Cryptanalysis of the SNOVA signature scheme

Peigen Li *[1,2] and Jintai Ding**[1,2]

[1]Beijing Institute of Mathematical Sciences and Applications, Beijing, China
[2]Yau Mathematical Sciences Center, Tsinghua University, Beijing, China

Abstract. SNOVA is a variant of a UOV-type signature scheme over a noncommutative ring. In this article, we demonstrate that certain parameters provided by authors in SNOVA fail to meet the NIST security level, and the complexities are lower than those claimed by SNOVA.

Keywords: multivariate public key cryptography· UOV · SNOVA

1 Introduction

Public key cryptosystems currently used such as RSA and ECC can be broken by a quantum computer executing Shor's algorithm [21] in polynomial time.Therefore, cryptosystems resistant to quantum computers are gaining increasing importance. There are many post-quantum cryptosystems based on different theory such as lattice theory, algebraic geometry, coding theory, and the isogeny theory of elliptic curves.

In 2022, the U.S. National Institute for Standards and Technology (NIST) on post-quantum cryptography (PQC) posted a call for additional digital signature proposals to be considered in the PQC standardization process. In 2023, 50 different signature schemes were submitted, including code-based signatures, isogeny signatures, lattice-based signatures, multivariate signatures, and others.

A multivariate public key cryptosystem (MPKC) has a set of quadratic polynomials over a finite field as its public key. Its security based on the difficulty of solving a system of multivariate quadratic polynomial equations over a finite field (MQ problem). Garey and Johnson proved [15] that MQ problem is NP-complete in general.

The oil and vinegar and later derived unbalanced oil and vinegar signature schemes(UOV) [19,18], are well-known signature schemes known for their efficiency and short signature. The UOV scheme has withstood attacks for more than 20 years and is still regarded as a secure signature scheme. Notably,, the Rainbow signature scheme proposed by Ding and Schmidt [8], a multilayer UOV variant, was selected as a third-round finalist in the NIST PQC project. However, both UOV and Rainbow have public keys much larger than other PQC candidates.

* Corresponding author, lpg22@bimsa.cn
** Corresponding author, jintai.ding@gmail.com

For multivariate signatures, the size of public key mainly depends on the number of variables, the number of equations, and the size of the finite field. Depending on different influencing factors, there are different research approaches to develop UOV variants. The first approach does not change the original design of UOV scheme, but only changes the way of key generation. The compression technique [20] developed by Petzoldt et al, which is based on the fact that a part of public key can be arbitrarily chosen before generating the secret key. This implies that a part of public key can be generated using a seed of pseudo-random number generator and the size of public key mainly depends on the dimension of the oil space, the number of equations and the size of the finite field. Note that this technique can be applied to various UOV variants. The second approach is to use polynomials defined over small field as the public key, while the signature and message spaces are defined over the extension field, see LUOV in [4]. But several of its parameters were broken by Ding et al. [10]. The third approach is to reduce the dimension of oil space in the **KeyGen** step. In the **Sign** step, they use different methods to induce a new oil space from the original oil space such that the dimension of the new oil space is greater or equal to the number of equations, for example, QR-UOV [13], MAYO [3], SNOVA [24]. The authors of QR-UOV [13] construct oil space over the extension field then mapping it into the vector space over base field by trace function or tensor product, see also [17]. The signature and message spaces are defined over the base field. BAC-UOV [22] is similar with QR-UOV but it is broken by Furue et al. [14]. For MAYO [3], they increasing the dimension of oil space by whipping up the oil and vinegar map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ into a larger map $\mathcal{P}^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$. The authors of SNOVA [24] choose the noncommutative matrix $\mathcal{R}$ of $l \times l$ matrices over $\mathbb{F}_q$ to be the coefficient ring and they construct a UOV-like scheme with coefficients in $\mathcal{R}$. Actually, we can construct oil space in the space $\mathbb{F}_q^{nl}$ and make tensor product with $\mathbb{F}_q^l$ to map such oil space into a new oil space of $\mathcal{R}^n$.

Our contributions In this paper, our focus is on the multivariate signature SNOVA scheme [24]. We observe that an SNOVA(v, o, q, l) scheme over $\mathcal{R}$ can be viewed as a UOV(lv, lo, q) scheme with l^2o equations over $\mathbb{F}_q$, rather than a UOV(l^2v, l^2o, q) scheme over $\mathbb{F}_q$ as claimed by the authors in [24]. Consequently, we demonstrate that some parameters provided by the authors in SNOVA can't meet the NIST security level, and the complexities are lower than they claimed. Additionally, the coefficient matrices of these l^2o equations induced by the SNOVA(v, o, q, l) scheme exhibit special forms and are not randomly generated. In most cases, we observe that the l^2o equations induced by SNOVA have more solutions than l^2o random equations from a UOV scheme. Therefore, the actual complexity of SNOVA may be lower than theoretically estimated. Applying the same method, we find that NOVA [23] has lower complexities claimed by the authors in their article, see Table 1.

2 SNOVA scheme

2.1 Description of SNOVA scheme

In [24], the authors introduce a UOV-type signatures over a noncommutative ring, which called SNOVA.

Let v, o, l be positive integers with $v > o$ and $\mathbb{F}_q$ a finite field with q elements. Let $\mathcal{R}$ be the ring of $l \times l$ matrices over the finite field $\mathbb{F}_q$. Set $n = v + o$ and $m = o$, $\mathbf{x} = (x_1, \cdots, x_n)^t, \mathbf{u} = (u_1, \cdots, u_n)^t \in \mathcal{R}^n$, $[P], [F]$ denote some $n \times n$ matrices whose entries are elements of $\mathcal{R}$. For each $Q \in \mathcal{R}$, $[\Lambda_Q]$ denote the $n \times n$ matrix in $\mathbf{M}_{n\times n}(\mathcal{R})$ whose diagonal elements are Q.

The space $\mathbb{F}_q[s]$. We first randomly choose an $l \times l$ symmetric matrix s such that the characteristic polynomial of s is irreducible. Set

$$\mathbb{F}_q[s] = \{a_0 + \cdots + a_{l-1}s^{l-1} : \ a_0, \cdots, a_{l-1} \in \mathbb{F}_q\}.$$

Note that $\dim_{\mathbb{F}_q} \mathbb{F}_q[s] = l$ and each nonzero element in $\mathbb{F}_q[s]$ is invertible and symmetric.

Central map. The central map of SNOVA scheme is $F = [F_1, \cdots, F_m] : \mathcal{R}^n \to \mathcal{R}^m$. Set $\Omega = \{(j,k) : \ 1 \le j, k \le n\} - \{(j,k) : \ m+1 \le j, k \le n\}$. For each i, F_i is the form of

$$\begin{aligned} F_i(x_1, \cdots, x_n) &= \sum_{\alpha=1}^{l^2} A_\alpha \cdot \Big(\sum_{(j,k)\in\Omega} x_j^t (Q_{\alpha 1} F_{i,jk} Q_{\alpha 2}) x_k \Big) \cdot B_\alpha \\ &= \sum_{\alpha=1}^{l^2} A_\alpha \cdot \mathbf{x}^t ([\Lambda_{Q_{\alpha 1}}][F_i][\Lambda_{Q_{\alpha 2}}])\mathbf{x} \cdot B_\alpha \end{aligned}$$

where $A_\alpha, B_\alpha, F_{i,jk}$ are the elements chosen randomly from $\mathcal{R}$ and $Q_{\alpha 1}, Q_{\alpha 2}$ are elements chosen randomly from $\mathbb{F}_q[s] - \{0\}$. Indeed, $[F_i] = (F_{i,jk})$ is the form of

$$[F_i] = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & 0 \end{pmatrix} \in \mathbf{M}_{n\times n}(\mathcal{R}).$$

Public key and private key. Let $T : \mathcal{R}^n \to \mathcal{R}^n$ be the map corresponding to the matrix

$$[T] = \begin{pmatrix} I_{v\times v} & T_{v\times o} \\ 0 & I_{o\times o} \end{pmatrix},$$

where $T_{v\times o}$ is a $v \times o$ matrix whose entries chosen randomly from $\mathbb{F}_q[s]$. $I_{v\times v}$ and $I_{o\times o}$ are the diagonal matrices with all entires being the identity matrix in $\mathcal{R}$.

Let $P = F \circ T$. Set $\mathbf{x} = [T] \circ \mathbf{u}$ and $P_i = F_i \circ T$. We get

$$P_i(\mathbf{u}) = \sum_{\alpha=1}^{l^2} \sum_{d_j=1}^{n} \sum_{d_k=1}^{n} A_\alpha \cdot u_{d_j}^t (Q_{\alpha 1} P_{i,d_j d_k} Q_{\alpha 2}) u_{d_k} \cdot B_\alpha$$
$$= \sum_{\alpha=1}^{l^2} A_\alpha \cdot \mathbf{x}^t ([\Lambda_{Q_{\alpha 1}}][P_i][\Lambda_{Q_{\alpha 2}}])\mathbf{x} \cdot B_\alpha$$

where $P_{i,d_j d_k} = \sum_{(j,k)\in\Omega} t_{j,d_j} \cdot F_{i,jk} \cdot t_{k,d_k}$. Note that

$$[P_i] = \begin{pmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{pmatrix} = [T]^t [F_i][T],\ i = 1, \cdots, m.$$

The public key of SNOVA consists of the map $P : \mathcal{R}^n \to \mathcal{R}^m$, i.e., the corresponding matrices $[P_i]$ for $i = 1, \cdots, m$, and matrices $A_\alpha, B_\alpha, Q_{\alpha k}$ for $\alpha = 1, \cdots, l^2$ and $k = 1, 2$. The private key of SNOVA is (F, T), i.e., the matrix $[T]$ and the matrices $[F_i]$ for $i = 1, \cdots, m$.

Signature. Let $Message$ be the message to be signed. Set $Hash(Message) = \mathbf{y} = (y_1, \cdots, y_m)^t \in \mathcal{R}^m$. We first choose random values $a_1, \cdots, a_v \in \mathcal{R}$ as the vinegar variables. Then, we can obtain a solution $(a_{v+1}, \cdots, a_n)$ for the equation

$$F(a_1, \cdots, a_v, x_{v+1}, \cdots, x_n) = \mathbf{y}.$$

If there is no solution to the equation, we choose new random values $a'_1, \cdots, a'_v \in \mathcal{R}$ and repeat the procedure. Set $\mathbf{x} = (a_1, \cdots, a_v, a_{v+1}, \cdots, a_n)^t$. Secondly, the signature is $\mathbf{sign} = T^{-1}(\mathbf{x})$.

Verification. Let $\mathbf{sign} = (s_1, \cdots, s_n)$ be the signature to be verified. If $Hash(Message) = P(\mathbf{sign})$, then the signature is accepted, otherwise rejected.

2.2 Structure of SNOVA

The authors assert in [24] that an SNOVA(v, o, q, l) scheme over $\mathcal{R}$ can be considered as a UOV$(l^2 v, l^2 o, q)$ scheme over $\mathbb{F}_q$. However, we argue that it should only be regarded as a UOV(lv, lo, q) scheme with $l^2 o$ equations over $\mathbb{F}_q$.

In fact, all the matrices $[F_i]$, $[T]$, and $[P_i]$ in the SNOVA scheme can be viewed as $ln \times ln$ matrices in $\mathbf{M}_{ln\times ln}(\mathbb{F}_q)$. Based on the design of the central map F, there exists an oil space of F over $\mathbb{F}_q$ with a dimension of ol. Set

$$\mathcal{O}_1 = \left\{ (0, \cdots, 0, a_{lv+1}, \cdots, a_{ln}) \in \mathbb{F}_q^{ln} :\ a_i \in \mathbb{F}_q \right\} \text{ and } \mathcal{O} = [T]^{-1}(\mathcal{O}_1) \subset \mathbb{F}_q^{ln}.$$

Note that $\dim_{\mathbb{F}_q} \mathcal{O} = lo$ and for any $\mathbf{u}, \mathbf{v} \in \mathcal{O}$, $0 \le j, k \le l-1$,we have

$$\mathbf{u}^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}] \right) \cdot \mathbf{v} = 0 \in \mathbb{F}_q \text{ for } i = 1, \cdots, m. \tag{2.1}$$

That is, $\Big([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\Big)\mathcal{O} \subset \mathcal{O}^{\perp}$ for $i = 1, \cdots, m$ and $0 \leq j, k \leq l-1$. Moreover, equation (2.1) implies that the subspace $\mathcal{O}$ is stable under the action of $[\Lambda_s]$. Furthermore, if we can find a subspace $\mathcal{O}' \subset \mathbb{F}_q^{ln}$ with dimension ol, and any elements $\mathbf{u}, \mathbf{v} \in \mathcal{O}'$ satisfy equation (2.1), then for any

$$\mathbf{x} \in \mathcal{O}' \otimes \mathbb{F}_q^l = \{\mathbf{u}^t \otimes e \in \mathcal{R}^n : \ \mathbf{u} \in \mathcal{O}', e \in \mathbb{F}_q^l\},$$

we have

$$P(\mathbf{x}) = 0 \in \mathcal{R}^m .$$

Given a target $\mathbf{t} \in \mathcal{R}^m$, we can utilize the subspace $\mathcal{O}' \otimes \mathbb{F}_q^l$ of $\mathcal{R}^n$ to find $\mathbf{x} \in \mathcal{R}^n$ such that $P(\mathbf{x}) = \mathbf{t}$.

3 Security Analysis

3.1 Complexity

Given a homogeneous multivariate quadratic map $P : \mathbb{F}_q^N \to \mathbb{F}_q^M$, we use $MQ(N, M, q)$ to denote the complexity of finding a non-trivial solution $\mathbf{u}$ satisfying $P(\mathbf{u}) = 0$ if such solution exists. Several algorithms for algebraically solving the quadratic system by computing Gröbner basis [5] include F_4 [11], F_5 [12] and XL [7] .

In this paper, we estimate the complexity of solving M homogeneous quadratic equations in N variables [6] as

$$3 \cdot \binom{N-1+d_{reg}}{d_{reg}}^2 \cdot \binom{N+1}{2}$$

field multiplications, where d_{reg} is equal to the degree of the first non-positive term in the series generated by

$$\frac{(1-t^2)^M}{(1-t)^N}.$$

The hybrid approach [1], which randomly guesses k ($k = 0, \cdots, N$) variables before computing a Gröbner basis. Hence the complexities are

$$\min_k q^k \cdot MQ(N-k+1, M, q)$$

field multiplications for the classical case and

$$\min_k q^{k/2} \cdot MQ(N-k+1, M, q)$$

field multiplications by using Grover's algorithm [16].

An underdetermined system can be reduced to an overdetermined system, then apply hybrid approach. There are many approaches listed in [24].

The number of gates required for an attack can be computed by

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

3.2 K-S attack

In UOV scheme, the K-S attack [18] obtains the subspace $T^{-1}(\mathcal{O}_1)$ of $\mathbb{F}_q^n$, where $\mathcal{O}_1$ is the oil subspace defined as

$$\mathcal{O}_1 := \{(0, \cdots, 0, \alpha_1, \cdots, \alpha_m)^t : \ \alpha_i \in \mathbb{F}_q\}.$$

The subspace $T^{-1}(\mathcal{O}_1)$ can induce an equivalent key. To obtain $T^{-1}(\mathcal{O}_1)$, the K-S attack chooses two invertible matrices W_1, W_2 from the set of linear combinations of the public keys $P_1, \cdots, P_m$. Then, it probabilistically recovers a part of the subspace $T^{-1}(\mathcal{O}_1)$. The complexities of K-S attack and quantum K-S attack are estimated by

$$\text{Comp}_{\text{K-S;classical}}\text{UOV} = q^{v-o-1} \cdot m^4$$

field multiplications and

$$\text{Comp}_{\text{K-S;quantum}}\text{UOV} = q^{\frac{v-o-1}{2}} \cdot m^4$$

field multiplications, respectively.

In the SNOVA scheme, we have claimed that SNOVA(v, o, q, l) scheme over $\mathcal{R}$ can be regarded as a UOV(lv, lo, q) scheme. In such case, we have

$$\text{Comp}_{\text{K-S;classical}}\text{SNOVA} = q^{lv-lo-1} \cdot (lo)^4$$

field multiplications and

$$\text{Comp}_{\text{K-S;quantum}}\text{SNOVA} = q^{\frac{lv-lo-1}{2}} \cdot (lo)^4$$

field multiplications, respectively.

3.3 Reconciliation Attack

The reconciliation attack [9] for UOV is similar to the UOV attack, trying to find $\mathbf{u} \in T^{-1}(\mathcal{O}_1)$ such that $P(\mathbf{u}) = 0$ and hence basis of $T^{-1}(\mathcal{O}_1)$ can be recovered. For SNOVA scheme, the reconciliation attack can be decomposed into a series of steps. Firstly, we may find an element $\mathbf{u} = (u_1, \cdots, u_{lv}, 0, \cdots, 0, 1)^t \in \mathbb{F}_q^{ln}$ such that

$$\mathbf{u}^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\right) \cdot \mathbf{u} = 0 \in \mathbb{F}_q \tag{3.1}$$

for $i = 1, \cdots, m$ and $0 \leq j, k \leq l-1$. There are $o \cdot l^2$ equations in (3.1). After finding such $\mathbf{u}$, we know that $[\Lambda_s]\mathbf{u}, \cdots, [\Lambda_{s^{l-1}}]\mathbf{u}$ are also solutions of (3.1) which are linear independent with $\mathbf{u}$. Secondly, using the equations (2.1), we get $2 \cdot o \cdot l^2$ linear equations for the other elements of $\mathcal{O}$. Hence the complexity of reconciliation attack is mainly centered on solving the equations (3.1).

Therefore, the complexities are

$$\text{Comp}_{\text{Reconciliation;classical}}\text{SNOVA} = \min_k q^k MQ(vl + 1 - k, o \cdot l^2, q)$$

field multiplications and

$$\mathrm{Comp}_{\mathrm{Reconciliation;quantum}}\mathrm{SNOVA} = \min_k q^{k/2} MQ(vl+1-k, o\cdot l^2, q)$$

field multiplications, respectively.

We observe that the equation (3.1) is easier to find solutions in the extension field $\mathbb{F}_{q^l}$. Because the characteristic polynomial of s is irreducible, all the eigenvalues of s lie in $\mathbb{F}_{q^l}$. Let $\lambda \in \mathbb{F}_{q^l}$ be an eigenvalue of s and $\xi \in (\mathbb{F}_{q^l})^l$ an eigenvector corresponding to λ. Let τ be the Frobenius element $z \mapsto z^q$ in the Galois group $\mathrm{Gal}(\mathbb{F}_{q^l}/\mathbb{F}_q)$ which can be easily induced an operator on vector space over $\mathbb{F}_{q^l}$. For $j = 0, \cdots, l-1$, we have

$$s\tau^j(\xi) = \tau^j(\lambda)\tau^j(\xi).$$

Thus for each j, $\tau^j(\xi)$ is an eigenvector corresponding to the eigenvalue $\tau^j(\lambda)$. In particular, $\{\xi, \tau^1(\xi), \cdots, \tau^{l-1}(\xi)\}$ are linear independent and so

$$\mathrm{Tr}(\xi) := \sum_{j=0}^{l-1} \tau^j(\xi) \in \mathbb{F}_q^l - \{0\}.$$

According to the construction of $\mathcal{O}$ in the subsection 2.2, we have

$$\mathcal{O} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^l} = [T]^{-1}\Big(\Big\{ (0, \cdots, 0, a_{lv+1}, \cdots, a_{ln}) \in \mathbb{F}_{q^l}^{ln} : \ a_i \in \mathbb{F}_{q^l} \Big\} \Big).$$

Hence, there is an element $\mathbf{u} = (\lambda_1\xi^t, \cdots, \lambda_v\xi^t, 0, \cdots, 0, \xi^t)^t \in \mathcal{O} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^l}$ satisfying the equation (3.1). Then the equation (3.1) becomes

$$\mathbf{u}^t \cdot \Big([\Lambda_{s^j}][P_i][\Lambda_{s^k}] \Big) \cdot \mathbf{u} = \lambda^{j+k} \mathbf{u}^t \cdot [P_i] \cdot \mathbf{u} = 0 \in \mathbb{F}_{q^l}\,.$$

That is

$$\mathbf{u}^t \cdot [P_i] \cdot \mathbf{u} = 0 \in \mathbb{F}_{q^l}\,. \tag{3.2}$$

for $i = 1, \cdots, m$. There are only m quadratic equations and v variables over $\mathbb{F}_{q^l}$. Indeed, $\mathbf{u} \in \mathcal{O} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^l}$ gives us more equations:

$$\mathbf{u}^t \cdot [P_i] \cdot \tau^j(\mathbf{u}) = 0 \in \mathbb{F}_{q^l} \tag{3.3}$$

for $i = 1, \cdots, m$ and $j = 0, \cdots, l-1$. In such case, set

$$\mathbf{v} := \mathrm{Tr}(\mathbf{u}) = \mathbf{u} + \tau(\mathbf{u}) + \cdots + \tau^{l-1}(\mathbf{u}) \in \mathbb{F}_q^{ln} - \{0\}.$$

We have

$$\begin{aligned}
\mathbf{v}^t \cdot \Big([\Lambda_{s^j}][P_i][\Lambda_{s^k}] \Big) \cdot \mathbf{v} &= \sum_{0 \le a,b \le l-1} \tau^a(\mathbf{u}^t) \cdot \Big([\Lambda_{s^j}][P_i][\Lambda_{s^k}] \Big) \cdot \tau^b(\mathbf{u}) \\
&= \sum_{0 \le a,b \le l-1} \tau^a(\lambda^j)\tau^b(\lambda^k)\tau^a\Big(\mathbf{u}^t \cdot [P_i] \cdot \tau^{b-a}(\mathbf{u}) \Big) \\
&= 0.
\end{aligned}$$

Conversely, each solution of (3.1) over $\mathbb{F}_q$ induces a solution of (3.2) over $\mathbb{F}_{q^l}$ whose form is $\mathbf{u} = (\lambda_1\xi^t, \cdots, \lambda_v\xi^t, 0, \cdots, 0, \xi^t)^t \in (\mathbb{F}_{q^l})^{ln}$. Indeed, suppose

$$\mathbf{u}_0 = (u_1, \cdots, u_{lv}, 0, \cdots, 0, 1)^t \in \mathbb{F}_q^{ln}$$

is a solution of (3.1). Then $[\Lambda_s]\mathbf{u}_0, \cdots, [\Lambda_{s^{l-1}}]\mathbf{u}_0$ are also solutions of (3.1) which are linear independent with $\mathbf{u}_0$. Hence we can find a solution

$$\mathbf{u} = (\lambda_1\xi^t, \cdots, \lambda_v\xi^t, 0, \cdots, 0, \xi^t)^t$$

in the subspace spanned by $\mathbf{u}_0, [\Lambda_s]\mathbf{u}_0, \cdots, [\Lambda_{s^{l-1}}]\mathbf{u}_0$ over $\mathbb{F}_{q^l}$. Moreover, the above $\mathbf{u}$ also satisfies (3.3).

3.4 Intersection Attack

Beullens proposed a new attack against UOV called the intersection attack in [2]. The intersection attack attempts to obtain an equivalent key by recovering the subspace $\mathcal{O}$. Let M_1, M_2 be two invertible matrices in the set of linear combinations of $\{[\Lambda_{s^j}][P_i][\Lambda_{s^k}]\}_{1\le i\le m, 0\le j,k\le l-1}$. By (2.1), we know that $M_1\mathcal{O}$ and $M_2\mathcal{O}$ are both subspaces of $\mathcal{O}^\perp$. Although $M_1\mathcal{O} \neq M_2\mathcal{O}$, we still have

$$\begin{aligned}\dim(M_1\mathcal{O} \cap M_2\mathcal{O}) &= \dim(M_1\mathcal{O}) + \dim(M_2\mathcal{O}) - \dim(M_1\mathcal{O} + M_2\mathcal{O}) \\ &\ge 2lo - \dim(\mathcal{O}^\perp) \\ &= 2lo - lv.\end{aligned}$$

In the case of 2lo > lv. Let $\mathbf{x}$ be an element in the intersection $M_1\mathcal{O} \cap M_2\mathcal{O}$, then both $M_1^{-1}\mathbf{x}$ and $M_2^{-1}\mathbf{x}$ are in $\mathcal{O}$. Therefore, $\mathbf{x}$ is a solution to the following system of quadratic equations

$$\begin{cases} (M_1^{-1}\mathbf{x})^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\right) \cdot (M_1^{-1}\mathbf{x}) = 0 \\ (M_2^{-1}\mathbf{x})^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\right) \cdot (M_2^{-1}\mathbf{x}) = 0 \\ (M_1^{-1}\mathbf{x})^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\right) \cdot (M_2^{-1}\mathbf{x}) = 0 \\ (M_2^{-1}\mathbf{x})^t \cdot \left([\Lambda_{s^j}][P_i][\Lambda_{s^k}]\right) \cdot (M_1^{-1}\mathbf{x}) = 0 \end{cases} \tag{3.4}$$

Note that the third and the fourth equations in (3.4) are same when $[P_i]$ is symmetric. Since there is a $2lo - lv$ dimensional subspace of solutions, we can impose $2lo - lv$ affine constraints on $\mathbf{x}$. Then the attack is reduced to find a solution to the above system of $4l^2o$ quadratic equations in $ln - (2lo - lv) = 2lv - lo$ variables. Therefore, the complexity is

$$\mathrm{Comp}_{\mathrm{Intersection}} = MQ(2lv - lo + 1, 4l^2o, q).$$

In the case of 2lo ≤ lv. The intersection $M_1\mathcal{O} \cap M_2\mathcal{O}$ may have no nontrivial vector. If $M_1\mathcal{O}$ and $M_2\mathcal{O}$ are uniformly random subspaces of $\mathcal{O}^\perp$, then the

probability that they have non-trivial intersection is approximately $q^{-lv+2lo-1}$. Therefore, the attack becomes a probabilistic algorithm for solving the system (3.4) with a probability of approximately $q^{-lv+2lo-1}$. In such case, the complexity is

$$\text{Comp}_{\text{Intersection}} = q^{lv-2lo+1} MQ(ln, 4l^2o, q).$$

Table 1. Table of classical complexity in $\log_2$(#gates)

SL	(v, o, q, l)	K-S	Reconciliation	Intersection
I	(28,17,16,2)	**109**/181	**117**/192	**77**/275
	(25,8,16,3)	223/617	174/231	680/819
	(24,5,16,4)	322/1221	191/286	1015/1439
III	(43,25,16,2)	**167**/293	**178**/279	276/439
	(49,11,16,3)	477/1373	231/530	1919/1631
	(37,8,16,4)	485/1861	292/424	1508/2192
V	(61,33,16,2)	**249**/453	**262**/386	395/727
	(66,15,16,3)	635/1841	307/707	2547/2178
	(60,10,16,4)	822/3205	360/812	2831/3602

Table 1 presents the classical complexity of respective attacks against the parameters submitted in [24]. In each pair of complexities, the left one denotes the complexity in classical gates using the analysis results in this article, and the right one denotes the complexity in classical gate given by [24]. Complexities that do not meet the security level of the NIST PQC project are highlighted in bold fonts. Furthermore, Table 1 also indicates that the complexity of SNOVA is generally lower than what the authors claimed in [24].

Acknowledgments. This work is supported by National Key R&D Program of China (No. 2021YFB3100100).

References

1. L. Bettale, J.-C Faugere, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009.
2. W. Beullens. Improved cryptanalysis of UOV and Rainbow. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 348–373. Springer, 2021.
3. W. Beullens. MAYO: practical post-quantum signatures from oil-and-vinegar maps. In *International Conference on Selected Areas in Cryptography*, pages 355–376. Springer, 2021.
4. W. Beullens and B. Preneel. Field lifting for smaller UOV public keys. In *Progress in Cryptology–INDOCRYPT 2017: 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings 18*, pages 227–246. Springer, 2017.

5. B. Buchberger. Ein algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *Ph. D. Thesis, Math. Inst., University of Innsbruck*, 1965.
6. C. Cheng, T. Chou, R. Niederhagen, and Bo-Yin Yang. Solving quadratic equations with XL on parallel architectures. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 356–373. Springer, 2012.
7. N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.
8. J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International conference on applied cryptography and network security*, pages 164–175. Springer, 2005.
9. J. Ding, B. Yang, C.-O Chen, M. Chen, and C. Cheng. New differential-algebraic attacks and reparametrization of rainbow. In *Applied Cryptography and Network Security: 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings 6*, pages 242–257. Springer, 2008.
10. J. Ding, Z. Zhang, J. Deaton, K. Schmidt, and F. Vishakha. New attacks on lifted unbalanced oil vinegar. In *the 2nd NIST PQC Standardization Conference*, 2019.
11. J.-C Faugere. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.
12. J.-C Faugere. A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, pages 75–83, 2002.
13. H. Furue, Y. Ikematsu, Y. Kiyomura, and T. Takagi. A new variant of unbalanced Oil and Vinegar using quotient ring: QR-UOV. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27*, pages 187–217. Springer, 2021.
14. H. Furue, K. Kinjo, Y. Ikematsu, Y. Wang, and T. Takagi. A structural attack on block-anti-circulant UOV at SAC 2019. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11*, pages 323–339. Springer, 2020.
15. M.-R. Garey and D.-S Johnson. Computers and intractability. *A Guide to the*, 1979.
16. L.-K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
17. Y. Hashimoto. An elementary construction of QR-UOV. *Cryptology ePrint Archive*, 2022.
18. A. Kipnis and A. Shamir. Cryptanalysis of the oil and vinegar signature scheme. In *Annual international cryptology conference*, pages 257–266. Springer, 1998.
19. J. Patarin. The oil and vinegar algorithm for signatures. In *Dagstuhl Workshop on Cryptography*, 1997.
20. A. Petzoldt, S. Bulygin, and J.-A Buchmann. Cyclicrainbow–a multivariate signature scheme with a partially cyclic public key. In *Progress in Cryptology-INDOCRYPT 2010: 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings 11*, pages 33–48. Springer, 2010.
21. P.-W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

22. A. Szepieniec and B. Preneel. Block-anti-circulant unbalanced oil and vinegar. In *Selected Areas in Cryptography–SAC 2019: 26th International Conference, Waterloo, ON, Canada, August 12–16, 2019, Revised Selected Papers 26*, pages 574–588. Springer, 2020.
23. L.C. Wang, P.E. Tseng, Y.L. Kuan, and C.Y. Chou. NOVA, a noncommutative-ring based unbalanced oil and vinegar signature scheme with key-randomness alignment. *Cryptology ePrint Archive*, 2022.
24. L.C. Wang, P.E. Tseng, Y.L. Kuan, and C.Y. Chou. A simple noncommutative UOV scheme. *Cryptology ePrint Archive*, 2022.