IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024CIP0003

Publicized:2024/09/20

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER

A New Cryptanalysis Against UOV-based Variants MAYO, QR-UOV and VOX*

Hiroki FURUE[†], ***Nonmember and*** **Yasuhiko IKEMATSU**[††], ***Member***

SUMMARY Multivariate public-key cryptography (MPKC) is considered as one of the main candidates for post-quantum cryptography (PQC). In MPKC, the MinRank attacks, which try to solve the MinRank problem obtained from a public key, are important since a lot of multivariate schemes are broken by these attacks. Among them, the rectangular MinRank attack was recently proposed for the Rainbow scheme by Beullens, and it tries to solve a new kind of MinRank problem obtained by transforming the public key of Rainbow. Due to this attack, it is known that the security level of Rainbow was reduced. Rainbow is a multi-layered variant of the UOV scheme, and UOV is considered having a resistance to all MinRank attacks since its public key consists of full rank matrices. Recently, there have been submitted three new variants of the UOV scheme having a small public key, MAYO, QR-UOV and VOX in the NIST PQC standardization of additional digital signature schemes. In this paper, we show that the rectangular MinRank attack is applicable to MAYO, QR-UOV and VOX. Moreover, we estimate the complexity of the attack. In particular, we report that all the parameter sets of VOX submitted to NIST PQC standardization are broken in at most 2^{55} gate operations.

key words: *post-quantum cryptography, multivariate public-key cryptography, UOV, QR-UOV, MAYO, VOX, MinRank attack.*

1. Introduction

Multivariate public-key cryptography (MPKC) [8] is considered as one of the main candidates for post-quantum cryptography (PQC) [2]. A lot of multivariate schemes have been proposed so far, and the UOV signature scheme [16], which was proposed by Kipnis et al. in 1999, is considered as a secure multivariate scheme.

Rainbow [9] is an improved signature scheme obtained by layering the structure of UOV, and was proposed by Ding et al. in 2005. Since Rainbow has more complicated structure than UOV, there exist a lot of attacks against Rainbow. In particular, MinRank attacks, which try to solve a MinRank problem obtained by the matrices of the public key, are applicable to Rainbow but not to UOV. Since Rainbow was considered to be more efficient than UOV even taking into account various attacks containing MinRank attacks, it was submitted to NIST PQC standardization [19] in 2016, and proceeded to the third round [10] in 2020. However, in 2021, Beullens broke the proposed parameters [10] of Rainbow in the third round by the simple attack [6] that uses a multi-layered structure of Rainbow. As a result, Rainbow is considered to be inefficient compared with UOV, and was not selected as a NIST PQC standardization scheme. In 2020, Beullens proposed another attack (the rectangular MinRank attack [3]) before the proposal of the simple attack [6]. The rectangular MinRank attack tries to solve a different MinRank problem obtained by transforming the matrices of the public key of Rainbow. It is known that the rectangular MinRank attack reduces the security level of the parameters in the third round [10], but not as much as the simple attack.

NIST announced to start the new project of the PQC standardization of additional digital signature schemes [20] in 2022 in order to ensure the variety of algorithms. In the additional NIST PQC standardization, 40 signature schemes were accepted to the first round in June 2023, and 11 among them are multivariate schemes. In MPKC, UOV [16] is considered to be a fundamental scheme, since it has no fatal attacks so far, and is constructed using simple algorithms. However, it has a drawback to be a large public key compared to other PQC such as lattice-based cryptosystems. To solve this problem, there have been proposed many UOV variants that try to reduce the public key size. Indeed, three UOV-based schemes, MAYO [4], QR-UOV [13], VOX [21], that have small public keys compared with the plain UOV were submitted to the additional NIST PQC standardization. Since these three schemes do not have the multi-layered structure unlike Rainbow, they were considered having a resistance to MinRank attacks, and the security analysis was done based on basic attacks of UOV: direct attack and UOV attack [17] and so on. Since MAYO, QR-UOV and VOX are compact signature schemes compared with UOV, they will attract attention in the additional NIST PQC standardization [20]. Thus, further security analysis for them are important.

In this paper, we show that the rectangular MinRank is applicable to MAYO, QR-UOV, and VOX. We confirm that the public keys of MAYO, QR-UOV, and VOX have a MinRank problem by applying a transformation performed in the rectangular MinRank attack. Moreover, we estimate the complexity of the attack following Beullens' estimation [3] in his rectangular MinRank attack against Rainbow, and we check by some experiments whether our estimation is reasonable. In particular, we report that all the parameter sets of VOX submitted to NIST PQC standardization are broken in at most 2^{55} gate operations by our attack. Moreover, the parameter of VOX for NIST security level I was broken in about 3 hours by our experiments. On the other hand, we see that the proposed parameters of MAYO and QR-UOV

[†]The author is with NTT Social Informatics Laboratories

[††]The author is with the Institute of Mathematics for Industry, Kyushu University

*The preliminary version of this paper was published at the 18th International Workshop on Security (IWSEC 2023) [11].

are secure against the rectangular MinRank attack, while the complexity of this attack is reasonably close or equal to that of the best existing attacks.

Our paper is organized as follows. In Section 2, we explain the construction of some multivariate public key cryptosystems. In Section 3, we recall the rectangular MinRank attack against Rainbow proposed by Beullens [3]. In Section 4, 5 and 6, we describe the rectangular MinRank attack against MAYO [4], QR-UOV [13] and VOX [21], respectively. Finally, we conclude our paper in Section 7.

2. Multivariate signature schemes

In this section, we explain the constructions of two multivariate signature schemes, UOV [16] and Rainbow [9]. Let $\mathbb{F}_q$ be a finite field with q elements throughout this paper.

2.1 General construction of multivariate signature scheme

Let n and m be two positive integers and we denote by $\mathbb{F}_q[x_1, \ldots, x_n]$ the polynomial ring in n variables over $\mathbb{F}_q$. For m quadratic polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$, we set the quadratic polynomial map $\mathcal{F} = (f_1, \ldots, f_m)$ as follows:

$$\mathcal{F} : \mathbb{F}_q^n \ni \mathbf{x} \mapsto (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) \in \mathbb{F}_q^m.$$

If a solution $\mathbf{x} \in \mathbb{F}_q^n$ to $\mathcal{F}(\mathbf{x}) = \mathbf{y}$ for any $\mathbf{y} \in \mathbb{F}_q^m$ can be computed easily and efficiently, then $\mathcal{F}$ is called an easily-invertible map. A multivariate scheme is constructed using such an easily-invertible map $\mathcal{F}$. Once $\mathcal{F}$ is given, randomly choose two invertible linear maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$, and compute the composite

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

to hide the easily-invertible map $\mathcal{F}$. Then the public key is given by $\mathcal{P} = (p_1, \ldots, p_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$. The secret key consists of $\{\mathcal{F}, \mathcal{T}, \mathcal{S}\}$.

The signature generation is performed as follows. For a message $\mathbf{m} \in \mathbb{F}_q^m$, first compute $\mathbf{m}' = \mathcal{T}^{-1}(\mathbf{m})$. Next, find a solution $\mathbf{x} = \mathbf{m}''$ to $\mathcal{F}(\mathbf{x}) = \mathbf{m}'$. Here, since $\mathcal{F}$ is easily-invertible, it can be solved easily. Finally, $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{m}'') \in \mathbb{F}_q^n$ is a signature of the message $\mathbf{m}$.

The verification is done by checking whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$.

2.2 UOV signature scheme

We explain the construction of the UOV signature scheme [16].

Let v and o be two integers such that $v > o > 0$ and put $n := v + o$. 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 the set of n variables $\mathbf{x} = (\mathbf{x}_v, \mathbf{x}_o)$.

The key generation is performed as follows. Randomly choose o quadratic polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ in the following form:

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

where $1 \le k \le o$. Then, $\mathcal{F} = (f_1, \ldots, f_o) : \mathbb{F}_q^n \to \mathbb{F}_q^o$ is an easily-invertible map as seen below. We randomly choose a linear invertible map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The public key is given by the composite $\mathcal{P} := \mathcal{F} \circ \mathcal{S} = (p_1, \ldots, p_o)$, and the secret key is $\{\mathcal{F}, \mathcal{S}\}$. Note that an invertible linear map $\mathcal{T} : \mathbb{F}_q^o \to \mathbb{F}_q^o$ is not necessary, since it does not change the structure of UOV.

The signature generation and verification processes are done as explained in 2.1. Here, in the signature generation, the equation $\mathcal{F}(\mathbf{x}) = \mathbf{m}'$ is easily solved as follows. Randomly choose an element $\mathbf{c} = (c_1, \ldots, c_v) \in \mathbb{F}_q^v$, and find a solution $\mathbf{d} \in \mathbb{F}_q^o$ to the following linear equations in $\mathbf{x}_o$:

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

where $\mathbf{m}' = (m_1', \ldots, m_o')$. If there is no solution, we choose another element $\mathbf{c}$. The obtained vector $(\mathbf{c}, \mathbf{d}) \in \mathbb{F}_q^n$ is a solution to $\mathcal{F}(\mathbf{x}) = \mathbf{m}'$.

2.3 Rainbow signature scheme

The Rainbow signature scheme [9] was proposed as a multi-layer variant of UOV.

Let v, o_1 and o_2 be positive integers and set $n := v + o_1 + o_2$, $m := o_1 + o_2$. We use three variable sets

$$\mathbf{x}_v = (x_1, \ldots, x_v), \quad \mathbf{x}_{o_1} = (x_{v+1}, \ldots, x_{v+o_1})$$
$$\mathbf{x}_{o_2} = (x_{v+o_1+1}, \ldots, x_n)$$

and put $\mathbf{x} = (\mathbf{x}_v, \mathbf{x}_{o_1}, \mathbf{x}_{o_2})$.

The easily-invertible map is generated as follows. Randomly choose m quadratic polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ in the following form:

$$f_1(\mathbf{x}) = \sum_{i,j=1}^{v} a_{i,j}^{(1)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} a_{i,j}^{(1)} x_i x_j,$$

$$\vdots$$

$$f_{o_1}(\mathbf{x}) = \sum_{i,j=1}^{v} a_{i,j}^{(o_1)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{v+o_1} a_{i,j}^{(o_1)} x_i x_j.$$

$$f_{o_1+1}(\mathbf{x}) = \sum_{i,j=1}^{v+o_1} a_{i,j}^{(o_1+1)} x_i x_j + \sum_{i=1}^{v+o_1} \sum_{j=v+o_1+1}^{n} a_{i,j}^{(o_1+1)} x_i x_j,$$

$$\vdots$$

$$f_m(\mathbf{x}) = \sum_{i,j=1}^{v+o_1} a_{i,j}^{(m)} x_i x_j + \sum_{i=1}^{v+o_1} \sum_{j=v+o_1+1}^{n} a_{i,j}^{(m)} x_i x_j.$$

Then, $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is an easily-invertible map of Rainbow. We randomly choose two linear invertible map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$. The public key is

given by the composite $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} = (p_1, \ldots, p_m)$, and the secret key is $\{\mathcal{F}, \mathcal{T}, \mathcal{S}\}$.

The signature generation is almost the same as UOV. In UOV, how to solve $\mathcal{F}(\mathbf{x}) = \mathbf{m}'$ is done by substituting a random value $\mathbf{c}$ in $\mathbf{x}_v$ and solving linear equations of $f_1, \ldots, f_o$ in $\mathbf{x}_o$. On the other hand, in Rainbow, it is done by substituting in $\mathbf{x}_v$ and solving linear equations of $f_1, \ldots, f_{o_1}$ in $\mathbf{x}_{o_1}$ and solving linear equations of $f_{o_1+1}, \ldots, f_m$ in $\mathbf{x}_{o_2}$. (See [9] for the detail.)

3. The rectangular MinRank attack against Rainbow

In this section, we explain the rectangular MinRank attack against Rainbow proposed by Beullens [3]. In 3.1, we state a lemma regarding matrix representations of the public key and secret key in order to describe the rectangular MinRank attack. In 3.2, we explain the idea of the rectangular MinRank attack. The description of the rectangular MinRank attack explained here is based on [15].

3.1 Matrix representation and deformation

First, we recall the matrix representation of quadratic polynomials. Let $g \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a homogeneous quadratic polynomial. Then there exists a unique symmetric matrix $G \in M_n(\mathbb{F}_q)$ such that

$$\mathbf{x} \cdot G \cdot {}^t\mathbf{y} = g(\mathbf{x}+\mathbf{y}) - g(\mathbf{x}) - g(\mathbf{y}) \quad \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n.$$

We call G the representation (symmetric) matrix of g. Here, $M_n(\mathbb{F}_q)$ means the matrix ring over $\mathbb{F}_q$ with size n.

Let $\mathcal{F} = (f_1, \ldots, f_m)$ be an easily-invertible map of a multivariate scheme and $\mathcal{P} = (p_1, \ldots, p_m)$ a corresponding public key. We set F_i to be the representation matrix of f_i and P_i that of p_i. Recall that the public key $\mathcal{P}$ satisfies $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ for some invertible linear maps $\mathcal{T}$ and $\mathcal{S}$. If we take $S \in M_n(\mathbb{F}_q)$ and $T \in M_m(\mathbb{F}_q)$ as $\mathcal{S}(\mathbf{x}) = \mathbf{x} \cdot S$ and $\mathcal{T}(\mathbf{y}) = \mathbf{y} \cdot T$, then we have

$$(P_1, \ldots, P_m) = \left(S \cdot F_1 \cdot {}^tS, \ldots, S \cdot F_m \cdot {}^tS\right) \cdot T. \quad (1)$$

By using this relation, some attacks for MPKC have been proposed so far, such as MinRank attacks. Unlike such attacks, the rectangular MinRank attack [3] was proposed by using a deformation of (1). We explain such a deformation in the following.

Let $(G_1, \ldots, G_m)$ be a set of n-by-n matrices over $\mathbb{F}_q$, and $\mathbf{g}_i^{(j)}$ denotes the j-th column vector of G_i, namely,

$$G_i = \begin{pmatrix} \mathbf{g}_i^{(1)} & \mathbf{g}_i^{(2)} & \cdots & \mathbf{g}_i^{(n)} \end{pmatrix} \in M_n(\mathbb{F}_q).$$

Then, we define the new set $(\tilde{G}_1, \ldots, \tilde{G}_n)$ of n-by-m matrices as follows:

$$\tilde{G}_1 := \begin{pmatrix} \mathbf{g}_1^{(1)} & \mathbf{g}_2^{(1)} & \cdots & \mathbf{g}_m^{(1)} \end{pmatrix},$$
$$\vdots$$
$$\tilde{G}_n := \begin{pmatrix} \mathbf{g}_1^{(n)} & \mathbf{g}_2^{(n)} & \cdots & \mathbf{g}_m^{(n)} \end{pmatrix}.$$

Then, when we apply this deformation to $(P_1, \ldots, P_m)$ and $(F_1, \ldots, F_m)$, the following lemma is easily proven from (1):

Lemma 1: [15, Lemma 5]

$$\left(\tilde{P}_1, \ldots, \tilde{P}_n\right) = \left(S \cdot \tilde{F}_1 \cdot T, \ldots, S \cdot \tilde{F}_n \cdot T\right) \cdot {}^tS.$$

3.2 Rectangular MinRank attack against Rainbow

We explain the original rectangular MinRank attack [3] against Rainbow proposed by Beullens.

Let $(F_1, \ldots, F_m)$ be the set of representation matrices of the easily-invertible map $\mathcal{F}$ of Rainbow in 2.3. Then, it is shown that $\tilde{F}_i$ has the following form:

$$\tilde{F}_i = \begin{cases} \begin{pmatrix} *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times o_1} & *_{o_1\times o_2} \\ 0_{o_2\times o_1} & *_{o_2\times o_2} \end{pmatrix} & (1 \le i \le v), \\ \begin{pmatrix} *_{v\times o_1} & *_{v\times o_2} \\ 0_{o_1\times o_1} & *_{o_1\times o_2} \\ 0_{o_2\times o_1} & *_{o_2\times o_2} \end{pmatrix} & (v+1 \le i \le v+o_1), \\ \begin{pmatrix} 0_{v\times o_1} & *_{v\times o_2} \\ 0_{o_1\times o_1} & *_{o_1\times o_2} \\ 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & (v+o_1+1 \le i \le n). \end{cases}$$

Let $(P_1, \ldots, P_m)$ be the set of representation matrices of the public key $\mathcal{P}$ of Rainbow in 2.3. Then, by Lemma 1, we have $(\tilde{P}_1, \ldots, \tilde{P}_n) = (S\tilde{F}_1T, \ldots, S\tilde{F}_nT) \cdot {}^tS$. Since $\tilde{F}_{v+o_1+1}, \ldots, \tilde{F}_n$ are of rank $\le o_2$, there exists a linear combination of $\tilde{P}_1, \ldots, \tilde{P}_n$ whose rank is $\le o_2$. Thus, $(\tilde{P}_1, \ldots, \tilde{P}_n)$ is an instance of MinRank problem with target rank o_2.

Now, we explain the rectangular Min Rank attack against Rainbow. Its purpose is to find a non-zero element of $O_2 \cdot S^{-1}$ using the above MinRank problem, where

$$O_2 := \left\{ (\overbrace{0, \ldots, 0}^{v+o_1}, \overbrace{*, \ldots, *}^{o_2}) \in \mathbb{F}_q^n \right\}.$$

By finding such an element, we can recover an equivalent secret key of Rainbow. We omit the method to recover an equivalent secret key, since the dominant part is to find a non-zero element of $O_2 \cdot S^{-1}$. See [3] for the detail.

More precisely, the rectangular MinRank attack is explained as follows. Since $\dim O_2 \cdot S^{-1} = o_2$, the vector space $O_2 \cdot S^{-1}$ intersects with the vector space $\left\{ (\overbrace{*, \ldots, *}^{v+o_1+1}, \overbrace{0, \ldots, 0}^{o_2-1}) \in \mathbb{F}_q^n \right\}$. Thus, there exists a non-zero n-by-1 vector $\mathbf{a}$ in $O_2 \cdot S^{-1}$ with the following form:

$$\mathbf{a} = (a_1, a_2, \ldots, a_{v+o_1+1}, 0, \ldots, 0) \in O_2 \cdot S^{-1}.$$

We want to find such a vector $\mathbf{a}$ by constructing two problems

that $\mathbf{a}$ satisfies. First, from $\mathbf{a}S \in O_2$, it is shown that

$$\sum_{i=1}^{v+o_1+1} a_i \tilde{P}_i = (\tilde{P}_1, \ldots, \tilde{P}_n) \cdot {}^t\mathbf{a} = (S\tilde{F}_1 T, \ldots, S\tilde{F}_n T) \cdot {}^t(\mathbf{a}S)$$

is a linear combination of $S\tilde{F}_{v+o_1+1}T, \ldots, S\tilde{F}_n T$. Thus, this linear combination $\sum_{i=1}^{v+o_1+1} a_i \tilde{P}_i$ is of rank $\leq o_2$. Namely, the vector $\mathbf{a}$ is a solution to the MinRank problem for $(\tilde{P}_1, \ldots, \tilde{P}_{v+o_1+1})$ with the target rank o_2. Second, since $\mathcal{F} = (f_1, \ldots, f_m)$ is zero on O_2, the public key $\mathcal{P} = (p_1, \ldots, p_m)$ is zero on $O_2 \cdot S^{-1}$. Thus we have $p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0$. As a result, the non-zero vector $\mathbf{a} = (a_1, \ldots, a_{v+o_1+1}, 0, \ldots, 0)$ we want to find is a common solution of the following problems.

(i) $\mathrm{Rank}\left(\sum_{i=1}^{v+o_1+1} a_i \tilde{P}_i\right) \leq o_2$,

(ii) $p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0$.

The rectangular MinRank attack [3] is the kind of attack that finds a common solution $\mathbf{a}$ of above problems (i) and (ii). These problems are solved using the support minor modeling method [1] and the bilinear XL algorithm [22]. We omit the complexity estimation for solving these problems, since it is similar to that of the rectangular MinRank attacks against MAYO and QR-UOV, which will be explained in Section 4 and 5.

Remark 1: If we apply the deformation of the representation matrices of the easily-invertible map $\mathcal{F} = (f_1, \ldots, f_o)$ of the plain UOV scheme in 2.2, then all of $(\tilde{F}_1, \ldots, \tilde{F}_n)$ are of full-rank. Thus, the corresponding deformation $(\tilde{P}_1, \ldots, \tilde{P}_n)$ of the public key does not have a MinRank problem. Therefore, the rectangular MinRank attack can not be applied for the plain UOV scheme.

4. Rectangular MinRank attack against MAYO

In this section, we show that the rectangular MinRank attack is applicable to MAYO [4]. Moreover, we give the complexity estimation following Beullens' estimation [3].

4.1 MAYO signature scheme

MAYO signature scheme is a variant of UOV proposed by Beullens [4]. The key generation is almost same as that of UOV, but how to take parameters is different. Let v, o, m be positive integers and set $n := v + o$. Randomly choose m quadratic polynomials $\mathcal{F} = (f_1, \ldots, f_m)$ in $\mathbb{F}_q[x_1, \ldots, x_n]$ in the following form:

$$f_k(\mathbf{x}) = \sum_{i,j=1}^{v} a_{i,j}^{(k)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} a_{i,j}^{(k)} x_i x_j, \tag{2}$$

where $1 \leq k \leq m$. Next, randomly choose an invertible linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Finally, the public key is given by $\mathcal{P} := \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. As seen in (2), the number m of polynomials f_i is not necessarily equal to o. More precisely, the number m would be taken larger than o in MAYO. This is the difference between UOV and MAYO in the key generation. The signature process is achieved by some techniques such as "whipping transformation". Since the attack stated below uses only information of the public key $\mathcal{P}$, we skip the details of signature and verification processes. See Section 3 in [4] for the details.

4.2 Rectangular MinRank attack

In this subsection, we explain that the rectangular MinRank attack is applicable to MAYO [4].

Let $(F_1, \ldots, F_m)$ be the set of representation matrices of the easily-invertible map $\mathcal{F}$ of MAYO. For the proposed parameters of MAYO in [4], we have $m > v > o$. From this relation, it is easily seen that the n-by-m matrices $\tilde{F}_{v+1}, \ldots, \tilde{F}_n$ are of rank $\leq v$ since they have the following form:

$$\begin{pmatrix} *_{v \times m} \\ 0_{o \times m} \end{pmatrix}.$$

Thus, as in Rainbow, the rectangular MinRank attack is applied to MAYO. To estimate the complexity in 4.3, we describe the attack in detail.

Let $(P_1, \ldots, P_m)$ be the set of representation matrices of the public key $\mathcal{P}$ of MAYO. Then, by Lemma 1, we have $(\tilde{P}_1, \ldots, \tilde{P}_n) = (S\tilde{F}_1, \ldots, S\tilde{F}_n) \cdot {}^tS$. Since $\tilde{F}_{v+1}, \ldots, \tilde{F}_n$ are of rank $\leq v$, there exists a linear combination of $\tilde{P}_1, \ldots, \tilde{P}_n$ whose rank is $\leq v$.

The rectangular MinRank attack against MAYO tries to find a non-zero element of $O \cdot S^{-1}$, where

$$O := \left\{ (\overbrace{0, \ldots, 0}^{v}, \overbrace{*, \ldots, *}^{o}) \in \mathbb{F}_q^n \right\}.$$

As in the case of Rainbow, the rectangular MinRank attack against MAYO is constructed as follows. Since $\dim O \cdot S^{-1} = o$, there exists a non-zero n-by-1 vector with the following form:

$$\mathbf{a} = (a_1, a_2, \ldots, a_{v+1}, 0, \ldots, 0) \in O \cdot S^{-1}.$$

Then, it is shown that

$$\sum_{i=1}^{v+1} a_i \tilde{P}_i = (\tilde{P}_1, \ldots, \tilde{P}_n) \cdot {}^t\mathbf{a} = (S\tilde{F}_1, \ldots, S\tilde{F}_n) \cdot {}^t(\mathbf{a}S)$$

is a linear combination of $S\tilde{F}_{v+1}, \ldots, S\tilde{F}_n$. Thus, this linear combination is of rank $\leq v$. As in the case of Rainbow, we want to find a common solution $\mathbf{a}$ of the following problems.

$$\text{(i) } \mathrm{Rank}\left(\sum_{i=1}^{v+1} a_i \tilde{P}_i\right) \leq v, \quad \text{(ii) } p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0.$$

By finding such a solution $\mathbf{a}$, we can recover an equivalent key of the secret key S of MAYO. See [4] for the detail.

4.3 Complexity analysis

In this subsection, we describe the estimation of the complexity to solve above problems (i) and (ii). This is done along Beullens' estimation [3] for the original rectangular MinRank attack against Rainbow.

First, consider problem (i). Fix an integer m' such that $v+1 \le m' \le m$. Let $\tilde{P}'_i$ be the $n \times m'$ submatrix constructed from the $(1,1)$-component to the (n,m')-component of $\tilde{P}_i$. Then one considers to apply the support minor modeling method [1] to the MinRank problem $(\tilde{P}'_1, \dots, \tilde{P}'_{v+1})$ with the target rank v. Let I' be the ideal in $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]$ generated by the bilinear equations obtained from the support minor modeling, where $\mathbf{c}$ is the set of $\binom{m'}{v}$ minor variables. (See [1] and [3] for the detail description.) For $b \in \mathbb{N}_{\ge 1}$, set

$$R'(b) := \sum_{i=1}^{b} (-1)^{i+1} \binom{m'}{v+i} \binom{n+i-1}{i} \binom{v+b-i}{b-i}.$$

Let $I'_{b,1}$ be the subspace of $(b,1)$-degree homogeneous polynomials of I' in $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]$. If the above MinRank problem behaves like a random instance, then $\dim_{\mathbb{F}_q} I'_{b,1}$ is predicted as $R'(b)$ for $1 \le b \le v+1$ by the result of Bardet et al. [1].

Next, one considers adding problem (ii) to I'. We assume that $p_1(\mathbf{a}), \dots, p_m(\mathbf{a})$ behaves like a semi-regular system, where $\mathbf{a} = (a_1, a_2, \dots, a_{v+1}, 0, \dots, 0)$. Let I be the ideal generated by I' and $p_1(\mathbf{a}), \dots, p_m(\mathbf{a})$, namely,

$$I := I' + \langle p_1(\mathbf{a}), \dots, p_m(\mathbf{a}) \rangle \subset \mathbb{F}_q[\mathbf{a}, \mathbf{c}].$$

We define

$$b_{\min} := \min \left\{ b \in \mathbb{N} \;\middle|\; \dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{c}]_{b,1} / I_{b,1} = 1 \right\}.$$

By applying to $I_{b_{\min},1}$ the bilinear XL algorithm [22] with Wiedemann algorithm [7], [23], we can find a solution $\mathbf{a}$ to problems (i) and (ii) with the following complexity:

$$\left(2(\log_2 q)^2 + \log_2 q\right) \cdot 3 \binom{m'}{v}^2 \binom{v + b_{\min}}{b_{\min}}^2 (v+1)^2 \quad (3)$$

Here, $2(\log_2 q)^2 + \log_2 q$ is the factor to convert from the number of multiplications in $\mathbb{F}_q$ to the gate count.

Following the idea of Beullens' estimation [3] to guess $b_{\min}$, we define two series in t_1 and t_2:

$$G'(t_1, t_2) := \frac{1}{(1-t_1)^{v+1}} + \binom{m'}{v} t_2 + \sum_{b=1}^{v+1} \left(\binom{m'}{v} \binom{v+b}{b} - R'(b) \right) t_1^b t_2$$

$$G(t_1, t_2) := G'(t_1, t_2) \cdot (1 - t_1^2)^m.$$

These series are derived to compute a part of the Hilbert series of $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]/I'$ and $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]/I$. However, due to some non-trivial syzygies, these are not perfectly equal to the Hilbert series of them (Also see Remark 2). We consider that $b_{\min}$ is predicted by

$$b_{\min}^{(\text{predict})} := \min \left\{ b \in \mathbb{N} \;\middle|\; G(t_1, t_2)_{b,1} \le 1 \right\}, \quad (4)$$

where $G(t_1, t_2)_{b,1}$ is the coefficient of $t_1^b t_2$. In Table 1, we experimented whether $b_{\min}$ is equal to $b_{\min}^{(\text{predict})}$ for some parameters. As seen in the table, we have $b_{\min} = b_{\min}^{(\text{predict})}$ for each m' between $v+1$ and m. From the experiments, we use $b_{\min}^{(\text{predict})}$ instead of $b_{\min}$, and theoretically estimate the time complexity of the rectangular MinRank attack against MAYO by (3). Table 2 shows the complexity of the attack against the parameters proposed in the additional NIST PQC standardization [5]. Here, m' in Table 2 represents the value between $v+1$ and m such that the complexity of the attack is minimum. The value $b_{\min}^{(\text{predict})}$ is given by (4) for this m'. "RecMin" in the table means the complexity of the rectangular MinRank attack against MAYO given by (3) as $b_{\min} = b_{\min}^{(\text{predict})}$. "Best" means the best complexity among the existing attacks stated in [5]. Here, the security level I, III and V given by NIST mean that all classical attacks require 2^{143}, 2^{207} and 2^{272} gates to break the scheme, respectively.

Table 1 Experiments for $b_{\min}$ and $b_{\min}^{(\text{predict})}$

(q, v, o, m)	m'	$b_{\min}$	$b_{\min}^{(\text{predict})}$
$(7, 5, 1, 6)$	6	4	4
$(7, 8, 1, 10)$	9	5	5
	10	4	4
$(7, 8, 2, 10)$	9	5	5
	10	4	4
$(16, 5, 1, 6)$	6	4	4
$(16, 8, 1, 10)$	9	5	5
	10	4	4
$(16, 8, 2, 10)$	9	5	5
	10	4	4

Table 2 Estimated gate count (in $\log_2(\#\text{gates})$) of the rectangular MinRank attack (RecMin) in 4.2 and the best existing attack (Best) in [5]

	(q, v, o, m)	m'	$b_{\min}^{(\text{predict})}$	RecMin	Best
I	$(16, 58, 8, 64)$	59	22	159	143
	$(16, 60, 18, 64)$	62	21	168	143
III	$(16, 89, 10, 96)$	90	33	231	207
V	$(16, 121, 12, 128)$	122	46	310	272

For example, for $(q, v, o, m) = (16, 58, 8, 64)$, the value m' runs between 59 and 64, and $m' = 59$ minimizes the complexity of the rectangular MinRank attack. Also, for $m' = 59$, we have $b_{\min}^{(\text{predict})} = 22$, and then the complexity of the attack is 2^{159} gates.

From Table 2, we see that the rectangular MinRank attack in 4.2 does not reduce the security level for the proposed parameters in [5]. However, since the complexity of the rectangular MinRank attack is reasonably close to that of

the best existing attack, we consider that one can not ignore the influence of the attack in setting a new parameter.

Remark 2: Define

$$R(b) := \binom{m'}{v}\binom{v+b}{b} - G(t_1, t_2)_{b,1}.$$

Following Beullens' estimation [3], it is considered that $R(b)$ predicts the dimension of $I_{b,1}$. Since there had been non-trivial syzygies in the quadratic equations obtained by problems (i) and (ii), $R(b)$ did not equal to the dimension of $I_{b,1}$ in our experiments in Table 1. However, since $R(b) - \dim I_{b,1}$ was very small, the values of $b_{\min}$ and $b_{\min}^{(\text{predict})}$ matched. From this, we can expect that those non-trivial syzygies do not affect the values of $b_{\min}$ and $b_{\min}^{(\text{predict})}$.

Note that if we take the influence of those syzygies into account, we have $b_{\min} \geq b_{\min}^{(\text{predict})}$. Thus, the estimated complexity of the rectangular MinRank attack by $b_{\min}^{(\text{predict})}$ gives a lower bound of the accurate complexity. Therefore, it does not change the fact that the currently proposed parameters of MAYO is secure against the rectangular MinRank attack.

5. Rectangular MinRank attack against QR-UOV

In this section, we show that the rectangular MinRank attack is applicable to QR-UOV [13]. Moreover, we give the complexity estimation following Beullens' estimation [3]. In QR-UOV, we assume that q is not even.

5.1 QR-UOV signature scheme

QR-UOV is a variant of UOV proposed by Furue et al. [13]. It is constructed by using a representation of an extension field in a matrix algebra over $\mathbb{F}_q$.

Let V, O, l be positive integers and set

$$v := Vl, o := Ol, N := V + O, n := v + o = Nl.$$

For an irreducible polynomial $f(t) \in \mathbb{F}_q[t]$ with degree l, we define the embedding

$$\phi : \mathbb{F}_{q^l} = \mathbb{F}_q[t]/(f(t)) \to M_l(\mathbb{F}_q)$$

by $(1, t, \ldots, t^{l-1}) \cdot \phi(g) = (g, gt, \ldots, gt^{l-1})$ for $g \in \mathbb{F}_{q^l}$. Then, by Theorem 1 in [13], there exists an invertible symmetric matrix $W \in M_l(\mathbb{F}_q)$ such that $W\phi(g)$ is symmetric for any $g \in \mathbb{F}_{q^l}$. We also define the following extended embedding:

$$\phi : M_N(\mathbb{F}_{q^l}) \ni (a_{ij}) \mapsto (\phi(a_{ij})) \in M_n(\mathbb{F}_q).$$

Then, we have $W^{(N)} \cdot \phi({}^tS) = {}^t\phi(S) \cdot W^{(N)}$ for any $S \in M_N(\mathbb{F}_{q^l})$, where

$$W^{(N)} := \begin{pmatrix} W & & \\ & \ddots & \\ & & W \end{pmatrix} \in M_n(\mathbb{F}_q).$$

QR-UOV is constructed by using these facts and achieved a small public key compared with UOV.

The key generation is done as follows. Randomly choose o symmetric matrices $F_1, \ldots, F_o$ in $M_N(\mathbb{F}_{q^l})$ in the following form:

$$F_i = \begin{pmatrix} *_V & *_{V\times O} \\ *_{O\times V} & 0_O \end{pmatrix}.$$

The easily-invertible map of QR-UOV is given by

$$f_i(\mathbf{x}) := \mathbf{x} \cdot W^{(N)} \cdot \phi(F_i) \cdot {}^t\mathbf{x} \quad (1 \leq i \leq o),$$

where $\mathbf{x} = (x_1, \ldots, x_n)$. Next, randomly choose an invertible matrix $S \in M_N(\mathbb{F}_{q^l})$. The public key $\mathcal{P} = (p_1, \ldots, p_o)$ is

$$p_i(\mathbf{x}) := \mathbf{x} \cdot {}^t\phi(S) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(S) \cdot {}^t\mathbf{x},$$

where $1 \leq i \leq o$. The signature and verification processes are the same of those of UOV.

5.2 Rectangular MinRank attack

In this subsection, we explain that the rectangular MinRank attack is applicable to QR-UOV [13].

First, since $W^{(N)} \cdot \phi(F_i)$ and ${}^t\phi(S) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(S)$ are symmetric, the representation matrix P_i of p_i is equal to $2 \cdot {}^t\phi(S) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(S)$. Next, by ${}^t\phi(S) \cdot W^{(N)} = W^{(N)} \cdot \phi({}^tS)$, we have

$$2^{-1} \cdot \{W^{(N)}\}^{-1} \cdot P_i = \phi({}^tS \cdot F_i \cdot S).$$

Thus, an attacker can obtain the matrices $\{{}^tS \cdot F_1 \cdot S, \ldots, {}^tS \cdot F_o \cdot S\}$ from the public key $(p_1, \ldots, p_m)$. Then we define the following quadratic polynomials over $\mathbb{F}_{q^l}$:

$$\bar{p}_i(\mathbf{y}) := \mathbf{y} \cdot {}^tS \cdot F_i \cdot S \cdot {}^t\mathbf{y},$$

where $\mathbf{y} = (y_1, \ldots, y_N)$. Here, note that $\{\bar{p}_1, \ldots, \bar{p}_o\}$ can be considered as the public key of MAYO with the parameter $v_{MAYO} = V, o_{MAYO} = O$ and $m_{MAYO} = o$, where v_{MAYO} is the number of vinegar-variables in MAYO and so on. For practical parameters of QR-UOV, we have $o > V$. Thus, as in the case of MAYO, we can apply the rectangular MinRank attack to $\bar{p}_1, \ldots, \bar{p}_o$. In this case, we want to find a common solution $\mathbf{a}$ of the following problems.

$$\text{(i) Rank}\left(\sum_{i=1}^{V+1} a_i \tilde{\bar{P}}_i\right) \leq V, \text{ (ii) } \bar{p}_1(\mathbf{a}) = \cdots = \bar{p}_o(\mathbf{a}) = 0.$$

Here $\mathbf{a} = (a_1, \ldots, a_{V+1}, 0, \ldots, 0)$ is a non-zero element of $\mathbb{F}_{q^l}^N$, and the N-by-o matrices $\tilde{\bar{P}}_i$ are the deformations of representation matrices $\bar{P}_i = 2 \cdot {}^tS \cdot F_i \cdot S$ of $\bar{p}_i$. By finding such a solution $\mathbf{a}$, we can recover an equivalent secret key of QR-UOV as in the case of MAYO.

5.3 Complexity analysis

In this subsection, we describe the estimation of the complexity to solve above problems (i) and (ii). This is also done

along Beullens' estimation [3] for the rectangular MinRank attack against Rainbow. Note that the characteristic of $\mathbb{F}_q$ is always odd in QR-UOV.

First, consider problem (i). Fix an integer o' such that $V+1 \le o' \le o$. Let $\tilde{\tilde{P}}'_i$ be the $N \times o'$ matrix obtained by removing the column vectors from $(o'+1)$-th to o-th of $\tilde{\tilde{P}}_i$. Then one considers to apply the support minor modeling method [1] to the MinRank problem $(\tilde{\tilde{P}}'_1, \ldots, \tilde{\tilde{P}}'_{V+1})$ with the target rank V. Let I' be the ideal in $\mathbb{F}_{q^l}[\mathbf{a}, \mathbf{c}]$ generated by the bilinear equations obtained from the support minor modeling, where $\mathbf{c}$ is the set of $\binom{o'}{V}$ minor variables. For $b \in \mathbb{N}$, let $I'_{b,1}$ be the subspace of $(b,1)$-degree homogeneous polynomials of I' in $\mathbb{F}_{q^l}[\mathbf{a}, \mathbf{c}]$, and set

$$R'(b) := \sum_{i=1}^{b} (-1)^{i+1} \binom{o'}{V+i} \binom{N+i-1}{i} \binom{V+b-i}{b-i}.$$

Next, one considers adding problem (ii). We assume that $\bar{p}_1(\mathbf{a}), \ldots, \bar{p}_o(\mathbf{a})$ behave as a semi-regular system, where $\mathbf{a} = (a_1, a_2, \ldots, a_{V+1}, 0, \ldots, 0)$. Let I be the ideal generated by I' and $\bar{p}_1(\mathbf{a}), \ldots, \bar{p}_o(\mathbf{a})$ in $\mathbb{F}_{q^l}[\mathbf{a}, \mathbf{c}]$. Moreover, set

$$\begin{aligned} G'(t_1, t_2) &:= \frac{1}{(1-t_1)^{v+1}} + \binom{o'}{V} t_2 \\ &\quad + \sum_{b=1}^{V+1} \left(\binom{o'}{V} \binom{V+b}{b} - R'(b) \right) t_1^b t_2, \\ G(t_1, t_2) &:= G'(t_1, t_2) \cdot (1-t_1^2)^o. \end{aligned}$$

Let $b_{\min} \in \mathbb{N}$ be the minimum of b such that

$$\dim_{\mathbb{F}_{q^l}} I_{b,1} = \dim_{\mathbb{F}_q} \mathbb{F}_{q^l}[\mathbf{a}, \mathbf{c}]_{b,1} - 1.$$

Finally, by applying to $I_{b_{\min},1}$ the bilinear XL algorithm [22] with Wiedemann algorithm [7], [23], we can find a solution $\mathbf{a}$ to problem (i) and (ii) with the following complexity:

$$(2(\log_2 q^l)^2 + \log_2 q^l) \cdot 3 \binom{o'}{V}^2 \binom{V+b_{\min}}{b_{\min}}^2 (V+1)^2 . \tag{5}$$

Following the idea of Beullens' estimation, we can state that $b_{\min}$ is predicted by

$$b_{\min}^{(\text{predict})} := \min \left\{ b \mid G(t_1, t_2)_{b,1} \le 1 \right\}, \tag{6}$$

where $G(t_1, t_2)_{b,1}$ is the coefficient of $t_1^b t_2$.

In Table 3, we experimented that $b_{\min}$ equals to $b_{\min}^{(\text{predict})}$ for some parameters. Here, since $\bar{p}_1, \ldots, \bar{p}_o$ are considered as the public key of MAYO with parameter $v_{MAYO} = V, o_{MAYO} = O$ and $m_{MAYO} = o = Ol$, we experimented for MAYO with such a parameter. As seen in Table 3, we have $b_{\min} = b_{\min}^{(\text{predict})}$. From the experiments, we use $b_{\min}^{(\text{predict})}$ instead of $b_{\min}$, and theoretically estimate the time complexity of the rectangular MinRank attack against QR-UOV. Table 4 shows the complexity of the attack against the proposed parameters in the additional NIST PQC standardization [12].

Table 3 Experiments for $b_{\min}$ and $b_{\min}^{(\text{predict})}$

(q, V, O, l)	o'	$b_{\min}^{(\text{predict})}$	$b_{\min}$
$(7, 5, 2, 3)$	6	4	4
$(7, 6, 3, 3)$	7	3	3
	8	3	3
	9	2	2
$(7, 7, 3, 3)$	8	4	4
	9	3	3
$(7, 8, 3, 3)$	9	5	5

Here, o' in Table 4 represents the value between $V+1$ and o such that the complexity of the attack is minimum. The value $b_{\min}^{(\text{predict})}$ is given by (6) for this o'. "RecMin" means the complexity of the rectangular MinRank attack against QR-UOV given by (5) as $b_{\min} = b_{\min}^{(\text{predict})}$. "Best" means the best complexity among all attacks stated in [12]. Note that the paper [12] already considers the rectangular MinRank attack to select the proposed parameters of QR-UOV via the preliminary version [11] of this paper.

Table 4 Estimated gate count (in $\log_2$(#gates)) of the rectangular MinRank attack (RecMin) in 5.2 and the best existing attack (Best) in [12]

	(q, V, O, l)	o'	$b_{\min}^{(\text{predict})}$	RecMin	Best
I	$(7, 74, 10, 10)$	75	18	162	148
	$(31, 55, 20, 3)$	56	20	153	151
	$(31, 60, 7, 10)$	61	19	157	152
	$(127, 52, 18, 3)$	53	22	158	150
III	$(7, 110, 14, 10)$	111	27	229	211
	$(31, 82, 29, 3)$	84	28	220	215
	$(31, 89, 10, 10)$	90	29	220	216
	$(127, 76, 26, 3)$	78	29	219	211
V	$(7, 149, 19, 10)$	150	35	292	277
	$(31, 108, 38, 3)$	109	40	279	279
	$(31, 112, 12, 10)$	113	41	290	275
	$(127, 102, 35, 3)$	105	35	277	277

For example, for $(q, V, O, l) = (7, 74, 10, 10)$, the value o' runs between 75 and 100, and $o' = 75$ minimizes the complexity of the rectangular MinRank attack. Also, for $o' = 75$, we have $b_{\min}^{(\text{predict})} = 18$, and then the complexity of the attack is 2^{162} gates.

From Table 4, we see that the proposed parameters of QR-UOV are secure against the rectangular MinRank attack in 5.2. As we can see in the parameter $(q, V, O, l) = (31, 108, 38, 3)$, the best attack for some parameters is the rectangular MinRank attack. In this way, we can not ignore the influence of this attack in setting a new parameter.

6. Rectangular MinRank attack against VOX

VOX [21] was proposed by Patarin et al. and is constructed by mixing some random quadratic polynomials into UOV. Moreover, using the technique of QR-UOV, VOX reduces the size of the public key.

Let V, O, l, t be positive integers and set $v := Vl, m = o := Ol, N := V + O, n := v + o = Nl$. Let ϕ, W be notations as in 5.1. The key generation is done as follows. Randomly choose t symmetric matrices $F_1, \ldots, F_t \in M_N(\mathbb{F}_{q^l})$ and $o-t$

symmetric matrices $F_{t+1}, \ldots, F_o$ in the following form:

$$F_i = \begin{pmatrix} *_V & *_{V\times O} \\ *_{O\times V} & 0_O \end{pmatrix} \in M_N(\mathbb{F}_{q^l}),\ (t+1 \le i \le o) \quad (7)$$

The easily-invertible map $\mathcal{F} = (f_1, \ldots, f_o)$ of VOX is

$$f_i(\mathbf{x}) := \mathbf{x} \cdot W^{(N)} \cdot \phi(F_i) \cdot {}^t\mathbf{x}, \quad (1 \le i \le o),$$

where $\mathbf{x} = (x_1, \ldots, x_n)$. Next, randomly choose invertible matrices $T \in M_o(\mathbb{F}_q)$ and $S \in M_N(\mathbb{F}_{q^l})$. Moreover, we define linear maps $\mathcal{T} : \mathbb{F}_q^o \to \mathbb{F}_q^o$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ associated with T and ${}^t\phi(S)$, respectively. Note that, due to the efficiency, T and S are took as having the following forms:

$$T = \begin{pmatrix} 1_t & * \\ 0 & 1_{o-t} \end{pmatrix}, \quad S = \begin{pmatrix} 1_V & * \\ 0 & 1_O \end{pmatrix}.$$

Then, the public key of VOX is given by $\mathcal{P} = (p_1, \ldots, p_o) := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^o$. See [21] for the details of signature and verification processes.

We explain that the rectangular MinRank attack is applicable to VOX. As in the case of QR-UOV, an attacker can obtain the set of matrices $({}^tS \cdot F_1 \cdot S, \ldots, {}^tS \cdot F_o \cdot S) \cdot T$ from the public key $(p_1, \ldots, p_o)$. We try to apply the rectangular MinRank problem to this set. Put

$$(\bar{P}_1, \ldots, \bar{P}_o) := ({}^tS \cdot F_1 \cdot S, \ldots, {}^tS \cdot F_o \cdot S) \cdot T.$$

Then, by the result in 3.1, we have the following

$$\left(\tilde{\bar{P}}_1, \ldots, \tilde{\bar{P}}_o\right) = \left({}^tS \cdot \tilde{F}_1 \cdot T, \ldots, {}^tS \cdot \tilde{F}_N \cdot T\right) \cdot S.$$

From the definition of $F_1, \ldots, F_o$, we have

$$\tilde{F}_i = \begin{pmatrix} *_{V\times t} & *_{V\times o-t} \\ *_{O\times t} & 0_{O\times o-t} \end{pmatrix},\ (V+1 \le i \le N).$$

Thus, if $t < O$ and $V < o - t$, then the $N \times o$ matrices $\tilde{F}_{V+1}, \ldots, \tilde{F}_N$ are of rank $t + V (< N, o)$ at most. Thus, we can consider the following MinRank problem over $\mathbb{F}_{q^l}$:

$$\mathrm{Rank}\left(\sum_{i=1}^{V+1} a_i \tilde{\bar{P}}_i\right) \le t + V. \quad (8)$$

For VOX, the rectangular MinRank attack is to solve this MinRank problem using the support minor modeling [1]. We can not add the quadratic equations $p_1 = \cdots = p_o = 0$ since $F_1, \ldots, F_t$ do not have the form (7). Note that it might be efficient to apply the support minor modeling to the transposition version of (8), namely, to the MinRank problem of $o \times N$ matrices ${}^t\tilde{\bar{P}}_1, \ldots, {}^t\tilde{\bar{P}}_{V+1}$ with rank $t + V$:

$$\mathrm{Rank}\left(\sum_{i=1}^{V+1} a_i \cdot {}^t\tilde{\bar{P}}_i\right) \le t + V. \quad (9)$$

If we get a solution $\mathbf{a} = (a_1, \ldots, a_{V+1}, 0, \ldots, 0) \in \mathbb{F}_{q^l}^N$ to (9), we can recover an equivalent key. Set $v_i := \mathbf{a} \cdot \bar{P}_i \cdot {}^t\mathbf{a} \in \mathbb{F}_{q^l}$ $(1 \le i \le o)$. For $t + 1 \le i \le o$, we find a vector $\mathbf{w}_i = {}^t(w_{i,1}, \ldots, w_{i,t}) \in \mathbb{F}_q^t$ such that

$$v_i - w_{i,1}v_1 - \cdots - w_{i,t}v_t = 0.$$

Since this is identified with l linear equations in t variables over $\mathbb{F}_q$ and we have $l = t$ in the proposed parameters of VOX [21], we can get such vectors $\mathbf{w} = (\mathbf{w}_{t+1}, \ldots, \mathbf{w}_o)$. Then, we can recover T by $\begin{pmatrix} 1_t & \mathbf{w} \\ 0 & 1_{o-t} \end{pmatrix}$. Once we recover T, an equivalent key of S is recovered using the same method as MAYO.

The complexity to solve (9) using the support minor modeling [1] is the dominant part of the rectangular MinRank attack against VOX. Fix an integer N' such that $t + V + 1 \le N' \le N$. Put

$$R'(b) := \sum_{i=1}^{b} (-1)^{i+1} \binom{N'}{t+V+i} \binom{o+i-1}{i} \binom{V+b-i}{b-i}.$$

Let $b_{\min} \in \mathbb{N}$ be the minimum of b such that

$$\binom{N'}{t+V} \binom{V+b}{b} - R'(b) \le 1.$$

Then, the complexity of the rectangular MinRank attack against VOX is given by

$$(2(\log_2 q^l)^2 + \log_2 q^l) \cdot 3 \binom{N'}{t+V}^2 \binom{V+b_{\min}}{b_{\min}}^2 \cdot (V+1)\,(t+V+1)\,.$$

Table 5 shows the complexity of the rectangular MinRank attack (9) against the parameters proposed in the additional NIST PQC standardization [21]. "RecMin" means the complexity of the rectangular MinRank against VOX. "Best" means the best complexity among the existing attacks stated in [21]. As seen in the table, the rectangular MinRank attack can break all three proposed parameters. For example, for $(q, V, O, l, t) = (251, 9, 8, 6, 6)$ of NIST security level I, VOX can be broken in 2^{51} gates.

Table 5 Estimated gate count (in $\log_2$(#gates)) of the rectangular MinRank attack (RecMin) and the best existing attack (Best) in [21]

	(q, V, O, l, t)	N'	$b_{\min}$	RecMin	Best
I	$(251, 9, 8, 6, 6)$	17	3	**51**	146
III	$(1021, 11, 10, 7, 7)$	20	3	**55**	210
V	$(4093, 13, 12, 8, 8)$	22	4	**55**	285

We executed some experiments for the parameter $(q, V, O, l, t) = (251, 9, 8, 6, 6)$ whether the rectangular MinRank attack can break this parameter in practice. Under an Intel Xeon Gold 6130 CPU @ 2.10 GHz with Magma V2.28-4, the average time in 5 experiments to break this parameter was about 11140 seconds (about 3 hours).

Remark 3: We reported our result in this section to the NIST PQC forum, and the authors of VOX proposed new parameter set in [18]. However, Guo et al. broke their new

parameters by improving our attack. See [14] for the details.

7. Conclusion

MAYO, QR-UOV and VOX are multivariate signature schemes obtained by improving the UOV signature scheme. Since they are compact signature schemes compared with UOV, they will attract attention as multivariate signature schemes in the additional standardization process for digital signature schemes by NIST. The security analysis of these schemes were done based on basic attacks: direct attack and UOV attack and so on. Thus, further security analysis for them are important. In this paper, we showed that the rectangular MinRank attack, which was originally proposed by Beullens against Rainbow, can be applied to MAYO, QR-UOV and VOX. Moreover, we estimated the complexity of this attack. In the analysis of MAYO and QR-UOV, we checked that our estimation is reasonable from some experiments in which the indicator $b_{\min}$ was equal to $b_{\min}^{(\text{predict})}$. As a result, we saw that the proposed parameters of MAYO and QR-UOV are secure against the rectangular MinRank attack, while the complexity of the attack is close or equal to that of the best existing attack. For example, the parameter $(q, v, o, m) = (16, 58, 8, 64)$ in MAYO has 2^{143} gates security for the existing attacks and 2^{159} gates for the rectangular MinRank attack. Therefore, we consider that it is necessary to analyze the rectangular MinRank attack when a new parameter of MAYO or QR-UOV is chosen. On the other hand, we showed that all the parameter sets of VOX submitted to NIST PQC standardization are broken in at most 2^{55} gate operations by our attack. Moreover, the parameter of VOX for NIST security level I was broken in about 3 hours by our experiment.

Acknowledgments
This work was supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Number JP19K20266, JP22KJ0554 and JP22K17889, Japan.

References

[1] Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R., Smith-Tone, D., Tillich, J.P, Verbel, J.: 'Improvements of algebraic attacks for solving the rank decoding and MinRank problems', ASIACRYPT 2020, LNCS 12491, pp.507-536, Springer
[2] Bernstein, D.J., Buchmann, J. and Dahmen, E. eds.: 'Post-Quantum Cryptography', Springer, 2009.
[3] Beullens, W.: 'Improved Cryptanalysis of UOV and Rainbow', EUROCRYPT 2021, LNCS 12696, pp. 348–373, Springer
[4] Beullens, W.: 'MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps', SAC 2021, LNCS 13203, pp. 355–376, Springer
[5] Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.: 'MAYO', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
[6] Beullens, W.: 'Breaking Rainbow Takes a Weekend on a Laptop'. CRYPTO 2022, LNCS 13508, pp. 464–479, Springer
[7] Cheng CM, Tung Chou T., Niederhagen R., Yang BY.: 'Solving Quadratic Equations with XL on Parallel Architectures', CHES 2012, LNCS, 7428, pp. 356–373. Springer, 2012.
[8] Ding, J., Petzoldt, A., Schmidt, D.S.: 'Multivariate Public Key Cryptosystems, Second Edition', Springer, 2020
[9] Ding, J., Schmidt, D.S.: 'Rainbow, a new multivariate polynomial signature scheme', ACNS 2005, LNCS 3531, pp.164–175, Springer
[10] Ding, J., Chen, M.S., Petzoldt, A., Schmidt, D.S., Yang, B.Y.: 'Rainbow', Technical report, National Institute of Standards and Technology, *Post-Quantum Cryptography*, ⟨https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-3-submissions⟩
[11] Furue, H., Ikematsu, Y.: 'A New Security Analysis Against MAYO and QR-UOV Using Rectangular MinRank Attack'.: IWSEC 2023, LNCS 14128, pp.101–116, Springer
[12] Furue, H., Ikematsu, Y., Hoshino, F., Takagi, T., Yasuda, K., Miyazawa, T., Saito, T., Nagai, A.: 'QR-UOV', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
[13] Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T.: 'A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV', ASIACRYPT 2021, LNCS 13093, pp. 187–217, Springer
[14] Guo, H., Ding, J.: 'A Practical MinRank Attack Against VOX', IACR Cryptology ePrint Archive, 2024/166
[15] Ikematsu, Y., Nakamura, S., Takagi, T.: 'Recent progress in the security evaluation of multivariate public-key cryptography', IET Information Security, 2022
[16] Kipnis, A., Patarin, L., Goubin, L.: 'Unbalanced Oil and Vinegar Schemes', EUROCRYPT 1999, LNCS 1592, pp. 206–222, Springer
[17] Kipnis A., Shamir A.: 'Cryptanalysis of the oil and vinegar signature scheme', CRYPTO 98, LNCS 1462, pp. 257–266. Springer
[18] Macario-Rat, G., Patarin, J., Cogliati, B., Faugère, J.C., Fouque, P.A., Goubin, L., Larrieu, R., Minaud, B.: 'Rectangular Attack on VOX', IACR Cryptology ePrint Archive, 2023/1822
[19] National Institute of Standards and Technology: 'Post-Quantum Cryptography Standardization', ⟨https://csrc.nist.gov/projects/post-quantum-cryptography⟩
[20] National Institute of Standards and Technology: 'Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process', ⟨https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf⟩
[21] Patarin, J., Cogliati, B., Faugère, J.C., Fouque, P.A., Goubin, L., Larrieu, R., Macario-Rat, G., Minaud, B.: 'VOX', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
[22] Smith-Tone D., Perlner, R.A.: 'Rainbow Band Separation is Better than we Thought', IACR Cryptology ePrint Archive, 2020/702
[23] Wiedemann, D.: 'Solving sparse linear equations over finite fields', IEEE Trans. Inform. Theory, 32(1), pp. 54–62, 1986

Hiroki Furue received his Ph.D. in information science and technology from the University of Tokyo, Japan in 2024. He is currently a researcher in NTT Social Informatics Laboratories. He has been engaged in the research of multivariate public key cryptosystems.

Yasuhiko Ikematsu received the PhD in mathematics in 2016 from Kyushu University. He was a research fellow in Institute of Mathematics for Industry, Kyushu University from 2016 to 2018 and in Department of Mathematical Informatics, University of Tokyo from April to December in 2018. He is currently an assistant professor in Institute of Mathematics for Industry, Kyushu University.