A Security Analysis on MQ-Sign

Ikematsu, Yasuhiko
Institute of Mathematics for Industry, Kyushu University

Jo, Hyungrok
Institute of Advanced Sciences, Yokohama National University

Yasuda, Takanori
Institute for the Advancement of Higher Education, Okayama University of Science

出版情報：pp.40-51, 2024-01-11. Springer
バージョン：
権利関係：

A security analysis on MQ-Sign

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

[1] Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka 819–0395, Japan
[2] Institute of Advanced Sciences, Yokohama National University, 79-7, Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan
[3] Institute for the Advancement of Higher Education, Okayama University of Science, 1-1, Ridaicho, Kita-ku, Okayama 700-0005, Japan
ikematsu@imi.kyushu-u.ac.jp, jo-hyungrok-xz@ynu.ac.jp, tyasuda@ous.ac.jp

Abstract. MQ-Sign is a variant of the UOV singature scheme proposed by Shim et al. It has been suggested as a candidate for the standardization of post-quantum cryptography in Republic of Korea (known as KpqC). However, recently Aulbach et al. proposed a practical key recovery attack against MQ-Sign-RS and MQ-Sign-SS with a simple secret key $\mathcal{S}$. In this paper, we propose another attack that is valid for the case of a general secret key $\mathcal{S}$.

1 Introduction

Post-Quantum Cryptography (PQC) [2] is a new generation cryptographic system that distinguishes itself from conventional cryptographic systems that rely on the hardness of integer factorization problems, and is globally popularized due to its resistance to attacks by Shor's quantum algorithm [10]. Currently, the National Institute of Standards and Technology (NIST) [7] is working towards the standardization of practical post-quantum cryptography systems that provide both adequate security and practicality. The ultimate objective is to promote these cutting-edge cryptographic systems in the near future. NIST announced the results [8] of its third round of selection in July 2022, with CRYSTALS-Kyber being chosen for the KEM category, and CRYSTALS-Dilithium, Falcon, and SPHINCS+ being selected for the signature category.

In February 2022, the Korean Post-Quantum Cryptography Competition (KpqC, for short) [4] was launched in South Korea for the standardization of post-quantum cryptography. In November 2022, the Round 1 of KpqC was announced, and 7 candidates (3 Lattice-based, 3 Code-based, and 1 Graph-based) were selected in the Public Key Encryption/Key-Establishment Algorithms category, while 9 candidates (5 Lattice-based, 1 Code-based, 1 Multivariate-based, 1 Isogeny-based, and 1 MPCitH-based) were selected in the Digital Signature Algorithms category.

In the pursuit of post-quantum digital signature schemes, multivariate cryptography has emerged as a promising candidate. MPKC (Multivariate Public

[4] The Korean Post-Quantum Cryptography Competition, www.kpqc.or.kr

Key Cryptography) is based on the hardness of the Multivariate Quadratic polynomial problem (MQ problem, for short), which asks to solve a system of multivariate quadratic equations over a finite field. MPKC is attractive due to its fast signature verification and small signature sizes. In particular, UOV [6] and Rainbow [5] have been actively researched as leading schemes in the area of MPKC in recent years. However, it is essential to note that Rainbow scheme [5], which was a finalist of NIST PQC standardization, has been broken by the attack proposed by Beullens [3]. Therefore, careful selection and analysis of multivariate signature schemes are necessary to ensure their security in practice.

The MQ-Sign [9] is a UOV-based signature scheme proposed by Shim et al., which was submitted to the KpqC competition for the standardization of post-quantum cryptography in the Republic of Korea. MQ-Sign acquired the efficiency by making the central map of UOV sparse. Recently, Aulbach et al. [1] proposed a practical key recovery attack against MQ-Sign-{R/S}S for the case that a secret key $\mathcal{S}$ has a simple form. Here, the suffixes "R" and "S" in "MQ-Sign-{R}{S}" respectively stand for the selection of the Vinegar $\times$ Vinegar quadratic parts using Random polynomials, and the selection of the Oil $\times$ Vinegar quadratic parts using Sparse polynomials. In this paper, we propose another attack against MQ-Sign-{R/S}S which is valid for the case of a general secret key $\mathcal{S}$.

We also provide the experimental results of our attack, which broke the proposed parameters of security level 1, 3, and 5 in [9] by a usual laptop within about 30 minutes.

This paper is organized as follows. In Section 2, we provide the explanation of the UOV signature scheme and its variant, MQ-Sign(-RS). In Section 3, we give a detailed description of a series of attack methods against MQ-Sign-RS. In Section 4, we demonstrate the results of implementation performed to validate the effectiveness of our attack. In Section 5, we conclude our results.

2 MQ-Sign

In this section, we explain the constructions of the UOV (Unbalanced Oil and Vinegar) signature scheme and its improved variant, MQ-Sign.

2.1 UOV

Let $\mathbb{F}_q$ be a finite field. Here, we briefly recall the construction of the UOV signature scheme [6]. Let v and o be two positive integers such that $v > o > 0$ and set $n := v + o$. We use two variable sets $\mathbf{x}_v = (x_1, \ldots, x_v)$, and $\mathbf{x}_o = (x_{v+1}, \ldots, x_n)$, and put $\mathbf{x} = (\mathbf{x}_v, \mathbf{x}_o)$. We call the first variables $\mathbf{x}_v$ the *vinegar variables* and the second variables $\mathbf{x}_o$ the *oil variables*.

Key Generation: Randomly choose o quadratic polynomials in the variables $\mathbf{x}$ in the following form:

$$\begin{aligned} f_1(\mathbf{x}) = f_1(\mathbf{x}_v, \mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} a_{i,j}^{(1)} x_i x_j, \\ &\vdots \\ f_o(\mathbf{x}) = f_o(\mathbf{x}_v, \mathbf{x}_o) &= \sum_{i,j=1}^{v} a_{i,j}^{(o)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} a_{i,j}^{(o)} x_i x_j. \end{aligned} \tag{1}$$

Here, each coefficient $a_{i,j}^{(k)}$ is randomly chosen from the finite field $\mathbb{F}_q$. Then, the set $\mathcal{F} = (f_1, \cdots, f_o)$ is called a *central map* of the UOV scheme. Once we randomly choose an invertible linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, the public key is given by the composite $\mathcal{P} := \mathcal{F} \circ \mathcal{S} = \{p_1, \cdots, p_o\}$, which is a set of o quadratic polynomials. Moreover, the secret key is $\{\mathcal{F}, \mathcal{S}\}$.

Signature Generation: Given a message $\mathbf{m} = (m_1, \ldots, m_o) \in \mathbb{F}_q^o$ to be signed, a signature $\mathbf{s}$ is generated as follows. First, randomly choose an element $\mathbf{c} = (c_1, \ldots, c_v) \in \mathbb{F}_q^v$. Second, we can easily obtain a solution $\mathbf{d} \in \mathbb{F}_q^o$ to the equations

$$f_1(\mathbf{c}, \mathbf{x}_o) = m_1, \cdots, f_o(\mathbf{c}, \mathbf{x}_o) = m_o,$$

since they are o linear equations in oil variables $\mathbf{x}_o$ from the form of (1). If there is no solution, we choose another element $\mathbf{c}$. Finally, we compute $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{c}, \mathbf{d}) \in \mathbb{F}_q^n$, which is a solution to $\mathcal{P}(\mathbf{x}) = \mathbf{m}$. This $\mathbf{s} \in \mathbb{F}_q^n$ is a signature of the message $\mathbf{m}$.

Verification: It is performed by checking whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$.

2.2 MQ-Sign-RS

MQ-Sign used here refers specifically to MQ-Sign-RS. MQ-Sign is constructed by making the central map in (2) sparse as follows.

$$\begin{aligned} f_1(\mathbf{x}) &= \sum_{i,j=1}^{v} \alpha_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v} \beta_i^{(1)} x_i x_{(i+1-2 \pmod o)+v+1}, \\ &\vdots \\ f_k(\mathbf{x}) &= \sum_{i,j=1}^{v} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i=1}^{v} \beta_i^{(k)} x_i x_{(i+k-2 \pmod o)+v+1}, \\ &\vdots \\ f_o(\mathbf{x}) &= \sum_{i,j=1}^{v} \alpha_{i,j}^{(o)} x_i x_j + \sum_{i=1}^{v} \beta_i^{(o)} x_i x_{(i+o-2 \pmod o)+v+1}. \end{aligned} \tag{2}$$

Here each $\beta_i^{(k)}$ is randomly chosen from $\mathbb{F}_q^\times$. The linear and constant terms are omitted as they are not relevant in our attack. The signature generation and verification are identical to those of the original UOV scheme.

3 Our proposed attack

In this section, we describe our attack against MQ-Sign-RS. In 3.1, we explain the representation of quadratic polynomials. In 3.2, we describe the representation of some quadratic polynomials in the central map of MQ-Sign-RS. In 3.3, 3.4 and 3.5, we state the idea of our attack and describe the algorithm to break MQ-Sign-RS.

3.1 Preliminary

We recall a relation between quadratic polynomials and square matrices. For a homogeneous quadratic polynomial

$$g(\mathbf{x}) = \sum_{1 \leqslant i \leqslant j \leqslant n} g_{ij} x_i x_j \in \mathbb{F}_q[\mathbf{x}],$$

we define the upper triangular matrix G^{up} by

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

Then, we obtain the following equality

$$g(\mathbf{x}) = \mathbf{x} \cdot G^{\mathrm{up}} \cdot {}^t\mathbf{x},$$

where ${}^t\mathbf{x}$ denotes the transpose of $\mathbf{x}$. It is clear that the map $g \mapsto G^{\mathrm{up}}$ is a bijective map between the set of homogeneous quadratic polynomials in $\mathbb{F}_q[\mathbf{x}]$ and the set of upper triangular (square) matrices of size n. Let $\mathcal{S}$ be a linear map on $\mathbb{F}_q^n$ and let S be its corresponding matrix of size n. Then, we have

$$g \circ \mathcal{S}(\mathbf{x}) = \mathbf{x} \cdot S \cdot G^{\mathrm{up}} \cdot {}^tS \cdot {}^t\mathbf{x}.$$

However, since $S \cdot G^{\mathrm{up}} \cdot {}^tS$ is not an upper triangular matrix in general, the corresponding upper triangular matrix of $g \circ \mathcal{S}(\mathbf{x})$ is not equal to $S \cdot G^{\mathrm{up}} \cdot {}^tS$.

To avoid this inequality, it is necessary to consider symmetric matrices. For the above quadratic polynomial $g(\mathbf{x})$, we define the following symmetric matrix:

$$G := G^{\mathrm{up}} + {}^tG^{\mathrm{up}}.$$

Then, the corresponding symmetric matrix of $g \circ \mathcal{S}(\mathbf{x})$ is equal to

$$S \cdot G \cdot {}^tS.$$

Thus, if $(F_1, \ldots, F_o)$ and $(P_1, \ldots, P_o)$ are 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

$$(P_1, \ldots, P_o) = \left(SF_1{}^tS, \ldots, SF_o{}^tS\right),$$

where S are the corresponding matrices of size n to the secret key $\mathcal{S}$. As a result, it is considered that the symmetric matrices of the public key $\mathcal{P}$ inherit some properties of the symmetric matrices of the central map $\mathcal{F}$.

Remark 1. Aulbach et al. [1] proposed a practical attack against MQ-Sign-{R/S}S in the case where S can be written as the secret key $S = \begin{pmatrix} 1_v & 0 \\ * & 1_o \end{pmatrix}$.

3.2 Representation matrices of the central map of MQ-Sign-RS

From the construction of the central map (2) of MQ-Sign-RS, the representation matrices $F_1, \ldots, F_o$ have the special form as follows:

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

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

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

$$F_4 = \left(\begin{array}{c|cccccccccc} & 0 & 0 & 0 & \beta_1^{(4)} & & & & & & \\ & & & & \vdots & \ddots & & & & & \\ & & & & \vdots & & \beta_{v-o}^{(4)} & & & & \\ & & & & \vdots & & & \beta_{v-o+1}^{(4)} & & & \\ & & & & \vdots & & & & \ddots & & \\ * & & & & \vdots & & & & & \beta_{o-3}^{(4)} & \\ & \beta_{o-2}^{(4)} & & & \vdots & & & & & 0 & \\ & & \beta_{o-1}^{(4)} & & \vdots & & & & & 0 & \\ & & & \beta_o^{(4)} & \vdots & & & & & 0 & \\ \hline & & & & \beta_{o+1}^{(4)} & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & \beta_v^{(4)} & & & & \\ \hline * & & & & & \multicolumn{5}{c}{\mathbf{0}} \end{array}\right)$$

We omit F_5 and later. We denote the right-hand side of F_i as F_i' $(i = 1, \ldots, o)$.

3.3 The idea of our attack

Now we describe the idea of our proposed attack. First, our purpose is to find o linear independent vectors $\mathbf{t}_1, \ldots, \mathbf{t}_o \in \mathbb{F}_q^n$ such that

$$ {}^t\mathbf{t}_i \cdot P_k \cdot \mathbf{t}_j = 0, \quad p_k(\mathbf{t}_i) = 0 \quad (1 \leqslant i, j, k \leqslant o). \tag{3}$$

It is well-known that if such vectors are recovered from the public key $\{p_1, \ldots, p_o\}$, then any signature can be forged easily.

Next, we utilize the special structure of $F_1, F_2, \ldots, F_o$ as described above. We set $T := {}^tS^{-1}$, denote by $\mathbf{t}_1, \ldots, \mathbf{t}_o$ the $v+1, \ldots, o$-th column vectors in T, and put $T' := \begin{pmatrix} \mathbf{t}_1 & \cdots & \mathbf{t}_o \end{pmatrix}$. Since S is the secret key, we see that these vectors $\mathbf{t}_1, \ldots, \mathbf{t}_o$ satisfy the above condition (3). Moreover, since $P_i = S \cdot F_i \cdot {}^tS$, we have $P_i \cdot T = S \cdot F_i$. From this, we obtain the following relations:

$$\begin{aligned} P_1 \cdot T' = S \cdot F_1', \quad P_2 \cdot T' = S \cdot F_2', \quad P_3 \cdot T' = S \cdot F_3', \\ \cdots \quad , \quad P_o \cdot T' = S \cdot F_o'. \end{aligned} \tag{4}$$

Furthermore, by setting $S = \begin{pmatrix} \mathbf{s}_1 & \cdots & \mathbf{s}_n \end{pmatrix} \in \mathbb{F}_q^{n \times n}$, we have the following relations using the description in Subsection 3.2.

$$\begin{aligned} cP_1 \cdot \mathbf{t}_o = \beta_o^{(1)} \cdot \mathbf{s}_o, \quad P_2 \cdot \mathbf{t}_1 = \beta_o^{(2)} \cdot \mathbf{s}_o, \quad P_3 \cdot \mathbf{t}_2 = \beta_o^{(3)} \cdot \mathbf{s}_o, \\ \cdots \quad , \quad P_o \cdot \mathbf{t}_{o-1} = \beta_o^{(o)} \cdot \mathbf{s}_o. \end{aligned} \tag{5}$$

Similarly, by (4), we have

$$\begin{aligned}
\beta_o^{(3)} \cdot P_2 \cdot \mathbf{t}_1 &= \beta_o^{(2)} \cdot P_3 \cdot \mathbf{t}_2, \\
\beta_{o-1}^{(4)} \cdot P_3 \cdot \mathbf{t}_1 &= \beta_{o-1}^{(3)} \cdot P_4 \cdot \mathbf{t}_2, \\
\beta_{o-2}^{(5)} \cdot P_4 \cdot \mathbf{t}_1 &= \beta_{o-2}^{(4)} \cdot P_5 \cdot \mathbf{t}_2, \\
&\vdots \\
\beta_3^{(o)} \cdot P_{o-1} \cdot \mathbf{t}_1 &= \beta_2^{(o-1)} \cdot P_o \cdot \mathbf{t}_2.
\end{aligned} \tag{6}$$

Remark 2. By (5), we see that the matrix $\left(P_1 \cdot \mathbf{t}_o \; P_2 \cdot \mathbf{t}_1 \; \cdots \; P_o \cdot \mathbf{t}_{o-1}\right)$ with size $n \times o$ is of rank one, since each column vector is generated by $\mathbf{s}_o$.

We would like to find $\mathbf{t}_1, \ldots, \mathbf{t}_o$ by solving the equations (5) and (6). Here, note that if we set $\mathbf{t}'_i := \beta_o^{(i+1),-1} \cdot \mathbf{t}_i$, then $\mathbf{t}'_1, \ldots, \mathbf{t}'_o$ also satisfy (3). Thus, it is enough to find $\mathbf{t}'_1, \ldots, \mathbf{t}'_o$ to break MQ-Sign-RS. Then, the above relations are rewritten as follows:

$$P_1 \cdot \mathbf{t}'_o = P_2 \cdot \mathbf{t}'_1 = P_3 \cdot \mathbf{t}'_2 = \cdots = P_o \cdot \mathbf{t}'_{o-1}. \tag{7}$$

Also,

$$\begin{aligned}
P_2 \cdot \mathbf{t}'_1 &= P_3 \cdot \mathbf{t}'_2, \\
P_3 \cdot \mathbf{t}'_1 &= \gamma^{(1)} \cdot P_4 \cdot \mathbf{t}'_2, \\
P_4 \cdot \mathbf{t}'_1 &= \gamma^{(2)} \cdot P_5 \cdot \mathbf{t}'_2, \\
&\vdots \\
P_{o-1} \cdot \mathbf{t}'_1 &= \gamma^{(o-3)} \cdot P_o \cdot \mathbf{t}'_2,
\end{aligned} \tag{8}$$

where $\gamma^{(i)} := \beta_{o-i}^{(i+2)} \cdot \beta_{o-i}^{(i+3),-1} \cdot \beta_o^{(3)} \cdot \beta_o^{(2),-1}$ $(i = 1, \ldots, o-3)$, which are unknown for an attacker.

We solve the above linear equations by guessing some $\gamma^{(i)}$ with brute force. By doing so, we can obtain the vectors $\mathbf{t}'_1, \ldots, \mathbf{t}'_o$ that are forgeable with any signature. In the following subsections, we describe the algorithm to solve the above equations (7) and (8).

3.4 How to recover $\mathbf{t}'_1$ and $\mathbf{t}'_2$

First step is to recover to $\mathbf{t}'_1$ and $\mathbf{t}'_2$.

From (8), since $\begin{pmatrix} \mathbf{t}'_1 \\ \mathbf{t}'_2 \end{pmatrix}$ is a non-zero element of the right kernel of the following matrix

$$\begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma^{(1)} \cdot P_4 \end{pmatrix} \in \mathbb{F}_q^{2n \times 2n},$$

the determinant of this matrix is zero. Since $\gamma^{(1)}$ is unknown, an attacker must collect candidates of $\gamma^{(1)}$. Therefore, we collect $\gamma_1 \in \mathbb{F}_q^\times$ such that the determinant of the matrix $\begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \end{pmatrix}$ is zero, which gives us the set $\mathit{\Gamma}_1$ defined as

$$\mathit{\Gamma}_1 := \left\{ \gamma_1 \in \mathbb{F}_q^\times \;\middle|\; \det \begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \end{pmatrix} = 0 \right\}.$$

Next, for such a $\gamma_1 \in \mathit{\Gamma}_1$, we find $\gamma_2 \in \mathbb{F}_q^\times$ such that the rank of the following matrix is less than $2n$:

$$\begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \\ P_4 & -\gamma_2 \cdot P_5 \end{pmatrix} \in \mathbb{F}_q^{2n \times 3n}.$$

Similarly, we define

$$\mathit{\Gamma}_2 := \left\{ (\gamma_1, \gamma_2) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times \;\middle|\; \det \begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \end{pmatrix} = 0, \;\; \mathrm{Rank} \begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \\ P_4 & -\gamma_2 \cdot P_5 \end{pmatrix} < 2n \right\}.$$

We construct $\mathit{\Gamma}_i$ for $i \geqslant 3$ in a similar way. When the number of $\mathit{\Gamma}_i$ is small for some i, we compute the right kernel of

$$\begin{pmatrix} P_2 & -P_3 \\ P_3 & -\gamma_1 \cdot P_4 \\ \vdots & \vdots \\ P_{i+2} & -\gamma_i \cdot P_{i+3} \end{pmatrix}$$

for all $(\gamma_1, \ldots, \gamma_i) \in \mathit{\Gamma}_i$ in order to recover $(\mathbf{t}'_1, \mathbf{t}'_2)$. It is worth noting that there exist some candidates of $(\mathbf{t}'_1, \mathbf{t}'_2)$ in this step.

3.5 How to recover the other vectors $\mathbf{t}'_3, \ldots, \mathbf{t}'_o$

In this subsection, we utilize the possible values of $\mathbf{t}'_1, \mathbf{t}'_2$ obtained in Subsection 3.4 to deduce the remaining vectors $\mathbf{t}'_3, \ldots, \mathbf{t}'_o$. By (7) and (2), we have the following linear equations regarding $\mathbf{t}'_3$:

$$P_2 \cdot \mathbf{t}'_1 - P_4 \cdot \mathbf{t}'_3 = 0, \quad {}^t\mathbf{t}'_1 \cdot P_k \cdot \mathbf{t}'_3 = 0, \quad {}^t\mathbf{t}'_2 \cdot P_k \cdot \mathbf{t}'_3 = 0 \quad (k = 1, \ldots, o).$$

By solving this linear equations, we obtain $\mathbf{t}'_3$.

Similarly, we have the following linear equations regarding $\mathbf{t}'_\ell$ for $\ell = 4, \ldots, o$:

$$P_2 \cdot \mathbf{t}'_1 - P_{(\ell+1 \pmod o)} \cdot \mathbf{t}'_\ell = 0, \quad {}^t\mathbf{t}'_j \cdot P_k \cdot \mathbf{t}'_\ell = 0 \quad (j = 1, \ldots, \ell-1,\ k = 1, \ldots, o)$$

Once we obtain $\mathbf{t}'_1, \ldots, \mathbf{t}'_o$, we check if those satisfy the condition (3). If not, we re-select another pair of $\mathbf{t}'_1$ and $\mathbf{t}'_2$.

4 Implementation results and complexity analysis

4.1 Experiments

In this subsection, we report the implementation results of our attack described in Section 3. All experiments in this subsection were conducted on a system with Apple M1 (8 cores), 16GB memory, macOS Ventura 13.3 ver. and using Magma V2.27-8 [4].

We conducted experiments to measure the timings of our attack for three parameters proposed in the original document [9]. For each parameter, we executed 5 experiments. Note that in our experiments we computed only $\Gamma_1, \Gamma_2, \Gamma_3$ and found the candidates of the pair $(\mathbf{t}'_1, \mathbf{t}'_2)$. All experiments were successful. In Table 1, we present the timings of our attack for each parameter.

4.2 Complexity

From Table 1, we assume that $\#\Gamma_1 \approx \#\Gamma_2 \approx \cdots \approx \#\Gamma_{o-3} \leqslant q$. To compute Γ_1, we need to perform $q \times (2n)^3$ operations. Similarly, to compute Γ_2, we need $\#\Gamma_1 \times q \times (2n)^3$ operations, and so on for $\Gamma_3, \ldots, \Gamma_{o-3}$. The total complexity to find $\mathbf{t}'_1, \mathbf{t}'_2$ is therefore $O(oq^2n^3)$. To find $\mathbf{t}'_3, \ldots, \mathbf{t}'_o$, we need to solve linear systems in n variables $o-3$ times, which results in a complexity of $O(on^3)$. Thus, the overall complexity of our attack is

$$O(oq^2n^3).$$

The complexity of our attack for level 1 is $46 \times 2^{16} \times 118^3 = 2^{28.4}$. For level 3, the complexity is $72 \times 2^{16} \times 184^3 = 2^{29.7}$, and for level 5, the complexity is $96 \times 2^{16} \times 244^3 = 2^{30.5}$.

5 Conclusion

MQ-Sign is a UOV-based signature scheme proposed by Shim et al. and submitted to the KpqC competition. Recently, Aulbach et al. proposed a practical key recovery attack against MQ-Sign-{R/S}S for the case where the secret key $\mathcal{S}$ has a simple form. Their attack was proposed by utilizing two properties: (i) Oil $\times$ Vinegar quadratic parts in the central map are sparse, and (ii) the secret key $\mathcal{S}$ has the form of $\begin{pmatrix} 1_v & 0 \\ * & 1_o \end{pmatrix}$. In this paper, we proposed an attack against MQ-Sign-{R/S}S without the property (ii). Due to our experiments, all the proposed parameters of MQ-Sign-RS can be broken in 30 minutes. Since our attack exploits only property (i), it can be applied to MQ-Sign-SS without modification. As a result, it is considered that MQ-Sign-SR and MQ-Sign-RR are secure among the four types of MQ-Sign.

Table 1. Timings of proposed attack algorithm and the cardinality of Γ_i ($i = 1, 2$, and 3) for the cases of security level 1, 3, and 5.

(q, v, o)	$\#\Gamma_1$	$\#\Gamma_2$	$\#\Gamma_3$	Cputime (s)
$(2^8, 72, 46)$	19	18	16	96
	21	18	16	99
	19	18	16	96
	19	18	16	95
	18	18	16	94
$(2^8, 112, 72)$	33	30	28	527
	30	30	28	514
	29	30	28	505
	31	30	28	517
	28	30	28	502
$(2^8, 148, 96)$	41	42	40	1613
	45	42	40	1644
	40	42	40	1602
	39	41	40	1077
	37	42	40	981

Acknowledgments

This research was in part conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan. This work was also supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Number JP22K17889, JP20K03741, Japan.

References

1. T. Aulbach, S. Samardjiska, and M. Trimoska, Practical key-recovery attack on MQ-Sign, Cryptology ePrint Archive, `https://ia.cr/2023/432`, 2023.
2. D.J. Bernstein, J. Buchmann, and E. Dahmen (Eds.): Post-Quantum Cryptography, Springer, 2009.
3. W. Beullens, Breaking Rainbow Takes a Weekend on a Laptop, CRYPTO 2022, LNCS, vol.13508, pp.464-479, Springer, 2022.
4. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., vol.24, no.3-4, pp.235-265, 1997.
5. J. Ding, and D.S. Schmidt, Rainbow, a new multivariate polynomial signature scheme, ACNS 2005, LNCS, vol.3531, pp.164-175, Springer, 2005.
6. A. Kipnis, L. Patarin, and L. Goubin, Unbalanced Oil and Vinegar Schemes, EUROCRYPT 1999, LNCS, vol.1592, pp.206-222, Springer, 1999.
7. National Institute of Standards and Technology, Post-Quantum Cryptography Standardization,
`https://csrc.nist.gov/projects/post-quantum-cryptography`

8. National Institute of Standards and Technology, Post-quantum cryptography, Round 3 submission, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions
9. K.-A. Shim, J. Kim, and Y. An, MQ-Sign: A New Post-Quantum Signature Scheme based on Multivariate Quadratic Equations: Shorter and Faster. https://www.kpqc.or.kr/images/pdf/MQ-Sign.pdf, 2022.
10. P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, In Proceedings 35th annual symposium on foundations of computer science, pp.124-134, IEEE, 1994.