A security analysis on MQ-Sign

Yasuhiko Ikematsu[1] Hyungrok Jo[2] Takanori Yasuda[3]

[1]Kyushu University, Japan
[2]Yokohama National University, Japan
[3]Okayama University of Science, Japan

July 14th 2023
The 6th KpqC Workshop

Contents

Introduction

MQ-Sign : an improved variant of the UOV signature scheme.

- Proposed by Kyung-Ah Shim, Jeongsu Kim, and Youngjoo An (NIMS[1]).
- Submitted to the KpqC competition.

Multivariate cryptography : - Good candidates for post-quantum cryptography

- Based on the hardness of solving systems of multivariate polynomial equations

[1]National Institute for Mathematical Sciences

UOV (Unbalanced Oil and Vinegar)

A brief history

1997	Oil & Vinegar signature (OV sign.)
1998	OV sign. is cryptanalyzed by KS attack.[2]
1999	Unbalanced Oil & Vinegar (UOV sign.)[3]
2005	Rainbow sign.[4]
2017	Rainbow sign. is submitted to NIST PQC standardization.
2020	Rainbow sign. is selected as a finalist for NIST PQC standardization
2022	Rainbow sign. is cryptanalyzed.[5]

[2] A. Kipnis and A. Shamir: Cryptanalysis of the oil & vinegar signature scheme, CRYPTO'98
[3] A. Kipnis, J. Patarin, and L. Goubin: Unbalanced Oil and Vinegar signature schemes, EUROCRYPT'99
[4] J. Ding, and D. Schmidt: Rainbow, a new multivariable polynomial signature scheme, ACNS'05
[5] W. Beullens: Breaking Rainbow Takes a Weekend on a Laptop, CRYPTO'22

UOV (Unbalanced Oil and Vinegar)[3]

$\mathbb{F}_q$: a finite field of q.

$V = \{1, \dots, v\}$: vinegar variables

$O = \{v+1, \dots, v+o\}$: oil variables

If $(x_1, \dots, x_v)$ are randomly chosen, it is easy to find a solution for $(x_{v+1}, \dots, x_{v+o})$, since it is a linear system!

n : the number of variables in the public key, $n = o + v$.

A central map $\mathcal{F}: \mathbb{F}_q^n \to \mathbb{F}_q^o$ of UOV, $\mathcal{F} = (\mathcal{F}^{(1)}, \dots, \mathcal{F}^{(o)})$ is o multivariate quadratic equations with n variables $x_1, \dots, x_n$ defined by

$$\mathcal{F}^{(k)}(\mathbb{x}) = \sum_{i,j \in V, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in O, j \in V} \beta_{ij}^{(k)} x_i x_j$$

$$\mathcal{F}^{(k)} = \mathcal{F}_{V,R}^{(k)} + \mathcal{F}_{OV,R}^{(k)}$$

[3] A. Kipnis, J. Patarin, and L. Goubin: Unbalanced Oil and Vinegar signature schemes, EUROCRYPT'99

UOV (Unbalanced Oil and Vinegar)

Signature scheme

Key generation

- Secret key : $(\mathcal{F}, \mathcal{S})$
- Public key : $P = \mathcal{F} \circ \mathcal{S}$

$\mathcal{S}: \mathbb{F}_q^n \to \mathbb{F}_q^n$, a random invertible affine map

signature | message

$$
\begin{tikzcd}
\sigma \in \mathbb{F}_q^n \arrow[rr, "P = \mathcal{F} \circ \mathcal{S}", "\text{Verification}"'] & & M \in \mathbb{F}_q^o \arrow[dl, "\mathcal{F}^{-1}"] \\
& \mathbb{F}_q^n \arrow[ul, "\mathcal{S}^{-1}"] \arrow[u, phantom, "\text{Sign}"] &
\end{tikzcd}
$$

1. $(s_1, \dots, s_v)$: randomly chosen.
2. Find a solution $(s_{v+1}, \dots, s_{v+o})$ satisfying $F^{(i)}(s_1, \dots, s_{v+o}) = m_i$ for $1 \le i \le o$.

Types of MQ-Sign

There are 4 types of central maps,

- $\mathcal{F}_{SS}^{(k)} = \mathcal{F}_{V,S}^{(k)} + \mathcal{F}_{OV,S}^{(k)}$ (MQ-Sign-SS)
- $\mathcal{F}_{RS}^{(k)} = \mathcal{F}_{V,R}^{(k)} + \mathcal{F}_{OV,S}^{(k)}$ (MQ-Sign-RS)
- $\mathcal{F}_{SR}^{(k)} = \mathcal{F}_{V,S}^{(k)} + \mathcal{F}_{OV,R}^{(k)}$ (MQ-Sign-SR)
- $\mathcal{F}_{RR}^{(k)} = \mathcal{F}_{V,R}^{(k)} + \mathcal{F}_{OV,R}^{(k)}$ (MQ-Sign-RR, same as UOV)

Our target

which derive the secret key size reduction by using sparse poly.

Here, $\mathcal{F}_{V,S}^{(k)} = \sum_{i=1}^{v} \alpha_i^{(k)} x_i x_{(i+k-1 \pmod v)+1}$ and $\longrightarrow \frac{v \times v}{2} \cdot o \to v \times o$

$\mathcal{F}_{OV,S}^{(k)} = \sum_{i=1}^{v} \beta_i^{(k)} x_i x_{(i+k-2 \pmod o)+v+1}$. $\longrightarrow (v \times o) \cdot o \to v \times o$

cf. $\mathcal{F}^{(k)}(\mathbb{x}) = \sum_{i,j \in V, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in O, j \in V} \beta_{ij}^{(k)} x_i x_j$

The central map of MQ-Sign-RS

Vinegar parts : Random polynomials

Oil-Vinegar parts : Sparse polynomials

$$f_1(\mathbb{x}) = \boxed{\sum_{i,j=1}^{v} \alpha_{i,j}^{(1)} x_i x_j} + \boxed{\sum_{i=1}^{v} \beta_i^{(1)} x_i x_{(i+1-2 \pmod{o})+v+1},}$$

$$\vdots$$

$$f_k(\mathbb{x}) = \sum_{i,j=1}^{v} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i=1}^{v} \beta_i^{(k)} x_i x_{(i+k-2 \pmod{o})+v+1},$$

$$\vdots$$

$$f_o(\mathbb{x}) = \sum_{i,j=1}^{v} \alpha_{i,j}^{(o)} x_i x_j + \sum_{i=1}^{v} \beta_i^{(o)} x_i x_{(i+o-2 \pmod{o})+v+1}.$$

Quad. poly. and square matrix

For a homogeneous quadratic polynomial

$$g(\mathbb{x}) = \sum_{i \le i \le j \le n} g_{ij} x_i x_j \in \mathbb{F}_q[\mathbb{x}]$$

define the upper triangular matrix G^{up} by

$$G^{\mathrm{up}} \coloneqq \begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ 0 & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{nn} \end{bmatrix} \in \mathbb{F}_q^{n \times n}$$

Then we have $g(\mathbb{x}) = \mathbb{x} \cdot G^{\mathrm{up}} \cdot {}^t\mathbb{x}$.
Here, ${}^t\mathbb{x}$ is the transpose of $\mathbb{x}$.

Quad. poly. and square matrix

We define the *symmetric matrix* G by

$$G \coloneqq G^{\mathrm{up}} + {}^{t}G^{\mathrm{up}}.$$

Let $(F_1, \ldots, F_o)$ and $(P_1, \ldots, P_o)$ be the corresponding symmetric matrices of the central map $\mathcal{F} = (f_1, \ldots, f_o)$ and the public key $\mathcal{P} = (p_1, \ldots, p_o)$.

Then we have

$$(P_1, \ldots, P_o) = (S \cdot F_1 \cdot {}^{t}S, \ldots, S \cdot F_o \cdot {}^{t}S).$$

Our proposed attack

A central map F_1

Oil-Vinegar parts : Sparse polynomials

$$
F_1 = \begin{array}{cc}
 & \begin{array}{c} \qquad\qquad\qquad o \end{array} \\
 & \left[\begin{array}{c|ccccccc}
 & \beta_1^{(1)} & & & & & & \\
 & & \beta_2^{(1)} & & & & & \\
 & & & \ddots & & & & \\
 & & & & \beta_{v-o}^{(1)} & & & \\
* & & & & & \beta_{v-o+1}^{(1)} & & \\
 & & & & & & \ddots & \\
 & & & & & & & \beta_o^{(1)} \\
\hdashline
 & \beta_{o+1}^{(1)} & & & & & & \\
 & & \ddots & & & & & \\
 & & & & \beta_v^{(1)} & & & \\
\hline
* & & & & \mathbf{0} & & &
\end{array}\right] v
\end{array}
$$

$$\mathcal{F}_{OV,S}^{(1)} = \sum_{i=1}^{v} \beta_i^{(1)} x_i x_{(i+1-2 \pmod{o})+v+1}$$

Our proposed attack

A central map F_2

$$F_2 = \begin{array}{cc} \begin{array}{c} o \end{array} & \\ \left[\begin{array}{c|ccccccc} & 0 & \beta_1^{(2)} & & & & & \\ & & & \ddots & & & & \\ & & & & \beta_{v-o}^{(2)} & & & \\ & & & & & \beta_{v-o+1}^{(2)} & & \\ * & & & & & & \ddots & \\ & & & & & & & \beta_{o-1}^{(2)} \\ & \beta_o^{(2)} & & & & & & 0 \\ \hdashline & & \beta_{o+1}^{(2)} & & & & & \\ & & & \ddots & & & & \\ & & & & \beta_v^{(2)} & & & \\ \hline * & \multicolumn{7}{c}{\mathbf{0}} \end{array}\right] & v \end{array}$$

$$\mathcal{F}_{OV,S}^{(2)} = \sum_{i=1}^{v} \beta_i^{(2)} x_i x_{(i+2-2 \pmod{o})+v+1}$$

Our proposed attack

A central map F_3

$$
\begin{array}{cc}
 & o \\
F_3 = \left[\begin{array}{c|cccccccc}
 & 0 & 0 & \beta_1^{(3)} & & & & & \\
 & & & & \ddots & & & & \\
 & & & & & \beta_{v-o}^{(3)} & & & \\
 & & & & & & \beta_{v-o+1}^{(3)} & & \\
 * & & & & & & & \ddots & \\
 & & & & & & & & \beta_{o-2}^{(3)} \\
 & \beta_{o-1}^{(3)} & & & & & & & 0 \\
 & & \beta_o^{(3)} & & & & & & 0 \\
\hdashline
 & & & \beta_{o+1}^{(3)} & & & & & \\
 & & & & \ddots & & & & \\
 & & & & & \beta_v^{(3)} & & & \\
\hline
 * & & & & & \mathbf{0} & & &
\end{array}\right] & v
\end{array}
$$

$$\mathcal{F}_{OV,S}^{(3)} = \sum_{i=1}^{v} \beta_i^{(3)} x_i x_{(i+3-2 \pmod{o})+v+1}$$

Aulbach et al.'s attack [6]

Aulbach et al.'s attack can be applied to

- $\mathcal{F}_{SS}^{(k)} = \mathcal{F}_{V,S}^{(k)} + \mathcal{F}_{OV,S}^{(k)}$ (MQ-Sign-SS)
- $\mathcal{F}_{RS}^{(k)} = \mathcal{F}_{V,R}^{(k)} + \mathcal{F}_{OV,S}^{(k)}$ (MQ-Sign-RS)

Key recovery attack combining the sparsity of the central map with key $\mathcal{S}$ having a special form with

However, in the original proposal, the key $\mathcal{S}$ should be a general form!

$$S = \begin{bmatrix} I_{v\times v} & \mathbf{0}_{v\times o} \\ * & I_{o\times o} \end{bmatrix}.$$

[6] Aulbach, T., Samardjiska, S., and Trimoska, M. (2023). Practical key-recovery attack on MQ-Sign. https://eprint.iacr.org/2023/432

Aulbach et al.'s attack [6]

$$\begin{bmatrix} P_i \end{bmatrix} = S \cdot F_i \cdot {}^tS$$

$$S = \begin{array}{c c} & \begin{array}{cc} v & o \end{array} \\ \begin{array}{c} v \\ o \end{array} & \begin{bmatrix} I_{v\times v} & \mathbf{0}_{v\times o} \\ S' & I_{o\times o} \end{bmatrix} \end{array}, \quad F_i = \begin{array}{c c} & \begin{array}{cc} v & o \end{array} \\ \begin{array}{c} v \\ o \end{array} & \begin{bmatrix} \ast & F_i' \\ \ast & \mathbf{0}_{o\times o} \end{bmatrix} \end{array}, \quad {}^tS = \begin{array}{c c} & \begin{array}{cc} v & o \end{array} \\ \begin{array}{c} v \\ o \end{array} & \begin{bmatrix} I_{v\times v} & {}^tS' \\ \mathbf{0}_{o\times v} & I_{o\times o} \end{bmatrix} \end{array}$$

It derives a linear system having vo number of linearly independent equations. (Can be solved efficiently by Gaussian elimination!)

Key recovery attack can be done in a few second for the proposed parameter of security level 5.

[6] Aulbach, T., Samardjiska, S., and Trimoska, M. (2023). Practical key-recovery attack on MQ-Sign. https://eprint.iacr.org/2023/432

Our proposed attack

Our attack can be applied to MQ-Sign-SS and MQ-Sign-RS.

We utilize the sparsity properties of the central maps.

Main aim.

Find o linear independent vectors $\mathbb{t}_1, \cdots, \mathbb{t}_o \in \mathbb{F}_q^n$ such that

$$ {}^t\mathbb{t}_i \cdot P_k \cdot \mathbb{t}_j = 0,\ p_k(\mathbb{t}_i) = 0\ (1 \leq i, j, k \leq o). \qquad (A) $$

(It derives that any signature can be forged easily.)

Our proposed attack

Main idea

From $(P_1, \dots, P_o) = (S \cdot F_1 \cdot {}^t S, \dots, S \cdot F_o \cdot {}^t S)$,

$$P_i = S \cdot F_i \cdot {}^t S \ (i = 1, \dots, o)$$

$$\Longrightarrow P_i \cdot {}^t S^{-1} = S \cdot F_i$$

$$\begin{bmatrix} \\ P_i \\ \\ \end{bmatrix} \cdot \begin{bmatrix} \\ {}^t S^{-1} \\ \\ \end{bmatrix} = \begin{bmatrix} \\ S \\ \\ \end{bmatrix} \cdot \begin{array}{cc} & \begin{array}{cc} v & o \end{array} \\ \begin{array}{c} v \\ o \end{array} & \begin{bmatrix} \\ F_i \\ \\ \end{bmatrix} \end{array}$$

Our proposed attack

Sparse subparts of central maps $F_i{}'$

Oil-Vinegar parts

$$\begin{bmatrix} P_i \end{bmatrix} \cdot \begin{array}{c} \qquad\quad o \\ \begin{bmatrix} {}^tS^{-1} \; \boxed{T'} \end{bmatrix} \end{array} = \begin{bmatrix} S \end{bmatrix} \cdot \begin{array}{cc} & \begin{array}{cc} \quad v \quad & o \end{array} \\ \begin{array}{c} v \\ o \end{array} & \begin{bmatrix} F_i & \boxed{F_i{}'} \end{bmatrix} \end{array}$$

$$T' = (\mathbb{t}_1 \ldots \mathbb{t}_o) \qquad S = (\mathbb{s}_1 \ldots \mathbb{s}_{v+o})$$

$$\begin{cases} P_1 \cdot T' = S \cdot F_1', \\ P_2 \cdot T' = S \cdot F_2', \\ P_3 \cdot T' = S \cdot F_3', \\ \qquad\quad \vdots \\ P_o \cdot T' = S \cdot F_o'. \end{cases}$$

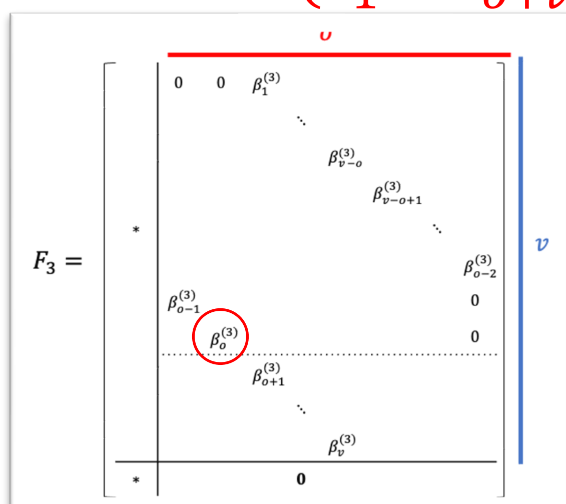
Our proposed attack

A generator $\mathbb{s}_o$

$$\begin{bmatrix} P_i \end{bmatrix} \cdot \begin{bmatrix} {}^tS^{-1} & \overbrace{\boxed{T'}}^{o} \end{bmatrix} = \begin{bmatrix} S \end{bmatrix} \cdot \begin{array}{c|cc} & v & o \\ \hline v & F_i & \boxed{F_i'} \\ o & & \end{array}$$

$$T' = (\mathbb{t}_1 \dots \mathbb{t}_o) \qquad S = (\mathbb{s}_1 \dots \mathbb{s}_{o+v})$$

$$\begin{aligned}
\Longrightarrow P_1 \cdot \mathbb{t}_o &= \beta_o^{(1)} \cdot \mathbb{s}_o, \\
P_2 \cdot \mathbb{t}_1 &= \beta_o^{(2)} \cdot \mathbb{s}_o, \\
P_3 \cdot \mathbb{t}_2 &= \beta_o^{(3)} \cdot \mathbb{s}_o, \\
&\vdots \\
P_o \cdot \mathbb{t}_{o-1} &= \beta_o^{(o)} \cdot \mathbb{s}_o
\end{aligned}$$



Our proposed attack

A generator $\mathbb{s}_o$

$$\begin{bmatrix} P_i \end{bmatrix} \cdot \begin{array}{c} \quad\quad o \\ \begin{bmatrix} {}^tS^{-1} & \boxed{T'} \end{bmatrix} \end{array} = \begin{bmatrix} S \end{bmatrix} \cdot \begin{array}{c|cc} & v & o \\ \hline v & \begin{bmatrix} F_i & \boxed{F_i'} \end{bmatrix} & \\ o & & \end{array}$$

$$T' = (\mathbb{t}_1 \dots \mathbb{t}_o) \qquad S = (\mathbb{s}_1 \dots \mathbb{s}_{o+v})$$

$$\begin{aligned} \Longrightarrow P_1 \cdot \mathbb{t}_o &= \beta_o^{(1)} \cdot \mathbb{s}_o, \\ P_2 \cdot \mathbb{t}_1 &= \beta_o^{(2)} \cdot \mathbb{s}_o, \\ P_3 \cdot \mathbb{t}_2 &= \beta_o^{(3)} \cdot \mathbb{s}_o, \\ &\vdots \\ P_o \cdot \mathbb{t}_{o-1} &= \beta_o^{(o)} \cdot \mathbb{s}_o \end{aligned}$$

$\Longrightarrow$ the matrix

$$(P_1 \cdot \mathbb{t}_o \; P_2 \cdot \mathbb{t}_1 \cdots P_o \cdot \mathbb{t}_{o-1})$$

with size $n \times o$ of rank one.

Our proposed attack

Solving for $(\mathbb{t}_1, \mathbb{t}_2)$

$$
\begin{cases}
P_1 \cdot \mathbb{t}_o = \beta_o^{(1)} \cdot \mathbb{s}_o, \\
P_2 \cdot \mathbb{t}_1 = \beta_o^{(2)} \cdot \mathbb{s}_o, \\
P_3 \cdot \mathbb{t}_2 = \beta_o^{(3)} \cdot \mathbb{s}_o, \\
\vdots \\
P_o \cdot \mathbb{t}_{o-1} = \beta_o^{(o)} \cdot \mathbb{s}_o.
\end{cases}
\qquad
\begin{cases}
\beta_o^{(3)} \cdot P_2 \cdot \mathbb{t}_1 = \beta_o^{(2)} \cdot P_3 \cdot \mathbb{t}_2, \\
\beta_{o-1}^{(4)} \cdot P_3 \cdot \mathbb{t}_1 = \beta_{o-1}^{(3)} \cdot P_4 \cdot \mathbb{t}_2, \\
\beta_{o-2}^{(5)} \cdot P_4 \cdot \mathbb{t}_1 = \beta_{o-2}^{(4)} \cdot P_5 \cdot \mathbb{t}_2, \\
\vdots \\
\beta_3^{(o)} \cdot P_{o-1} \cdot \mathbb{t}_1 = \beta_2^{(o-1)} \cdot P_o \cdot \mathbb{t}_2.
\end{cases}
\quad (B)
$$

In order to solve these quadratic polynomials for $(\mathbb{t}_1, \mathbb{t}_2)$ with unknown β, it is necessary to guess β's properly.

Our proposed attack

Solving for $(\mathbb{t}'_1, \mathbb{t}'_2)$

If we re-set $\mathbb{t}'_i \coloneqq \beta_o^{(i+1),-1} \cdot \mathbb{t}_i$, then $\mathbb{t}'_1, \dots, \mathbb{t}'_o$ also satisfy the properties (A) of 'Main aim'.

From (B),

$$\begin{cases} P_2 \cdot \mathbb{t}'_1 = P_3 \cdot \mathbb{t}'_2, \\ P_3 \cdot \mathbb{t}'_1 = \gamma^{(1)} \cdot P_4 \cdot \mathbb{t}'_2, \\ P_4 \cdot \mathbb{t}'_1 = \gamma^{(2)} \cdot P_5 \cdot \mathbb{t}'_2, \\ \quad \vdots \\ P_{o-1} \cdot \mathbb{t}'_1 = \gamma^{(o-3)} \cdot P_o \cdot \mathbb{t}'_2, \end{cases}$$

Guessing some $\gamma^{(i)}$ with brute force, solve these relations for $(\mathbb{t}'_1, \mathbb{t}'_2)$.

where $\gamma^{(i)} \coloneqq \beta_{o-i}^{(i+2)} \cdot \beta_{o-i}^{(i+3),-1} \cdot \beta_o^{(3)} \cdot \beta_o^{(2),-1}$ $(i = 1, \dots, o-3)$.

In a similar way, we can deduce the equations for getting $(\mathbb{t}'_3, \dots, \mathbb{t}'_o)$.

Please refer to our paper for details.

Implementation result

(q, v, o)	Cputime (s)
$(2^8, 72, 46)$ security level 1	96
	99
	96
	95
	94
$(2^8, 112, 72)$ security level 3	527
	514
	505
	517
	502
$(2^8, 148, 96)$ security level 5	1613
	1644
	1602
	1077
	981

- Found the candidates of the pair $(\mathbb{t}'_1, \mathbb{t}'_2)$.

- Conducted on a system with Apple M1 (8 cores), 16GB memory, macOS Ventura 13.3 ver. Using Magma V2.27-8.

Conclusions

- Aulbach et al. proposed a practical key recovery attack against MQ-Sign-SS/RS by utilizing two properties:

  (1) OV parts in central map are sparse.

  (2) the secret key $\mathcal{S}$ having the form of

$$S = \begin{bmatrix} I_{v\times v} & \mathbf{0}_{v\times \boldsymbol{o}} \\ * & I_{o\times o} \end{bmatrix}.$$

- We propose an attack against MQ-Sign-RS/SS without the property (2).

- The MQ-Sign-SR/RR are considered as secure among the four types of MQ-Sign.

Thank you for listening!

Contact information

jo-hyungrok-xz@ynu.ac.jp

hyungrok.jo@gmail.com