

A-24 多変数多項式ベース署名方式 UOV の公開鍵の安全性に関する考察

平岡美咲, 工藤桃成
(福岡工業大学情報工学部情報通信工学科)

1. はじめに

量子計算機の出現によりRSA暗号や楕円曲線暗号は危殆化するとされ、耐量子計算機暗号の研究が進められている。その一つが多変数多項式(MQ)問題の求解困難性に基づく公開鍵暗号である。MQ問題とは、有限体上の2次多項式系を解く問題であり、署名方式UOV (Unbalanced Oil and Vinegar) [1]はその代表例である。UOVの安全性に関する議論では、公開鍵多項式の係数(特に2次斉次部分の係数)が独立一様に分布すると仮定して議論がなされる。本研究では、この仮定に着目し、その妥当性を統計的な手法により評価する。

2. 多変数多項式ベース署名方式UOV

UOVのパラメータは、自然数 n, o, v (但し $n = v + o$ か $o < v$) と素数 q である。以下では、要素数 q の有限体を \mathbb{F}_q と表す。また、自然数 k に対して、 \mathbb{F}_q の要素を成分にもつ k 次元ベクトルの全体を \mathbb{F}_q^k と表す。**■鍵生成** 各 $i \in \{1, 2, \dots, o\}$ に対し、有限体 \mathbb{F}_q 上の n 変数2次多項式 $f_i(x_1, \dots, x_n)$ をランダムに生成する。但し、 f_i は x_{v+i}, \dots, x_n のみからなる2次の項をもたないとする。その上で、 $F = (f_1, \dots, f_o)$ とおく。次に、 \mathbb{F}_q 上の n 次正則行列 S をランダム生成する。そして、 $P = (f_1((x_1, \dots, x_n) \cdot S), \dots, f_o((x_1, \dots, x_n) \cdot S))$ を求める。その上で公開鍵を P 、秘密鍵を (F, S) とする。

■署名生成 平文としてベクトル $M = (M_1, \dots, M_o) \in \mathbb{F}_q^o$ を選び、連立方程式 $f_i(x_1, \dots, x_n) = M_i$ ($i = 1, \dots, o$) の解 $a = (a_1, \dots, a_n) \in \mathbb{F}_q^n$ を1つ求める。その上で $s = a \cdot S^{-1} \in \mathbb{F}_q^n$ を計算し、 s を署名値とする。

■検証 平文 M 、署名 s 、公開鍵 P に対し、 $P(s) = M$ が成り立てば検証成功とする。

UOVの推奨パラメータとしては、 $(n, o, v, q) = (244, 96, 148, 256)$ などがあり、 q として奇素数を用いる場合は大きさの近い $q = 257$ が用いられる。

3. 実験方法

パラメータ組 (n, o, v, q) を固定し、標本数を N とする。ただし、 $v/o \approx 3/2$ とする。本実験では、2節で述べた鍵生成を N 回繰り返す、公開鍵 P を N 個生成する。生成された公開鍵を $P^{(i)} = (p_1^{(i)}, \dots, p_o^{(i)})$ ($1 \leq i \leq N$) とする。以下の方法で χ^2 検定を行う。

1) **一様性(係数別)検定** $s = n(n+1)/2$ とおき、 x_1, \dots, x_n に関する2次単項式の全てを t_1, \dots, t_s とおく。各 t_k に対し、以下を実行する。

1-1) 各 $i \in \{1, \dots, N\}$ に対し、 $P^{(i)}$ から無作為に $p_j^{(i)}$ を選び、 t_k の係数を標本として保存する。

1-2) 1-1)で得られた N 個の標本が \mathbb{F}_q 上の離散一様分布に従っていないことを帰無仮説として、 χ^2 統計量を用いて適合度検定を行う。ここで、自由度は $q-1$ である。

2) **独立性(係数ペア)検定** 各単項式ペア (t_i, t_j) ($1 \leq i < j \leq s$) に対し、1)と同様の方法で N 個の標本(各標本は t_i の係数と t_j の係数のペア)を抽出し、独立性を判定する。自由度は $(q-1)^2$ であることに注意する。これをもとに、 p 値を算出して棄却率を評価する。

いずれの検定も有意水準を $\alpha = 0.05$ とし、 $p < \alpha$ となる割合を棄却率とする。 $p \leq \alpha$ で帰無仮説を棄却するものとする。一様性検定では、これに加えて p 値の平均値、中央値及び χ^2 統計量の平均を算出する。独立性検定では、多項式ごとの棄却率を比較し、平均値とばらつきを評価する。多重検定補正は行わず、各検定を独立に扱う。

5. 実験結果

パラメータ組 $(n, o, v, q) = (60, 24, 36, 257)$ について、標本数を $N = 3000$ に設定し、3節で説明した実験を行った。この条件において、 χ^2 検定の適用条件(独立性・十分な期待度数)はいずれも満たされていることに注意する。具体的には、期待度数は一様性検定では $N/q \approx 11.7 > 5$ 、独立性検定では $N/q^2 \approx 3.5 > 5$ である。また、実験環境は次の通りである。

OS: Windows 10 Home 64bit

CPU: AMD Ryzen3 4300U with Radeon Graphics

メモリ: 8GB, 開発環境: VScode

Python(実行にはJupyter Notebook拡張機能を使用)実験の結果、一様性、独立性ともに棄却率は理論期待5%と整合した。まず、表1に、一様性検定の結果 $(n(n+1)/2)$ 回の平均)を示す。 p 値の平均および中央値はいずれも0.5付近であり、統計量の平均値も自由度256に近く、係数分布は理論上一様分布と矛盾しなかった。

表1: 検定1の結果

棄却率	χ^2 値の平均	p 値の平均	p 値の中央値
5.495%	256.1	0.498	0.494

表2に示す独立性検定の結果では、棄却率は全体で約5.5%に留まり、多項式ごとの差も1本あたり約9.7万ペア中80件程度と小さく、独立性仮定と矛盾しなかった。

表2: 検定2の結果

多項式1本あたりの検定ペア数	棄却率	多項式ごとの棄却率平均
97159	5.49%	$\pm 0.08\%$

以上より、係数分布の一様性・独立性はいずれも統計的に矛盾を示さず、公開鍵係数が独立一様ランダムに生成されたとする仮定と整合的である。

6. まとめと今後の課題

本稿では、多変数多項式ベース署名方式UOVの公開鍵多項式について、その係数が独立一様ランダムに生成された場合と同様に振舞うことを、 χ^2 検定により実験的に確認した。今後の課題として、(1) 他の n, v, q や拡大体(特に $q = 2^m$) の場合、(2) 標本数を増やした場合、(3) χ^2 検定以外の手法による検証、などが挙げられる。これらの課題に取り組み、UOVの公開鍵多項式における係数の分布仮定について、より広範な範囲のパラメータ組に対し妥当性を確認したい。

参考文献

[1] A. Kipnis, J. Patarin, and L. Goubin: Unbalanced oil and vinegar signature schemes, In: Proceedings of EUROCRYPT 1999, LNCS, pp.206-222, Springer, 1999.