# Revisiting the security analysis of SNOVA

Yasuhiko Ikematsu and Rika Akiyama

**Abstract** SNOVA is a multivariate signature scheme submitted to the additional NIST PQC standardization project started in 2022. SNOVA is constructed by incorporating the structure of the matrix ring over a finite field into the UOV signature scheme, and the core part of its public key is the UOV public key whose coefficients consist of matrices. As a result, SNOVA dramatically reduces the public key size compared to UOV. In this paper, we recall the construction of SNOVA, and reconsider its security analysis. In particular, we investigate key recovery attacks applied to the core part of the public key of SNOVA in detail. Due to our analysis, we show that some parameters of SNOVA submitted in the additional NIST PQC standardization do not satisfy the claimed security levels.

**Key words:** PQC, MPKC, UOV, 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 mul-

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

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

tivariate quadratic equations over a finite field (MQ problem), and are one of the main candidate of PQC.

NIST started the PQC standardization project [14] 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 [15] (called the additional NIST PQC standardization in this paper). In the additional NIST PQC standardization, 40 signature schemes were accepted to the first round in June 2023, and 10 among them are multivariate schemes.

In MPKC, UOV [12] 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. SNOVA is a variant of UOV with small public key proposed by Wang et al. [18] in 2022, and was submitted to the additional NIST PQC standardization [19]. This is constructed by improving UOV using a non-commutative ring (mainly a matrix ring). More specifically, SNOVA is defined by changing the coefficient field $\mathbb{F}_q$ of polynomials in UOV into the matrix ring $M_l(\mathbb{F}_q)$. The public key of UOV constructed in such a way forms the core part of SNOVA. Moreover, by mixing and transforming the core part with elements of a subfield in $M_l(\mathbb{F}_q)$, the public key of SNOVA is constructed. The papers [18, 19] claim that SNOVA avoids some existing attacks of UOV because of using such a non-commutative ring, and increases the security for forgery attacks because of using the technique of mixing and transforming. As a result, the size of the public key of SNOVA [19] is quite smaller than that of the UOV scheme in [4]. Since SNOVA is a new proposed signature scheme, it is necessary to thoroughly analyze its security.

In this paper, we reorganize the construction of SNOVA, and reconsider its security analysis. First, we explain the construction of the core part without using the matrix ring $M_l(\mathbb{F}_q)$. The paper [18] states that the core part is a polynomial system whose almost coefficients are zero (i.e.sparse polynomials), and therefore the technique of mixing and transforming are applied. In fact, 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 [19] for $l = 2$ submitted in the additional NIST PQC standardization do not satisfy the claimed security levels.

This paper is organized as follows. In Section 2, we reorganize the construction of SNOVA. In Section 3, we recall the security analysis of SNOVA in [19]. In Section 4, we reconsider the security of SNOVA using the result in Section 2. In Section 5, we conclude our paper.

## 2 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 [18, 19]. In 2.1, we describe the construction of UOV [12] which is a underlying scheme of SNOVA. In 2.2-2.4, we explain the construction of SNOVA.

### 2.1 UOV

We describe the key generation, signature generation and verification of UOV in this subsection. Let $v, o$ be two 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 $(q, v, o)$. Randomly choose $o$ square matrices $F_1, \ldots, F_o$ with size $n$ over $\mathbb{F}_q$ in the following form:

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

Namely, each $F_k$ $(1 \leq k \leq o)$ is a matrix whose lower right components are zero. Here, each coefficient $a_{ij}^{(k)}$ is randomly chosen from the finite field $\mathbb{F}_q$. We define $o$ quadratic polynomials $f_1, \ldots, f_o$ in $n$ variables $\mathbf{x}$ as follows:

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

From the form of $F_k$, it is clear that $f_k(\mathbf{x})$ is a linear polynomial regarding variables $\mathbf{x}_o$ when $\mathbf{x}_v$ is fixed as scalars. We define a quadratic map $\mathcal{F} = (f_1, \ldots, f_o) : \mathbb{F}_q^n \to \mathbb{F}_q^o$, 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 $G_k$ and quadratic polynomials $g_k$ $(1 \leq k \leq o)$:

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

It is clear that $g_k(\mathbf{x}) = f_k(\mathbf{x} \cdot T)$. Then, the secret key of UOV with parameter $(q, v, o)$ is given by $(f_1, \ldots, f_o, \mathcal{T})$, and the public key is the set of quadratic polynomials $(g_1, \ldots, g_o)$, which is equal to the quadratic map $\mathcal{G} := \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^o$.

The signature generation and verification processes for UOV are done as follows. Let $\mathbf{m} = (m'_1, \ldots, m'_o) \in \mathbb{F}_q^o$ be a message to be signed. First, randomly choose an element $\mathbf{c} = (c_1, \ldots, c_v) \in \mathbb{F}_q^v$. Next, find a solution $\mathbf{d} \in \mathbb{F}_q^o$ to the following $o$ linear equations in $\mathbf{x}_o$:

$$f_1(\mathbf{c}, \mathbf{x}_o) = m'_1, \cdots, f_o(\mathbf{c}, \mathbf{x}_o) = m'_o. \tag{4}$$

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 $\mathcal{F}(\mathbf{x}) = \mathbf{m}$. Finally, $\mathbf{s} := (\mathbf{c}, \mathbf{d}) \cdot T^{-1}$, which is a solution to $\mathcal{G}(\mathbf{x}) = \mathbf{m}$, is a signature of $\mathbf{m}$. The verification process is done by checking whether $\mathcal{G}(\mathbf{s}) = \mathbf{m}$ or not.

It is known that the size of the public key of UOV can be reduced using the technique of Petzoldt et al. [17] without declining the security. Moreover, the secret key $T \in \mathrm{GL}_n(\mathbb{F}_q)$ is often taken as follows:

$$T = \begin{pmatrix} 1_v & 0_{v \times o} \\ T_0 & 1_o \end{pmatrix}, \tag{5}$$

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 1) of UOV [4] based on the latest MPKC security analysis, and submitted it to the additional NIST PQC standardization project [15].

**Table 1** The proposed parameters of UOV [4] 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 |

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 [2, 3], QR-UOV [9, 8], VOX [16] and SNOVA [18, 19].

## 2.2 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 [18, 19] (See Remark 1 for the explanation of the difference as well).

In UOV, a matrix $G_k$ has generated only one quadratic polynomial $g_k(\mathbf{x})$ as in (3). In SNOVA, this one-to-one correspondence ($G_k \mapsto g_k$) is improved as follows. Let $l$ be a positive integer, and $F_1, \ldots, F_o, G_1, \ldots, G_o$ be matrices defined as in (1) and (3) with parameter $(q, lv, lo)$. 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:

$$\mathbf{x}_v^{(i)} = (x_1^{(i)}, \ldots, x_{lv}^{(i)}), \quad \mathbf{x}_o^{(i)} = (x_{lv+1}^{(i)}, \ldots, x_{ln}^{(i)}).$$

Then, we define two systems of quadratic polynomials $f_{k,ij} = f_{k,ij}(\mathbf{X})$ and $g_{k,ij} = g_{k,ij}(\mathbf{X})$ $(1 \le k \le o, 1 \le i, j \le l)$:

$$f_k = \begin{pmatrix} f_{k,11}(\mathbf{X}) & \ldots & f_{k,1l}(\mathbf{X}) \\ \vdots & \ddots & \vdots \\ f_{k,l1}(\mathbf{X}) & \ldots & f_{k,ll}(\mathbf{X}) \end{pmatrix} := \mathbf{X} \cdot F_k \cdot {}^t\mathbf{X},$$

$$g_k = \begin{pmatrix} g_{k,11}(\mathbf{X}) & \ldots & g_{k,1l}(\mathbf{X}) \\ \vdots & \ddots & \vdots \\ g_{k,l1}(\mathbf{X}) & \ldots & g_{k,ll}(\mathbf{X}) \end{pmatrix} := \mathbf{X} \cdot G_k \cdot {}^t\mathbf{X}.$$

We call $G_1, \ldots, G_o$ the core matrices of SNOVA and $\{g_{k,ij}\}$ the core (quadratic) polynomials of SNOVA.

It is clear that $g_{k,ij}(\mathbf{X}) = f_{k,ij}(\mathbf{X} \cdot T)$, 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 $\{g_{k,ij}\}$ can be identified with the public key of UOV with parameter $(q, l^2v, l^2o)$, and we can execute the same process of UOV in 2.1 as the signature generation. The verification process is done by using the quadratic map $(g_1, \ldots, g_o) = \{g_{k,ij}\} : M_{l \times ln}(\mathbb{F}_q) \to M_l(\mathbb{F}_q)^o$.

A verifier can construct $l^2o$ quadratic polynomials $\{g_{k,ij}\}$ in $l^2n$ variables $\mathbf{X}$ from only the core matrices $G_1, \ldots, G_o$. In particular, a core matrix $G_k$ generates $l^2$ quadratic polynomials. Thus, if the core matrices $G_1, \ldots, G_o$ are the public key, then the size of the public key is small compared with $\{g_{k,ij}\}$. This is the main technique to reduce the size of the public key used in SNOVA. Note that, as stated in 2.3 below, the core polynomials are vulnerable for a forgery attack. SNOVA will be constructed by further improving this technique.

*Remark 1* Wang et al. [18, 19] 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 el-

ement 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.

### 2.3 A forgery attack for the core polynomials $\{g_{k,ij}\}$

As stated in [18], SNOVA is constructed by improving the technique in 2.2, since the core polynomials $\{g_{k,ij}\}$ 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 $\{g_{k,ij}\}$ are actually vulnerable for a forgery attack. In this subsection, we show the method to forge a signature for the core polynomials $\{g_{k,ij}\}$.

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

$$g_{k,ij}(\mathbf{X}) = M_{ij}^{(k)},\ (1 \leq i, j \leq l,\ 1 \leq k \leq o). \tag{6}$$

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

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

$$g_{1,11}(\mathbf{x}^{(1)}) = M_{11}^{(1)}, \ldots, g_{o,11}(\mathbf{x}^{(1)}) = M_{11}^{(o)}$$

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 $\mathbf{x}^{(2)}$:

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

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 (6).

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.

## 2.4 Construction of SNOVA

In this subsection, we describe the construction of SNOVA, and explain how the authors of SNOVA [18] resolve the vulnerability of the core polynomials $\{g_{k,ij}\}$.

There are two techniques in order to resolve the vulnerability of the core polynomials. First one is mixing the core matrices $G_1, \ldots, G_o$, and second is transforming them by elements of a subfield in the matrix ring $M_l(\mathbb{F}_q)$.

### 2.4.1 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 $p_k$:

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

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

Here, $h_k$ and $p_k$ are the sets of $l^2$ quadratic polynomials $\mathcal{H}_k = \{h_{k,ij}\}_{ij}$ and $\mathcal{P}_k = \{p_{k,ij}\}_{ij}$ in the variables $\mathbf{X}$, respectively. By modifing in this way, it is considered to be difficult to apply the forgery attack in 2.3 to $\mathcal{P} = \{p_{k,ij}\}_{k,ij}$. 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 $Q_{ij}$.

### 2.4.2 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 $h_k, p_k$ using these $Q_{ij}$ and

$T$, the signature generation algorithm works. In fact, we have

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

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 in 2.1.

### 2.4.3 Summary

As a result, the construction of SNOVA is sumarized as follows. Let $\{F_k\}_{1 \leq k \leq o}$ be the set of $ln \times ln$ matrices whose lower right is zero. Randomly choose the following:

1. a matrix $T_0 \in M_{o \times v}(\mathcal{A})$, and set

$$T = \begin{pmatrix} 1_{lv} & 0_{lv \times lo} \\ T_0 & 1_{lo} \end{pmatrix},$$

2. $l \times l$ matrices $A_1, \ldots, A_{l^2}$ and $B_1, \ldots, B_{l^2}$,
3. 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 $\{G_k := TF_k{}^tT\}_k$, and $\{A_i, B_i, R_{i1}, R_{i2}\}_i$.

The signature generation and verification are done as stated in 2.1. The verifier generates $p_k$ from the public key. 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 $G_1, \ldots, G_o$. Moreover, we can apply the technique of Petzoldt et al. [17] to $G_1, \ldots, G_o$. The following table (Table2) is the parameter set of SNOVA proposed in [19], which was submitted to the additional NIST PQC standardization.

## 3 Security analysis of SNOVA in [19]

In this section, we recall the security analysis of SNOVA stated in [19]. In 3.1, we review the security analysis of UOV. In 3.2, we explain how the authors of SNOVA [19] analyzed the security of SNOVA.

**Table 2** The proposed parameters of SNOVA [19] in the additional NIST PQC standardization project

| | $(q, v, o, l)$ | Public key size (bytes) | Signature size (bytes) |
|---|---|---|---|
| I | $(16, 28, 17, 2)$ | 9826 | 90 |
| | $(16, 25, 8, 3)$ | 2304 | 149 |
| | $(16, 24, 5, 4)$ | 1000 | 232 |
| III | $(16, 43, 25, 2)$ | 31250 | 240 |
| | $(16, 49, 11, 3)$ | 5990 | 270 |
| | $(16, 37, 8, 4)$ | 4096 | 360 |
| V | $(16, 61, 33, 2)$ | 71874 | 188 |
| | $(16, 66, 15, 3)$ | 15188 | 365 |
| | $(16, 60, 10, 4)$ | 8000 | 560 |

## 3.1 Review of the security analysis of UOV

Before we state the security analysis of SNOVA in [19], we recall the security analysis of UOV. The security of UOV with the parameter $(q, v, o)$ is mainly estimated using the following attacks.

### 3.1.1 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 $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ in $n = v + o$ variables. Since it is enough to find a solution to the system $\mathcal{P}(\mathbf{x}) = \mathbf{m}$, 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 $F_4$ [6], $F_5$ [7] and XL [21] are often considered. Then, 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

$$\min_k q^k \cdot 3 \binom{o - k + D_{o+1-k,o}}{D_{o+1-k,o}}^2 \binom{o + 2 - k}{2}, \tag{7}$$

where $0 \leq k \leq o$ 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 [20] 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. [10] and

Hashimoto [11]. To be exact, the complexity of the direct attack for UOV is given by using such techniques.

### 3.1.2 Kipnis-Shamir (KS) attack

The KS attack was proposed by Kipnis and Shamir [13], and is a key recovery attack for UOV. This attack utilizes the special form of $F_1, \ldots, F_o$ in (1).

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

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

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

$$(P'_1, \ldots, P'_o) = \left(T \cdot F'_1 \cdot {}^tT, \ldots, T \cdot F'_o \cdot {}^tT\right). \tag{8}$$

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 set the vinegar space $\mathcal{V}$ and the oil space $\mathcal{O}$ in $\mathbb{F}_q^n$ as follows:

$$\mathcal{V} := \mathrm{Span}\{e_1, \ldots, e_v\}, \quad \mathcal{O} := \mathrm{Span}\{e_{v+1}, \ldots, e_n\}.$$

Then the KS attack tries to find vectors of the twisted oil space

$$\mathcal{O} \cdot T^{-1} := \mathrm{Span}\{e_{v+1}T^{-1}, \ldots, e_nT^{-1}\} \tag{9}$$

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 $O(q^{v-o})$.

### 3.1.3 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 [5]. 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 .

### 3.1.4 Intersection attack

The intersection attack was proposed by Beullens [1], 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 $\mathbf{x}$:

$$\begin{aligned} &p_1(\mathbf{x}Q^{-1}) = \cdots = p_o(\mathbf{x}Q^{-1}) = 0, \\ &p_1(\mathbf{x}R^{-1}) = \cdots = p_o(\mathbf{x}R^{-1}) = 0, \\ &\mathbf{x} \cdot Q^{-1} \cdot P'_1 \cdot R^{-1} \cdot {}^t\mathbf{x} = \cdots = \mathbf{x} \cdot Q^{-1} \cdot P'_o \cdot R^{-1} \cdot {}^t\mathbf{x} = 0. \end{aligned} \tag{10}$$

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 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 [1], 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

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

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 and SNOVA 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 (10) 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 (10) 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

$$\min_k q^{v-2o+1} q^k \cdot 3 \binom{n-k-1+D_{n-k,M}}{D_{n-k,M}}^2 \binom{n-k+1}{2}, \tag{12}$$

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

#### 3.1.5 Collision attack

As a cryptographic attack, the collision attack is considered for UOV. Although omitted in Section 2, 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 $\mathbf{m}$. Here, $\mathcal{H}$ is a hash function. 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 [4] for the detail.

### 3.2 Review of the security analysis of SNOVA

In this subsection, we briefly review the attacks used in the SNOVA document [19] in order to analyze the security of SNOVA.

#### 3.2.1 Forgery attack

A forgery attack tries to find a valid signature $(\mathbf{m}, \mathbf{s})$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{m}$ from only the information of the public key. The direct attack and the collision attack explained in 3.1 are applied to SNOVA as forgery attacks. See the document [19] for the details.

#### 3.2.2 Key recovery attack

A key recovery attack for SNOVA tries to find a secret key $T$ or an equivalent key. The key recovery attacks in the document [19] are considered using the information of the core matrices of SNOVA. As stated in Remark 1, the core matrices $G_1, \ldots, G_o$ are originally defined using the $n \times n$ matrices $F_k = (F_{k,ij})_{1 \leq i,j \leq n}$ over $M_l(\mathbb{F}_q)$. Moreover, the core quadratic polynomials $\{g_{k,ij}\}$ generated by $G_1, \ldots, G_o$ can be seen as the public key of UOV with the parameter $(q, l^2v, l^2o)$ as mentioned in 2.2. We call such a UOV instance

**Table 3** The complexity estimation (in $\log_2(\#\text{gates})$) evaluated in the document of SNOVA [19]

| | $(q, v, o, l)$ | 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 |

$\{g_{k,ij}\}$ the core polynomial UOV. The authors of SNOVA considered whether each key recovery attack can be applied to the core matrices $G_1, \ldots, G_o$ and the core polynomial UOV $\{g_{k,ij}\}$, and analyzed their complexity estimations.

(i) KS attack:

The authors of SNOVA considered that since the components of $F_1, \ldots, F_o$ 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 $G_1, \ldots, G_o$. On the other hand, they considered the KS attack for the core polynomial UOV $\{g_{k,ij}\}$. Since the core polynomial UOV is an instance of UOV with parameter $(q, l^2v, l^2o)$, 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 $\{g_{k,ij}\}$. Since the core polynomial UOV is an instance of UOV with parameter $(q, l^2v, l^2o)$, 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 $(q, l^2v, l^2o)$. Its complexity is given by using the estimation in 3.1.4.

(iv) Equivalent attack:

This attack tries to recover $T$ using the relation

$$T^{-1} \cdot G_k \cdot {}^tT^{-1} = F_k \ \ (1 \leq k \leq o),$$

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 [19] 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 $\{g_{k,ij}\}$ with rank $lv$. Then, they estimated the complexity of MinRank problem with $l^2o$ square matrices of size $l^2v$ 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 3 shows the proposed parameters of SNOVA in the additional NIST PQC standardization and the complexity estimations they gave in the document [19]. Here, the following formula is used to express the complexity in gate counts:

$$\#\text{gates} = \#\text{field multiplication} \cdot (2(\log_2 q)^2 + \log_2 q).$$

## 4 Revisiting the security analysis of SNOVA

In this section, we reconsider the security analysis of SNOVA based on the construction we reorganized in Section 2.

### 4.1 Forgery attack

In the document of SNOVA [19], the authors discuss only the direct attack and the collision attack as forgery attacks. As shown in 2.3, the core polynomials $\{g_{k,ij}\}$ have a practical forgery attack. Though there exists no improvement of the forgery attack in 2.3 for $\{p_{k,ij}\}$ at present, it might be necessary to prove that any improvement of the forgery attack in 2.3 cannot be applied to SNOVA.

### 4.2 Key recovery attack

As seen in 3.2, 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 $G_1, \ldots, G_o$ in 2.2 can be identified with a part of the public key of UOV with parameter $(q, lv, lo)$. Thus, we can apply some key recovery attacks of UOV to the core matrices $G_1, \ldots, G_o$. Moreover, since the secret key $T$ in 2.4.3 is in $M_n(\mathcal{A})$, we can make some key recovery attacks more efficient.

(i) KS attack:

The core matrices $G_1, \ldots, G_o$ are public information and have the structure of UOV with parameter $(q, lv, lo)$. Therefore, the KS attack works for $G_1, \ldots, G_o$, and its complexity is $O(q^{l(v-o)})$. This version of the KS attack is efficient compared with the KS attack in 3.2.2 (i).

(ii) Reconciliation attack:

We can also apply the reconciliation attack to the core matrices $G_1, \ldots, G_o$ 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 $G_1, \ldots, G_o$ are not symmetric matrices, 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 $\mathbf{x} \in \mathcal{O} \cdot T^{-1}$. Here we define the oil space $\mathcal{O}$ as follows:

$$\mathcal{O} := \{(\overbrace{0, \ldots, 0}^{lv}, \overbrace{*, \ldots, *}^{lo}) \in \mathbb{F}_q^{ln}\}.$$

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 2.4.2. 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

$$\mathbf{x} \cdot S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j \cdot {}^t\mathbf{x} = 0, \ (0 \leq i, j \leq l-1, 0 \leq k \leq o). \tag{13}$$

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 (13) 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 $G_k$ is not symmetric, two polynomials $\mathbf{x} \cdot S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j \cdot {}^t\mathbf{x}$ and $\mathbf{x} \cdot S_{\mathrm{diag}}^j \cdot G_k \cdot S_{\mathrm{diag}}^i \cdot {}^t\mathbf{x}$ are not necessarily equal. Therefore, the complexity of the reconciliation attack is evaluated by

$$\min_k q^k \cdot 3 \binom{lv - k + D_{lv+1-k,l^2o}}{D_{lv+1-k,l^2o}}^2 \binom{lv + 2 - k}{2}, \tag{14}$$

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

(iii) Intersection attack:

We can apply the intersection attack to the core matrices $G_1, \ldots, G_o$. Let $Q, R$ be two randomly chosen invertible linear combinations of $G_1, \ldots, G_o$. 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

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

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

$$\begin{aligned}
&\mathbf{x} \cdot Q^{-1}S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j {}^tQ^{-1} \cdot {}^t\mathbf{x} = 0,\\
&\mathbf{x} \cdot Q^{-1}S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j {}^tR^{-1} \cdot {}^t\mathbf{x} = 0,\\
&\mathbf{x} \cdot R^{-1}S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j {}^tQ^{-1} \cdot {}^t\mathbf{x} = 0,\\
&\mathbf{x} \cdot R^{-1}S_{\mathrm{diag}}^i \cdot G_k \cdot S_{\mathrm{diag}}^j {}^tR^{-1} \cdot {}^t\mathbf{x} = 0.
\end{aligned} \tag{15}$$

As a result, the intersection attack for the core matrices $G_1, \ldots, G_o$ finds an element $\mathbf{x} \cdot Q^{-1}$ in the twisted oil space $\mathcal{O} \cdot T^{-1}$ by solving the above system, if $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R \neq 0$. Since the system (15) has $2l$ redundant equations, it is reduced to a system of $4l^2o - 2l$ 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 $M := 4l^2o - 2l$ homogeneous quadratic equations in $N := ln - (2lo - lv - 1) = 2lv - lo + 1$ variables. Moreover, our experiments in Table 4 show that this reduced system behaves like a random system of $M$ homogeneous quadratic equations in $N$ 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, $\mathrm{Rank}_d$ and $\#\mathrm{Columns}_d$ mean the rank and the number of columns of the Macaulay matrix at degree $d$ for the reduced system of (15). For the case of $v < 2o$, since the reduced system has only one solution up to a scalar factor, $\mathrm{Rank}_d$ is always less than or equal to $\#\mathrm{Columns}_d - 1$. Actually, the marked number by boldface in the table is equal to $\#\mathrm{Columns}_d - 1$. The reduced system can be solved at degree $d$ where $\mathrm{Rank}_d = \#\mathrm{Columns}_d - 1$ using the XL Wiedemann algorithm. The complexity to solve the reduced system is given by

$$\min_k q^k \cdot 3 \binom{N-k-1+D_{N-k,M}}{D_{N-k,M}}^2 \binom{N-k+1}{2}, \tag{16}$$

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 $\mathcal{O} \cdot T^{-1}Q \cap \mathcal{O} \cdot T^{-1}R$ is non zero is around $1/q^{lv-2lo+1}$. Thus, the system (15) is a system of $M := 4l^2o - 2l$ 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 4 show that the system (15) 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, $\mathrm{Rank}_d = \#\mathrm{Columns}_d$ can happen with high probability.

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

$$\min_k q^{lv-2lo+1} q^k \cdot 3 \binom{ln-k-1+D_{ln-k,M}}{D_{ln-k,M}}^2 \binom{ln-k+1}{2}, \tag{17}$$

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 3.2 (iv) is the full reconciliation attack (see 3.3 in [1]), and contains that of the reconciliation attack in 4.2 (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.

(v) MinRank attack:

For any $k, i, j$, we have $g_{k,ij}(\mathbf{X}) = g_{k,ij}(\mathbf{x}^{(i)}, \mathbf{x}^{(j)})$. In particular, $g_{k,ii}(\mathbf{X}) = g_{k,ii}(\mathbf{x}^{(i)})$. Thus, it is clear that the representation matrix of $g_{k,ii}$ is of rank $lv$ at most. Therefore, the MinRank problem stated in 3.2.2 (v) is a trivial MinRank problem. Namely, it seems that solutions to the MinRank problem

**Table 4** The rank and the number of columns of the Macaulay matrix at each degree $d$ for the system (15), where $q = 16$. For the case of $v < 2o$, we consider the reduced system of $M$ equations in $N$ variables.

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

are not useful for an attacker. It is considered not to need to analyze this MinRank attack.

From the above, we could indeed apply the key recovery attacks to the core matrices $G_1, \ldots, G_o$, and it is efficient compared with the key recovery attacks for the core polynomial UOV $\{g_{k,ij}\}$. 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 $G_1, \ldots, G_o$.

**Table 5** Our complexity estimation (in $\log_2(\#\text{gates})$) evaluated in Section 4

| | $(q, v, o, l)$ | 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.

*Remark 2* By using the fact that $G_1, \ldots, G_o$ are not symmetric, we made the reconciliation attack and the intersection attack more efficient. Thus, if we choose $G_1, \ldots, G_k$ as symmetric matrices, then we might be able to improve the security of SNOVA, and furthermore, make the public key smaller.

## 5 Conclusion

SNOVA was proposed as an efficient variant of UOV having small public key by using the structure of a non-commutative matrix ring, and was submitted to the additional NIST PQC standardization project. In this paper, we reorganized the construction of SNOVA. In particular, we explained its construction without using the structure of the non-commutative matrix ring. By this explanation, we showed that the key recovery attacks can be applied to the core part of SNOVA. As a result, by such attacks, some parameters of SNOVA submitted in the additional NIST PQC standardization do not satisfy the claimed security levels.

**Acknowledgements** This work was partially supported by JSPS KAKENHI Grant Number JP19K20266, Japan.

## References


1. Beullens, W.: 'Improved Cryptanalysis of UOV and Rainbow', EUROCRYPT 2021, LNCS 12696, pp. 348–373, Springer
2. Beullens, W.: 'MAYO: Practical Post-quantum Signatures from Oil-and-Vinegar Maps', SAC 2021, LNCS 13203, pp. 355–376, Springer
3. Beullens, W., Campos, F., Celi, S., Hess, B., Kannwischer, M.: 'MAYO', Specification document of NIST PQC Standardization of Additional Digital Signature Scheme (2023)
4. 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)
5. 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
6. Faugère, J.C.: 'A new efficient algorithm for computing Gröbner bases (F4)', Journal of Pure and Applied Algebra, 1999, Vol.139, pp. 61–88
7. Faugère, J.C.: 'A new efficient algorithm for computing Gröbner Bases without reduction to zero (F5)', ISSAC 2002, pp. 75–83
8. 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)
9. 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
10. Furue, H., Nakamura, S., Takagi, T.: 'Improving Thomae-Wolf algorithm for solving underde- termined multivariate quadratic polynomial problem', PQCrypto2021, LNCS 12841, pp.65–78.
11. Hashimoto, Y., 'An improvement of algorithms to solve under-defined systems of multivariate quadratic equations', JSIAM Letters, Vol.15 (2023), pp.53–56
12. Kipnis, A., Patarin, L., Goubin, L.: 'Unbalanced Oil and Vinegar Schemes', EUROCRYPT 1999, LNCS 1592, pp. 206–222, Springer
13. Kipnis A., Shamir A.: 'Cryptanalysis of the oil and vinegar signature scheme', CRYPTO 98, LNCS 1462, pp. 257–266. Springer
14. National Institute of Standards and Technology: 'Post-Quantum Cryptography Standardization', ⟨https://csrc.nist.gov/projects/post-quantum-cryptography⟩
15. 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⟩
16. 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)
17. 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)
18. Wang, L.C., Tseng, P.E., Kuan, Y.L., Chou, C.Y.: 'A Simple Noncommutative UOV Scheme', IACR Cryptology ePrint Archive, 2022/1742
19. 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)
20. Thomae, E., Wolf, C.: 'Solving underdetermined systems of multivariate quadratic equations revisited', PKC2012, LNCS 7293, pp.156–171.

21. Yang, B.Y., Chen, J.M.: 'All in the XL family: Theory and practice', ICISC 2004, LNCS 3506, pp.67-86, Springer