New security analysis for UOV-based signature candidates with small public key size

Yasuhiko Ikematsu, Hiroki Furue and Rika Akiyama

Abstract Among candidates for the NIST PQC additional call for digital signatures, there exist seven UOV-based multivariate schemes. Further, four UOV-based candidates, MAYO, QR-UOV, VOX, and SNOVA, achieve small public key size compared with the plain UOV. This work gives a new security analysis for these UOV variants with small public keys. Our main contributions are the following two points: First, we show that the rectangular MinRank attack originally proposed on the Rainbow scheme by Beullens is applicable to MAYO, QR-UOV, and VOX. Second, we explain the construction of SNOVA from a different point of view from the original papers, and reconsider its security analysis. Through our analysis, we show that all parameters of VOX and some parameters of SNOVA submitted in the additional call do not satisfy the claimed security levels.

Key words: PQC, MPKC, UOV, MAYO,QR-UOV, VOX, SNOVA

1 Introduction

It is considered that by Shor's algorithm, the existing cryptosystems are broken with a large scale quantum computer. Therefore, it is required to develop cryptosystems resistant to quantum computer attacks, which are called post-quantum cryptosystems (PQC). Multivariate public key cryptosystems (MPKC) are based on the difficulty of the problem to find a solution to multivariate quadratic equations over a finite field (MQ problem), and are one of the main candidate of PQC.

Yasuhiko Ikematsu
Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka 819–0395, Japan. e-mail: `ikematsu@imi.kyushu-u.ac.jp`

Hiroki Furue
Department of Mathematical Informatics, The University of Tokyo,7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan. e-mail: `furue-hiroki261@g.ecc.u-tokyo.ac.jp`

Rika Akiyama
NTT Social Informatics Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo, 180–8585, Japan. e-mail: `rika.akiyama@ntt.com`

*This paper is based on our two papers [11] and [18].

NIST started the PQC standardization project [23] in 2016. Via some rounds, NIST announced in 2022 that the three signature schemes (Dilithium, Falcon, SPHINCS+) will be standardized. However, in order to ensure the variety of algorithms, NIST also announced to start the new project of the PQC standardization of additional digital signature schemes [24]. 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 [19] 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, four UOV-based schemes, MAYO [3], QR-UOV [13], VOX [25], and SNOVA [29], that have small public keys compared with the plain UOV were submitted to the additional NIST PQC standardization.

This work gives a new security analysis for these UOV variants with small public keys. First, we show that the rectangular MinRank attack originally proposed on the Rainbow scheme is applicable to MAYO, QR-UOV, and VOX. Second, we explain the construction of SNOVA, and reconsider its security analysis.

In the first point, we show that the rectangular MinRank is applicable to some UOV variants. This rectangular MinRank attack was originally proposed on Rainbow by Beullens [2] and succeeded in reducing the security level of Rainbow. In this paper, we confirme that the public keys of MAYO, QR-UOV, and VOX have a MinRank problem when we apply a transformation performed in the rectangular MinRank attack. Moreover, we estimate the complexity of the attack following Beullens' estimation [2] in his rectangular MinRank attack against Rainbow, and we check by some experiments whether our estimation is reasonable. Due to our analysis, we show that all parameters of VOX submitted in the additional NIST PQC standardization in June 2023 do not satisfy the claimed security levels. On the other hand, we see that the proposed parameters of MAYO and QR-UOV are secure against the rectangular MinRank attack, while the complexity of the attack is reasonably close or equal to that of the best known attacks.

In the second point, we reorganize the construction of SNOVA [29], and reconsider its security analysis. We explain the construction of the core part of SNOVA without using the matrix ring $M_l(\mathbb{F}_q)$. The core part is a polynomial system whose almost coefficients are zero (i.e. sparse polynomials), and therefore the technique of mixing and transforming was applied in SNOVA to strengthen its security. We show in this paper that the core part is vulnerable for a forgery attack. Next, as a reconsideration of the security analysis, we explain that all existing key recovery attacks for UOV can be applied to the core part of SNOVA. Moreover, we propose efficient versions of the reconciliation attack and the intersection attack for the core part of SNOVA. Finally, due to our analysis, we show that some parameters of SNOVA [29] for $l = 2$ submitted in the additional NIST PQC standardization do not satisfy the claimed security levels. Note that this security analysis is inherent to the construction of SNOVA and will not affect the security of other UOV variants. Against our new security analysis, the authors of SNOVA have recently proposed new parameters in the recent version of ePrint (2024-02-08) [28]. We confirmed that these new parameters are secure against our proposed security analysis. We note that Li et al. also report the result regarding the KS attack, reconciliation attack and intersection attack as an independent work in [21], and seem to further improve the reconciliation attack than our result.

This paper is organized as follows. In Section 2, we recall the construction and security analysis of UOV. In Section 3, we describe the rectangular MinRank attack for MAYO, QR-UOV and VOX. In

Section 4, we recall the construction of SNOVA. In Section 5, we reconsider the security of SNOVA using the result in Section 4. In Section 6, we conclude our paper.

2 Unbalanced Oil Vinegar scheme (UOV)

2.1 The key generation of UOV with parameter (q, v, o, m)

Let v, o, m be positive integers, $\mathbb{F}_q$ the finite field with q elements, 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*.

We explain the key generation of UOV with parameter (q, v, o, m). Randomly choose m square matrices $F_1, \ldots, F_m$ with size n over $\mathbb{F}_q$ in the following form:

$$F_k = \begin{pmatrix} a_{11}^{(k)} & \ldots & a_{1v}^{(k)} & a_{1v+1}^{(k)} & \ldots & a_{1n}^{(k)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{v1}^{(k)} & \ldots & a_{vv}^{(k)} & a_{vv+1}^{(k)} & \ldots & a_{vn}^{(k)} \\ a_{v+11}^{(k)} & \ldots & a_{v+1v}^{(k)} & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{(k)} & \ldots & a_{nv}^{(k)} & 0 & \ldots & 0 \end{pmatrix}. \tag{1}$$

Here, each coefficient $a_{ij}^{(k)}$ is randomly chosen from the finite field $\mathbb{F}_q$. We define m quadratic polynomials $f_1, \ldots, f_m$ in n variables $\mathbf{x}$ as follows:

$$f_k(\mathbf{x}) = \mathbf{x} \cdot F_k \cdot {}^t\mathbf{x} \quad (1 \leq k \leq m). \tag{2}$$

From the form of F_k, it is clear that $f_k(\mathbf{x})$ is a linear polynomial regarding variables $\mathbf{x}_o$.We define a quadratic map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, and randomly choose a linear invertible map $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Let T be the $n \times n$ matrix such that $\mathcal{T}(\mathbf{x}) = \mathbf{x} \cdot T$. We compute the following matrices P_k and quadratic polynomials p_k $(1 \leq k \leq m)$:

$$P_k := T \cdot F_k \cdot {}^tT, \quad p_k(\mathbf{x}) := \mathbf{x} \cdot P_k \cdot {}^t\mathbf{x}. \tag{3}$$

It is clear that $p_k(\mathbf{x}) = f_k(\mathbf{x} \cdot T)$. Then, the secret key of UOV with parameter (q, v, o, m) is given by $(f_1, \ldots, f_m, \mathcal{T})$, and the public key is the set of quadratic polynomials $(p_1, \ldots, p_m)$, which is equal to the quadratic map $\mathcal{P} := \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. We skip the signature generation and verification processes for UOV.

Remark 1 In general, the UOV scheme [19] satisfies the condition $m = o$, which is necessary in the signature generation of UOV. However, in order to state MAYO [3, 4], QR-UOV [13, 12] and VOX [25] in later sections, it is convenient not to assume the condition $m = o$.

It is known that the size of the public key of UOV can be reduced using the technique of Petzoldt et al. [26] without declining the security. Moreover, the secret key $T \in \mathrm{GL}_n(\mathbb{F}_q)$ is often taken as

$$T = \begin{pmatrix} 1_v & 0_{v\times o} \\ T_0 & 1_o \end{pmatrix}, \tag{4}$$

where T_0 is taken as a random $o \times v$ matrix. It is known that even if the form of T is restricted in this way, it does not affect the security of UOV.

Beullens et al. proposed new parameters (Table 6 in the appendix) of UOV [5] based on the latest MPKC security analysis, and submitted it to the additional NIST PQC standardization project [24]. A drawback of UOV is a large public key size compared with other PQC such as lattice-based and isogeny-based cryptosystems. To reduce such a drawback, there have been submitted some variants such as MAYO [3, 4], QR-UOV [13, 12], VOX [25] and SNOVA [28, 29].

2.2 Review of the security analysis of UOV

We recall the security analysis of UOV with the parameter (q, v, o, o), i.e., the plain UOV.

Direct attack

In MPKC, the direct attack tries to directly and algebraically solve an instance of the MQ problem related to the public key $\mathcal{P} = (p_1, \ldots, p_o)$. This attack is a forgery attack. For UOV, the direct attack finds a solution to the underdetermined system of o inhomogeneous quadratic equations $\mathcal{P}(\mathbf{x}) = \mathcal{H}(\mathbf{m})$ in $n = v + o$ variables, where $\mathbf{m}$ is a message to be signed and $\mathcal{H}$ is a hash function. Since it is enough to find a solution to the system $\mathcal{P}(\mathbf{x}) = \mathcal{H}(\mathbf{m})$, such a system can be reduced to a system of o homogeneous quadratic equations in $o+1$ variables by fixing v variables in $\mathbf{x}$ and by homogenizing it. To solve such a reduced system, Gröbner basis algorithms such as F_4 [9], F_5 [10] and XL [31] are often considered. The complexity of solving the system of o homogeneous quadratic equations in $o+1$ variables using the XL Wiedemann algorithm with the hybrid approach is given by

$$\min_k q^k \cdot 3 \binom{o - k + D_{o+1-k,o}}{D_{o+1-k,o}}^2 \binom{o+2-k}{2}, \tag{5}$$

where $0 \le k \le o$ is the number of fixed variables in the hybrid approach, and $D_{o+1-k,o}$ is given by the smallest integer d for which the coefficient of t^d in the function $\dfrac{(1-t^2)^o}{(1-t)^{o+1-k}}$ is less than or equal to 1. For the underdetermined case, Thomae-Wolf [30] proposed the technique to reduce the size of the MQ problem (namely, the numbers of variables and equations). Moreover, their technique was improved by Furue et al. [14] and Hashimoto [17]. To be exact, the complexity of the direct attack for UOV is given by using such techniques.

Kipnis-Shamir (KS) attack

The KS attack was proposed by Kipnis and Shamir [20], and is a key recovery attack for UOV.

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

$$\mathbf{x} \cdot H \cdot {}^t\mathbf{y} = h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y}) \quad \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n. \tag{6}$$

We call H the symmetric representation matrix of h. Second, we set F_k to be the symmetric representation matrix of f_k, and P_k that of p_k. Moreover, let T be the $n \times n$ matrix such that $\mathcal{T}(\mathbf{x}) = \mathbf{x} \cdot T$. It is clear that

$$(P_1, \ldots, P_o) = \left(T \cdot F_1 \cdot {}^tT, \ldots, T \cdot F_o \cdot {}^tT\right). \tag{7}$$

Finally, let $\{e_1, \ldots, e_n\}$ be a standard basis of $\mathbb{F}_q^n$, that is, $e_1 = (1, 0, \ldots, 0)$ and so on. We define the vinegar space $\mathcal{V}$ and the oil space $\mathcal{O}$ in $\mathbb{F}_q^n$ by $\mathcal{V} := \mathrm{Span}\{e_1, \ldots, e_v\}$, and $\mathcal{O} := \mathrm{Span}\{e_{v+1}, \ldots, e_n\}$. Then the KS attack tries to find vectors of the twisted oil space

$$\mathcal{O} \cdot T^{-1} := \mathrm{Span}\{e_{v+1}T^{-1}, \ldots, e_nT^{-1}\} \tag{8}$$

by computing stable subspaces of XY^{-1} for various two invertible matrices $X, Y \in \mathrm{Span}\{P_1, \ldots, P_o\}$. If the KS attack succeeds, an attacker can find an invertible matrix T' such that $\mathcal{O} \cdot T^{-1}T' = \mathcal{O}$, which is an equivalent secret key. Namely, the attacker can forge a signature for any message using T'. The complexity of the KS attack is given by $O(q^{v-o})$.

Reconciliation attack

Any element in the twisted oil space $\mathcal{O} \cdot T^{-1}$ is a solution to the system of quadratic equations $p_1(\mathbf{x}) = \cdots = p_o(\mathbf{x}) = 0$. A key recovery attack that finds such a solution is called the reconciliation attack [7]. Since the dimension of $\mathcal{O}$ is o, the system $p_1(\mathbf{x}) = \cdots = p_o(\mathbf{x}) = 0$ can be reduced to a system of o quadratic equations in $n - o = v$ variables. However, since v is relatively larger than o, such a reduced system has a lot of solutions which do not belong to the twisted oil space $\mathcal{O} \cdot T^{-1}$. Due to this fact, the reconciliation attack is harder than the direct attack in general .

Intersection attack

The intersection attack was proposed by Beullens [2], and is obtained by combining with the reconciliation attack and the KS attack. Assume that the parameters v, o satisfy the condition $v < 2o$. For simplicity, we set $Q = P_1$ and $R = P_2$. If P_1 and P_2 are not invertible, then we choose two invertible linear combinations of $P_1, \ldots, P_o$ as Q and R. The intersection attack tries to find a non-zero element $\mathbf{x}$ of $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ $(\subset \mathcal{V} \cdot {}^tT)$. Since $\mathbf{x}Q^{-1}, \mathbf{x}R^{-1} \in \mathcal{O} \cdot T^{-1}$, such an element $\mathbf{x}$ satisfies the following $3o$ quadratic equations in n variables $\mathbf{x}$:

$$\begin{aligned} &p_1(\mathbf{x}Q^{-1}) = \cdots = p_o(\mathbf{x}Q^{-1}) = 0, \quad p_1(\mathbf{x}R^{-1}) = \cdots = p_o(\mathbf{x}R^{-1}) = 0, \\ &\mathbf{x} \cdot Q^{-1} \cdot P_1 \cdot R^{-1} \cdot {}^t\mathbf{x} = \cdots = \mathbf{x} \cdot Q^{-1} \cdot P_o \cdot R^{-1} \cdot {}^t\mathbf{x} = 0. \end{aligned} \tag{9}$$

Here, we have

$$\mathbf{x} \cdot Q^{-1} \cdot P_1 \cdot R^{-1} \cdot {}^t\mathbf{x} = 2p_2(\mathbf{x}R^{-1}),\ \mathbf{x} \cdot Q^{-1} \cdot P_2 \cdot R^{-1} \cdot {}^t\mathbf{x} = 2p_1(\mathbf{x}Q^{-1})$$

when we set $Q = P_1$ and $R = P_2$. Note that even if we choose two invertible linear combinations of $P_1, \ldots, P_o$ as Q and R, we will obtain two linear dependences. Moreover, the dimension of $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ is at least $2o - v$ under the condition $v < 2o$. Therefore, the system can be reduced to a system of $3o - 2$ homogeneous quadratic equations in $n - (2o - v - 1) = 2v - o + 1$ variables. According to Beullens' analysis [2], such a reduced system can be identified with a random system of $M := 3o - 2$ homogenous quadratic equations in $N := 2v - o + 1$ variables. Then, the complexity to solve the reduced system is given by

$$\min_k q^k \cdot 3 \binom{N-k-1+D_{N-k,M}}{D_{N-k,M}}^2 \binom{N-k+1}{2}, \tag{10}$$

where $0 \leq k \leq N-1$ is the number of fixed variables in the hybrid approach.

If the condition $v < 1.5o$ is satisfied, then the intersection attack can be more efficient. However, since the proposed parameters of UOV variants do not satisfy such a condition, we do not explain the attack for $v < 1.5o$.

The intersection attack for $v \geq 2o$ is considered as follows. The probability that $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ is non zero is around $1/q^{v-2o+1}$. Thus, the system (9) is a system of $M = 3o-2$ quadratic homogeneous equations in n variables $\mathbf{x}$, and has a solution belonging to $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ at the probability $1/q^{v-2o+1}$. If the system (9) does not have a non-zero solution in $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$, then we reselect Q, R. Therefore, the complexity to find a non-zero element $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ is given by

$$\min_k q^{v-2o+1} q^k \cdot 3 \binom{n-k-1+D_{n-k,M}}{D_{n-k,M}}^2 \binom{n-k+1}{2}, \tag{11}$$

where $n - M \leq k \leq n-1$ is the number of fixed variables in the hybrid approach.

Collision attack

As a cryptographic attack, the collision attack is considered for UOV. Strictly speaking, the signature generation of UOV finds a solution $\mathbf{x} = \mathbf{s}$ to $\mathcal{P}(\mathbf{x}) = \mathcal{H}(\mathbf{m}||r)$ for a given message $\mathbf{m}$ and randomly chosen salt r, and outputs $(\mathbf{s}, r)$ as a signature of $\mathbf{m}$. Then the collision attack is to try to find a pair (i, j) satisfying $\mathcal{P}(\mathbf{s}_i) = \mathcal{H}(\mathbf{m}||r_j)$ by collecting a lot of vectors $\{\mathbf{s}_i\}_i$ and salts $\{r_j\}_j$. See the document [5] for the detail.

3 Rectangular MinRank attack against MAYO, QR-UOV and VOX

In this section, we explain the rectangular MinRank attack against MAYO, QR-UOV and VOX. The rectangular MinRank attack was originally proposed on Rainbow by Beullens [2]. Moreover, [11] shows that the rectangular MinRank attack is applicable to MAYO and QR-UOV.

3.1 Preliminary

We consider the case of a general multivariate scheme in this subsection. Let $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be an easily-invertible map of a general multivariate scheme, $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m, \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be the secret key, and $\mathcal{P} = (p_1, \ldots, p_m)$ be the corresponding public key. Recall that $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ holds. We set F_i to be the symmetric representation matrix of f_i and P_i that of p_i. If we take $S \in M_m(\mathbb{F}_q)$ and $T \in M_n(\mathbb{F}_q)$ as $\mathcal{S}(\mathbf{x}) = \mathbf{x} \cdot S$ and $\mathcal{T}(\mathbf{y}) = \mathbf{y} \cdot T$, then, we have

$$(P_1, \ldots, P_m) = \left(T \cdot F_1 \cdot {}^tT, \ldots, T \cdot F_m \cdot {}^tT\right) \cdot S \tag{12}$$

By using this relation, some attacks for MPKC have been proposed so far, such as MinRank attacks.

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,

$$G_i = \left(\mathbf{g}_i^{(1)} \ \mathbf{g}_i^{(2)} \ \cdots \ \mathbf{g}_i^{(n)} \right) \in M_n(\mathbb{F}_q).$$

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

$$\tilde{G}_1 := \left(\mathbf{g}_1^{(1)} \ \mathbf{g}_2^{(1)} \ \cdots \ \mathbf{g}_m^{(1)} \right), \tilde{G}_2 := \left(\mathbf{g}_1^{(2)} \ \mathbf{g}_2^{(2)} \ \cdots \ \mathbf{g}_m^{(2)} \right), \ldots \tilde{G}_n := \left(\mathbf{g}_1^{(n)} \ \mathbf{g}_2^{(n)} \ \cdots \ \mathbf{g}_m^{(n)} \right).$$

Then, when we apply this deformation to $(P_1, \ldots, P_m)$ and $(F_1, \ldots, F_m)$, the following is easily proven from (12):

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

Unlike the case of general MinRank attacks using (12), the rectangular MinRank attack [2] was proposed by using this deformation $\left(\tilde{P}_1, \ldots, \tilde{P}_n \right)$.

3.2 Rectangular MinRank attack for UOV when $m > v$

The rectangular MinRank attack can be applied to UOV with the parameter (q, v, o, m) having the condition $m > v$. Let $(F_1, \ldots, F_m)$ be the set of representation matrices of the easily-invertible map $\mathcal{F}$ of UOV with the parameter (q, v, o, m). From this condition, it is easily seen that the deformation matrices $\tilde{F}_{v+1}, \ldots, \tilde{F}_n \in M_{n \times m}(\mathbb{F}_q)$ are of rank $\leq v$ since they have the following form:

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

Let $(P_1, \ldots, P_m)$ be the set of representation matrices of the public key $\mathcal{P}$. Then, we have $(\tilde{P}_1, \ldots, \tilde{P}_n) = (T\tilde{F}_1, \ldots, T\tilde{F}_n) \cdot {}^tT$. Since $\tilde{F}_{v+1}, \ldots, \tilde{F}_n$ are of rank $\leq v$, there exists a linear combination of $\tilde{P}_1, \ldots, \tilde{P}_{v+1} \in M_{n \times m}(\mathbb{F}_q)$ whose rank is $\leq v$.

The rectangular MinRank attack against UOV with the parameter (q, v, o, m) under $m > v$ tries to find a non-zero element of the twisted oil space $\mathcal{O} \cdot T^{-1}$. The rectangular MinRank attack is constructed as follows. Since $\dim \mathcal{O} \cdot T^{-1} = o$, there exists a non-zero n-by-1 vector with the following form:

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

Then, it is shown that $\sum_{i=1}^{v+1} a_i \tilde{P}_i = (\tilde{P}_1, \ldots, \tilde{P}_n) \cdot {}^t\mathbf{a} = (T\tilde{F}_1, \ldots, T\tilde{F}_n) \cdot {}^t(\mathbf{a} \cdot T)$ is a linear combination of $T\tilde{F}_{v+1}, \ldots, T\tilde{F}_n$. Thus, this linear combination is of rank $\leq v$. Namely, the vector $\mathbf{a}$ gives a solution to the MinRank problem for $(\tilde{P}_1, \ldots, \tilde{P}_{v+1})$ with the target rank v. Moreover, for $i = 1, \ldots, m$, we have $p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0$, where $\mathcal{P} = (p_1, \ldots, p_m)$ is a public key of UOV. As a result, the vector $\mathbf{a} = (a_1, a_2, \ldots, a_{v+1}, 0, \ldots, 0)$ we want to find is a common solution of the following problems.

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

3.3 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 [2] for the original rectangular MinRank attack against Rainbow.

First, consider problem (i). Fix an integer m' such that $v+1 \leq m' \leq m$. 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 $(\tilde{P}'_1, \ldots, \tilde{P}'_{v+1})$ 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 [2] for the detail description.) For $b \in \mathbb{N}_{\geq 1}$, 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 $1 \leq b \leq v+1$ by the result of Bardet et al. [1].

Next, one considers adding problem (ii) to I'. We assume that $p_1(\mathbf{a}), \ldots, p_m(\mathbf{a})$ behaves like 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 $p_1(\mathbf{a}), \ldots, p_m(\mathbf{a})$, namely,

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

We define

$$b_{\min} := \min \left\{ b \in \mathbb{N} \;\middle|\; \dim_{\mathbb{F}_q} I_{b,1} = \dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{c}]_{b,1} - 1 \right\}. \tag{13}$$

By applying to $I_{b_{\min},1}$ the bilinear XL algorithm [27] with Wiedemann algorithm [32, 6], we can find a solution $\mathbf{a}$ to problems (i) and (ii) with the following complexity:

$$3 \binom{m'}{v}^2 \binom{v+b_{\min}}{b_{\min}}^2 (v+1)^2. \tag{14}$$

Following the idea of Beullens' estimation [2], in order to guess $b_{\min}$, we define the following two series in t_1 and t_2:

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

These series are derived to compute a part of the Hilbert series of $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]/I'$ and $\mathbb{F}_q[\mathbf{a}, \mathbf{c}]/I$. Then we consider that $b_{\min}$ is predicted by

$$b_{\min}^{(\text{predict})} := \min \left\{ b \in \mathbb{N} \mid G(t_1, t_2)_{b,1} \leq 1 \right\}, \tag{15}$$

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

Remark 2 The complexity of (i) by the support minor modeling is given by replacing $b_{\min}$ with $b'_{\min}$ in (14), where

$$b'_{\min} := \min\left\{b \in \mathbb{N} \mid R'(b) \geq \dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{c}]_{b,1} - 1\right\}.$$

3.4 Rectangular MinRank attack against MAYO signature scheme

MAYO signature scheme is a variant of the UOV scheme proposed by Beullens [3]. The public key is almost same as that of UOV with the parameter (q, v, o, m). Note that the signature process is achieved by some techniques such as "whipping transformation".

Here, we estimate the complexity of the rectangular MinRank attack against MAYO. In Table 7 in the appendix, we confirmed that $b_{\min}$ is equal to $b_{\min}^{(\text{predict})}$ for some small parameters of MAYO. From the experiments in Table 7, we use $b_{\min}^{(\text{predict})}$ instead of $b_{\min}$, and theoretically estimate the complexity of the rectangular MinRank attack against MAYO by (14).

Table 1 shows the complexity of the attack against the parameters proposed in [4]. Here, m' in Table 1 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 (15) for this m'. "RecMin" in the table means the complexity of the rectangular MinRank attack against MAYO given by (14) as $b_{\min} = b_{\min}^{(\text{predict})}$. "Best" means the best complexity among the existing attacks stated in [4].

Table 1 Estimated gate count of the rectangular MinRank attack (RecMin) and the best known attack (Best) in MAYO [4]

(q, v, o, m)	m'	$b_{\min}^{(\text{predict})}$	RecMin $\log_2(\#\text{gates})$	Best $\log_2(\#\text{gates})$
$(16, 58, 8, 64)$	59	22	159	143
$(16, 60, 18, 64)$	62	21	168	143
$(16, 89, 10, 96)$	90	33	231	207
$(16, 121, 12, 128)$	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 1, we see that the rectangular MinRank attack does not reduce the security level for the proposed parameters in [4].

Remark 3 Define

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

Following Beullens' estimation [2], it is considered that $R(b)$ predicts the dimension of $I_{b,1}$. In our experiments in Table 7 in the appendix, 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 $I_{b,1}$. 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.

3.5 Rectangular MinRank attack against QR-UOV

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

QR-UOV is constructed by using representation of an extension field in a matrix algebra over $\mathbb{F}_q$. Let V, O, l be positive integers and set $v := Vl, m = o := Ol, N := V + O, n := v + o = Nl$. 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 $W^{(N)} \cdot \phi({}^tT) = {}^t\phi(T) \cdot W^{(N)}$ for any $T \in M_N(\mathbb{F}_{q^l})$, where

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

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 $\mathcal{F} = (f_1, \ldots, f_o)$ of QR-UOV is given by

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

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

$$p_i(\mathbf{x}) := \mathbf{x} \cdot {}^t\phi(T) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(T) \cdot {}^t\mathbf{x}, \quad (1 \le i \le o). \tag{16}$$

We explain how the rectangular MinRank attack is applied to QR-UOV. First, since $W^{(N)} \cdot \phi(F_i)$ and ${}^t\phi(T) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(T)$ are symmetric, the symmetric representation matrix P_i of p_i is equal to $2 \cdot {}^t\phi(T) \cdot W^{(N)} \cdot \phi(F_i) \cdot \phi(T)$. Next, by ${}^t\phi(T) \cdot W^{(N)} = W^{(N)} \cdot \phi({}^tT)$, we have

$$2^{-1} \cdot W^{(N),-1} \cdot P_i = \phi({}^tT \cdot F_i \cdot T).$$

Thus, an attacker can obtain the matrices $\{{}^tT\cdot F_1\cdot T,\ldots,{}^tT\cdot F_o\cdot T\}$ from the public key $\{p_1,\ldots,p_o\}$. It is clear that these matrices are the symmetric representation matrices of UOV with the parameter (q^l, V, O, o). Since we have $o = lO > V$ for the proposed parameters of QR-UOV, we can apply the rectangular MinRank attack to these matrices.

As in the case of MAYO, we did some experiments regarding $b_{\min}$ and confirmed that $b_{\min} = b_{\min}^{(\mathrm{predict})}$ in Table 8 in the appendix. Thus, we use $b_{\min}^{(\mathrm{predict})}$ instead of $b_{\min}$, and theoretically estimate the time complexity of the rectangular MinRank attack against QR-UOV.

Table 2 shows the complexity of the attack against the proposed parameters in [12]. Here, m' in Table 2 represents the value between $V+1$ and o such that the complexity of the attack is minimum. The value $b_{\min}^{(\mathrm{predict})}$ is given by (15) for this m'. "RecMin" means the complexity of the rectangular MinRank attack against QR-UOV given by (14) as $b_{\min} = b_{\min}^{(\mathrm{predict})}$. "Best" means the best complexity among the existing attacks stated in [12].

Table 2 Estimated gate count of the rectangular MinRank attack (RecMin) and the best known attack (Best) in QR-UOV [12]

Security level	(q,V,O,l)	m'	$b_{\min}^{(\mathrm{predict})}$	RecMin $\log_2(\#\mathrm{gates})$	Best $\log_2(\#\mathrm{gates})$
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 m' runs between 75 and 100, and $m' = 75$ minimizes the complexity of the rectangular MinRank attack. Also, for $m' = 75$, we have $b_{\min}^{(\mathrm{predict})} = 18$, and then the complexity of the attack is 2^{162} gates. From Table 2, we see that the proposed parameters of QR-UOV are secure against the rectangular MinRank attack.

3.6 Rectangular MinRank attack against VOX

VOX [25] 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 notations ϕ, W be as in 3.5. 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:

$$F_i = \begin{pmatrix} *_V & *_{V\times O} \\ *_{O\times V} & 0_O \end{pmatrix} \in M_N(\mathbb{F}_{q^l}),\ (t+1 \le i \le o). \tag{17}$$

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

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

where $\mathbf{x} = (x_1, \dots, x_n)$. Next, randomly choose invertible matrices $S \in M_o(\mathbb{F}_q)$ and $T \in M_N(\mathbb{F}_{q^l})$. Moreover, we define linear maps $\mathcal{S} : \mathbb{F}_q^o \to \mathbb{F}_q^o$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ associated with S and ${}^t\phi(T)$, respectively. Then, the public key of VOX is given by $\mathcal{P} = (p_1, \dots, p_o) := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^o$.

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

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

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

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

From the definition of $F_1, \dots, F_o$, 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 $\tilde{F}_{V+1}, \dots, \tilde{F}_N$ are of rank $t + V$ at most. Thus, we can consider the following MinRank problem over $\mathbb{F}_{q^l}$:

$$\mathrm{Rank}\left(\sum_{i=1}^{V+1} a_i \tilde{\bar{P}}_i\right) \le t + V. \tag{18}$$

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 $F_1, \dots, F_t$ are random matrices. Note that it is efficient to apply the support minor modeling to the transposition version, namely, to the MinRank problem of $o \times N$ matrices ${}^t\tilde{\bar{P}}_1, \dots, {}^t\tilde{\bar{P}}_{V+1}$ with rank $t + V$:

$$\mathrm{Rank}\left(\sum_{i=1}^{V+1} a_i \cdot {}^t\tilde{\bar{P}}_i\right) \le t + V. \tag{19}$$

If we get a solution $\mathbf{a} = (a_1, \dots, a_{V+1}, 0, \dots, 0) \in \mathbb{F}_{q^l}^N$ to (19), we can recover an equivalent key in polynomial time.

Table 3 shows the complexity of the rectangular MinRank attack (19) against the parameters of VOX submitted in the additional NIST PQC standardization in June 2023 [25]. "RecMin" means the complexity of the rectangular MinRank attack (19) using the support minor modeling [1]. "Best" means the best complexity among the existing attacks stated in [25]. As seen in the table, the rectangular MinRank attack can break all three proposed parameters. For example, for $(q, V, O, l, t) = (251, 9, 8, 6, 6)$, VOX can be broken in 51 gates.

Table 3 Estimated complexity of the rectangular MinRank attack (RecMin) and the best known attack (Best) in VOX [25]

Security level	(q, V, O, l, t)	RecMin $\log_2(\#\text{gates})$	Best $\log_2(\#\text{gates})$
I	$(251, 9, 8, 6, 6)$	**51**	146
III	$(1021, 11, 10, 7, 7)$	**55**	210
V	$(4093, 13, 12, 8, 8)$	**55**	285

Remark 4 We reported our result in this subsection to the NIST PQC forum, and the authors of VOX proposed new parameter sets in [22]. However, Guo et al. broke their new parameters by improving our attack. See [16] for the details.

4 Reorganizing the construction of SNOVA

In this section, we explain the construction of SNOVA. In particular, we state it from a different point of view from the original papers [28, 29].

4.1 Main technique to reduce the public key size used in SNOVA

In this subsection, we explain the technique of SNOVA to reduce the size of the public key of UOV. We note that the explanation here is different from the description in [28, 29] (See Remark 5).

In UOV in 2.1, a matrix P_k has generated only one quadratic polynomial $p_k(\mathbf{x})$ as in (3). In SNOVA, this one-to-one correspondence ($P_k \mapsto p_k$) is improved as follows. Let l be a positive integer, and $F_1, \ldots, F_o, P_1, \ldots, P_o$ be matrices defined as in (1) and (3) with parameter (q, lv, lo, o). We have $P_i = T \cdot F_i \cdot {}^tT$. We prepare a matrix variable $\mathbf{X} := \begin{pmatrix} \mathbf{x}^{(1)} \\ \vdots \\ \mathbf{x}^{(l)} \end{pmatrix}$, where $\mathbf{x}^{(i)} = (x_1^{(i)}, \ldots, x_{ln}^{(i)})$. We also divide $\mathbf{x}^{(i)}$ into two subsets $\mathbf{x}_v^{(i)} = (x_1^{(i)}, \ldots, x_{lv}^{(i)})$, $\mathbf{x}_o^{(i)} = (x_{lv+1}^{(i)}, \ldots, x_{ln}^{(i)})$. Then, we define two systems of quadratic polynomials $f'_{k,ij} = f'_{k,ij}(\mathbf{X})$ and $p'_{k,ij} = p'_{k,ij}(\mathbf{X})$ $(1 \le k \le o, 1 \le i, j \le l)$:

$$f'_k = \begin{pmatrix} f'_{k,11}(\mathbf{X}) & \ldots & f'_{k,1l}(\mathbf{X}) \\ \vdots & \ddots & \vdots \\ f'_{k,l1}(\mathbf{X}) & \ldots & f'_{k,ll}(\mathbf{X}) \end{pmatrix} := \mathbf{X} \cdot F_k \cdot {}^t\mathbf{X}, \quad p'_k = \begin{pmatrix} p'_{k,11}(\mathbf{X}) & \ldots & p'_{k,1l}(\mathbf{X}) \\ \vdots & \ddots & \vdots \\ p'_{k,l1}(\mathbf{X}) & \ldots & p'_{k,ll}(\mathbf{X}) \end{pmatrix} := \mathbf{X} \cdot P_k \cdot {}^t\mathbf{X}.$$

We call $P_1, \ldots, P_o$ the core matrices of SNOVA and $\{p'_{k,ij}\}$ the core (quadratic) polynomials of SNOVA.

It is clear that $p'_{k,ij}(\mathbf{X}) = f'_{k,ij}(\mathbf{X} \cdot T)$, and $f'_{k,ij}(\mathbf{X})$ is a linear polynomial regarding variables $\mathbf{x}_o^{(1)}, \ldots, \mathbf{x}_o^{(l)}$ when $\mathbf{x}_v^{(1)}, \ldots, \mathbf{x}_v^{(l)}$ are fixed as scalars. Thus, the core polynomials $\{p'_{k,ij}\}$ can be identified with the public key of UOV with parameter (q, l^2v, l^2o, l^2o).

The verification process is done by using the quadratic map $(p'_1, \ldots, p'_o) = \{p'_{k,ij}\} : M_{l\times ln}(\mathbb{F}_q) \to M_l(\mathbb{F}_q)^o$. A verifier can construct l^2o quadratic polynomials $\{p'_{k,ij}\}$ in l^2n variables $\mathbf{X}$ from only the core matrices $P_1, \ldots, P_o$. In particular, a core matrix P_k generates l^2 quadratic polynomials. Thus, if the core matrices $P_1, \ldots, P_o$ are the public key, then the size of the public key is small compared with $\{p'_{k,ij}\}$. This is the main technique to reduce the size of the public key used in SNOVA. Note that, the core polynomials are vulnerable for a forgery attack. SNOVA will be constructed by further improving this technique.

Remark 5 Wang et al. [28, 29] explained the technique used in SNOVA in a slightly different method. They define an $n \times n$ matrix $F_k = (F_{k,ij})_{1\le i,j\le n}$ as a matrix over the matrix ring $M_l(\mathbb{F}_q)$. Namely, each component $F_{k,ij}$ is an element of $M_l(\mathbb{F}_q)$. However, since $M_n(M_l(\mathbb{F}_q)) = M_{ln}((\mathbb{F}_q)$, their construction is equivalent to the above our construction.

4.2 A forgery attack for the core polynomials $\{p'_{k,ij}\}$

As stated in [28], SNOVA is constructed by improving the technique in 4.1, since the core polynomials $\{p'_{k,ij}\}$ are sparse quadratic polynomials. The authors of SNOVA considered that the core part might be vulnerable. Due to our analysis, the consideration is right, and the core polynomials $\{p'_{k,ij}\}$ are actually vulnerable for a forgery attack. In this subsection, we show the method to forge a signature for the core polynomials $\{p'_{k,ij}\}$.

Let $\mathbf{M} = (M^{(1)}, \ldots, M^{(o)}) \in M_l(\mathbb{F}_q)^o$ be a message to be signed. To forge a signature for this $\mathbf{M}$, we must solve the quadratic equations

$$p'_{k,ij}(\mathbf{X}) = M^{(k)}_{ij},\ (1 \le i, j \le l,\ 1 \le k \le o). \tag{20}$$

Here, we note that $p'_{k,ij}(\mathbf{X})$ is a polynomial in variables $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(j)}$ by its definition.

First, we have $p'_{k,11}(\mathbf{X}) = p'_{k,11}(\mathbf{x}^{(1)})$. Therefore, the system of equations

$$p'_{1,11}(\mathbf{x}^{(1)}) = M^{(1)}_{11}, \ldots, p'_{o,11}(\mathbf{x}^{(1)}) = M^{(o)}_{11}$$

is o quadratic equations in ln variables $\mathbf{x}^{(1)}$. Since the parameter o used in SNOVA is small, it is efficient to find a solution to this system. Let $\mathbf{y}^{(1)} \in \mathbb{F}_q^{ln}$ be a solution to this system.

Next, we focus on the system of equations in $\mathbf{x}^{(2)}$:

$$\begin{aligned}
&p'_{1,12}(\mathbf{y}^{(1)}, \mathbf{x}^{(2)}) = M^{(1)}_{12}, \ldots, p'_{o,12}(\mathbf{y}^{(1)}, \mathbf{x}^{(2)}) = M^{(o)}_{12},\\
&p'_{1,21}(\mathbf{y}^{(1)}, \mathbf{x}^{(2)}) = M^{(1)}_{21}, \ldots, p'_{o,21}(\mathbf{y}^{(1)}, \mathbf{x}^{(2)}) = M^{(o)}_{21},\\
&p'_{1,22}(\mathbf{x}^{(2)}) = M^{(1)}_{22}, \ldots, p'_{o,22}(\mathbf{x}^{(2)}) = M^{(o)}_{22}.
\end{aligned}$$

This is equivalent to the system of o quadratic equations in $ln - 2o$ variables since the first two system are $2o$ linear equations. Thus, it is also easy to solve this system. Let $\mathbf{y}^{(2)}$ be a solution to this second system.

By repeating similar processes, we finally obtain the system of o quadratic equations in $ln-2(l-1)o$ variables. If v, o satisfy $ln-2(l-1)o \geq o$, then the final system has a solution $\mathbf{y}^{(l)}$ with a high probability. As a result, we obtain a solution $\mathbf{y} = (\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(l)})$ to (20).

Since the parameters v, o satisfy $v > o$ in general, the condition $ln - 2(l-1)o > o$ are satisfied. Thus, this forgery attack works.

4.3 Construction of SNOVA

In this subsection, we describe the construction of SNOVA, and explain how the authors of SNOVA [28] resolve the vulnerability of the core polynomials $\{p'_{k,ij}\}$.

There are two techniques in order to resolve the vulnerability of the core polynomials. First one is mixing the core matrices $P_1, \ldots, P_o$, and second is transforming them by elements of a subfield in the matrix ring $M_l(\mathbb{F}_q)$.

4.3.1 Mixing the core matrices

Randomly choose $l \times l$ matrices $A_1, \ldots, A_{l^2}$ and $B_1, \ldots, B_{l^2}$. Moreover, randomly choose $ln \times ln$ matrices $Q_{11}, \ldots, Q_{l^2 1}$ and $Q_{12}, \ldots, Q_{l^2 2}$. Then we define the polynomial matrices h_k and g_k:

$$h_k := \sum_{i=1}^{l^2} A_i \cdot \mathbf{X} \cdot Q_{i1} \cdot F_k \cdot Q_{i2} \cdot {}^t\mathbf{X} \cdot B_i, \quad (1 \leq k \leq o).$$

$$g_k := \sum_{i=1}^{l^2} A_i \cdot \mathbf{X} \cdot Q_{i1} \cdot P_k \cdot Q_{i2} \cdot {}^t\mathbf{X} \cdot B_i, \quad (1 \leq k \leq o).$$

Here, h_k and g_k are the sets of l^2 quadratic polynomials $\mathcal{H}_k = \{h_{k,ij}\}_{ij}$ and $\mathcal{G}_k = \{g_{k,ij}\}_{ij}$ in the variables $\mathbf{X}$, respectively. By modifying in this way, it is considered to be difficult to apply the forgery attack in 4.2 to $\mathcal{G} = \{g_{k,ij}\}_{k,ij}$. However, it is also difficult to execute the signature generation algorithm, since $h_{k,ij}$ is NOT a linear polynomial regarding variables $\mathbf{x}_o^{(1)}, \ldots, \mathbf{x}_o^{(l)}$ because of the multiplication of Q_{ij}. To resolve this issue, it is necessary to use a subfield in multiplying of Q_{ij}.

4.3.2 Transforming by a subfield

First, let S be a symmetric matrix in $M_l(\mathbb{F}_q)$ such that its characteristic polynomial is irreducible over $\mathbb{F}_q$. Then the algebra $\mathcal{A}$ generated by S in $M_l(\mathbb{F}_q)$ forms an l-dimensional subfield in $M_l(\mathbb{F}_q)$.

Next, randomly choose non-zero $l \times l$ matrices $R_{11}, \ldots, R_{l^2 1}$ and $R_{12}, \ldots, R_{l^2 2}$ in $\mathcal{A}$. Set

$$Q_{ij} := \begin{pmatrix} R_{ij} & & \\ & \ddots & \\ & & R_{ij} \end{pmatrix} \in M_n(\mathcal{A}) \subset M_{ln}(\mathbb{F}_q).$$

Moreover, we choose the secret key T from $M_n(\mathcal{A}) \subset M_{ln}(\mathbb{F}_q)$. Since $\mathcal{A}$ is commutative, we have $Q_{ij}T = TQ_{ij}$. By defining h_k, g_k using these Q_{ij} and T, the signature generation algorithm works. In fact, we have

$$Q_{i1} \cdot P_k \cdot Q_{i2} = Q_{i1} \cdot T \cdot F_k \cdot {}^tT \cdot Q_{i2} = T \cdot Q_{i1} F_k Q_{i2} \cdot {}^tT.$$

Here, $Q_{i1}F_kQ_{i2}$ is a matrix whose lower right components are zero as in (1). Thus, $h_{k,ij}$ is a linear polynomial regarding variables $\mathbf{x}_o^{(1)}, \ldots, \mathbf{x}_o^{(l)}$ when $\mathbf{x}_v^{(1)}, \ldots, \mathbf{x}_v^{(l)}$ are fixed as scalars. Therefore, we can apply the signature generation algorithm of UOV.

4.3.3 Summary

As a result, the construction of SNOVA is summarized as follows. Randomly choose the following:

1. $ln \times ln$ matrices $F_1, \ldots, F_o$ whose lower right components are zero,
2. a matrix $T_0 \in M_{o\times v}(\mathcal{A})$, and set $T = \begin{pmatrix} 1_{lv} & 0_{lv\times lo} \\ T_0 & 1_{lo} \end{pmatrix}$,
3. $l \times l$ matrices $A_1, \ldots, A_{l^2}$ and $B_1, \ldots, B_{l^2}$,
4. non-zero matrices $R_{11}, \ldots, R_{l^2 1}$ and $R_{12}, \ldots, R_{l^2 2}$ in $\mathcal{A}$, and set $Q_{ij} := \begin{pmatrix} R_{ij} & & \\ & \ddots & \\ & & R_{ij} \end{pmatrix} \in M_{ln}(\mathbb{F}_q)$.

Then, the secret key is $\{F_k\}_k, T$, and the public key is $\{P_k := TF_k{}^tT\}_k$, and $\{A_i, B_i, R_{i1}, R_{i2}\}_i$.

The verifier generates g_k from the public key in the verification process. Here, since the data $\{A_i, B_i, R_{i1}, R_{i2}\}$ are generated randomly, we can compress them to a seed. As a result, the public key size almost depends on $P_1, \ldots, P_o$. Moreover, we can apply the technique of Petzoldt et al. [26] to $P_1, \ldots, P_o$.

5 Revisiting the security analysis of SNOVA

In this section, we recall the security analysis of SNOVA stated in [29]. In 5.1, we explain how the authors of SNOVA [29] analyzed the security of SNOVA.

5.1 Review of the security analysis of SNOVA

In this subsection, we briefly review the key recovery attacks used in the SNOVA document [29] in order to analyze the security of SNOVA.

A key recovery attack for SNOVA tries to find a secret key T or an equivalent key. The key recovery attacks in the document [29] are considered using the information of the core matrices of SNOVA. As stated in Remark 5, the core matrices $P_1, \ldots, P_o$ are originally defined using the $n \times n$ matrices $F_k = (F_{k,ij})_{1\le i,j\le n}$ over $M_l(\mathbb{F}_q)$. Moreover, the core quadratic polynomials $\{p'_{k,ij}\}$ generated by $P_1, \ldots, P_o$ can be seen as the public key of UOV with the parameter (q, l^2v, l^2o, l^2o). We call such a UOV instance $\{p'_{k,ij}\}$ the core polynomial UOV. The authors of SNOVA considered

Table 4 The complexity estimation (in $\log_2(\#\text{gates})$) evaluated in the document of SNOVA [29]

	(q,v,o,l)	Direct attack	Collision attack	KS attack	Intersection attack	Equivalent attack	MinRank attack
I	$(16,28,17,2)$	171	151	181	275	192	151
	$(16,25,8,3)$	175	159	617	819	231	148
	$(16,24,5,4)$	188	175	1221	1439	286	150
III	$(16,43,25,2)$	231	215	293	439	279	212
	$(16,49,11,3)$	230	213	1373	1631	530	215
	$(16,37,8,4)$	291	271	1861	2192	424	217
V	$(16,61,33,2)$	308	279	453	727	386	279
	$(16,66,15,3)$	307	285	1841	2178	707	280
	$(16,60,10,4)$	355	335	3205	3602	812	278

whether each key recovery attack can be applied to the core matrices $P_1,\dots,P_o$ and the core polynomial UOV $\{p'_{k,ij}\}$, and analyzed their complexity estimations.

(i) KS attack:

The authors of SNOVA considered that since the components of $F_1,\dots,F_o$ are in the non-commutative ring $M_l(\mathbb{F}_q)$, the oil space $\mathcal{O}$ cannot be defined. From such a consideration, they concluded that the KS attack can not be applied to the core matrices $P_1,\dots,P_o$. On the other hand, they considered the KS attack for the core polynomial UOV $\{p'_{k,ij}\}$. Since the core polynomial UOV is an instance of UOV with parameter (q,l^2v,l^2o,l^2o), its complexity is given by $O(q^{l^2(v-o)})$.

(ii) Reconciliation attack:

In the document, the reconciliation attack is applied to only the core polynomial UOV $\{p'_{k,ij}\}$. Since the core polynomial UOV is an instance of UOV with parameter (q,l^2v,l^2o,l^2o), this attack solves the quadratic system of l^2o equations in l^2v variables. They concluded that this attack is not efficient compared to the direct attack.

(iii) Intersection attack:

As in the case of the KS attack, they considered only the intersection attack for the core polynomial UOV, that is, the intersection attack for an instance of UOV with parameter (q,l^2v,l^2o,l^2o). Its complexity is given by using the estimation in 2.2.

(iv) Equivalent attack:

This attack tries to recover T using the relation $T^{-1}\cdot P_k\cdot {}^tT^{-1}=F_k\ \ (1\le k\le o)$, and the fact that the lower right $lo\times lo$ submatrix of each F_k is zero. Since $T^{-1}=\begin{pmatrix}1_{lv} & 0_{lv\times lo}\\ -T_0 & 1_{lo}\end{pmatrix}$ and T_0 consists of lvo unknowns, this attack forms l^2o^3 quadratic equations in lvo variables. By solving these quadratic equations, the secret key T is recovered. See [29] for its complexity estimation.

(v) MinRank attack:

The author of SNOVA discovered that there exists a linear combination of the representation matrices of the core polynomial UOV $\{p'_{k,ij}\}$ with rank lv. Then, they estimated the complexity of MinRank problem with l^2o square matrices of size l^2n and the target rank lv. While they did not give a method to recover an equivalent key from a solution to the MinRank problem, they adopted this complexity to the security estimation of SNOVA from a conservative point of view.

Table 4 shows the proposed parameters of SNOVA in the additional NIST PQC standardization and the complexity estimations they gave in the document [29].

5.2 Revisiting the security analysis of SNOVA

In this subsection, we reconsider the security analysis of SNOVA based on the construction we reorganized in Section 4.

As seen in 5.1, the authors of SNOVA claimed that since SNOVA and its core matrices are constructed using the non-commutative ring $M_l(\mathbb{F}_q)$, some key recovery attacks cannot be applied to SNOVA. However, the core matrices $P_1, \ldots, P_o$ can be identified with a part of the public key of UOV with parameter (q, lv, lo, o). Thus, we can apply some key recovery attacks of UOV to the core matrices $P_1, \ldots, P_o$. Moreover, since the secret key T is in $M_n(\mathcal{A})$, we can make some key recovery attacks more efficient.

<u>(i) KS attack:</u>

The core matrices $P_1, \ldots, P_o$ are public information and have the structure of UOV with parameter (q, lv, lo, o). Therefore, the KS attack works for $P_1, \ldots, P_o$, and its complexity is $O(q^{l(v-o)})$. This version of the KS attack is efficient compared with the KS attack in 5.1 (i).

<u>(ii) Reconciliation attack:</u>

We can also apply the reconciliation attack to the core matrices $P_1, \ldots, P_o$ to recover the secret key T or an equivalent key. Moreover, by using the fact that the secret key T is in $M_n(\mathcal{A})$ and $P_1, \ldots, P_o$ are not necessarily symmetric matrices in SNOVA, we can make the reconciliation attack more efficient.

Let $\mathbf{x}$ be a non-zero element in the twisted oil space $\mathcal{O} \cdot T^{-1}$, namely $\mathbf{x} \in \mathcal{O} \cdot T^{-1}$, where the oil space $\mathcal{O}$ is defined by $\mathcal{O} := \{(\overbrace{0, \ldots, 0}^{lv}, \overbrace{*, \ldots, *}^{lo}) \in \mathbb{F}_q^{ln}\}$. Since T is in $M_n(\mathcal{A})$, the secret key T is commutative with

$$S_{\mathrm{diag}} := \begin{pmatrix} S & & \\ & \ddots & \\ & & S \end{pmatrix} \in M_{ln}(\mathbb{F}_q),$$

where S is the $l \times l$ symmetric matrix in 4.3.2. Thus, we have for $i = 0, \ldots, l-1$,

$$\mathbf{x} \cdot S_{\mathrm{diag}}^i \in \mathcal{O} \cdot T^{-1} S_{\mathrm{diag}}^i = \mathcal{O} \cdot S_{\mathrm{diag}}^i T^{-1} = \mathcal{O} \cdot T^{-1}.$$

From this, we have

$$\mathbf{x} \cdot S_{\mathrm{diag}}^i \cdot P_k \cdot S_{\mathrm{diag}}^j \cdot {}^t\mathbf{x} = 0, \ (0 \le i, j \le l-1, 0 \le k \le o). \tag{21}$$

By solving this system, we might be able to obtain an element in the twisted oil space $\mathcal{O} \cdot T^{-1}$. Since the dimension of $\mathcal{O} \cdot T^{-1}$ is lo, this system (21) can be reduced to a system of $l^2 o$ homogeneous quadratic equations in $ln - (lo - 1) = lv + 1$ variables, which has only one solution belonging to the twisted oil space up to a scalar factor. Here, since P_k is not necessarily symmetric for the case of SNOVA, two polynomials $\mathbf{x} \cdot S_{\text{diag}}^i \cdot P_k \cdot S_{\text{diag}}^j \cdot {}^t\mathbf{x}$ and $\mathbf{x} \cdot S_{\text{diag}}^j \cdot P_k \cdot S_{\text{diag}}^i \cdot {}^t\mathbf{x}$ are not necessarily equal. Therefore, the complexity of the reconciliation attack is evaluated by

$$\min_k q^k \cdot 3 \binom{lv - k + D_{lv+1-k,l^2o}}{D_{lv+1-k,l^2o}}^2 \binom{lv + 2 - k}{2}, \tag{22}$$

where $\max\{0, lv + 1 - l^2 o\} \leq k \leq lv$ is the number of fixed variables in the hybrid approach.

(iii) Intersection attack:

We can apply the intersection attack to the core matrices $P_1, \ldots, P_o$. Let Q, R be two randomly chosen invertible linear combinations of $P_1, \ldots, P_o$. Let $\mathbf{x}$ be an element in $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R$. Since we have $\mathbf{x}Q^{-1}, \mathbf{x}R^{-1} \in \mathcal{O} \cdot T^{-1}$, we obtain

$$\mathbf{x} \cdot Q^{-1} S_{\text{diag}}^i, \ \ \mathbf{x} \cdot R^{-1} S_{\text{diag}}^i \in \mathcal{O} \cdot T^{-1} \ (0 \leq i \leq l-1).$$

From this, we have for $0 \leq i, j \leq l - 1, 0 \leq k \leq o$

$$\begin{aligned} &\mathbf{x} \cdot Q^{-1} S_{\text{diag}}^i \cdot P_k \cdot S_{\text{diag}}^j {}^t Q^{-1} \cdot {}^t\mathbf{x} = 0, \quad \mathbf{x} \cdot Q^{-1} S_{\text{diag}}^i \cdot P_k \cdot S_{\text{diag}}^j {}^t R^{-1} \cdot {}^t\mathbf{x} = 0, \\ &\mathbf{x} \cdot R^{-1} S_{\text{diag}}^i \cdot P_k \cdot S_{\text{diag}}^j {}^t Q^{-1} \cdot {}^t\mathbf{x} = 0, \quad \mathbf{x} \cdot R^{-1} S_{\text{diag}}^i \cdot P_k \cdot S_{\text{diag}}^j {}^t R^{-1} \cdot {}^t\mathbf{x} = 0. \end{aligned} \tag{23}$$

As a result, the intersection attack for the core matrices $P_1, \ldots, P_o$ finds an element $\mathbf{x} \cdot Q^{-1}$ in $\mathcal{O} \cdot T^{-1}$ by solving the above system, if $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R \neq 0$. Since the system (23) has $2l$ redundant equations, it is reduced to a system of $4l^2 o - 2l$ homogeneous quadratic equations in ln variables.

The case $v < 2o$

In this case, the dimension of $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R$ is at least $2lo - lv > 0$. Thus the system can be reduced a system of $M := 4l^2 o - 2l$ homogeneous quadratic equations in $N := ln - (2lo - lv - 1) = 2lv - lo + 1$ variables. Moreover, our experiments in Table 9 in the appendix show that this reduced system behaves like a random system of M homogeneous quadratic equations in N variables. The complexity to solve the reduced system is given by

$$\min_k q^k \cdot 3 \binom{N - k - 1 + D_{N-k,M}}{D_{N-k,M}}^2 \binom{N - k + 1}{2}, \tag{24}$$

where $0 \leq k \leq N - 1$ is the number of fixed variables in the hybrid approach.

The case $v \geq 2o$

In this case, the probability that $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R \neq 0$ is around $1/q^{lv-2lo+1}$. Thus, the system (23) is a system of $M := 4l^2 o - 2l$ homogeneous quadratic equations in ln variables, and has a solution belonging to $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R$ at the probability $1/q^{lv-2lo+1}$. Our experiments in Table 9 in the appendix show that the system (23) in the case $v \geq 2o$ also behaves like a random system of M homogeneous quadratic equations in ln variables. Note that, for the case of $v \geq 2o$, the reduced system does not have non-zero solutions when $\mathcal{O} \cdot T^{-1} Q \cap \mathcal{O} \cdot T^{-1} R = 0$. For that reason, $\text{Rank}_d = \#\text{Columns}_d$ can happen with high probability in Table 9.

The complexity to find a non-zero element in $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ is given by

$$\min_{k} q^{lv-2lo+1} q^k \cdot 3 \binom{ln-k-1+D_{ln-k,M}}{D_{ln-k,M}}^2 \binom{ln-k+1}{2}, \tag{25}$$

where $\max\{0, ln-M\} \leq k \leq ln-1$ is the number of fixed variables in the hybrid approach.

(iv) Equivalent attack:
It is clear that the equation system of the equivalent attack in 5.1 (iv) is the full reconciliation attack (see 3.3 in [2]), and contains that of the reconciliation attack in 5.2 (ii). The dominant part of the equivalent attack is considered to be the part of the reconciliation attack . Therefore, it is enough to analyze the reconciliation attack.

From the above, we could indeed apply the key recovery attacks to the core matrices $P_1, \ldots, P_o$, and it is efficient compared with the key recovery attacks for the core polynomial UOV $\{p'_{k,ij}\}$. Thus, it is considered that we should analyze the security of the core matrices instead of the core polynomial UOV. Table 5 shows the complexity estimations of KS attack, reconciliation attack and intersection attack for the core matrices $P_1, \ldots, P_o$.

Table 5 Our complexity estimation (in $\log_2$(#gates)) evaluated in 5.2

	(q, v, o, l)	KS attack	Reconciliation attack	Intersection attack
I	$(16, 28, 17, 2)$	**93**	**132** ($k = 2$)	**87** ($k = 0$)
	$(16, 25, 8, 3)$	209	209 ($k = 15$)	221 ($k = 0$)
	$(16, 24, 5, 4)$	309	270 ($k = 30$)	349 ($k = 0$)
III	$(16, 43, 25, 2)$	**149**	**193** ($k = 6$)	**120** ($k = 0$)
	$(16, 49, 11, 3)$	461	438 ($k = 66$)	529 ($k = 0$)
	$(16, 37, 8, 4)$	469	388 ($k = 45$)	507 ($k = 0$)
V	$(16, 61, 33, 2)$	**229**	**277** ($k = 17$)	**167** ($k = 1$)
	$(16, 66, 15, 3)$	617	575 ($k = 87$)	690 ($k = 0$)
	$(16, 60, 10, 4)$	805	695 ($k = 112$)	922 ($k = 0$)

Here, the security level I, III and V mean that all classical attacks require $2^{143}, 2^{207}$ and 2^{272} classical gates to break the scheme, respectively. From this table, the parameters for $l = 2$ do not satisfy the claimed security levels.

6 Conclusion

We gave a new security analysis for UOV variants with small public keys, MAYO,QR-UOV,VOX, and SNOVA. First, we showed that the rectangular MinRank attack originally proposed on the Rainbow scheme by Beullens is applicable to MAYO, QR-UOV, and VOX. Second, we reorganized the construction of SNOVA, and reconsider its security analysis. Through our analysis, we showed that all parameters of VOX and some parameters of SNOVA submitted in the NIST PQC additional call for digital signatures do not satisfy the claimed security levels.

Acknowledgements 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. Beullens, W.: 'Improved Cryptanalysis of UOV and Rainbow', EUROCRYPT 2021, LNCS 12696, pp. 348–373, Springer
3. Beullens, W.: 'MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps', SAC 2021, LNCS 13203, pp. 355–376, Springer
4. Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.: 'MAYO', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
5. Beullens, W., Chen, M-S., Ding, J., Gong, B., Kannwischer, M.J., Patarin, J., Peng, B.Y., Schmidt, D., Shih, C.J., Tao, C., Yang, B.Y.: 'UOV', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
6. 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.
7. Ding, J., Yang, B.Y., Chen, C.H. O., Chen, M.S., Cheng, C.M.: 'New differential-algebraic attacks and reparametrization of Rainbow', ACNS 2008, LNCS 5037, pp. 242–257, Springer
8. Ding, J., Gong, B., Guo, H., He, X., Jin, Y., Pan, Y., Schmidt, D., Tao, C., Xie, D., Yang, B.Y., Zhao, Z.: 'TUOV', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
9. Faugère, J.C.: 'A new efficient algorithm for computing Gröbner bases (F4)', Journal of Pure and Applied Algebra, 1999, Vol.139, pp. 61–88
10. Faugère, J.C.: 'A new efficient algorithm for computing Gröbner Bases without reduction to zero (F5)', ISSAC 2002, pp. 75–83
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. Furue, H., Nakamura, S., Takagi, T.: 'Improving Thomae-Wolf algorithm for solving underde- termined multivariate quadratic polynomial problem', PQCrypto2021, LNCS 12841, pp.65–78.
15. Goubin, L., Cogliati, B., Faugère, J.C., Fouque, P.A., Larrieu, R., Gilles M.R., Minaud, B., Patarin, J.: 'PROV', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
16. Guo, H., Ding, J.: 'A Practical MinRank Attack Against VOX', IACR Cryptology ePrint Archive, 2024/166
17. Hashimoto, Y., 'An improvement of algorithms to solve under-defined systems of multivariate quadratic equations', JSIAM Letters, Vol.15 (2023), pp.53–56
18. Ikematsu, Y., Akiyama, R.: 'Revisiting the security analysis of SNOVA', IACR Cryptology ePrint Archive, 2024/096
19. Kipnis, A., Patarin, L., Goubin, L.: 'Unbalanced Oil and Vinegar Schemes', EUROCRYPT 1999, LNCS 1592, pp. 206–222, Springer

20. Kipnis A., Shamir A.: ‘Cryptanalysis of the oil and vinegar signature scheme’, CRYPTO 98, LNCS 1462, pp. 257–266. Springer
21. Li, P., Ding, J.: ‘Cryptanalysis of the SNOVA signature scheme’, IACR Cryptology ePrint Archive, 2024/110
22. 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
23. National Institute of Standards and Technology: ‘Post-Quantum Cryptography Standardization’, ⟨https://csrc.nist.gov/projects/post-quantum-cryptography⟩
24. 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⟩
25. 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)
26. Petzoldt, A., Bulygin, S., Buchmann, J.-A.: ‘CyclicRainbow - a multivariate signature scheme with a partially cyclic public key’, INDOCRYPT 2010, LNCS, vol. 6498, pp. 33–48. Springer (2010)
27. Smith-Tone D., Perlner, R.A.: ‘Rainbow Band Separation is Better than we Thought’, IACR Cryptology ePrint Archive, 2020/702
28. Wang, L.C., Tseng, P.E., Kuan, Y.L., Chou, C.Y.: ‘A Simple Noncommutative UOV Scheme’, IACR Cryptology ePrint Archive, 2022/1742
29. Wang, L.C., Chou, C.Y., Ding, J., Kuan, Y.L., Li, M.S., Tseng, B.S., Tseng, P.E., Wang, C.C.: ‘SNOVA’, Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
30. Thomae, E., Wolf, C.: ‘Solving underdetermined systems of multivariate quadratic equations revisited’, PKC2012, LNCS 7293, pp.156–171.
31. Yang, B.Y., Chen, J.M.: ‘All in the XL family: Theory and practice’, ICISC 2004, LNCS 3506, pp.67-86, Springer
32. Wiedemann, D.: ‘Solving sparse linear equations over finite fields’, IEEE Trans. Inform. Theory, 32(1), pp. 54–62, 1986

Appendix A The proposed parameters of UOV [5]

Table 6 The proposed parameters of UOV [5] in the additional NIST PQC standardization project

Security level	(q, v, o)	Public key (bytes)	Signature (bytes)
I	$(256, 68, 44)$	43576	128
	$(16, 96, 64)$	66576	96
III	$(256, 112, 72)$	189232	200
V	$(256, 148, 96)$	446992	260

Appendix B Experimental results

<u>MAYO</u>

In Table 7, 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.

Table 7 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

QR-UOV

In Table 8, we experimented that $b_{\min}$ is equal to $b_{\min}^{(\text{predict})}$ for some parameters. As seen in Table 8, we have $b_{\min} = b_{\min}^{(\text{predict})}$.

Table 8 Experiments for $b_{\min}$ and $b_{\min}^{(\text{predict})}$

(q,V,O,l)	m'	$b_{\min}^{(\text{predict})}$	$b_{\min}$
$(7,5,2,3)$	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

SNOVA

The upper half of Table 9 shows that the reduced systems stated in the case of $v < 2o$ in 5.2 (iii) behave like a random system of $M := 4l^2o - 2l$ homogeneous quadratic equations in $N := ln - (2lo - lv - 1) = 2lv - lo + 1$ variables. Here, H_d is the dimension of degree d part I_d of the homogeneous ideal I generated by a semi-regular system of M homogeneous quadratic equations in N variables. The dimension H_d is computed by using the coefficient of t^d in $\frac{1-(1-t^2)^M}{(1-t)^N}$. Moreover, Rank_d and $\#\text{Columns}_d$ mean the rank and the number of columns of the Macaulay matrix at degree d for the reduced system of (23). For the case of $v < 2o$, since the reduced system has only one solution up to a scalar factor, Rank_d is always less than or equal to $\#\text{Columns}_d - 1$. Actually, the marked number by boldface in the table is equal to $\#\text{Columns}_d - 1$.

The lower half of Table 9 shows that the system (23) in the case $v \geq 2o$ also behaves like a random system of $M := 4l^2o - 2l$ homogeneous quadratic equations in ln variables. Note that, for the case of $v \geq 2o$, the reduced system does not have non-zero solutions when $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R = 0$. For that reason, $\text{Rank}_d = \#\text{Columns}_d$ can happen with high probability in Table 9.

Table 9 The rank and the number of columns of the Macaulay matrix at each degree d for the system (23). For the case of $v < 2o$, we consider the reduced system of M equations in N variables.

(q, v, o, l)		$d = 2$	$d = 3$	$d = 4$	$d = 5$	$d = 6$
	H_d	60	1260	10626		
$(16, 7, 4, 2)$	Rank$_d$	60	1260	**10625**		
	#Columns$_d$	231	1771	10626		
	H_d	138	4278	46376		
$(16, 7, 4, 3)$	Rank$_d$	138	4278	**46375**		
	#Columns$_d$	496	5456	46376		
	H_d	248	10168	135751		
$(16, 7, 4, 4)$	Rank$_d$	248	10168	**135750**		
	#Columns$_d$	861	12341	135751		
	H_d	76	2052	25878	169911	
$(16, 9, 5, 2)$	Rank$_d$	76	2052	25878	**169910**	
	#Columns$_d$	378	3654	27405	169911	
	H_d	174	6960	123410		
$(16, 9, 5, 3)$	Rank$_d$	174	6960	**123409**		
	#Columns$_d$	820	11480	123410		
	H_d	312	16536	367290		
$(16, 9, 5, 4)$	Rank$_d$	312	16536	**367289**		
	#Columns$_d$	1431	26235	367290		
	H_d	28	448	3430	15504	
$(16, 6, 2, 2)$	Rank$_d$	28	448	3430	15504	
	#Columns$_d$	136	816	3876	15504	
	H_d	66	1584	17550		
$(16, 6, 2, 3)$	Rank$_d$	66	1584	17550		
	#Columns$_d$	300	2600	17550		
	H_d	120	3840	52360		
$(16, 6, 2, 4)$	Rank$_d$	120	3840	52360		
	#Columns$_d$	528	5984	52360		
	H_d	28	504	4410	25116	100947
$(16, 7, 2, 2)$	Rank$_d$	28	504	4410	25116	100947
	#Columns$_d$	171	1140	5985	26334	100947
	H_d	66	1782	22803	169911	
$(16, 7, 2, 3)$	Rank$_d$	66	1782	22803	169911	
	#Columns$_d$	378	3654	27405	169911	
	H_d	120	4320	72780	658008	
$(16, 7, 2, 4)$	Rank$_d$	120	4320	72780	658008	
	#Columns$_d$	666	8436	82251	658008	