多変数署名方式と その安全性解析について

池松 泰彦
(九州大学マス・フォア・インダストリ研究所)

情報数理セミナー@日大

2024年8月21日

Institute of Mathematics for Industry
Kyushu University

概要

- ✓ 多変数多項式問題を使った暗号技術がある(MPKC)
- ✓ UOVが昔から生き残っている方式として知られている
- ✓ アメリカの標準化コンペにおいてUOVが注目を集めている
- ✓ UOVは署名長が短く・処理効率が良い

解説内容

- MPKC、特にUOVを解説
- 安全性解析について時間が許す限り説明

§1 研究背景

■ 暗号理論

公開鍵暗号基盤

RSA暗号(1978)
楕円曲線暗号(1985)

耐量子計算機暗号(Post-Quantum Cryptography)

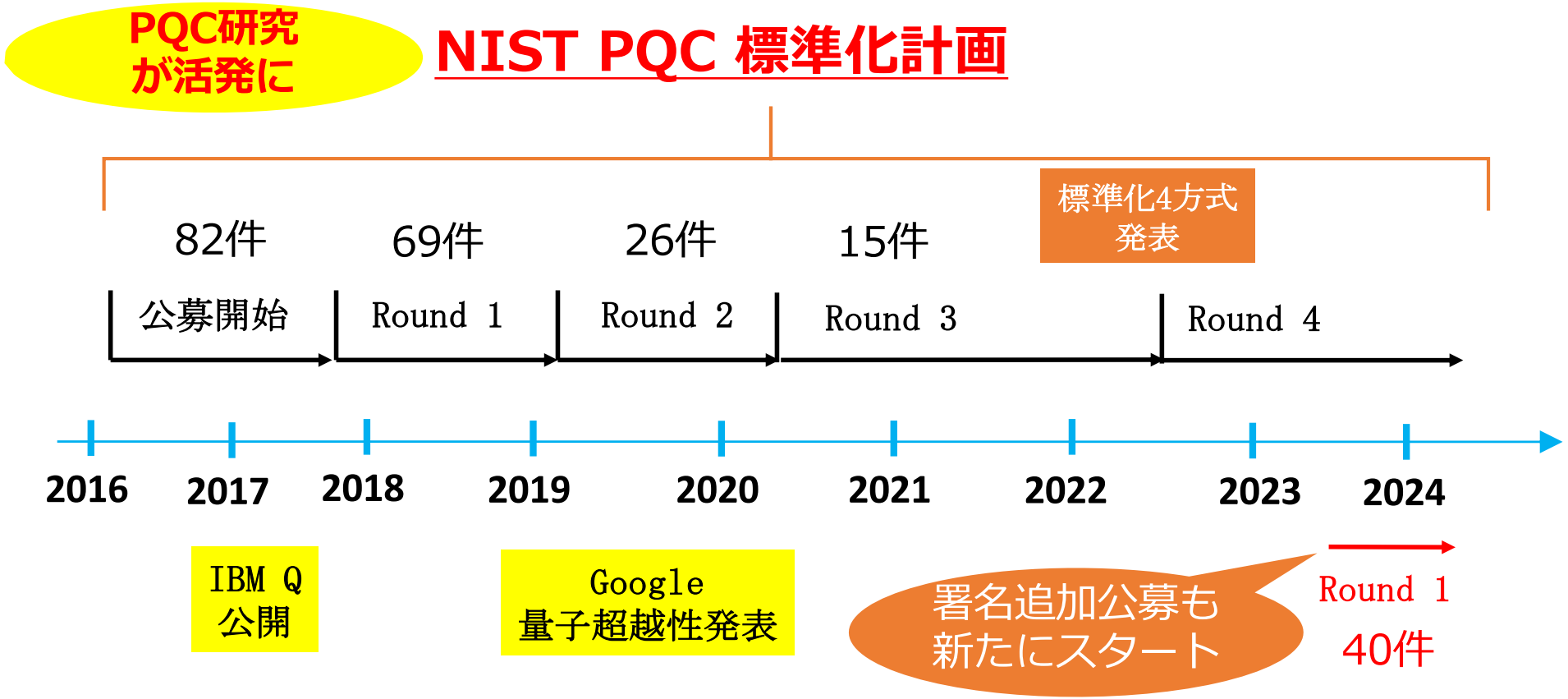
■ いつまでに？

- ✓ 大規模量子計算機の開発にはまだまだ時間はかかると予想されている
- ✓ しかし暗号の変更・移行はかなりの労力・期間を要する
- ✓ さらに今ある暗号文が量子計算機開発後に解読される可能性も
- ✓ そのため、PQCの開発は喫緊の課題である

§2 NIST PQC標準化計画

- **デジタル署名，公開鍵暗号，鍵共有の3つの暗号アルゴリズムを選定し標準化するための(アメリカの)プロジェクト**

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



NIST・・・National Institute of Standards and Technology (アメリカ国立標準技術研究所)

https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

§3 PQCの研究

■ PQCには素因数分解、離散対数以外の数学問題が使われる

- **格子問題・・・格子の最短ベクトル、最近ベクトル探索**
- **符号問題・・・ランダム誤り訂正符号の復号**
- **同種写像問題・・・楕円曲線間の同種写像計算**
- **多変数多項式問題・・・多変数二次連立方程式の求解**

第一回NIST PQC標準化では1つも選ばれなかった

■ 現在、暗号の重要な転換期にある

- 今標準化されると今後長く使用される
- 多変数多項式から標準化される方式を開発したい!

§4 多変数多項式暗号(MPKC)

■ 多変数多項式暗号(Multivariate Public Key Cryptography)

✓ 多変数二次多項式問題(MQ問題)の求解困難性を利用した暗号技術

例: 次の $\mathbb{F}_{31}$上の連立二次多項式を考える：

$$p_1 = 11x_1^2 + 24x_1x_2 + 5x_1x_3 + 22x_2^2 + x_2x_3 + 17x_3^2,$$
$$p_2 = 27x_1^2 + 29x_1x_2 + 24x_2^2 + 27x_2x_3 + 19x_3^2,$$
$$p_3 = 4x_1^2 + 6x_1x_2 + x_1x_3 + 25x_2^2 + 27x_2x_3 + 26x_3^2.$$

$$P := (p_1, p_2, p_3) : \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$

$(x_1, x_2, x_3) = (0,1,1)$ ⟹ $P(0,1,1) = (9,8,16)$ 代入計算は易しい

$P(x_1, x_2, x_3) = (9,8,16)$ ⟹ $(x_1, x_2, x_3) = \pm(0,1,1)$ 求解は難しい

✓ 1988年に日本の松本・今井らにより導入[1]

✓ 耐量子計算機暗号(PQC)の候補として現在活発に研究されている

✓ NIST PQC 追加公募ではUOV[2]が注目を集めている

NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV).

[1] Matsumoto, T et al.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, EUROCRYPT1988
[2] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes, EUROCRYPT'99

§5 MQ問題

■ MQ (Multivariate Quadratic) 問題

$p_1, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$ 二次多項式

$$p_1(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_i^{(1)} x_i + c^{(1)},$$

$$\vdots$$

$$p_m(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_i^{(m)} x_i + c^{(m)}.$$

Find $z \in \mathbb{F}_q^n$ s.t. $p_1(z) = \cdots = p_m(z) = 0$.

この問題はNP-完全であることが示されている[GJ79]

[GJ79] M. R. Garey et al., Computers and Intractability: A guide to the theory of NP-completeness

■ Fukuoka MQ Challenge*

- ✓ MQ問題の困難性評価を目的としたコンテスト
- ✓ 問題は6つのTypeに分かれる

Type	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ
$GF(q)$	$GF(2)$	$GF(256)$	$GF(31)$	$GF(2)$	$GF(256)$	$GF(31)$
変数	n	n	n	n	n	n
式数	$2n$	$2n$	$2n$	$2n/3$	$2n/3$	$2n/3$

Type Ⅰ, Ⅱ, Ⅲは暗号方式、Type Ⅳ, Ⅴ, Ⅵは署名方式に対応する

*https://www.mqchallenge.org

Fukuoka MQ Challenge

Type I | Type II | Type III | Type IV | Type V | Type VI

	Number of Variables (n)	Seed (0,1,2,3,4)	Date	Contestants	Computational Resource	Data
1	38	3	2020/08/03	Tung Chou, Ruben Niederhagen, Bo-Yin Yang	XL with block Wiedemann, 2x AMD EPYC 7742	Details
2	37	1	2019/06/27	Takuma Ito, Naoyuki Shinohara, Shigenori Uchiyama	F4-style based algorithm to solve MQ problems, 4 x Intel(R) Xeon(R) CPU E5-4669 v4, 2.20GHz, 1TB RAM	Details
3	37	0	2020/07/03	Tung Chou, Ruben Niederhagen, Bo-Yin Yang	XL with block Wiedemann, 2x AMD EPYC 7742	Details

§6 一般的構成

■ 定義. 二次中心写像

$$f_1(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(1)} x_i x_j,$$
$$\vdots$$
$$f_m(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(m)} x_i x_j$$

$F := (f_1, \dots, f_m): \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ を二次写像として，
任意の元 $d \in \mathbb{F}_q^m$ に対して，$F(x) = d$ は少ない計算量で解けるもの.

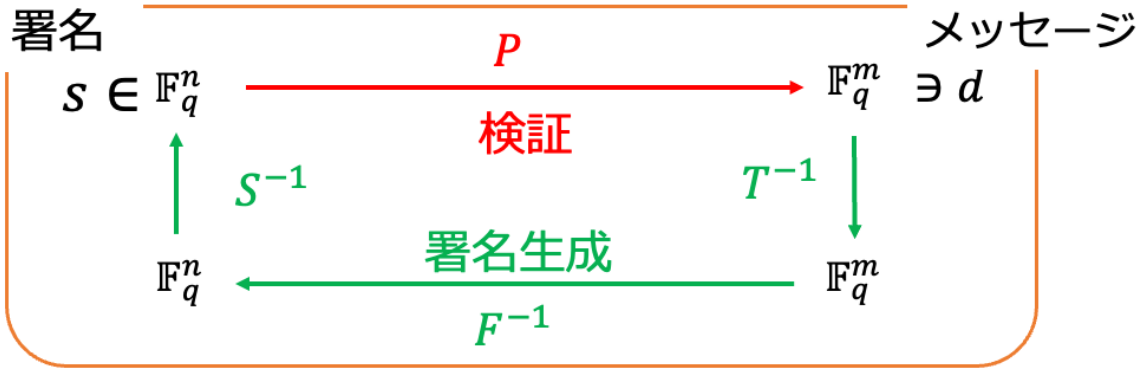
■ 秘密鍵

$F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ 二次中心写像

$S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$
$T : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$) ランダムな可逆な線型写像

■ 公開鍵 $P := T \circ F \circ S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ 二次写像 Fの構造が隠れる

$= (p_1, \dots, p_m)$



MQ問題が安全性と関連している

§7 Unbalanced Oil Vinegar(UOV)

次の$\mathbb{F}_5$上の二次方程式の解は簡単に見つかる!

$$f_1 \coloneqq 2x_1^2 + x_1x_2 + x_2^2 + x_2x_3 + x_3^2 + x_1x_4 + x_2x_4 + x_3x_5 = 1$$

$$f_2 \coloneqq x_1^2 - x_1x_2 + 2x_2^2 + x_2x_3 - x_3^2 + x_1x_5 - x_2x_4 + x_3x_4 - x_3x_5 = 2$$

$$S = \begin{pmatrix} -1 & 1 & -1 & 0 & 1 \\ 0 & 3 & 1 & 2 & 3 \\ -1 & 2 & -1 & 2 & 3 \\ 3 & 0 & 3 & 0 & 0 \\ 0 & 1 & 3 & 1 & 3 \end{pmatrix}$$

$g_i \coloneqq f_i(x \cdot S)$ を計算すると

$$g_1 = x_1^2 + 2x_1x_2 + 2x_2^2 - x_2x_3 + 2x_3^2 + x_1x_4 + 2x_1x_5 - x_2x_4 - x_2x_5 - x_3x_4 + x_3x_5 + x_4^2 + x_4x_5 + 3x_5^2 = 1$$

$$g_2 = 2x_1^2 - x_1x_3 + 3x_2^2 + 2x_3^2 + 3x_1x_5 + 3x_2x_5 + x_3x_4 + 2x_3x_5 - x_5^2 = 1$$

§8 UOVの一般的構成

■ パラメータ: $v, o \in \mathbb{N}$, $n = v + o$

$$x = (x_1, \ldots, x_v), \quad x' = (x_{v+1}, \ldots, x_{v+o}), \quad n\text{-変数}$$

vinegar変数　　oil変数

■ UOV 中心多項式

係数は$\mathbb{F}_q$から全てランダムに選択する

$$f_1(x, x') = \sum a_{i,j}^{(1)} x_i x_{v+j} + quad\ poly.\ in\ x$$
$$\vdots$$
$$f_o(x, x') = \sum a_{i,j}^{(o)} x_i x_{v+j} + quad\ poly.\ in\ x$$

■ UOV 秘密鍵

$$F := (f_1, , \ldots, f_o) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^o$$
$$S: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \qquad \text{正則線型写像}$$

■ UOV 公開鍵

$$P := F \circ S = (p_1, , \ldots, p_o) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^o$$

§9 UOVのパラメータ

1999年 Unbalanced Oil & Vinegar (UOV)署名方式が提案される[1]

◘NIST追加公募で提案されたパラメータ(by Beullens et al.)

NIST security category	parameter (q, v, o)	Public key size	Sign size
I	$(16,96,64)$	66.6 KB	96 B
I	$(256,68,44)$	43.6 KB	128 B
III	$(256,112,72)$	189.2 KB	200 B
V	$(256,148,96)$	446.9 KB	260 B

✓ 公開鍵サイズが格子・同種ベースと比べて大きい

✓ UOVの改良方式がNISTの追加公募にいくつも投稿された