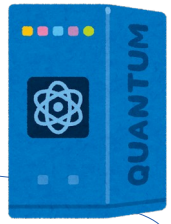
NIST 耐量子計算機暗号計画の追加署名方式プロジェクト第二ラウンドにおける多変数多項式署名方式 UOV とその変種の動向

中村周平（茨城大学）

2025 年 8 月 18-19 日
第 9 回情報数理セミナー@日本大学理工学部



量子計算機を利用した情報社会

現在の我々の情報社会

量子計算機の急速な開発

主な対応：

① 耐量子計算機暗号

② 量子暗号（量子鍵配送）

情報セキュリティ

暗号（公開鍵暗号）

困難な数学問題 … 安全性の根拠

多項式時間での求解可能

危殆化

- RSA 暗号
- EC 暗号

- 素因数分解問題
- 離散対数問題

① 耐量子計算機暗号

耐量子計算機暗号

量子計算機でも求解困難

- 格子暗号
- 符号暗号
- 多変数暗号
- 同種暗号
- ハッシュ暗号

- 最短ベクトル問題
- 復号問題
- 連立代数方程式問題
- 同種写像問題
- ハッシュ関数衝突問題

NIST （米国標準技術研究所）による耐量子計算機暗号標準化プロジェクト

(cf. https://csrc.nist.gov/projects/post-quantum-cryptography)

これまでの経過

	暗号化	署名
2016: 公募開始	82 件	= 59 + 23
2017: Round 1 の候補発表	69 件	= 48 + 21
2019: Round 2 の候補発表	26 件	= 17 + 9
2020: Round 3 の最終候補	7 件	= 4 + 3
代替候補	8 件	= 5 + 3

2022:
- 格子暗号・ Hash 暗号の標準化を決定
- 残りの暗号化方式は引き続き Round 4 へ
- 署名方式の追加プロセスを 2023 年から開始

耐量子計算機暗号標準化プロセス： 2022 年度標準化決定方式

Type	PKE/KEM	Signature
格子暗号	CRYSTALS-Kyber	CRYSTALS-Dilithum, FALCON
Hash 暗号		SPHINCS+

耐量子計算機暗号標準化プロセス : Round 4 (2022.7.5)

Type	PKE/KEM
符号暗号	BIKE, Classical McEliece, HQC
同種暗号	SIKE

耐量子計算機暗号 追加署名方式プロセス : Round 1 (40 件 , 2023.7.1)

Type	Signature
符号暗号	Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave
同種暗号	SQIsign
格子暗号	EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS
MPC 系	CROSS, MIRA, MiRitH, MQOM, Biscuit, PERK, RYDE, SDitH
多変数系	3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
共通鍵系	AIMer, Ascon-Sign, FAEST, SPHINCS-alpha
その他	ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

耐量子計算機暗号標準化プロセス : NIST announcement (2025.5.11)

Type	PKE/KEM
符号暗号	BIKE, Classical McEliece, HQC
同種暗号	SIKE

耐量子計算機暗号 追加署名方式プロセス : Round 2 (14 件 , 2024.10.24)

Type	Signature
符号暗号	Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave
同種暗号	SQIsign
格子暗号	EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS
MPC 系	CROSS, Mirath(MIRA/MiRitH), MQOM, Biscuit, PERK, RYDE, SDitH
多変数系	3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX
共通鍵系	AIMer, Ascon-Sign, FAEST, SPHINCS-alpha
その他	ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

SCOPE

- NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
- NIST may also be interested in signature schemes that have short signatures and fast verification.
- Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

cf. D. Moody, The onramp submissions, In response to NIST's call for additional digital signatures, NIST PQC Seminars, 2023.6.9

目次

目次

記号

q：奇素数のべき

$\mathbb{F}_q$：位数 q の有限体

$\mathrm{Mat}_{m\times n}(\mathbb{F}_q)$：有限体を係数に取る $m \times n$ 行列全体のなす集合

$\mathrm{SymMat}_{n\times n}(\mathbb{F}_q)$：有限体を係数に取る $n \times n$ 対称行列全体のなす集合

$$\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m \qquad \text{where } \mathcal{F}_i \in \mathbb{F}_q[x_1, \ldots, x_n]$$
$$\boldsymbol{a} \mapsto (\mathcal{F}_1(\boldsymbol{a}), \ldots, \mathcal{F}_m(\boldsymbol{a}))$$

UOV とその解析

多変数多項式署名方式 UOV は主に次の 3 つのアルゴリズムからなる .

$\mathrm{UOV}(q, v, o, m)$ with $n = v + o$

① 写像生成（鍵生成）

秘密鍵
- $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$　全単射線形写像
- $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$　UOV 写像（逆像元計算容易な二次写像）

⇒ 公開鍵　$\mathcal{P} := \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

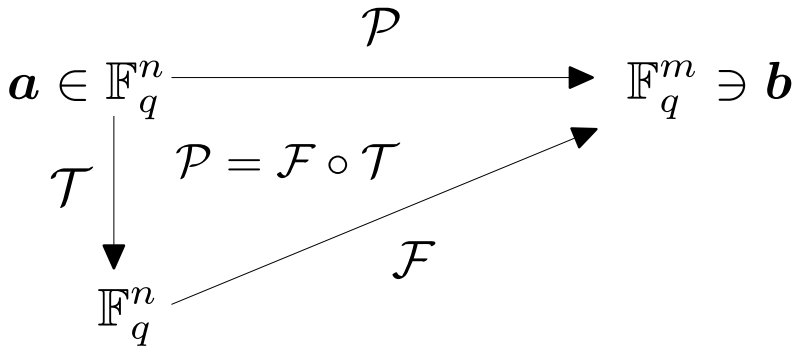
※ 秘密鍵を知っていると逆像元計算が容易な二次写像

② 逆像元計算（署名生成）

$$\boldsymbol{b} \in \mathbb{F}_q^m \Rightarrow \boldsymbol{a}' \in \mathcal{F}^{-1}(\{\boldsymbol{b}\}) \Rightarrow \boldsymbol{a} := \mathcal{T}^{-1}(\boldsymbol{a}')$$

③ 代入計算（署名検証）

$$\boldsymbol{a} \in \mathbb{F}_q^n \Rightarrow \boldsymbol{b} = \mathcal{P}(\boldsymbol{a}) \in \mathbb{F}_q^m$$



例：署名を用いて公開鍵の持ち主かどうか検証する

① 鍵生成

公開鍵 $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

秘密鍵 $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$

文書 $\boldsymbol{b} \in \mathbb{F}_q^m$

$\boldsymbol{b} \in \mathbb{F}_q^m$

② 署名生成

$\boldsymbol{a} \in \mathcal{P}^{-1}(\{\boldsymbol{b}\})$ 署名

$(\boldsymbol{a}, \boldsymbol{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q^m$

$\boldsymbol{b} = \mathcal{P}(\boldsymbol{a})?$ ③ 検証

UOV 写像：

$$\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$
$$\text{s.t. } \mathcal{F}_k(\boldsymbol{x}) = \sum_{1 \le i \le v, i \le j \le n} a_{ij} x_i x_j \quad (a_{ij} \in \mathbb{F}_q) = {}^t\boldsymbol{x} F_k \boldsymbol{x}$$

UOV 写像での逆像元計算： $\boldsymbol{a}' \in \mathcal{F}^{-1}(\{\boldsymbol{b}\})$, $o \ge m$ 署名のための条件

1. $a'_1, \ldots, a'_v \in \mathbb{F}_q$
2. $\overline{\mathcal{F}}_k(a'_1, \ldots, a'_v, x_{v+1}, \ldots, x_n) = \sum_{1 \le i \le j \le v} a_{ij} a'_i a'_j + \sum_{1 \le i \le v, v+1 \le j \le n} a_{ij} a'_i x_j$
3. $\overline{\mathcal{F}} = (\overline{\mathcal{F}}_1, \ldots, \overline{\mathcal{F}}_m) : \mathbb{F}_q^o \to \mathbb{F}_q^m$, 線型写像
4. $(a'_{v+1}, \ldots, a'_n) \in \overline{\mathcal{F}}^{-1}(\boldsymbol{b})$
5. $\boldsymbol{a}' := (a'_1, \ldots, a'_n) \in \mathcal{F}^{-1}(\{\boldsymbol{b}\})$

全射でない

全射である

署名偽造，秘密鍵復元

文書

目的：公開鍵 P の作成者になりすます．

$\boldsymbol{b} \in \mathbb{F}_q^m$ $\xrightarrow{\boldsymbol{b} \in \mathbb{F}_q^m}$ $\boldsymbol{b} \in \mathbb{F}_q^m$

$\boldsymbol{b} = \mathcal{P}(\boldsymbol{a}')$ $\xleftarrow{(\boldsymbol{a}', \boldsymbol{b}) \in \mathbb{F}_q^n \times \mathbb{F}_q^m}$ $\boldsymbol{a}' \in \mathcal{P}^{-1}(\{\boldsymbol{b}\})$

署名偽造： $\mathcal{P}(\boldsymbol{x}) = \boldsymbol{b}$ から解 $\boldsymbol{a}'$ を求める．

秘密鍵復元： 公開鍵 $\mathcal{P}$ から秘密鍵 $\mathcal{F}, \mathcal{T}$ を求める．

→ 署名された全ての文書に対して署名偽造可能

UOV に対する秘密鍵復元

※ 説明のため q を奇数とする .

$$\mathcal{F} = (\mathcal{F}_1, \ldots, \mathcal{F}_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

$$\text{s.t. } \mathcal{F}_k(\boldsymbol{x}) = \sum_{1 \le i \le v, i \le j \le n} a_{ij} x_i x_j \quad (a_{ij} \in \mathbb{F}_q) = {}^t\boldsymbol{x} F_k \boldsymbol{x}$$

$$\therefore F_k = \begin{pmatrix} a_{11} & \cdots & a_{1v}/2 & a_{1\,v+1}/2 & \cdots & a_{1n}/2 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{1v}/2 & \cdots & a_{vv} & a_{v\,v+1}/2 & \cdots & a_{vn}/2 \\ a_{1\,v+1}/2 & \cdots & a_{v\,v+1}/2 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{1\,n}/2 & \cdots & a_{v\,n}/2 & 0 & \cdots & 0 \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$$

(v 行, o 行; v 列, o 列)

$$\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n, \quad \mathcal{T}(\boldsymbol{x}) = T\boldsymbol{x} \quad (T \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q))$$

$$T = \begin{pmatrix} 1 & & & t_{1\,v+1} & \cdots & t_{1\,n} \\ & \ddots & & \vdots & \ddots & \vdots \\ & & 1 & t_{v\,v+1} & \cdots & t_{v\,n} \\ & & & 1 & & \\ & O & & & \ddots & \\ & & & & & 1 \end{pmatrix} \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$$

(v 行, o 列)

$$\Rightarrow \mathcal{P} = (\mathcal{P}_1, \ldots, \mathcal{P}_m) = \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n \text{ s.t. } \mathcal{P}_k(\boldsymbol{x}) = {}^t\boldsymbol{x} P_k \boldsymbol{x}$$

$$\therefore P_k = {}^t T F_k T \ (1 \leq \forall k \leq m)$$

秘密鍵復元 : 公開鍵 $P_1, \ldots, P_m$ から秘密鍵 $F_1, \ldots, F_m, T$ を求める .

UOV(q, v, o, m) 秘密鍵復元問題 $n := o + v, \quad q :$ odd

Given: $P_1, \ldots, P_m \in \mathrm{Mat}_{n \times n}(\mathbb{F}_q)$

Find: $F_1, \ldots, F_m, T \in \mathrm{Mat}_{n \times n}(\mathbb{F}_q)$ s.t.

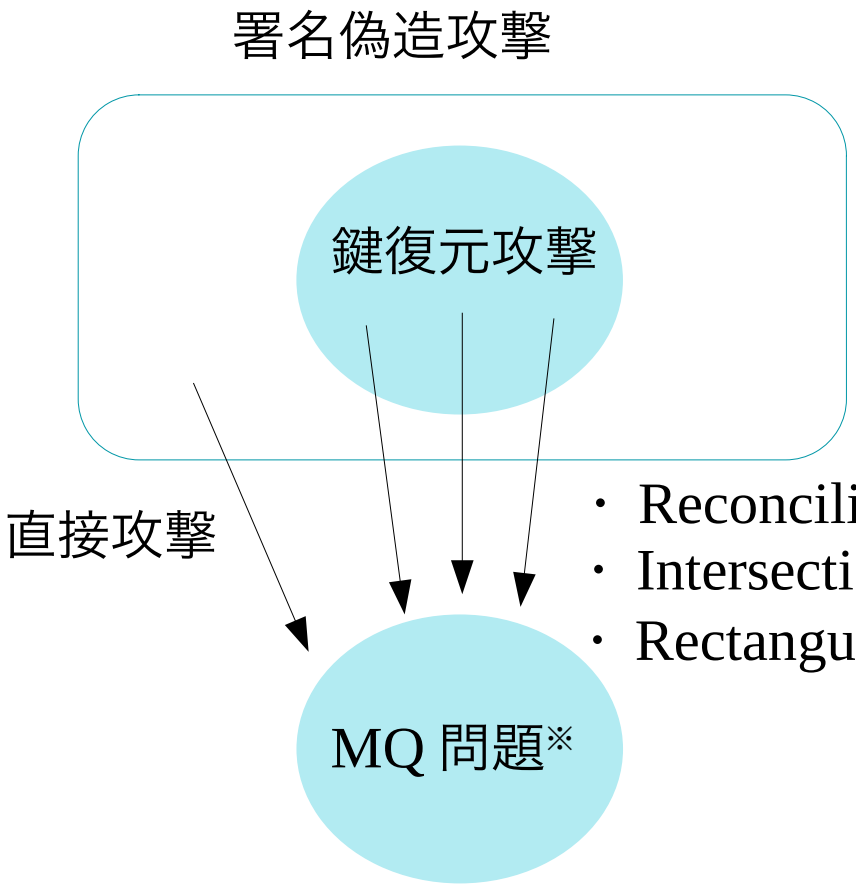
1. $P_k = {}^t T F_k T, \quad 1 \leq \forall k \leq m$

2. $F_k = \begin{pmatrix} F_k^{11} & F_k^{12} \\ {}^t F_k^{12} & O_{o \times o} \end{pmatrix}, \quad T = \begin{pmatrix} I_v & T^{12} \\ O_{o \times v} & I_o \end{pmatrix}$

where $F_k^{11} \in \mathrm{SymMat}_{v \times v}(\mathbb{F}_q), F_k^{12}, T^{12} \in \mathrm{Mat}_{v \times o}(\mathbb{F}_q)$

秘密鍵復元攻撃 = “ 秘密鍵復元問題を解くアルゴリズム”

UOV に対する代数的攻撃手法



- Reconciliation 攻撃 [DYC+2008]
- Intersection 攻撃 [Beu2022]
- Rectangular Minrank 攻撃 [Beu2022], [FI2023]

※ 連立二次方程式問題

Rectangular MinRank 攻撃 [Beu2021],[FI2023]

(Rectangular) MinRank 問題

Given: $A_1, \ldots, A_m \in \mathrm{Mat}_{a\times b}(\mathbb{F}_q), r \in \mathbb{Z}_{\geq 0}$

Find: $t_1, \ldots, t_m \in \mathbb{F}_q$ s.t. $\mathrm{rank}\left(\sum_{i=1}^{m} t_i A_i\right) \leq r$

$$\Leftrightarrow \dim \mathrm{Ker}\left(\sum_{i=1}^{m} t_i A_i\right) \geq a - r$$

連立方程式問題への帰着手法

例 : Kipnis-Shamir 手法

$$\boldsymbol{y}_j \left(\sum_{i=1}^{m} x_i A_i\right) = 0 \qquad (1 \leq j \leq a - r)$$

例 : 小行列式手法

$$\mathrm{Minors}^{r+1}\left(\sum_{i=1}^{m} x_i A_i\right)$$

$(r + 1)$ 次小行列式全体

UOV から MinRank 問題への帰着

UOV 写像

$$\begin{matrix} & F_1 & & & & & & & F_m \\ v\left\{\right. & \begin{pmatrix} * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \end{pmatrix} & & & & & & & \begin{pmatrix} * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \end{pmatrix} \\ o\left\{\right. & \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix} & , \ldots , & & & & & & \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix} \\ & \underbrace{\quad\quad}_{v}\ \underbrace{\quad\quad}_{o} & & & & & & & \end{matrix}$$

$F_*^{[i]}$: $F_1, \ldots, F_m$ の i 行ベクトルのなす行列

$$v < m \Rightarrow \mathrm{rank}(F_*^{[v+i]}) < m$$

$$\begin{matrix} & F_*^{[1]} & & & & & & F_*^{[v]} & & & & & & F_*^{[v+1]} & & & & & & F_*^{[v+o]} \\ m\left\{\right. & \begin{pmatrix} * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \end{pmatrix} & , \ldots , & \begin{pmatrix} * & \cdots & * & * & \cdots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & * & \cdots & * \end{pmatrix} & , & \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix} & , \ldots , & \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix} \\ & \underbrace{\quad\quad}_{v}\ \underbrace{\quad\quad}_{o} & & & & & & & & & & & & & & & & & \end{matrix}$$

注意 $(P_1, \ldots, P_m) = ({}^tTF_1{}^tT, \ldots, TF_m{}^tT)$

$$\Rightarrow (P_*^{[1]}, \ldots, P_*^{[n]}) = ({}^tTF_*^{[1]}, \ldots, {}^tTF_*^{[n]})T$$

$$(P_*^{[1]}, \ldots, P_*^{[n]})T^{-1} = ({}^tTF_*^{[1]}, \ldots, {}^TF_*^{[n]})$$

$$T^{-1} = \begin{pmatrix} t'_{11} & \cdots & t'_{1n} \\ \vdots & \ddots & \vdots \\ t'_{n1} & \cdots & t'_{nn} \end{pmatrix}$$

$$\therefore t'_{1i}P_*^{[1]} + \cdots + t'_{ni}P_*^{[n]} = {}^tTF_*^{[i]}$$

$$v < m \Rightarrow \mathrm{rank}(F_*^{[v+i]}) < m$$
$$\Rightarrow \mathrm{rank}(TF_*^{[v+i]}) < m$$

UOV からの Rectangular MinRank 問題

$$\text{Given: } P_*^{[1]}, \ldots, P_*^{[n]} \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q), m \in \mathbb{Z}_{\geq 0}$$

$$\text{Find: } t_1, \ldots, t_n \in \mathbb{F}_q \text{ s.t. } \mathrm{rank}\left(\sum_{i=1}^{n} t_i P_*^{[i]}\right) < m$$