{}^t\mathbf{x}_v\\ {}^t\mathbf{x}_o\end{pmatrix}.$$

ここで, $*_{v,v}$ は $v\times v$ 行列を, $0_{o,o}$ はサイズが $o\times o$ の零行列を表す. ここで現れる対称行列を F_i と書くことにする. この F_i は f_i の表現行列と呼ばれる. 秘密鍵 $\mathcal{S}$ に対応する $n\times n$ 行列を S と記す. つまり, $\mathbf{x}\in\mathbb{F}_q^n$ に対して, $\mathcal{S}(\mathbf{x})=\mathbf{x}\cdot S$ が成り立つようにとる. 関係 $p_i=f_i\circ\mathcal{S}$ から, p_i の表現行列は $P_i := S\cdot F_i\cdot{}^tS$ なる. 集合 $\{e_1,\ldots,e_n\}$ を $\mathbb{F}_q^n$ の標準基底とする, つまり $e_1=(1,0,\ldots,0)$ などとする. 次のように twisted oil 空間 O を定義する:

$$O := \mathrm{Span}\{e_{v+1},\ldots,e_n\}\cdot S^{-1}. \tag{2}$$

KS attack は twisted oil 空間 O を公開鍵の表現行列から求める攻撃である. 具体的には, $\mathrm{Span}\{P_1,\ldots,P_o\}$ から元 X,Y を選び, XY^{-1} の不変部分空間を計算することで求める. そのとき, 攻撃者は $O\cdot S^{-1}S'=O$ となる可逆な線型写像 S' を復元でき, これが同値な秘密鍵になるので, 偽造が可能となる. KS attack の計算量は $q^{v-o}\cdot o^4$ となることが知られている.

Reconciliation attack [12]: KS attack で述べた事実を使えば, $\mathcal{P}(\mathbf{x})=\mathbf{0}$ が twisted oil 空間 O を含むことがわかる. そのとき, reconciliation attack とは, $\mathcal{P}(\mathbf{x})=\mathbf{0}$ から twisted oil 空間を秘密鍵なしで復元する攻撃のことである. この攻撃は, 署名を偽造する direct attack と異なり, (同値な) 秘密鍵を復元する攻撃であることに注意する. また, UOV では $v>o$ であることから $\mathcal{P}(\mathbf{x})=\mathbf{0}$ はおよそ $v=n-o$ 次元の解空間を持つため, o 次元の twisted oil 空間以外の解が含まれる. よって, 解空間での探索コストが必要となり, この攻撃は UOV ではあまり有効な攻撃とはみなされていない. しかし, 次の MAYO で述べるように, これは MAYO に対しては有効となる.

2.3 MAYO

署名方式 MAYO は 2021 年 Beullens によって提案された UOV の変種である [5]. ここでは, MAYO で扱われる鍵生成のみについて説明する. その他の署名生成, 署名検証などについては原論文 [5] を見よ.

$\mathbb{F}_q$ を位数 q の有限体, 三つの正の整数 v,o,m $(m>v>o)$ を用意し, $n=v+o$ とする. また, vinegar 変数 $\mathbf{x}_v=(x_1,\ldots,x_v)$ と oil 変数 $\mathbf{x}_o=(x_{v+1},\ldots,x_n)$ を用意し, $\mathbf{x}=(\mathbf{x}_v,\mathbf{x}_o)$ とする.

鍵生成: 次のような UOV 多項式からなる n 変数 m 個の二次多項式系を一様ランダムにとる:

$$\begin{aligned} f_1(\mathbf{x}) = f_1(\mathbf{x}_v,\mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(1)}x_ix_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} a_{i,j}^{(1)}x_ix_j,\\ &\vdots \\ f_m(\mathbf{x}) = f_m(\mathbf{x}_v,\mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(m)}x_ix_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} a_{i,j}^{(m)}x_ix_j. \end{aligned} \tag{3}$$

このとき, $\mathcal{F}=(f_1,\cdots,f_m):\mathbb{F}_q^n\to\mathbb{F}_q^m$ が定まる. 可逆な線型写像 $\mathcal{S}:\mathbb{F}_q^n\to\mathbb{F}_q^n$ を一様ランダムに選ぶことで, UOV の公開鍵は写像の合成によって $\mathcal{P}:=\mathcal{F}\circ\mathcal{S}=\{p_1,\cdots,p_m\}$ で構成される. 秘密鍵は $\{\mathcal{F},\mathcal{S}\}$ である.

説明からわかるように, UOV との違いは, UOV 多項式を o 個とるのではなく, o とは異なる整数 m を用意して, UOV 多項式を m 個とる所である. 署名生成は公開鍵を多重にすることで行われるが, 詳しくは原論文 [5] を見よ.

MAYO の攻撃については, 2.2 で述べた UOV の reconciliation attack が有効となる. つまり, 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ を考えると, これは twisted oil 空間を解に含む. ここでこの方程式系は, $n=v+o$ 変数, m 個の二次多項式からなるが, MAYO のパラメータでは $m>n$ となっていることから, $\mathcal{P}(\mathbf{x})=\mathbf{0}$ を解けば, 探索なしで twisted oil 空間を復元できると考えられる. Reconciliation attack とその計算量評価については以下の仮定が正しいと考えて行われる.

- 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ の解空間は twisted oil 空間に一致する.
- 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ は semi-regular でない.
- $o-1$ 個の変数 (例えば $x_{v+2},\ldots,x_n$) に 0 を代入すれば, 方程式系の解空間は 1 次元となる.

この仮定の元で, $x_{v+2},\ldots,x_n$ を固定した v 変数 m 個の方程式系を Hybrid Weidemann XL アルゴリズムで解く計算

量が次のように与えられる：

$$\min_{0\le k\le v} q^k \cdot 3\binom{v-k+D_{reg}}{D_{reg}}^2\binom{v-k}{2}.$$

ここで D_{reg} は, 多項式 $\frac{(1-t^2)^m}{(1-t)^{v-k}}$ における t^d の係数が 0 以下となる最小の整数 d を表す. 5 章では, 上記仮定を UOV 多項式系の Hilbert 級数の結果を用いて検証する.

3. Hilbert 級数

ここでは, まず多項式環のイデアルの Hilbert 級数の定義を説明する. 次に, semi-regular system の定義を述べ, その Hilbert 級数の公式を紹介する.

3.1 Hilbert 級数の定義

$R=\mathbb{F}_q[x_1,\ldots,x_n]$ を $\mathbb{F}_q$ 上の n 変数多項式環とする. R は次数付き環であるので, $R=\oplus_{i=0}^{\infty}R_i$ と分解できる. ここで, R_i は次数が i の単項式全体が生成する部分空間である. 次に, m 個の斉次多項式 $g_1,\ldots,g_m\in\mathbb{F}_q[x_1,\ldots,x_n]$ が生成するイデアルを I とする. また, $I_i:=I\cap R_i$ とする. I は斉次イデアルなので, $I=\oplus_{i=0}^{\infty}I_i$ が成り立つ.

定義 1. 次の級数を商環 R/I の Hilbert 級数と呼ぶ:

$$\mathrm{HS}_{R/I}(t):=\sum_{i=0}^{\infty}\dim_{\mathbb{F}_q}(R_i/I_i)\cdot t^i.$$

厳密には R/I の Hilbert 級数であるが, 簡単のためここでは I の Hilbert 級数と呼ぶことに注意する.

例. (1) $I=0$ の時, I の Hilbert 級数は $\mathrm{HS}_R(t)=\frac{1}{(1-t)^n}$ となる.

(2) $0\le k\le n$ に対して, $I=\langle x_1,\ldots,x_k\rangle$ とすると, I の Hilbert 級数は $\mathrm{HS}_{R/I}(t)=\frac{1}{(1-t)^{n-k}}$ である.

定義 2. 二つの級数 $\sum_{i=0}^{\infty}a_it^i$, $\sum_{i=0}^{\infty}b_it^i$ に対して,

$$\sum_{i=0}^{\infty}a_it^i\preceq\sum_{i=0}^{\infty}b_it^i$$

を任意の i に対して $a_i\le b_i$ となることと定義する.

次の補題は明らかである:

補題 1. *(1)* 二つの斉次イデアル I, J に対して $I\supset J$ であれば, $HS_{R/I}(t)\preceq HS_{R/J}(t)$ が成り立つ.

(2) 斉次二次多項式系 $g_1,\ldots,g_m$ が生成するイデアルを I とする. また, $\mathcal{S}:\mathbb{F}_q^n\to\mathbb{F}_q^n$ を可逆な線型写像とし, $g_1\circ\mathcal{S},\ldots,g_m\circ\mathcal{S}$ が生成するイデアルと $I_{\mathcal{S}}$ とする. このとき, $\mathcal{S}$ は *Hilbert* 級数を変えない. つまり, 次が成り立つ:

$$HS_{R/I_{\mathcal{S}}}(t)=HS_{R/I}(t).$$

3.2 Semi-regularity

ここでは, semi-regular system と呼ばれる多項式系を定義し, その Hilbert 級数がどのような公式で表されるかを説明する. m 個の斉次二次多項式 $g_1,\ldots,g_m\in\mathbb{F}_q[x_1,\ldots,x_n]$ が生成するイデアルを I とする. 各 $j=0,\ldots,m-1$ に対して, 商環 $S^{(j)}:=R/\langle g_1,\ldots,g_j\rangle$ を定義する. このとき, 各 $i\in\mathbb{N}$ に対して, $S_i^{(j)}=R_i/\langle g_1,\ldots,g_j\rangle_i$ とすると, $S^{(j)}=\oplus_{i=0}^{\infty}S_i^{(j)}$ が成り立つ. R 加群準同型 $\Phi^{(j)}:S^{(j)}\ni h\to f_{j+1}h\in S^{(j)}$ は, それぞれ $S_i^{(j)}$ を $S_{i+2}^{(j)}$ に写すので, その制限を $\Phi_i^{(j)}:S_i^{(j)}\to S_{i+2}^{(j)}$ と書くことにする.

定義 3. (i) $R_d=I_d$ となる最小の自然数 $d\in\mathbb{N}$ を $g_1,\ldots,g_m$ の degree of regularity と呼び, D_{reg} で表す. またそのような d が存在しない場合は $D_{reg}=\infty$ と定める.

(ii) 各 $j=0,\ldots,m-1$ と各 $i=0,\ldots,D_{reg}-2$ に対して, $\Phi_i^{(j)}:S_i^{(j)}\to S_{i+2}^{(j)}$ が必ず単射または全射となるとき, $g_1,\ldots,g_m$ を semi-regular system と呼ぶ (本来 $n\le m$ の場合 regular と呼ばれるがここでは semi-regular で統一する).

定理 1. *(i)* $g_1,\ldots,g_m$ を *semi-regular* な斉次二次多項式系とし, それらが生成するイデアルを I とする. このとき,

$$HS_{R/I}(t)=\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+$$

が成り立つ. ここで, $[*]_+$ は, 中にある級数 $*$ を展開した際に, 係数が *0* 以下になった項を含めてそれ以降の全ての係数をゼロにする操作を表す. 例えば, $[1+t-t^2+2t^3+\cdots]_+=1+t$ である.

(ii) $g_1,\ldots,g_m$ の *Hilbert* 級数が $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+$ で与えられた時, $g_1,\ldots,g_m$ は *semi-regular* になる.

(iii) $g_1,\ldots,g_m$ の *Hilbert* 級数を $HS_{R/I}(t)$ とすると, 以下を満たす:

$$\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+\preceq HS_{R/I}(t).$$

つまり, *semi-regular* の *Hilbert* 級数 $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+$ は, n 変数 m 個の斉次二次多項式系が生成するイデアルの *Hilbert* 級数の中で $\preceq$ に関する最小元になる.

以下いくつかのパラメータ q,n,m をとり, 一様ランダムに与えた $\mathbb{F}_q$ 上の n 変数 m 個の斉次二次多項式系が semi-regular になる確率を実験で求める. 実験は各パラメータで 100 回行い, semi-regular になった回数を表示する. 計算機代数システム Magma [8] を使い, ランダムな二次多項式系を生成し, その Hilbert 級数を関数コマンド `HilbertSeries` で計算した. 結果を表 1 に表す.

表からわかるように最も現れたものは semi-regular

表 1 $\mathbb{F}_q$ 上の n 変数 m 個の斉次二次多項式系を一様ランダムに取り, それが生成するイデアル I の Hilbert 級数を 100 回求め, 最も現れたものとそれが現れた回数を記載

パラメータ (q,n,m)	最頻出の Hilbert 級数	現れた回数
$(11,8,5)$	$\frac{(1+t)^5}{(1-t)^3} = \left[\frac{(1-t^2)^5}{(1-t)^8}\right]_+$	100
$(11,8,6)$	$\frac{(1+t)^6}{(1-t)^2} = \left[\frac{(1-t^2)^6}{(1-t)^8}\right]_+$	100
$(11,8,7)$	$\frac{(1+t)^7}{(1-t)} = \left[\frac{(1-t^2)^7}{(1-t)^8}\right]_+$	100
$(11,8,8)$	$(1+t)^8 = \left[\frac{(1-t^2)^8}{(1-t)^8}\right]_+$	91
$(11,8,9)$	$42t^4+48t^3+27t^2+8t+1 = \left[\frac{(1-t^2)^9}{(1-t)^8}\right]_+$	94

に対応する Hilbert 級数であることがわかる. 例えば, $q=11, n=8, m=8$ の時, 100 回実験し 91 回 semi-regular となった. 以上のように semi-regular system はパラメータを固定した際, 確率的にはよく現れる多項式系であることが実験からわかる.

4. UOV 多項式の Hilbert 級数

この章では, UOV に現れる多項式系が生成するイデアルの Hilbert 級数について考察する.

4.1 UOV 多項式の性質

三つの正の整数 v, o, m を取り, 次のような UOV 多項式からなる $n = v + o$ 変数 m 個の二次多項式系を考える:

$$f_1(\mathbf{x}) = f_1(\mathbf{x}_v, \mathbf{x}_o) = \sum_{i,j=1}^{v} a_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} a_{i,j}^{(1)} x_i x_j,$$

$$\vdots$$

$$f_m(\mathbf{x}) = f_m(\mathbf{x}_v, \mathbf{x}_o) = \sum_{i,j=1}^{v} a_{i,j}^{(m)} x_i x_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} a_{i,j}^{(m)} x_i x_j.$$

さらに, 可逆な線型写像 $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ をとり, $p_1 = f_1 \circ \mathcal{S}, \ldots, p_m = f_m \circ \mathcal{S}$ とする. これは MAYO の公開鍵であり, $m = o$ ならば UOV の公開鍵であることに注意する.

このとき, $p_1, \ldots, p_m$ が生成するイデアルの Hilbert 級数を考察したいが, 3.1 の補題 1(2) からそれは $f_1, \ldots, f_m$ の Hilbert 級数を考えれば十分である. 従って, $I = \langle f_1, \ldots, f_m \rangle$ として, Hilbert 級数 $\mathrm{HS}_{R/I}(t)$ を考察する.

まず, 明らかに $I \subset \langle x_1, \ldots, x_v \rangle$ であるので, 補題 1(1) から次が成り立つ:

$$\frac{1}{(1-t)^o} \preceq \mathrm{HS}_{R/I}(t).$$

また, 定理 1(iii) より次が成り立つ:

$$\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+ \preceq \mathrm{HS}_{R/I}(t).$$

これら二つからより強く, 次のことが証明できる:

補題 2. *イデアル $I = \langle f_1, \ldots, f_m \rangle$ が UOV 多項式から生成されるならば, Hilbert 級数 $HS_{R/I}(t)$ は次の関係式を持つ:*

$$SW\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+, \frac{1}{(1-t)^o}\right\} \preceq HS_{R/I}(t).$$

ここで, $SW\left\{\sum_{i=0}^{\infty} a_i t^i, \sum_{i=0}^{\infty} b_i t^i\right\} = \sum_{i=0}^{j-1} a_i t^i + \sum_{i=j}^{\infty} b_i t^i$ であり, j は $a_i < b_i$ となる最小の整数である.

Proof. まず明らかに, $\mathrm{Max}\left\{\sum_{i=0}^{\infty} a_i t^i, \sum_{i=0}^{\infty} b_i t^i\right\} = \sum_{i=0}^{\infty} \max\{a_i, b_i\} t^i$ とすれば,

$$\mathrm{Max}\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+, \frac{1}{(1-t)^o}\right\} \preceq \mathrm{HS}_{R/I}(t).$$

が成り立つ. そこで左辺が $\mathrm{SW}\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+, \frac{1}{(1-t)^o}\right\}$ に一致することを示せばよい. (これを Max = SW と書く.)

まず, $v \geq m$ の場合を考える. このとき, $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+ = \frac{(1-t^2)^m}{(1-t)^n} = \frac{(1+t)^m}{(1-t)^{n-m}}$ となる. ここで,

$$\frac{(1+t)^m}{(1-t)^{n-m}} = (1+t)^m \left(\sum_i t^i\right)^{n-m}, \quad \frac{1}{(1-t)^o} = \left(\sum_i t^i\right)^o$$

なので, $n-m \geq o$ であることから $\frac{(1+t)^m}{(1-t)^{n-m}} \succeq \frac{1}{(1-t)^o}$ が成り立つ. よって $v \geq m$ の場合は Max = SW となる.

次に, $m \geq v$ の場合を示す. このとき, $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+ = \left[\frac{(1+t)^v(1-t^2)^{m-v}}{(1-t)^o}\right]_+$ となる. o に関する帰納法で示す. $o = 0$ のときは, Max = SW は明らかである. $o > 0$ のときも正しいと仮定する. このとき, $\sum_i a_i t^i := \left[\frac{(1+t)^v(1-t^2)^{m-v}}{(1-t)^o}\right]_+$, $\sum_i b_i t^i := \frac{1}{(1-t)^o}$ とおくと, 仮定から $a_i \leq b_i$ ならば, $a_{i+1} \leq b_{i+1}$ となる. ここで, $o+1$ の場合を考えると

$$\frac{(1+t)^v(1-t^2)^{m-v}}{(1-t)^{o+1}} = \sum_i \left(\sum_{k=0}^{i} a_k\right) t^i,$$

$$\frac{1}{(1-t)^{o+1}} = \sum_i \left(\sum_{k=0}^{i} b_k\right) t^i$$

となる. したがって, もし $\sum_{k=0}^{i} a_k \leq \sum_{k=0}^{i} b_k$ ならば, ある i_0 $(0 \leq i_0 \leq i)$ で $a_{i_0} \leq b_{i_0}$ となるのもがあるので, a_i, b_i の満たす条件から, $a_{i+1} \leq b_{i+1}$ となり, $\sum_{k=0}^{i+1} a_k \leq \sum_{k=0}^{i+1} b_k$ が成り立つ. このことから $o+1$ についても Max = SW が成り立つことがいえる. 以上から $m \geq v$ でも証明された. □

定義 4. パラメータ $v, o, m \in \mathbb{N}$ に対して,

$$\mathrm{HS}_{v,o,m}(t) := \mathrm{SW}\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+, \frac{1}{(1-t)^o}\right\}$$

と定義する. ただし $n = v + o$ である.

ここで証明で述べたように $v \geq m$ のときは $\mathrm{HS}_{v,o,m}(t) = \frac{(1-t^2)^m}{(1-t)^n}$ となることに注意する.

表 2 UOV 多項式系の最頻出 Hilbert 級数の実験結果

パラメータ (q,v,o,m)	最頻出の Hilbert 級数	現れた回数	パラメータ (q,v,o,m) に対応する $\mathrm{HS}_{v,o,m}(t)$
$(11,5,2,4)$	$\frac{(1-z^2)^4}{(1-t)^7}$	100 回	左に同じ
$(11,5,2,5)$	$\frac{(1-z^2)^5}{(1-t)^7}$	100 回	左に同じ
$(11,5,2,6)$	$\frac{-5t^6-9t^5-5t^4+5t^3+9t^2+5t+1}{(1-t)^2}$	100 回	$\frac{t^{64}-t^7-5t^6-9t^5-5t^4+5t^3+9t^2+5t+1}{(1-t)^2}$
$(11,5,2,7)$	$\frac{15t^7-14t^5-14t^4+8t^2+5t+1}{(1-t)^2}$	86 回	左に同じ
$(11,5,2,8)$	$\frac{9t^6+6t^5-22t^4-5t^3+7t^2+5t+1}{(1-t)^2}$	99 回	左に同じ
$(11,5,3,4)$	$\frac{(1-t^2)^4}{(1-t)^8}$	100 回	左に同じ
$(11,5,3,5)$	$\frac{(1-t^2)^5}{(1-t)^8}$	100 回	左に同じ
$(11,5,3,6)$	$\frac{-5t^6-9t^5-5t^4+5t^3+9t^2+5t+1}{(1-t)^3}$	100 回	$\frac{54t^{125}-49t^{124}-6t^{123}+t^7+5t^6+9t^5+5t^4-5t^4-5t^3-9t^2-5t-1}{-(1-t)^3}$
$(11,5,3,7)$	$\frac{15t^7-14t^5-14t^4+8t^2+5t+1}{(1-t)^3}$	100 回	$\frac{8t^{17}-t^{16}-8t^{15}-t^9-5t^8-8t^7+14t^5+14t^4-8t^2-5t-1}{-(1-t)^3}$
$(11,5,3,8)$	$\frac{35t^8-50t^7-14t^6+14t^5+22t^4+5t^3-7t^2-5t-1}{-(1-t)^3}$	90 回	左に同じ

4.2 UOV 多項式の Hilbert 級数の初期実験

ここでは, 実際にパラメータ v,o,m を動かした場合の Hilbert 級数の実験結果を述べる. パラメータを固定しても, さまざまな Hilbert 級数が出てくるため一意に決まらない. そこで, 3.2 の実験で見たように, 斉次二次多項式系を一様ランダムに取った場合 semi-regular system の Hilbert 級数が最も多く出てきたことを参考に, UOV 多項式系を一様ランダムに取った場合の最頻出の Hilbert 級数が何であるかを実験する. さらに, それを $\mathrm{HS}_{v,o,m}(t)$ と比較する. 実験結果を表 2 に記載する. パラメータは $(q,v,o,m)=(11,5,2,4),(11,5,3,4)$ からそれぞれ m を $+1$ ずつ増やしたケースを実験した.

表 2 の実験結果から UOV 多項式系の最頻出の Hilbert 級数について次のことが考察できる:

(Ⅰ) $m \le v$ のとき, Hilbert 級数は $\mathrm{HS}_{v,o,m}(t)$ に一致しており, 多項式系は semi-regular となる.

(Ⅱ) $n=v+o \le m$ のとき, Hilbert 級数は $\mathrm{HS}_{v,o,m}(t)$ に一致している.

(Ⅲ) $n=v+o \ge m$ のときは, o を $+1$ した場合, Hilbert 級数は $\frac{1}{1-t}$ 倍される.

これらの考察は上記のパラメータに対して成り立つものであるので, 4.3 でより広いパラメータに対して同様のことが成り立つかの追加実験を行うこととする.

4.3 追加実験

4.2 の初期実験を受けて, ここでは考察 (Ⅰ), (Ⅱ), (Ⅲ) に関する追加実験を行う.

考察 (Ⅰ) 多くのパラメータで考察 (Ⅰ) が成り立つかを検証する. 方法としては, $m \le v$ を満たす各パラメータ (q,v,o,m) に対して 100 回実験をし, Hilbert 級数が $\mathrm{HS}_{v,o,m}(t)$ に一致した回数を計測した. 表 3 がその結果である.

これから, $m \le v$ の場合の Hilbert 級数は $\mathrm{HS}_{v,o,m}(t)$, つまり $\frac{(1-t^2)^m}{(1-t)^n}$ と予測できる.

表 3 $m \le v$ の場合の UOV 多項式系の Hilbert 級数が $\mathrm{HS}_{v,o,m}(t)$ に一致した回数 (100 回中)

初期パラメータ (q,v,o,m_0)	$(q,v,o,m=m_0+r)$ $r=0$	$r=1$	$r=2$	$r=3$
$(3,7,4,4)$	100	100	100	100
$(3,8,4,5)$	100	100	100	100
$(7,9,4,6)$	100	100	100	100
$(13,10,3,7)$	100	100	100	100
$(31,11,3,8)$	100	100	100	100

考察 (Ⅱ) 同様に, 考察 (Ⅱ) についても $n \le m$ を満たす各パラメータで Hilbert 級数が $\mathrm{HS}_{v,o,m}(t)$ に一致しているかを検証した.

表 4 $n \le m$ の場合の UOV 多項式系の最頻出 Hilbert 級数が $\mathrm{HS}_{v,o,m}(t)$ に一致するかの実験.

初期パラメータ (q,v,o,m_0)	$(q,v,o,m=m_0+r)$ $r=0$	$r=1$	$r=2$	$r=3$
$(3,5,2,9)$	92	99	94	100
$(3,6,3,11)$	94	98	99	100
$(7,6,4,12)$	100	100	97	100
$(13,7,3,12)$	100	100	100	100
$(31,8,3,11)$	100	100	100	100

全ての実験で $\mathrm{HS}_{v,o,m}(t)$ に一致するとは限らなかったが, 高い確率で一致することがわかった. したがって, $n \le m$ の場合でも $\mathrm{HS}_{v,o,m}(t)$ と予測できる.

考察 (Ⅲ) 最後に, 考察 (Ⅲ) に対する実験を行う. つまり, パラメータ (q,v,o,m) が $n=v+o \ge m$ を満たすとき, パラメータ $(q,v,o+1,m)$ の (最頻出)Hilbert 級数が (q,v,o,m) の (最頻出)Hilbert 級数の $1/(1-t)$ 倍であるかをより広いパラメータに対して実験する. 表 5 では, $v+o=m$ が成り立っているパラメータ (q,v,o,m) から, o を $+1$ ずつした場合の 100 回中の最頻出 Hilbert 級数を求め, $1/(1-t)$ 倍

されていることを確認した.

表 5 $v+o=m$ が成り立っているパラメータ (q,v,o,m) から, o を +1 ずつした場合の最頻出 Hilbert 級数の実験

パラメータ (q,v,o,m)	最頻出の Hilbert 級数	現れた回数
$(3,3,2,5)$	$\mathrm{HS}_{3,2,5}(t)$	51
$(3,3,3,5)$	$\mathrm{HS}_{3,2,5}(t)\cdot\frac{1}{(1-t)}$	96
$(3,3,4,5)$	$\mathrm{HS}_{3,2,5}(t)\cdot\frac{1}{(1-t)^2}$	100
$(3,3,5,5)$	$\mathrm{HS}_{3,2,5}(t)\cdot\frac{1}{(1-t)^3}$	100
$(5,4,2,6)$	$\mathrm{HS}_{4,2,6}(t)$	72
$(5,4,3,6)$	$\mathrm{HS}_{4,2,6}(t)\cdot\frac{1}{(1-t)}$	100
$(5,4,4,6)$	$\mathrm{HS}_{4,2,6}(t)\cdot\frac{1}{(1-t)^2}$	100
$(5,4,5,6)$	$\mathrm{HS}_{4,2,6}(t)\cdot\frac{1}{(1-t)^3}$	100
$(7,5,4,9)$	$\mathrm{HS}_{5,4,9}(t)$	84
$(7,5,5,9)$	$\mathrm{HS}_{5,4,9}(t)\cdot\frac{1}{(1-t)}$	100
$(7,5,6,9)$	$\mathrm{HS}_{5,4,9}(t)\cdot\frac{1}{(1-t)^2}$	100
$(7,5,7,9)$	$\mathrm{HS}_{5,4,9}(t)\cdot\frac{1}{(1-t)^3}$	100
$(31,6,4,10)$	$\mathrm{HS}_{6,4,10}(t)$	98
$(31,6,5,10)$	$\mathrm{HS}_{6,4,10}(t)\cdot\frac{1}{(1-t)}$	100
$(31,6,6,10)$	$\mathrm{HS}_{6,4,10}(t)\cdot\frac{1}{(1-t)^2}$	100
$(31,6,7,10)$	$\mathrm{HS}_{6,4,10}(t)\cdot\frac{1}{(1-t)^3}$	100

この実験結果から, $n\geq m$ が成り立っている場合, そこから o を一つ増やすと Hilbert 級数は $1/(1-t)$ 倍されることが予測できる.

4.4 予測公式導出

4.3 の追加実験の結果から UOV 多項式系の最頻出 Hilbert 級数の予測公式が導出できる.

予測公式. パラメータ (q,v,o,m) を持つ UOV 多項式系 $f_1,\ldots,f_m$ が生成するイデアル I の最頻出 Hilbert 級数は以下に一致すると予測できる:

(A) $v\geq m$ の場合,

$$\mathrm{HS}_{R/I}(t)=\frac{(1-t^2)^m}{(1-t)^n}$$

(B) $n\geq m\geq v$ の場合,

$$\mathrm{HS}_{R/I}(t)=\mathrm{SW}\left\{(1+t)^m,\frac{1}{(1-t)^{m-v}}\right\}\cdot\frac{1}{(1-t)^{n-m}}$$

(C) $m\geq n$ の場合,

$$\mathrm{HS}_{R/I}(t)=\mathrm{SW}\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+,\frac{1}{(1-t)^o}\right\}$$

(A), (C) は考察 (I), (II) から従う. (B) が導出される理由は以下の通りである. まず, パラメータ v,o,m は $n=v+o\geq m\geq v$ を満たすので, それとは別にパラメータ $(q,v,m-v,m)$ を持つ UOV 多項式系を考える. これは条件から (C) の場合になるので, その Hilbert 級数は

$$\mathrm{SW}\left\{(1+t)^m,\frac{1}{(1-t)^{m-v}}\right\}\tag{4}$$

で与えられる. そして, $(q,v,m-v,m)$ の oil 次元 $m-v$ に $o-(m-v)=n-m$ を加えれば, 元のパラメータ (q,v,o,m) になるので, 考察 (III) から Hilbert 級数は (4) を $1/(1-t)^{n-m}$ 倍すればよい. そのときそれは (B) に一致する.

以上のように, いくつかの実験によって, UOV 多項式系が生成する Hilbert 級数の予測公式が導出できた.

5. MAYO の安全性解析

この章では, Hilbert 級数予測公式を使って, MAYO [5] の reconciliation attack [12] について考察する.

MAYO への reconciliation attack の計算量評価では, 以下の仮定が使われていた.

(i) 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ の解空間は twisted oil 空間に一致する.
(ii) 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ は semi-regular でない.
(iii) $o-1$ 個の変数 (例えば $x_{v+2},\ldots,x_n$) に 0 を代入すれば, 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ の解空間は 1 次元となる.

ここでは 4.4 で導出した予測公式を使って, それら仮定の妥当性を調べる.

まず (i) について考える. $\mathcal{P}$ が生成するイデアルの Hilbert 級数は補題 1 から $\mathcal{F}=(f_1,\ldots,f_m)$ が生成するイデアル I の Hilbert 級数に一致する. パラメータ (v,o,m) は $m\geq n$ を満たすので, 4.4 から Hilbert 級数は

$$\mathrm{HS}_{R/I}(t)=\mathrm{SW}\left\{\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+,\frac{1}{(1-t)^o}\right\}$$

となる. この場合, $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+$ は t の多項式であるため, Hilbert 級数はある次数 D 以降では $1/(1-t)^o$ に切り替わる. そこで, $1/(1-t)^o$ に切り替わる最小の D を D_{UOV} と書くことにする. これは,

$$D_{UOV}=\min\{d\in\mathbb{N}\mid\langle f_1,\ldots,f_m\rangle_d=\langle x_1,\ldots,x_v\rangle_d\}$$

に一致する. 従って, MAYO の公開鍵 $\{p_1,\ldots,p_m\}$ が生成するイデアル J に対して,

$$J_{D_{UOV}}=\langle x_1\circ\mathcal{S},\ldots,x_v\circ\mathcal{S}\rangle_{D_{UOV}}$$

が成り立つこともわかる. さらに, J の根基イデアル $\sqrt{J}$ は $\langle x_1\circ\mathcal{S},\ldots,x_v\circ\mathcal{S}\rangle$ となる. このことから, $p_1=\cdots=p_m=0$ つまり $\mathcal{P}(\mathbf{x})=\mathbf{0}$ の解空間は twisted oil 空間に一致することがわかる.

次に (ii) について示す. これは, Hilbert 級数 $\mathrm{HS}_{R/I}(t)$

が, 上で述べたことから, $\left[\frac{(1-t^2)^m}{(1-t)^n}\right]_+$ に一致していないため, $\mathcal{P}$ は semi-regular にはならない.

最後に, (iii) を考える. $o-1$ 個の変数 (例えば $x_{v+2},\ldots,x_n$) に 0 を代入することは, 方程式系 $\mathcal{P}(\mathbf{x})=\mathbf{0}$ の解空間を $v+1$ 次元部分空間 $\{(x_1,\ldots,x_{v+1},0,\ldots,0)\in\mathbb{F}_q^n\}$ に制限することであるので, o 次元 twisted oil 空間との交わりは高確率で 1 次元になる. 従って, $\mathcal{P}(\mathbf{x})=\mathbf{0}$ において $o-1$ 個の変数に 0 を代入すれば解空間は 1 次元になる.

以上から, MAYO への reconciliation attack の計算量評価で使われている仮定が, 今回導出した予測公式によって, 妥当であることが分かった.

6. おわりに

この論文では, UOV 多項式系が生成するイデアルの Hilbert 級数について考えた. 具体的には, いくつかのケースを計算機実験することで Hilbert 級数の予測公式を導出した. さらに, その結果を使い UOV の変種である MAYO に対する reconciliation attack の解析を行うことができた. これは計算量評価を変えないが MAYO の構造を詳しく知る上で欠かせない結果であると考える.

今後の課題として, 今回の考察を元にした reconciliation attack の改良や, UOV 以外に HFE や QR-UOV などの Hilbert 級数の予測公式がどのようになるのか, が考えられる. また, ここで与えた予測公式がなぜ導き出されるのかを説明することも課題であり, それには, semi-regular の定義のように, 対応するイデアルの代数的性質を求めることが必要となると思われる.

謝辞 本研究の一部は, JSPS 科研費 JP22K17889 の助成を受けたものです.

参考文献

[1] Bardet, M., Faugère, J.C., Salvy, B. and Yang, B.Y.: Asymptotic behavior of the index of regularity of quadratic semi-regular polynomial systems, 8th International Symposium on Effective Methods in Algebraic Geometry (MEGA), pp.1-14 (2005)

[2] Bernstein, D.J., Buchmann, J. and Dahmen, E. (Eds.): Post-Quantum Cryptography, Springer (2009).

[3] Bettale, L., Faugère, J.C. and Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology, 3: 177- 197 (2009).

[4] Beullens, W.: Improved Cryptanalysis of UOV and Rainbow, EUROCRYPT 2021, pp.348-373.

[5] Beullens, W.: MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps, SAC 2021, pp.355-376.

[6] Beullens, W.: Breaking Rainbow Takes a Weekend on a Laptop. IACR Cryptol. ePrint Arch. 2022/214.

[7] Courtois, N.T., , Klimov, A., Patarin J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, EUROCRYPT 2000, pp.392-407

[8] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language, J. Symbolic Comput, Vol.24, pp.235-265 (1997).

[9] Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D.S. and Yang, B.Y.: Rainbow, Technical report, National Institute of Standards and Technology, Post-Quantum Cryptography, ⟨https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-submissions⟩

[10] Ding, J., Gower, J.E. and Schmidt, D.S.: Multivariate Public Key Cryptosystems, Springer (2006).

[11] Ding, J. and Schmidt, D.S.: Rainbow, a new multivariate polynomial signature scheme, ACNS 2005, LNCS, Vol.3531, pp.164–175, Springer (2005).

[12] Ding, J., Yang, B.Y., Chen, C.H.O., Che, M.S. and Cheng, C.M.: New differential-algebraic attacks and reparametrization of Rainbow. ACNS 2008, LNCS, Vol. 5037, pp. 242-257. Springer (2008).

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

[14] Faugère, J.C.: A new efficient algorithm for computing Gröbner Bases without reduction to zero (F5), ISSAC 2002, pp. 75-83 (2002).

[15] Furue H., Ikematsu Y., Kiyomura Y., Takagi T.: A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. ASIACRYPT 2021, pp.187-217

[16] Kipnis, A., Patarin, L. and Goubin, L.: Unbalanced Oil and Vinegar Schemes, EUROCRYPT 1999, LNCS, Vol.1592, pp.206-222, Springer (1999).

[17] Kipnis, A. and Shamir, A.: Cryptanalysis of the Oil and Vinegar signature scheme. *CRYPTO 1998*, LNCS, Vol.1462, pp. 257-266. Springer (1998).

[18] Matsumoto, T. and Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, *EUROCRYPT 1988*, LNCS, Vol.330, pp. 419–453, Springer (1988).

[19] National Institute of Standards and Technology, Post-Quantum Cryptography Standardization, ⟨https://csrc.nist.gov/projects/post-quantum-cryptography⟩

[20] Wiedemann, D.: Solving sparse linear equations over finite fields, IEEE Trans. Inform. Theory, 32(1), pp. 54–62, 1986.