耐量子計算機暗号と量子情報の数理

多変数多項式暗号１：署名方式の構成

古江 弘樹

東京大学 情報理工学系研究科 数理情報学専攻 博士課程2年

2022/8/4

概要

耐量子計算機暗号（Post Quantum Cryptography）

- **多変数多項式暗号**
  - 有限体上の二次多項式系の求解問題（MQ 問題）に基づいて構成
- 格子暗号
- 同種写像暗号
- 符号暗号
- ハッシュ関数署名

本講演では
署名方式の構成法を
中心に紹介していく

NIST PQC における多変数多項式暗号

NIST Post-Quantum Cryptography Standardization

- Round 1 2017/12~

  多変数多項式暗号 9 / 69 件（署名方式：7 件、暗号方式：2 件）

- Round 2 2019/01~

  多変数多項式暗号 4 / 26 件（署名方式：4 件、暗号方式：0 件）

- Round 3 2020/07~

  多変数多項式暗号 2 / 15 件（署名方式：2 件、暗号方式：0 件）

  (Finalist: **Rainbow**, Alternate candidate: **GeMSS**)

- Selected Algorithms, Round 4 には選ばれなかった

目次

- **多変数多項式暗号**
- Matsumoto-Imai
- HFE
- UOV
- Rainbow
- QR-UOV
- まとめ

MQ 問題

$\mathbb{F}_q$：要素数 q の有限体

有限体 $\mathbb{F}_q$ 上の連立二次方程式の求解問題

- n : 変数の数
- m : 多項式の数

MQ (Multivariate Quadratic equations) 問題

Given $\mathcal{F} = (f_1, \ldots, f_m) \in \mathbb{F}_q[x_1, \ldots, x_n]^m$ with $\deg f_i = 2$,

find *one* solution $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$ such that

$$\mathcal{F}(a_1, \ldots, a_n) = \mathbf{0} \in \mathbb{F}_q^m.$$

多変数多項式暗号

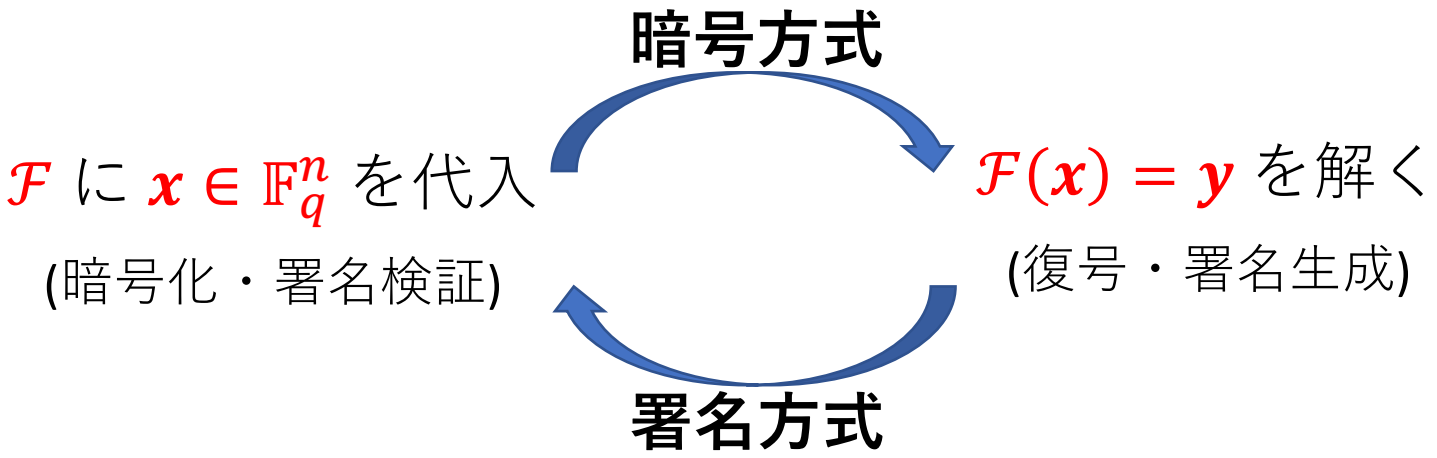
MQ function $\mathcal{F}$

・解を求めるのは困難 (**NP-complete** [Garay and Johnson, 79])

・解を確かめるのは容易

$\mathcal{F}$ に解 $(a_1, \ldots, a_n)$ を代入すれば良い

秘密鍵を利用すれば効率的に解の計算が可能な $\mathcal{F}$ を準備

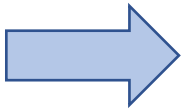


多項式の次数について

次数が 3 次以上の多項式は使用しないのか？

・ひとつの多項式あたりのデータサイズが増える

n 変数 2 次
$\binom{n+2}{2}$ 単項式



n 変数 3 次
$\binom{n+3}{3}$ 単項式

・安全性が飛躍的に向上するわけではない

2 次のケースでの求解手法 (F4, F5, XL) がそのまま適用可能

・いくつかの手法が提案されている

Cubic UOV [X. Nie et al., Inscrypt'15]
Cubic ABC [Ding et al., PQCrypto'14]
Cubic MFE [Lu et al., Int. J. Netw. Secur.'18]

多変数多項式署名

以降、署名方式に話を限定する

- Round 2 以降の多変数多項式暗号は全て署名方式
- いくつかの暗号方式が提案されている

  （そのうち多くに対して効率的な攻撃手法が提案）

  - Matsumoto-Imai (Encryption) [Matsumoto, Imai, EUROCRYPT 1988]
  - Simple Matrix (ABC) encryption scheme [Tao et al., PQCrypto 2013]
  - Rectangular Simple Matrix [Tao et al., Finite Fields Th. App. 2015]
- 次ページより、標準的な署名方式の構成方法を紹介

  ※ 例外：Identification Scheme に基づいた構成（MQDSS など）

  [Chen et al., ASIACRYPT 2016]

鍵生成

・ n ：変数の数
・ m : 多項式の数　　$(n \geq m)$

① **中心写像 [Central map]**

$\mathcal{F} = (f_1, \ldots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m$　　**[quadratic map]**

・$\forall \boldsymbol{y} \in \mathbb{F}_q^m$ に対して、$\mathcal{F}(\boldsymbol{x}) = \boldsymbol{y}$ をみたすひとつの $\boldsymbol{x} \in \mathbb{F}_q^n$ を効率的に計算可能（以降 $\mathcal{F}^{-1}$ と表記）

・構成方法は各方式に依存

$\mathcal{F}$ の構造を隠す

② $\mathcal{T}: \mathbb{F}_q^m \to \mathbb{F}_q^m, \mathcal{S}: \mathbb{F}_q^n \to \mathbb{F}_q^n$ **[affine map]**

③ $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$　　**[quadratic map]**

Public Key: $\mathcal{P}$, Secret Key: $(\mathcal{T}, \mathcal{F}, \mathcal{S})$

署名生成と検証方法

Alice: $(\mathcal{T}, \mathcal{F}, \mathcal{S})$

Message : $\boldsymbol{m} \in \mathbb{F}_q^m$

Signature

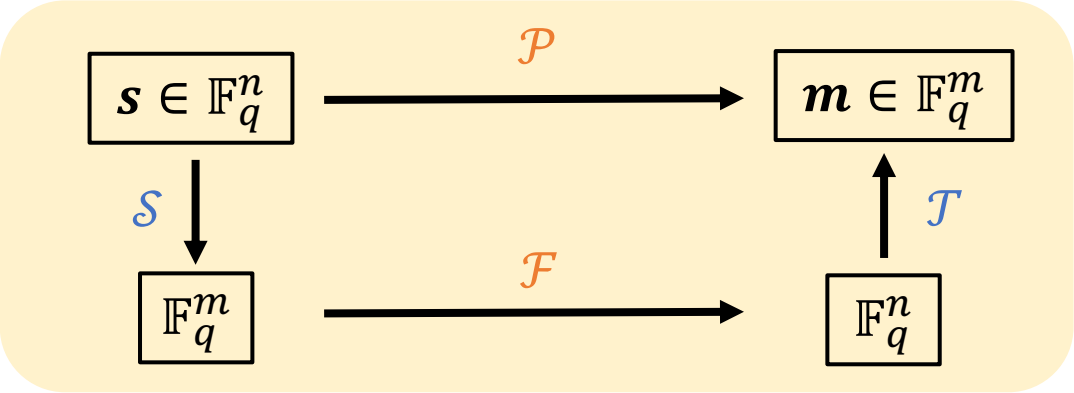
$$\boldsymbol{s} = \underbrace{\mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}}_{\mathcal{P}^{-1}}(\boldsymbol{m})$$

$\boldsymbol{m}, \boldsymbol{s}$

Bob: $\mathcal{P}$

Verification

$$\boldsymbol{m} \stackrel{?}{=} \underbrace{\mathcal{P}(\boldsymbol{s})}_{\mathcal{P} \circ \mathcal{P}^{-1}(\boldsymbol{m})}$$



特徴

Advantage

・署名長が小さい

ex) Rainbow (Round 3) は Security Level (SL) 1 で約 500 bits

約 140-bit security

・効率的な実装が可能

比較的小さいサイズの有限体上で構成可能（$\mathbb{F}_{2^8}$ など）

Disadvantage

・多くの方式で安全性証明が存在しない

・公開鍵、秘密鍵のサイズが大きい

一般的に $O(mn^2)$　　ex) Rainbow (Round 3) の公開鍵は SL1 で約 50 KB

安全性

多くの方式で安全性証明はなされていない

（例外：MQDSS など）

以下の 2 つの問題の困難性に依拠すると考えられている

- **MQ problem**
- **Extended Isomorphism of Polynomials (EIP) problem**

> $\mathcal{P}(=\mathcal{T}\circ\mathcal{F}\circ\mathcal{S})$ を入力として、$(\mathcal{T},\mathcal{F},\mathcal{S})$ もしくは同様の性質を満たす $(\mathcal{T}',\mathcal{F}',\mathcal{S}')$ を求める問題。

MQ, EIP に対する求解アルゴリズムの

計算量を考慮してパラメータが設定されている

行列表現

二次多項式：$p_k(x_1, \ldots, x_n) = \sum_{i \le j} a_{i,j} x_i x_j$

$$MP_k = \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \cdots & a_{2,n} \\ 0 & 0 & a_{3,3} & & a_{3,n} \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 0 & a_{n,n} \end{bmatrix} \in \mathbb{F}_q^{n \times n}$$

$$p_k(x_1, \ldots, x_n) = (x_1, \ldots, x_n) \cdot MP_k \cdot (x_1, \ldots, x_n)^\top$$

※ $(n+1) \times (n+1)$ 行列を用いることで、
線形項・定数項を表現可能

・用途に応じて**対称行列**を用いる

行列表現

公開鍵: $\mathcal{P} = (p_1, \ldots, p_m) \Rightarrow MP_1, \ldots, MP_m$

秘密鍵: $\mathcal{F} = (f_1, \ldots, f_m) \Rightarrow MF_1, \ldots, MF_m$

$\mathcal{S}$: $\mathbb{F}_q^n \to \mathbb{F}_q^n \Rightarrow MS \in \mathbb{F}_q^{n \times n}$

※ $\mathcal{S}(x_1, \ldots, x_n) = (x_1, \ldots, x_n) \cdot MS$

$\mathcal{T}$: $\mathbb{F}_q^m \to \mathbb{F}_q^m \Rightarrow MT \in \mathbb{F}_q^{m \times m}$

※ $\mathcal{T}(x_1, \ldots, x_m) = (x_1, \ldots, x_m) \cdot MT$

$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ より

$$(MP_1, \ldots, MP_m) = (MS \cdot MF_1 \cdot MS^{\top}, \ldots, MS \cdot MF_n \cdot MS^{\top}) \cdot MT$$

多変数多項式署名

Big Field

Matsumoto-Imai [1988]

HFE [1996]

SFLASH [2002]

HFEv- [1999]

- Gui [2015]
- GeMSS [2017]

Small Field

OV [1997]

UOV [1999]

- Rainbow [2005]
- LUOV [2017]
- QR-UOV [2021]
- MAYO [2021]

NIST round 1 and 2 candidates

NIST round 3 candidates

本講演で取り扱う手法

目次

- 多変数多項式暗号
- **Matsumoto-Imai**
- HFE
- UOV
- Rainbow
- QR-UOV
- まとめ

Big Field

Small Field

Matsumoto-Imai (MI) [Matsumoto, Imai, EUROCRYPT 1988]

- Matumoto, Imai によって 1988 年に提案
- 最初に提案された多変数多項式暗号方式のひとつ
- 1995 年に Patarin によって攻撃手法が提案 [Patarin, CRYPTO 1995]
- HFE などが本方式に基づいて構成されている

準備

- $q = 2^r$
- $g(t) \in \mathbb{F}_q[t]$：既約多項式（次数 n）
- $\mathbb{E} = \mathbb{F}_q[t]/g(t) \cong \mathbb{F}_{q^n}$
- ϕ: $\mathbb{F}_q^n \rightarrow \mathbb{E}$

$$(x_1, \ldots, x_n) \longmapsto x_1 + x_2 t + \cdots + x_n t^{n-1}$$

$1, t, t^2, \ldots, t^{n-1}$ は $\mathbb{E}$ の $\mathbb{F}_q$ 上の基底

Central Map

$\mathcal{F}$ の構成法

$$0 < \theta < n,\ \gcd\left(q^n - 1, q^\theta + 1\right) = 1$$

$$\bar{\mathcal{F}}(X) = X^{q^\theta+1} : \mathbb{E} \to \mathbb{E}$$

$$\mathcal{F} = \phi^{-1} \circ \bar{\mathcal{F}} \circ \phi : \mathbb{F}_q^n \to \mathbb{F}_q^n$$

$\bar{\mathcal{F}}$ の構造を利用した
攻撃によって破られた
[Patarin, CRYPTO 1995]

$\mathcal{F}^{-1}$ ($\bar{\mathcal{F}}^{-1}$) の計算方法

$\gcd\left(q^n - 1, q^\theta + 1\right) = 1$ より、

$h\left(q^\theta + 1\right) \equiv 1\ mod\ (q^n - 1)$ となる整数 h が存在

$Y = \bar{\mathcal{F}}(X) = X^{q^\theta+1}$ とおくと

$$Y^h = X^{h\left(q^\theta+1\right)} = X^{k(q^n-1)+1} = X$$

Central Map

・ $\mathcal{F}$ は二次多項式系　$(X = x_1 + x_2 t + \cdots + x_n t^{n-1})$

$$X^{q^\theta+1} = X^{q^\theta} \cdot X$$

$(x_1 + x_2 t + \cdots + x_n t^{n-1})^q$

$= x_1^q + (x_2 t)^q + \cdots + (x_n t^{n-1})^q$

$= x_1 + x_2 t^q + \cdots + x_n t^{(n-1)q}$

$1, t, \ldots, t^{n-1}$ の線形和で記述可能

各係数の次数は1次

$x_1 + x_2 t + \cdots + x_n t^{n-1}$

各係数の次数は1次

$X^{q^\theta+1}$ の各係数は $x_1, \ldots, x_n$ についての2次式

例

- $q = 2, n = 3, \theta = 2$
- $\mathbb{E} = \mathbb{F}_2[t]/(t^3 + t + 1)$
- $\bar{\mathcal{F}}(X) = X^{q^\theta+1} = X^5$

$$\bar{\mathcal{F}} \circ \phi(x_1, x_2, x_3) = (x_1 + x_2 t + x_3 t^2)^5$$

$$= (x_1 + x_2 t + x_3 t^2)^4 \cdot (x_1 + x_2 t + x_3 t^2)$$

$$= (x_1 + x_2 \underbrace{t^4}_{= t + t^2} + x_3 \underbrace{t^8}_{= t^2}) \cdot (x_1 + x_2 t + x_3 t^2)$$

$$= (x_1 + x_2 t + (x_2 + x_3) t^2) \cdot (x_1 + x_2 t + x_3 t^2)$$

$$= (x_1^2 + x_2^2) + (x_2^2 + x_2 x_3 + x_3^2) t + (x_1 x_2 + x_2^2 + x_2 x_3 + x_3^2) t^2$$

Central map

$\mathcal{F} = (f_1, f_2, f_3)$

$$f_1 = x_1^2 + x_2^2$$
$$f_2 = x_2^2 + x_2 x_3 + x_3^2$$
$$f_3 = x_1 x_2 + x_2^2 + x_2 x_3 + x_3^2$$

目次

- 多変数多項式暗号
- Matsumoto-Imai
- **HFE**
- UOV
- Rainbow
- QR-UOV
- まとめ

HFE

[Patarin, EUROCRYPT 1996]

Hidden Fields Equations (HFE)

- 1996 年に Patarin によって提案
- MI を攻撃手法に対して安全化する形で提案

$\mathcal{F}$ の構成法　$D \in \mathbb{N}$

$$\bar{\mathcal{F}}(X) = \sum_{i,j=0}^{q^i+q^j \le D} \alpha_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \le D} \beta_i X^{q^i} + \gamma$$

$$(\alpha_{ij}, \beta_i, \gamma \in \mathbb{E})$$

$$\mathcal{F} = \phi^{-1} \circ \bar{\mathcal{F}} \circ \phi$$

MI から構成を一般化

(MI: $\bar{\mathcal{F}}(X) = X^{q^\theta+1}$)

HFE

$$\bar{\mathcal{F}}(X) = \sum_{i,j=0}^{q^i+q^j \le D} \alpha_{ij} X^{q^i+q^j} + \sum_{i=0}^{q^i \le D} \beta_i X^{q^i} + \gamma$$

$$= X^{q^i} \cdot X^{q^j}$$

それぞれ $1, t, \ldots, t^{n-1}$ の各係数は

$x_1, \ldots, x_n$ についての一次式　$(X = x_1 + x_2 t + \cdots + x_n t^{n-1})$

（MI と同様）

$\mathcal{F}^{-1}$ ($\bar{\mathcal{F}}^{-1}$) の計算方法

・$\bar{\mathcal{F}}$ は X についての一変数多項式であるため

多項式時間で逆像を計算可能

（e.g., Berlekamp's algorithm, Cantor-Zassenhaus algorithm）

HFE Modifications

- HFE の安全性はパラメータDに強く依存する
- Dを大きくすると署名生成の効率性が下がる
- 安全性を高めるための改良法が提案される
  - Minus (–)
  - Projection (p)
  - Vinegar (v)
- HFEv- (HFE with minus and vinegar modifications)
  から派生した Gui, GeMSS が NIST の候補に選ばれる
- 2021年に Tao らによって (v), (-) が安全性の向上に
  効果的ではないことが示される　[Tao et al., CRYPTO 2021]

目次

- 多変数多項式暗号
- Matsumoto-Imai
- HFE
- **UOV**
- Rainbow
- QR-UOV
- まとめ

Big Field

Small Field

UOV

[Kipnis et al., EUROCRYPT 1999]

Unbalanced Oil and Vinegar (UOV)

- Oil and Vinegar (OV) [Patarin, 1997] から
  パラメータを修正するかたちで、
  Kipnis らによって 1999 年に提案される
- Rainbow, LUOV などが本方式に基づいて構成される
- 公開鍵は $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$ の形で構成される
  （線型写像 $\mathcal{T}$ は安全性に影響しない）
- 現時点で安全な方式であると考えられている

Central Map

$\mathcal{F}$ の構成法　　$v \in \mathbb{N}$（一般的には $v = n - m$）

$x_1, \ldots, x_v$: **vinegar** variables

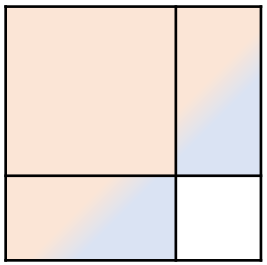
$x_{v+1}, \ldots, x_n$: **oil** variables

※ $v > n - v = m$ (**unbalanced**)

$$\mathcal{F} = (f_1, \ldots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$f_k = \sum_{i=1}^{n} \sum_{j=1}^{v} a_{i,j}^{(k)} x_i x_j$$　　※ 一次、定数項は省略

$MF_k =$



⇦ $m \times m$

Central Map

$\mathcal{F}^{-1}$ の計算法

① $x_1, \ldots, x_v$ (vinegar variables) をランダムに固定

$$f_k = \sum_{i=1}^{n}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j$$

$$= \sum_{i=1}^{v}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j + \sum_{i=v+1}^{n}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j$$

② $x_{v+1}, \ldots, x_n$ (oil variables) についての線形方程式を解く

(m equations, m variables)

※② で解が存在しない場合、 ① に戻る

例

・$q = 3, n = 4, m = 2, v = 2$

$$\begin{cases} f_1(\boldsymbol{x}) = x_1^2 + 2x_1x_2 + 2x_1x_4 + x_2^2 + 2x_2x_4 \\ f_2(\boldsymbol{x}) = x_1x_2 + x_1x_4 + x_2x_3 + 2x_2x_4 \end{cases}$$

Solve $\mathcal{F}(\boldsymbol{x}) = (0,1)$

Fix $(x_1, x_2) = (0,2) \Rightarrow$ $\begin{cases} x_4 + 1 = 0 \\ 2x_3 + x_4 = 1 \end{cases}$

ランダムな値

$(x_3, x_4) = (1,2)$

$\Rightarrow \mathcal{F}(0,2,1,2) = (0,1)$

目次

- 多変数多項式暗号
- Matsumoto-Imai
- HFE
- UOV
- **Rainbow**
- QR-UOV
- まとめ

Rainbow

[Ding, Schmidt, ACMS 2005]

Rainbow

- Ding, Schmidt によって 2005 年に提案
- UOV を**多層化**することによって構成
- UOV と比較して鍵長・署名長を削減
- 2022 年に Beullens によって新たな攻撃手法が提案される
  （パラメータの大幅な増加）

[Beullens, CRYPTO 2022]

Central Map

$\mathcal{F}$ の構成法　(v, o_1, o_2)　※$n = v + o_1 + o_2, m = o_1 + o_2$

$\underbrace{x_1, \cdots, x_v}_{v}, \underbrace{x_{v+1}, \cdots, x_{v+o_1}}_{o_1}, \underbrace{x_{v+o_1+1}, \cdots, x_n}_{o_2}$

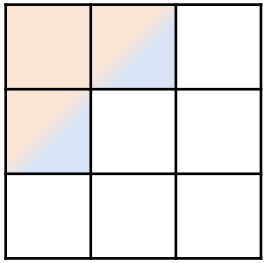
$$\mathcal{F} = (f_1, \cdots, f_m): \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$f_k = \sum_{i=1}^{v+o_1} \sum_{j=1}^{v} \alpha_{ij}^{(k)} x_i x_j \qquad (1 \le k \le o_1)$$

$$f_k = \sum_{i=1}^{n} \sum_{j=1}^{v+o_1} \alpha_{ij}^{(k)} x_i x_j \qquad (o_1 + 1 \le k \le m)$$

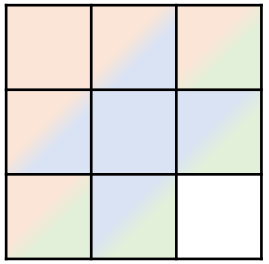
$(1 \le k \le o_1)$

$MF_k =$



$(o_1 + 1 \le k \le m)$

$MF_k =$



Central Map

$\mathcal{F}^{-1}$ の計算法

① $x_1, \ldots, x_v$ の値をランダムに固定

$(1 \le k \le o_1) \quad f_k = \sum_{i=1}^{v}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j + \sum_{i=v+1}^{v+o_1}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j$

② $x_{v+1}, \ldots, x_{v+o_1}$ についての線型方程式を解く(o_1 equations, o_1 variables)

③ $x_1, \ldots, x_v, x_{v+1}, \ldots, x_{v+o_1}$ を $f_{o_1+1}, \cdots, f_m$ に代入

$$f_k = \sum_{i=1}^{v}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j + \sum_{i=v+1}^{v+o_1}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j + \sum_{i=v+1}^{v+o_1}\sum_{j=v+1}^{v+o_1} a_{ij}^{(k)} x_i x_j + \sum_{i=v+o_1+1}^{n}\sum_{j=1}^{v} a_{ij}^{(k)} x_i x_j + \sum_{i=v+o_1+1}^{n}\sum_{j=v+1}^{v+o_1} a_{ij}^{(k)} x_i x_j$$

④ $x_{v+o_1+1}, \ldots, x_n$ についての線型方程式を解く

(o_2 equations, o_2 variables)

UOV との関係性

- 基本的に多項式の数 m は MQ 問題を解く計算量により決定される
- UOV では $v(=n-m) \approx 2m$ とする必要がある (UOV attack)

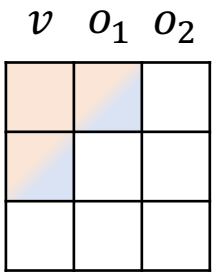
  ⇨ n が大きい値になる
- Rainbow では、$f_1, \ldots, f_m$ で Oil 変数として振る舞うのは $x_{v+o_1+1}, \ldots, x_n$ のみ

  （$x_{v+1}, \ldots, x_{v+o_1}$ は$f_1, \ldots, f_{o_1}$ でのみ Oil 変数）
- $v + o_1 \approx 2o_2$ を満たせば良い
- $m = o_1 + o_2$ に対して v を比較的小さくとれる

  ⇨ $n\ (= v + m)$ が小さくなる

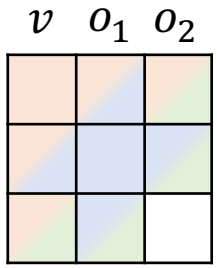
MinRank 問題

$(1 \le k \le o_1)$

$MF_k =$ 

$\Rightarrow \operatorname{rank} MF_k = v + o_1$

$(o_1 + 1 \le k \le m)$

$MF_k =$ 

$\Rightarrow \operatorname{rank} MF_k = n$

MinRank 問題

Given $A_1, \ldots, A_k \in \mathbb{F}_q^{a \times b}$ and $r < \operatorname{Min}\{a, b\}$,

find $t_1, \ldots, t_k \in \mathbb{F}_q$ such that $\operatorname{rank}(\sum_i t_i A_i) \le r$.

EIP を MinRank とみなせる（解が秘密鍵 $\mathcal{T}$ に対応）

- HFE にも適用可能
- 求解手法は次の講演で紹介する

目次

- 多変数多項式暗号
- Matsumoto-Imai
- HFE
- UOV
- Rainbow
- **QR-UOV**
- まとめ

QR-UOV

[F. et al., ASIACRYPT 2021]

Quotient Ring (QR) UOV

- 2021 年に Furue らによって提案される
- UOV と同様に公開鍵は $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$ の形で構成される
- 公開鍵、秘密鍵を行列で表現

$$MP_k = MS^{\mathsf{T}} \cdot MF_k \cdot MS$$

- UOV の公開鍵、秘密鍵（行列）に**剰余環** $(\mathbb{F}_q[x]/(f))$ の構造を導入することで構成
- UOV から**公開鍵長を削減**

Quotient Ring $\mathbb{F}_q[x]/(f)$ の行列表現

[定義] Polynomial Matrix Φ_g^f

$\ell \in \mathbb{N},\ f \in \mathbb{F}_q[x]\ (\deg f = \ell)$

$\forall g \in \mathbb{F}_q[x]/(f)$, $\ell \times \ell$ 行列 Φ_g^f:

$$(1, x, \ldots, x^{\ell-1})\Phi_g^f = (g, xg, \ldots, x^{\ell-1}g)$$

例）$q = 2,\ f = x^3 + x + 1,\ \ g = ax^2 + bx + c\ (a, b, c \in \mathbb{F}_2)$

⇨ $$\Phi_g^f = \begin{pmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{pmatrix}$$

3×3 行列を
3 つの要素で表現可能

公開鍵 $MP_i\ (i = 1, \ldots, m)$ に Φ_g^f を
導入できれば、公開鍵長を削減可能

UOV への適用

$$\{\Phi_g^f | g \in \mathbb{F}_q[x]/(f)\} \cong \mathbb{F}_q[x]/(f)$$

- $\Phi_{g_1}^f + \Phi_{g_2}^f = \Phi_{g_1+g_2}^f$
- $\Phi_{g_1}^f \cdot \Phi_{g_2}^f = \Phi_{g_1 \cdot g_2}^f$

Secret key $MS, MF_i (i = 1, \ldots, m)$: block Φ_g^f matrix $\begin{pmatrix} \Phi_{g_{11}}^f & \Phi_{g_{12}}^f & \Phi_{g_{13}}^f \\ \Phi_{g_{21}}^f & \Phi_{g_{22}}^f & \Phi_{g_{23}}^f \\ \Phi_{g_{31}}^f & \Phi_{g_{32}}^f & \Phi_{g_{33}}^f \end{pmatrix}$

$\Rightarrow$ Public key $MP_i = MS^{\mathsf{T}} \cdot MF_i \cdot MS (i = 1, \ldots, m)$:

block Φ_g^f matrix?

MS^{T} は Φ_g^f とは限らない

UOV への適用

$W \in \mathbb{F}_q^{\ell \times \ell}$ s.t. $\forall g \in \mathbb{F}_q[x]/(f)$, $W\Phi_g^f$: **symmetric**

- MF_i: block $W\Phi_g^f$ matrices $(i = 1, \ldots, m)$
- MS : block Φ_g^f matrix

$$\left(\Phi_{g_2}^f\right)^\top \left(W\Phi_{g_1}^f\right)\Phi_{g_2}^f = \left(\Phi_{g_2}^f\right)^\top W^\top \Phi_{g_1}^f \Phi_{g_2}^f \quad [W \text{ is symmetric since } \Phi_1^f = I_\ell.]$$

$$= \left(W\Phi_{g_2}^f\right)^\top \Phi_{g_1}^f \Phi_{g_2}^f$$

$$= \left(W\Phi_{g_2}^f\right)\Phi_{g_1}^f \Phi_{g_2}^f = W\Phi_{g_2 g_1 g_2}^f$$

MP_i $(= MS^\top \cdot MF_i \cdot MS)$: **block $W\Phi_g^f$ matrices**

Quotient Ring $\mathbb{F}_q[x]/(f)$ の行列表現

Proposition

- $f = x^\ell - ax^i - 1 \left(a \in \mathbb{F}_q, 1 \leq i \leq \ell - 1\right)$
- $W = \begin{pmatrix} J_i & 0_{i\times(\ell-i)} \\ 0_{(\ell-i)\times i} & J_{\ell-i} \end{pmatrix}$ ※ $J_\ell := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$

$\Rightarrow W\Phi_g^f$: **対称行列**

例）$q = 2,\ f = x^3 + x + 1,\ g = ax^2 + bx + c\ (a, b, c \in \mathbb{F}_2)$

$$\Phi_g^f = \begin{pmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{pmatrix} \Rightarrow W\Phi_g^f = \begin{pmatrix} a & c & b \\ c & b & a+c \\ b & a+c & b+c \end{pmatrix}$$

$$W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

QR-UOV

鍵生成

① **既約多項式**: $f = x^{\ell} - ax^{i} - 1$（安全性のため）

$W \in \mathbb{F}_q^{\ell \times \ell}$ s.t. $\forall g \in \mathbb{F}_q[x]/(f)$, $W\Phi_g^f$: 対称

② MF_i: block $W\Phi_g^f$ matrices $(i = 1, \ldots, m)$

MS : block Φ_g^f matrix

③ 公開鍵の表現行列 MP_i $(i = 1, \ldots, m)$ を

$MP_i = MS^{\top} \cdot MF_i \cdot MS$によって求める

$\Rightarrow MP_i$: block $W\Phi_g^f$ matrices

QR-UOV

⇒ MP_i : Block $W\Phi_g^f$ Matrix

$$\left(\begin{array}{ccc|ccc} 0 & 5 & 1 & 3 & 0 & 1 \\ 5 & 1 & 1 & 0 & 1 & 3 \\ 1 & 1 & 1 & 1 & 3 & 3 \\ \hline 6 & 5 & 6 & 0 & 5 & 4 \\ 5 & 6 & 3 & 5 & 4 & 1 \\ 6 & 3 & 2 & 4 & 1 & 3 \end{array}\right)$$

$(q = 7, f = x^3 - 3x - 1)$

$n \times n$ 行列を n^2/ℓ 個の成分で表現可能

（ブロックサイズ: $\ell \times \ell$）

公開鍵長を削減

安全性

- **EIP**: $\mathbb{F}_{q^\ell}$ 上の UOV とみなせる
- **MQ**: ランダムな MQ と同様の振る舞いを見せることを実験的に確認

公開鍵長・署名長の比較

NIST Security Level 1 (143 gates security)

※ Czypek らによる公開鍵長の削減手法を適用 [Czypek et al., CHES 2012]

（Rainbow に対しては Petzoldt による手法を適用 [Petzoldt, PQCrypto 2020]）

方式	パラメータ	public key (KB)	signature (B)
UOV *	$(q, n, m) = (256,112,44)$	278.4	112.0
Rainbow *	$(q, v, o_1, o_2) = (256,68,32,48)$	258.4	164.0
QR-UOV	$(q, v, m, \ell) = (7,189,72,3)$	**23.8**	**113.9**

*: https://groups.google.com/a/list.nist.gov/g/pqc-forum

※ 処理速度は UOV, Rainbow が効率的

目次

- 多変数多項式暗号
- Matsumoto-Imai
- HFE
- UOV
- Rainbow
- QR-UOV
- **まとめ**

まとめ

・多変数多項式問題に基づく署名方式の標準的な
構成方法について紹介した

・主要な多変数多項式署名方式を紹介した

MI, HFE, UOV, Rainbow, QR-UOV

・主要な攻撃方法としては MQ 問題、MinRank 問題
の求解などがあげられる

今後の課題（署名方式の構成）

・既存方式の効率化は可能か

- 公開鍵サイズの削減など

・新たな中心写像の構成