Extending the Applicability of Algebraic Key Recovery Attacks on the UOV Signature Scheme

Yasuhiko Ikematsu[1] and Hiroki Furue[2]

[1] Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan
ikematsu@imi.kyushu-u.ac.jp
[2] NTT Social Informatics Laboratories, Tokyo, Japan
hiroki.furue@ntt.com

Abstract. The Unbalanced Oil and Vinegar (UOV) scheme was proposed by Kipnis et al. in 1999 as a multivariate signature scheme. Owing to its small signature size and its resistance to various attacks over more than two decades, UOV has become one of the leading candidates in multivariate public key cryptography. In 2025, Ran proposed a novel algebraic key recovery attack exploiting the algebraic structure of UOV, which reduced the security of several parameter sets of UOV and its variants submitted to the second round of the NIST PQC standardization process for additional signatures. This attack was improved by Jin et al., and Furue and Ikematsu, forming a line of attacks that has significantly advanced the cryptanalysis of UOV. However, Ran's attack is applicable only when $v < 2m$, where v denotes the number of vinegar variables and m the number of public polynomials. In fact, when $v \geq 2m$, an additional kernel element of the ideal generated by the public polynomials appears, preventing the attack from recovering the oil subspace. A similar issue arises in the improvements by Jin et al., and Furue and Ikematsu. In this paper, we propose a method that overcomes this issue, extending the applicability of this line of attacks to the case where such an additional kernel element appears. Applying our method to SNOVA via the lifting technique of Nakamura et al., we show that the claimed security levels of some parameter sets of SNOVA in the second round of NIST PQC standardization process for additional signatures are reduced. In particular, for the parameter set $(v, o, q, l) = (37, 17, 16, 2)$ of NIST security level I, although Ran's attack is not applicable, our method reduces the estimated security to 2^{103} gate operations, which matches the complexity of the attack by Bros et al. in 2026.

Keywords: post-quantum cryptography · multivariate public key cryptography · unbalanced oil and vinegar (UOV).

1 Introduction

It is well known that widely used public key cryptosystems such as RSA and ECC can be broken by large-scale quantum computers using Shor's algorithm [15]. This has motivated intensive research on post-quantum cryptography (PQC),

which aims to develop cryptosystems that remain secure against attacks by quantum computers.

The Unbalanced Oil and Vinegar (UOV) scheme [9] was proposed by Kipnis et al. in 1999 as a multivariate signature scheme. Owing to its small signature size and its resistance to various attacks over more than two decades, UOV has attracted considerable attention in the NIST PQC standardization process for additional signatures [12]. On the other hand, one drawback of UOV is its large public key. To address this issue, several variants with compact public keys, including MAYO [2], QR-UOV [7], and SNOVA [16], have been proposed. These four schemes were all selected as third round candidates in the NIST PQC standardization process for additional signatures [13].

Recently, Ran [14] proposed a novel algebraic key recovery attack exploiting the algebraic structure of UOV. The attack truncates a Macaulay matrix in the XL algorithm using the existence of the oil subspace, resulting in a more efficient key recovery attack. Consequently, the security of several second round parameter sets of UOV and MAYO was reduced. Ran's attack was originally proposed only for characteristic 2. It was subsequently generalized by Jin et al. [8] to arbitrary characteristic p, and further extended by Furue and Ikematsu [6] to the more general setting of p^ℓ-truncated polynomial rings.

One limitation of this line of attacks is that they are not applicable when an additional kernel element arises from the public key. Let I be the ideal generated by the public key $p_1, \ldots, p_m$ of UOV in the truncated polynomial ring $R^{(2)} = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle$, where q is a power of 2 in the case of Ran's attack. Then, Ran's attack aims to find the degree v kernel element M associated with the oil subspace such that $M \cdot p_i = 0 \in R^{(2)}$ for every i. Here v is the number of vinegar variables. However, Ran's attack fails when $v \geq 2m$. Indeed, for the degree $2m(\leq v)$ polynomial $P := p_1 \cdots p_m$, we have $P \cdot p_i = 0$ for every i. Then, this additional kernel element P prevents us from finding the kernel element M, obstructing the recovery of the oil subspace. Similar limitations also appear in the subsequent attacks of Jin et al. [8] and Furue and Ikematsu [6].

In this paper, we propose a new method for recovering the oil subspace even in the presence of such an additional kernel element P. Our method is based on a structural analysis of the kernel space, which enables us to reconstruct vectors in the oil subspace from a nonzero kernel element. We experimentally confirm that the proposed method successfully recovers the oil subspace for small parameter sets even when the additional kernel element P exists. Finally, we apply the proposed method to SNOVA [16] and show that it further reduces the security of several parameter sets compared with [16].

Note that Ran's attack against SNOVA was improved by Bros et al. [4]. Unlike our method, their improvement exploits the block-ring structure of SNOVA rather than improving the attack against plain UOV. The attack of [4] applies to 10 of the 11 SNOVA parameter sets submitted to the second round of the NIST PQC standardization process for additional signatures, and outperforms the claimed security estimates for eight of them. On the other hand, our method for SNOVA first applies the lifting technique introduced by Nakamura et al. [11]

to reduce SNOVA(v, o, q, l) to a plain UOV(v, o, o) over the finite field $\mathbb{F}_{q^l}$. We then apply our method to the resulting plain UOV instance, and analyze the security of SNOVA. Our method is applicable to three parameter sets, achieving the same complexity as Bros et al. [4] for all three. Although our method has a narrower range of applicability to SNOVA than Bros et al.'s attack [4], it extends the range of the applicability of the line of attacks proposed by Ran [14], Jin et al. [8], and Furue and Ikematsu [6] against plain UOV. Therefore, our results are useful for selecting parameters for future UOV-based signature schemes. Note that the above discussion concerns the parameter sets of SNOVA submitted to the second round of the NIST PQC standardization process for additional signatures. Following earlier cryptanalytic results, these parameter sets are already planned to be updated for the third round.

This paper is organized as follows. Section 2 introduces the UOV scheme and the three main key recovery attacks. Section 3 reviews Ran's attack and its subsequent generalizations by Jin et al., and Furue and Ikematsu. Section 4 presents our improvement to this line of attacks. Section 5 provides experimental results. Section 6 discusses the security of UOV and its variants submitted to the second round of the NIST PQC standardization process. Finally, Section 7 concludes the paper.

2 The UOV signature scheme

In this section, we recall the construction of the UOV scheme [9]. Moreover, we review three key recovery attacks against UOV.

2.1 UOV

Let $\mathbb{F}_q$ be a finite field with q elements, and let v, o, m be three positive integers. Set $n = v + o$ and the polynomial ring $R = \mathbb{F}_q[\mathbf{x}]$ in n variables over $\mathbb{F}_q$, where $\mathbf{x} = (x_1, \ldots, x_n)$.

The key generation of UOV is given as follows. First, randomly choose n linearly independent linear polynomials $y_1, \ldots, y_n$ in $\mathbf{x}$ and set $\mathbf{y} = (y_1, \ldots, y_n)$. Next, randomly choose m quadratic polynomials in $\mathbf{y}$ with the following form:

$$f_k(\mathbf{y}) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{i,j}^{(k)} y_i y_j \quad (1 \leq k \leq m), \tag{1}$$

where $\alpha_{i,j}^{(k)} \in \mathbb{F}_q$. Let $p_k(\mathbf{x})$ be the quadratic polynomial obtained by expressing $f_k(\mathbf{y})$ in terms of $\mathbf{x}$, i.e., by substituting $y_i = y_i(\mathbf{x})$ for all $i = 1, \ldots, n$. Then the public key of UOV is given by $\{p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})\}$. The secret key is given by the set of n linear polynomials $\{y_1, \ldots, y_n\}$ and the central polynomials $\{f_1(\mathbf{y}), \ldots, f_m(\mathbf{y})\}$.

The signature generation is given as follows. Let $\mathbf{h} \in \mathbb{F}_q^m$ be a message to be signed. The signer chooses a random vector $(a_1, \ldots, a_v) \in \mathbb{F}_q^v$ and obtains a

system of m linear equations in the o variables $y_{v+1}, \ldots, y_n$:

$$f_k(a_1, \ldots, a_v, y_{v+1}, \ldots, y_n) = h_k \quad (1 \leq k \leq m).$$

If the system has a solution, let $(a_{v+1}, \ldots, a_n) \in \mathbb{F}_q^o$ be one such solution. Then the solution $\mathbf{x} = \mathbf{s} \in \mathbb{F}_q^n$ to $y_1(\mathbf{x}) = a_1, \ldots, y_n(\mathbf{x}) = a_n$ is a signature of the message $\mathbf{h}$. If the system has no solution, the signer chooses another random vector $(a_1, \ldots, a_v)$ and repeats the procedure.

The verification is done by checking $p_1(\mathbf{s}) = h_1, \ldots, p_m(\mathbf{s}) = h_m$.

Remark 1. In practical parameter sets of UOV, the parameters satisfy $o = m$. In this case, the resulting linear system has a solution with high probability.

Remark 2. While $y_1, \ldots, y_n$ are randomly chosen in the above, there exists an efficient method to choose $y_1, \ldots, y_n$ without affecting the security of the UOV scheme as follows:

$$\begin{aligned}
y_1 &= x_1 + t_{v+1}^{(1)} x_{v+1} + \cdots + t_n^{(1)} x_n, \\
y_2 &= x_2 + t_{v+1}^{(2)} x_{v+1} + \cdots + t_n^{(2)} x_n, \\
&\vdots \\
y_v &= x_v + t_{v+1}^{(v)} x_{v+1} + \cdots + t_n^{(v)} x_n, \\
y_{v+1} &= x_{v+1}, \\
&\vdots \\
y_n &= x_n,
\end{aligned}$$

where the coefficients $t_j^{(i)}$ are randomly chosen from $\mathbb{F}_q$.

2.2 Key recovery attacks

In this subsection, we briefly recall three known key recovery attacks against the UOV scheme: the Kipnis–Shamir attack [10], the reconciliation attack [5], and the intersection attack [1].

We define the oil subspace $\mathcal{O}$ of the UOV scheme by

$$\mathcal{O} := \left\{ \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n \;\middle|\; y_1(\mathbf{x}) = \cdots = y_v(\mathbf{x}) = 0 \right\}.$$

It is well known that, once an attacker finds a nonzero vector in $\mathcal{O}$, the attacker can efficiently recover the entire oil subspace $\mathcal{O}$ and generate valid signatures for arbitrary messages using it. Therefore, the main objective of key-recovery attacks against UOV is to find a nonzero element of the oil subspace $\mathcal{O}$.

Kipnis-Shamir (KS) attack [10]
This attack tries to find a nonzero element of the oil subspace $\mathcal{O}$ using the

symmetric matrices associated to the public key $\{p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})\}$. For any $1 \leq k \leq m$, there exists a unique symmetric matrix $P_k \in M_n(\mathbb{F}_q)$ such that

$$\mathbf{x}_1 \cdot P_k \cdot {}^t\mathbf{x}_2 = p_k(\mathbf{x}_1 + \mathbf{x}_2) - p_k(\mathbf{x}_1) - p_k(\mathbf{x}_2), \quad \mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_q^n.$$

Then the KS attack tries to find a nonzero element of the oil subspace $\mathcal{O}$ by computing invariant subspaces of XY^{-1} for various two invertible matrices $X, Y \in \mathrm{Span}\{P_1, \ldots, P_m\}$. The complexity of the KS attack is given by $O(q^{v-o})$.

Reconciliation attack [5]
Any element in the oil subspace $\mathcal{O}$ is a solution to the system of quadratic equations

$$p_1(\mathbf{x}) = \cdots = p_m(\mathbf{x}) = 0. \tag{2}$$

Since the solution set of (2) contains the o-dimensional oil subspace $\mathcal{O}$, the reconciliation attack searches for a nonzero solution of (2) by fixing o variables and solving the resulting system in the remaining $n - o$ variables.

As stated in Section 3, Ran [14] proposed an efficient algorithm to solve the system (2) without fixing some variables for the case of $\mathrm{char}(\mathbb{F}_q) = 2$.

Intersection attack [1]
The intersection attack is obtained by combining the reconciliation attack and the KS attack. For simplicity, we assume that the parameters v, o satisfy the condition $v < 2o$. We choose two invertible linear combinations Q_1 and Q_2 of the symmetric matrices $P_1, \ldots, P_m$. The intersection attack tries to find a nonzero element $\mathbf{x}$ of $\mathcal{O} \cdot Q_1 \cap \mathcal{O} \cdot Q_2$. Since $\mathbf{x}Q_1^{-1}, \mathbf{x}Q_2^{-1} \in \mathcal{O}$, such an element $\mathbf{x}$ satisfies the following $3m$ quadratic equations in n variables $\mathbf{x}$:

$$\begin{aligned}
&p_1(\mathbf{x}Q_1^{-1}) = \cdots = p_m(\mathbf{x}Q_1^{-1}) = 0,\\
&p_1(\mathbf{x}Q_2^{-1}) = \cdots = p_m(\mathbf{x}Q_2^{-1}) = 0,\\
&\mathbf{x} \cdot Q_1^{-1} \cdot P_1 \cdot Q_2^{-1} \cdot {}^t\mathbf{x} = \cdots = \mathbf{x} \cdot Q_1^{-1} \cdot P_m \cdot Q_2^{-1} \cdot {}^t\mathbf{x} = 0.
\end{aligned}$$

Note that there are two linear dependences among the above equations (see [1]). Moreover, the dimension of $\mathcal{O} \cdot Q_1 \cap \mathcal{O} \cdot Q_2$ is at least $2o - v$ under the condition $v < 2o$. Therefore, the system can be reduced to a system of $3m-2$ homogeneous quadratic equations in $n - (2o - v - 1) = 2v - o + 1$ variables. Such a reduced system is expected to behave like a random system of $M := 3m-2$ homogeneous quadratic equations in $N := 2v-o+1$ variables, and its complexity can therefore be estimated using the degree of regularity of random quadratic systems.

3 Review of the line of attacks initiated by Ran

In this section, we first review the wedge product attack proposed by Ran [14]. We then discuss the subsequent works by Jin et al. [8] and Furue and Ikematsu [6]. In this paper, following Furue and Ikematsu [6], we describe all these attacks in the unified framework of truncated polynomial rings $R^{(p)}$. This replaces the exterior-algebra formulation of Ran [14] and the symmetric-algebra formulation of Jin et al. [8].

3.1 Ran's wedge product attack

Ran [14] proposed an efficient algorithm for solving (2) in the reconciliation attack using the exterior algebra $\bigwedge \mathbb{F}_q^n$. Since

$$\bigwedge \mathbb{F}_q^n \cong \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle,$$

we can describe the attack in terms of the truncated polynomial ring

$$R^{(2)} := \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle.$$

Let $y_1, \ldots, y_n$ be linear polynomials used in the key generation of the UOV scheme. Note that $\{y_1, \ldots, y_v\}$ defines the oil subspace $\mathcal{O}$. Since $\mathrm{char}(\mathbb{F}_q) = 2$, we have

$$\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^2, \ldots, x_n^2 \rangle = \mathbb{F}_q[y_1, \ldots, y_n]/\langle y_1^2, \ldots, y_n^2 \rangle.$$

Thus, from the form of $f_k(\mathbf{y})$ in (1), we have

$$p_k(\mathbf{x}) \cdot y_1 \cdots y_v = f_k(\mathbf{y}) \cdot y_1 \cdots y_v = 0 \in R^{(2)} \quad (1 \leq k \leq m).$$

Ran's attack aims to recover this kernel element $M := y_1 \cdots y_v \in R^{(2)}$ by exploiting the relation $p_k(\mathbf{x}) \cdot M = 0$. More precisely, consider the space

$$\mathcal{S}_v := \left\{ h \in R_v^{(2)} \;\middle|\; p_k(\mathbf{x}) \cdot h = 0 \ \in R^{(2)} \ (1 \leq k \leq m) \right\},$$

where $R_v^{(2)}$ denotes the degree-v homogeneous component of $R^{(2)}$. For suitable parameters, this space is expected to be one-dimensional and generated by M, i.e., $\mathcal{S}_v = \mathbb{F}_q \cdot M$. Hence, in such cases, M can be recovered up to a nonzero scalar multiple by computing $\mathcal{S}_v$. Once M is recovered, the oil subspace $\mathcal{O}$ can be efficiently reconstructed (see [14] for details).

However, the above expectation cannot hold in general. If $v \geq 2m$, it is clear that a polynomial of the form $g \cdot p_1 \cdots p_m$ with $\deg(g) = v - 2m$ belongs to $\mathcal{S}_v$. Therefore, the above expectation that $\mathcal{S}_v$ is generated by M cannot hold in general. Moreover, there may exist another oil subspace other than $\mathcal{O}$ when $v \geq \frac{o-1}{2}m$. In this case as well, $\mathcal{S}_v$ may have solutions other than M. That is why Ran's attack [14] is typically considered only for parameters satisfying

$$v < \min\{\tfrac{o-1}{2}, 2\}m.$$

Next, we consider the condition under which $\mathcal{S}_v = \mathbb{F}_q \cdot M$ is expected to hold, which is typically analyzed via the Hilbert series. First, consider the non-degenerate bilinear form

$$R_o^{(2)} \times R_v^{(2)} \ni (g_1, g_2) \mapsto g_1 g_2 \in R_n^{(2)}.$$

Then $\mathcal{S}_v$ is equal to the annihilator $I_o^{\perp}$ of $I_o \subset R_2^{(o)}$ with respect to this bilinear form. Here, I_o denotes the degree-o component of the ideal I generated by

$p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ in $R^{(2)}$. Next, let Y be the ideal generated by $y_1, \ldots, y_v$, and let Y_o denote its degree-o component. Since $Y_o^{\perp} = \mathbb{F}_q \cdot M$, the condition

$$\mathcal{S}_v = \mathbb{F}_q \cdot M$$

is equivalent to

$$I_o^{\perp} = Y_o^{\perp}, \text{ or equivalently, } I_o = Y_o.$$

Therefore, since $Y_o^{\perp} \subset I_o^{\perp}$ and $\dim Y_o^{\perp} = 1$, the equality $\mathcal{S}_v = \mathbb{F}_q \cdot M$ holds if and only if

$$\dim I_o^{\perp} = 1.$$

To estimate $\dim I_o^{\perp}$, we use the non-degeneracy of the bilinear form, which gives

$$\dim I_o^{\perp} = \dim(R^{(2)}/I)_o.$$

Assuming that $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ form a semi-regular sequence in $R^{(2)}$, the Hilbert series of $R^{(2)}/I$ is given by

$$\left[\frac{(1+z)^n}{(1+z^2)^m} \right]. \tag{3}$$

If the coefficient of z^o in (3) is at most one, then the Hilbert series predicts that $\dim(R^{(2)}/I)_o = 1$, and hence $\dim I_o^{\perp} = 1$. Therefore, we expect that $\mathcal{S}_v = \mathbb{F}_q \cdot M$ whenever the coefficient of z^o in (3) is at most one.

In this case, the complexity of Ran's attack is given by

$$3\binom{n+1}{2} \cdot T(n, o, 2)^2.$$

Here, for integers $a, b \geq 0$, $T(a, b, p)$ is defined by

$$T(a, b, p) = \sum_{i=0}^{\lfloor b/p \rfloor} (-1)^i \binom{a}{i} \binom{b - pi + a - 1}{a - 1},$$

which is the dimension of $(\mathbb{F}_q[x_1, \ldots, x_a]/\langle x_1^p, \ldots, x_a^p \rangle)_b$.

3.2 Jin et al.'s attack

Jin et al. [8] proposed a generalization of Ran's attack for $\mathrm{char}(\mathbb{F}_q) = p \geq 2$ using the p-reduced symmetric algebra:

$$\overline{\mathrm{Sym}}(\mathbb{F}_q^n) = \mathbb{F}_q \oplus \mathbb{F}_q^n \oplus \mathbb{F}_q^{n^{\otimes 2}} \oplus \cdots / \left\langle \mathbf{z}^{\otimes p}, \mathbf{z} \otimes \mathbf{w} - \mathbf{w} \otimes \mathbf{z} \,\middle|\, \mathbf{z}, \mathbf{w} \in \mathbb{F}_q^n \right\rangle.$$

Similar to Ran's attack, Jin et al.'s attack can be explained via the truncated polynomial ring

$$R^{(p)} := \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^p, \ldots, x_n^p \rangle,$$

since we have an isomorphism $\overline{\mathrm{Sym}}(\mathbb{F}_q^n) \cong R^{(p)}$ as stated in [8]. To precisely explain Jin et al.'s attack via the truncated polynomial ring $R^{(p)}$, we need two lemmas.

Lemma 1. *(i)* $R^{(p)} = \bigoplus_{d=0}^{n(p-1)} R_d^{(p)}$ *is a graded ring, where* $R_d^{(p)}$ *denotes the degree-d homogeneous component of* $R^{(p)}$*, and* $R_{n(p-1)}^{(p)}$ *is a one-dimensional space spanned by* $x_1^{p-1} \cdots x_n^{p-1} = y_1^{p-1} \cdots y_n^{p-1}$.
(ii) For any $0 \leq d \leq n(p-1)$*, the following is a non-degenerate bilinear form:*

$$\Phi_d : R_d^{(p)} \times R_{n(p-1)-d}^{(p)} \ni (g_1, g_2) \mapsto g_1 g_2 / x_1^{p-1} \cdots x_n^{p-1} \in \mathbb{F}_q,$$

where $g_1 g_2 / x_1^{p-1} \cdots x_n^{p-1}$ *means the coefficient of* $x_1^{p-1} \cdots x_n^{p-1}$ *in* $g_1 g_2$.

Lemma 2. *We define the polynomial* M *of degree* $v(p-1)$ *as* $M := y_1^{p-1} \cdots y_v^{p-1}$. *Let* Y *be the ideal generated by* $y_1, \ldots, y_v$ *in* $R^{(p)}$. *For any* d*, we denote by* $Y_d^{\perp}$ *the annihilator of* Y_d *regarding the bilinear form* Φ_d*, namely,*

$$Y_d^{\perp} := \left\{ g \in R_{n(p-1)-d}^{(p)} \;\middle|\; \Phi_d(h, g) = 0 \text{ for all } h \in Y_d \right\}.$$

Then we have

$$Y_d^{\perp} = \langle M \rangle_{n(p-1)-d} \text{ and } \dim Y_d^{\perp} = \dim(R^{(p)}/Y)_d = T(o, d, p).$$

In particular, for $d > o(p-1)$*, we have* $\langle M \rangle_{n(p-1)-d} = 0$*, and thus* $Y_d^{\perp} = 0$.

Now, we explain the idea of Jin et al.'s attack [8]. The key observation is that recovering a nonzero element of $Y_d^{\perp}$ is sufficient to recover the oil subspace $\mathcal{O}$. By Lemma 2, every nonzero element of $Y_d^{\perp}$ is of the form

$$g(y_{v+1}, \ldots, y_n) \cdot M$$

for some polynomial $g(y_{v+1}, \ldots, y_n)$. Moreover, Jin et al. [8] showed that the oil subspace $\mathcal{O}$ can be recovered from such a polynomial by computing its permanent minor. Therefore, the main task is to compute a nonzero element of $Y_d^{\perp}$. In general, this is difficult. However, for some suitable degree D, it may happen that

$$I_D = Y_D, \tag{4}$$

where I is the ideal generated by $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ in $R^{(p)}$. Taking annihilators with respect to Φ_D, we obtain

$$I_D^{\perp} = Y_D^{\perp}.$$

Here,

$$I_D^{\perp} := \{ g \in R_{n(p-1)-D}^{(p)} \mid \Phi_D(h, g) = 0 \text{ for all } h \in I_D \}.$$

Since I_D is determined by the public key, a nonzero element of $I_D^{\perp}$ can be computed as an element of the right kernel of the degree-D Macaulay matrix. Hence, under (4), we can compute a nonzero element of $Y_D^{\perp}$. Thus, Jin et al.'s attack reduces to estimating a degree D for which (4) holds.

In [8], the smallest integer D for which (4) holds can be estimated as follows. If we assume that $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ are semi-regular in $R^{(p)}$, then the Hilbert series of $R^{(p)}/I$ is given by

$$\left[\frac{(1 + z + \cdots + z^{p-1})^n}{(1 + z^2 + \cdots + z^{2(p-1)})^m} \right]. \tag{5}$$

Then D is estimated as the smallest degree such that the coefficient of z^D is less than or equal to $\dim Y_D^{\perp} = T(o, D, p)$. In this case, the complexity of Jin et al.'s attack [8] is given by

$$3\binom{n+1}{2}\left(T(n, D, p) - T(o, D, p) + 1\right)^2.$$

Remark 3. As a generalization of the discussion in Subsection 3.1, if

$$D \leq (n - 2m)(p - 1)$$

holds, then Jin et al.'s attack does not succeed. In fact, if so, for any $r \in R^{(p)}_{(n-2m)(p-1)-D}$ the product $r \cdot p_1(\mathbf{x})^{p-1} \cdots p_m(\mathbf{x})^{p-1}$ is an element of $I_D^{\perp}$ but may not belong to $Y_D^{\perp}$. In this case, the above equality (4) does not hold, since $I_D^{\perp} \neq Y_D^{\perp}$. This suggests that the attack does not succeed in this parameter range.

3.3 Furue and Ikematsu's attack

Furue and Ikematsu [6] reformulated the attacks of Ran [14] and Jin et al. [8] in terms of truncated polynomial rings, avoiding the use of exterior and symmetric algebras. Moreover, by introducing the p^{ℓ}-truncated polynomial rings

$$R^{(p^{\ell})} := \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^{p^{\ell}}, \ldots, x_n^{p^{\ell}} \rangle,$$

they relaxed the restriction on the solving degree appearing in the XL algorithm. Ran's and Jin et al.'s attacks require the condition $D \leq o(p - 1)$. In fact, if $D > o(p - 1)$, then $Y_D^{\perp} = 0$ holds by Lemma 2. Consequently, if the degree D obtained from (6) satisfies $D > o(p - 1)$, then one expects that $I_D^{\perp} = 0$. In this case, elements of $I_D^{\perp}$ no longer contain meaningful information related to M, making the attack no longer applicable. Therefore, the condition $D \leq o(p - 1)$ is necessary. In Furue and Ikematsu [6], this condition enlarges the admissible range to $D \leq o(p^{\ell} - 1)$ by introducing $R^{(p^{\ell})}$, thereby extending the parameter regime in which the attack framework applies.

Furthermore, Furue and Ikematsu applied their idea not only to the reconciliation attack [5] but also to the intersection attack [1]. See [6] for details.

4 An improvement on the attacks initiated by Ran

Set

$$P := p_1(\mathbf{x})^{p-1} \cdots p_m(\mathbf{x})^{p-1}, \quad M := y_1^{p-1} \cdots y_v^{p-1}.$$

The attacks in Section 3 described above first estimate a degree D for which $I_D = Y_D$ using the Hilbert series, compute a nonzero element of $I_D^{\perp}$ via a Macaulay matrix, and then recover the oil subspace $\mathcal{O}$ from this element. These attacks succeed under the assumption that $I_D = Y_D$, or equivalently, $I_D^{\perp} = Y_D^{\perp} =$

$\langle M \rangle_{n(p-1)-D}$. When this condition fails, the kernel $I_D^{\perp}$ contains polynomials that are unrelated to M, and the key recovery procedure in Section 3 is no longer guaranteed to succeed. For example, as in Remark 3, when $D \leq (n-2m)(p-1)$, the space $I_D^{\perp}$ contains multiples of P which are unrelated to M. Consequently, in this case, the attacks fail.

In this section, we propose an improvement on the attacks of Section 3 in the case where $I_D^{\perp}$ is generated by P and M, i.e.,

$$I_D^{\perp} = \langle P, M \rangle_{n(p-1)-D}.$$

We also derive conditions under which this equality $I_D^{\perp} = \langle P, M \rangle_{n(p-1)-D}$ holds and analyze the complexity of the improved attack.

Note that the case of p^{ℓ} can be handled by a straightforward modification of the arguments for the case of p. Therefore, we focus on the case of p in this paper.

4.1 Proposed attack

We explain the idea of our attack. We assume that there exists a positive integer D such that $I_D^{\perp}$ is generated by P and M, namely,

$$I_D^{\perp} = \langle P, M \rangle_{n(p-1)-D}. \tag{6}$$

Thus, any polynomial h in $I_D^{\perp}$ can be written as $h = g_1 P + g_2 M$ for some $g_1, g_2 \in R^{(p)}$. Since $y_i \cdot M = 0$ for all $i = 1, \ldots, v$, we have $y_i h = y_i g_1 P$, namely,

$$y_i h \in \langle P \rangle. \tag{7}$$

Using this property (7), we will find a subspace containing $y_1, \ldots, y_v$ and recover the oil subspace $\mathcal{O}$.

Before describing our attack, we recall the construction of the truncated Macaulay matrix of degree D. Let $\mathrm{Mon}_D^{(p)}(\mathbf{x})$ denote the set of degree-D monomials that are not divisible by any of $x_1^p, \ldots, x_n^p$. We multiply each polynomial $p_k(\mathbf{x})$ by all monomials of degree $D-2$ in $\mathbf{x}$ to generate the following set of degree-D polynomials:

$$G = \left\{ a \cdot p_k(\mathbf{x}) \;\middle|\; a \in \mathrm{Mon}_{D-2}^{(p)}(\mathbf{x}), k = 1, \ldots, m \right\}.$$

We then construct a coefficient matrix $\mathcal{M}_D^{(p)}$ for the set G with respect to $\mathrm{Mon}_D^{(p)}(\mathbf{x})$, which is called the truncated Macaulay matrix. Namely, the rows of $\mathcal{M}_D^{(p)}$ correspond to the polynomials in G, the columns correspond to the monomials in $\mathrm{Mon}_D^{(p)}(\mathbf{x})$, and the (g, a)-entry for $g \in G$ and $a \in \mathrm{Mon}_D^{(p)}(\mathbf{x})$ is given by the coefficient of a in g. Note that, although the order of monomials is not essential, we use the lexicographic order on $\mathrm{Mon}_D^{(p)}(\mathbf{x})$ in this paper. The following lemma follows immediately from the definition of the truncated Macaulay matrix.

Lemma 3. *The following map is a linear isomorphism:*

$$Ker\ \mathcal{M}_D^{(p)} \ni \begin{pmatrix} w_1 \\ w_2 \\ \vdots \end{pmatrix} \mapsto \sum_i w_i \cdot \left(\frac{x_1^{p-1} \cdots x_n^{p-1}}{t_i} \right) \in I_D^{\perp},$$

where Ker means the right kernel and $t_1, t_2, \ldots$ *denote the elements of* $\mathrm{Mon}_D^{(p)}(\mathbf{x})$ *listed in lexicographic order.*

Now, we describe our attack.

Step 1.

First, we construct the truncated Macaulay matrix $\mathcal{M}_D^{(p)}$ of degree D from the public key $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$.

Step 2.

Next, we compute a nonzero element ${}^t(w_1, w_2, \ldots)$ of the right kernel of $\mathcal{M}_D^{(p)}$. Then we define the polynomial $h \in R_{n(p-1)-D}^{(p)}$ by

$$h = \sum_i w_i \cdot \left(\frac{x_1^{p-1} \cdots x_n^{p-1}}{t_i} \right),$$

which is in $I_D^{\perp}$ by Lemma 3. Thus, by the assumption (6), h can be written as

$$h = g_1 P + g_2 M.$$

Step 3.

For a linear polynomial L in n-variables $\mathbf{x}$, we consider the condition

$$L \cdot h \in \langle P \rangle. \tag{8}$$

As observed in (7), each of $y_1, \ldots, y_v$ satisfies this condition. Namely, the space

$$\mathcal{L} := \left\{ L \in R_1^{(p)} \;\middle|\; L \cdot h \in \langle P \rangle \right\}$$

contains $y_1, \ldots, y_v$. Thus our purpose is to recover this space, which is done as follows. Let $L = \sum_{i=1}^n \beta_i x_i$ be an arbitrary linear polynomial, where each β_i is unknown and consider the condition:

$$\sum_{i=1}^n \beta_i x_i \cdot h \in \langle P \rangle. \tag{9}$$

This forms a system of linear equations involving the variables $\beta_1, \ldots, \beta_n$. In fact, since $x_i \cdot h$ is of degree $n(p-1) - D + 1$ and P is of degree $2m(p-1)$, the condition (9) can be written as the following linear equations:

$$\sum_{i=1}^n \beta_i x_i \cdot h + \sum_{\mathbf{t} \in \mathrm{Mon}_{(n-2m)(p-1)-D+1}^{(p)}(\mathbf{x})} \gamma_{\mathbf{t}}\, \mathbf{t} \cdot P = 0. \tag{10}$$

Algorithm 1 Proposed attack

Require: Public key $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$, degree D
Ensure: a nonzero element of the oil subspace $\mathcal{O}$

1: Construct the truncated Macaulay matrix $\mathcal{M}_D^{(p)}$ from $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$
2: Compute a nonzero vector $(w_i)_i$ in the right kernel of $\mathcal{M}_D^{(p)}$
3: Define

$$h = \sum_i w_i \cdot \frac{x_1^{p-1} \cdots x_n^{p-1}}{t_i}$$

where t_i are elements of $\mathrm{Mon}_D^{(p)}(\mathbf{x})$
4: Construct the linear system:

$$zh \in \langle P \rangle, \quad z = \sum_{i=1}^{n} \beta_i x_i$$

5: Translate the condition into a linear system in variables $\beta_1, \ldots, \beta_n$
6: Solve the linear system
7: **return** a nonzero element of the oil space $\mathcal{O}$

Then,

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \beta_i x_i \;\middle|\; \text{there exists } \{\gamma_{\mathbf{t}}\}_{\mathbf{t}} \text{ such that (10) is satisfied} \right\}.$$

Namely, $\mathcal{L}$ can be recovered by solving (10) and projecting the solution space onto the coordinates $(\beta_1, \ldots, \beta_n)$.

Step 4.

Choose a basis $\{b_1(\mathbf{x}), \ldots, b_t(\mathbf{x})\}$ of $\mathcal{L}$. Then solve the linear system

$$b_1(\mathbf{x}) = \cdots = b_t(\mathbf{x}) = 0.$$

A nonzero solution is expected to be a nonzero element of the oil subspace $\mathcal{O}$, since $\mathcal{L}$ contains $y_1, \ldots, y_v$.

Remark 4. If the chosen h in Step 2 is of the form $h = g_1 P$, then in (9), any linear polynomial (not only y_i) satisfies the same condition. Hence, the oil subspace cannot be recovered. In particular, if

$$\langle P, M \rangle_{n(p-1)-D} = \langle P \rangle_{n(p-1)-D},$$

then every element of $I_D^{\perp}$ is of the form $h = g_1 P$, and thus no choice of h avoids the above situation.

Moreover, even in the following case:

$$\langle P, M \rangle_{n(p-1)-D+1} = \langle P \rangle_{n(p-1)-D+1},$$

the condition (9) is satisfied by arbitrary linear polynomials, not only by y_i, and therefore the oil subspace cannot be recovered. Therefore, our attack needs the following two conditions:

$$\langle P, M\rangle_{n(p-1)-D} \neq \langle P\rangle_{n(p-1)-D} \quad \text{and} \quad \langle P, M\rangle_{n(p-1)-D+1} \neq \langle P\rangle_{n(p-1)-D+1}.$$

4.2 Investigation of the ideal $\langle P, M\rangle$

As mentioned in Remark 4, if $\langle P, M\rangle_{n(p-1)-D} = \langle P\rangle_{n(p-1)-D}$ or $\langle P, M\rangle_{n(p-1)-D+1} = \langle P\rangle_{n(p-1)-D+1}$ holds, our proposed attack fails to work since all linear polynomials satisfy the condition (9). Therefore, it is crucial to find the specific values D that ensure $\langle P, M\rangle_{n(p-1)-D} \neq \langle P\rangle_{n(p-1)-D}$ and $\langle P, M\rangle_{n(p-1)-D+1} \neq \langle P\rangle_{n(p-1)-D+1}$. Moreover, it is necessary to estimate the dimensions of $\langle P, M\rangle_d$ and $\langle P\rangle_d$ for evaluating the complexity of our attack. Throughout this subsection, we assume that $n \geq 2m$; otherwise, $P = 0$ identically in $R^{(p)}$.

First, we study the ideal $\langle P\rangle$. Since $\langle P\rangle$ is a principal ideal of $R^{(p)}$, there exists an ideal J such that

$$(R^{(p)}/J)(-2m(p-1)) \ni h \bmod J \overset{\sim}{\longmapsto} h \cdot P \in \langle P\rangle$$

is an isomorphism of graded $R^{(p)}$-modules. Here J corresponds to the annihilator of P in $R^{(p)}$, i.e., $J = \mathrm{Ann}(P)$. Recall that $I = \langle p_1, \ldots, p_m\rangle$ is the ideal generated by the public polynomials. Since $p_i \cdot P = 0$ in $R^{(p)}$ for all $i = 1, \ldots, m$, we clearly have $I \subset J$. Thus, we have the following inequality:

$$\dim\langle P\rangle_{d+2m(p-1)} = \dim(R^{(p)}/J)_d \leq \dim(R^{(p)}/I)_d$$

for any $0 \leq d \leq (n-2m)(p-1)$. Moreover, since $\langle P\rangle \subset I^{\perp}$, we have the following inequality:

$$\dim\langle P\rangle_{d+2m(p-1)} \leq \min\left\{\dim(R^{(p)}/I)_d,\ \dim(R^{(p)}/I)_{(n-2m)(p-1)-d}\right\}. \quad (11)$$

Here, we used the equation $\dim I^{\perp}_{d+2m(p-1)} = \dim(R^{(p)}/I)_{(n-2m)(p-1)-d}$.

Next, we experiment for the dimensions appearing in (11) and $\dim\langle P, M\rangle_{d+2m(p-1)}$. Table 1 shows the experimental results with respect to

$$\dim\langle P\rangle_{d+2m(p-1)},\ \dim\langle P, M\rangle_{d+2m(p-1)},\ \dim(R^{(p)}/I)_d,\ \dim(R^{(p)}/I)_{(n-2m)(p-1)-d},$$

including the theoretical values

$$\dim\langle M\rangle_{d+2m(p-1)} = T(o, (n-2m)(p-1)-d, p),$$
$$\dim R^{(p)}_{d+2m(p-1)} = T(n, d+2m(p-1), p).$$

For each parameter set in Table 1, the experiments were executed 5 times with randomly generated instances. For example, consider the first parameter set $(q, v, o, m) = (16, 6, 4, 4)$ with $n = v + o = 10$ variables. Since $\mathrm{char}(\mathbb{F}_q) = p = 2$,

Table 1. Experimental dimensions of ideals and quotient rings. The experimental values are obtained from 5 trials for each parameter set. The value d ranges from 0 to $(n-2m)(p-1)$. For readability, the degree indices of $\langle P\rangle$, $\langle M\rangle$, $\langle P,M\rangle$, $R^{(p)}/I$ and $R^{(p)}$ are placed in the second line of the column headers. The asterisk in 3* indicates that the dimension of $\langle P\rangle_{d+2m(p-1)}$ was 230 in one trial, while it was 231 in the other 4 trials.

Parameters (q,v,o,m)	d	$\langle P\rangle$ $_{d+2m(p-1)}$	$\langle M\rangle$ $_{d+2m(p-1)}$	$\langle P,M\rangle$ $_{d+2m(p-1)}$	$(R^{(p)}/I)$ $_{d}$	$(R^{(p)}/I)$ $_{(n-2m)(p-1)-d}$	$R^{(p)}$ $_{d+2m(p-1)}$
(16, 6, 4, 4)	0	1	6	7	1	41	45
	1	10	4	10	10	10	10
	2	1	1	1	41	1	1
(16, 7, 4, 4)	0	1	4	5	1	121	165
	1	11	6	17	11	51	55
	2	11	4	11	51	11	11
	3	1	1	1	121	1	1
(16, 8, 5, 5)	0	1	10	11	1	221	286
	1	13	10	23	13	73	78
	2	13	5	13	73	13	13
	3	1	1	1	221	1	1
(16, 10, 5, 5)	0	1	1	2	1	953	3003
	1	15	5	20	15	855	1365
	2	100	10	110	100	380	455
	3	100	10	100	380	100	105
	4	15	5	15	855	15	15
	5	1	1	1	953	1	1
(81, 5, 4, 3)	0	1	10	11	1	449	1554
	1	9	16	25	9	441	882
	2	42	19	61	42	282	414
	3	129	16	129	129	129	156
	4	42	10	42	282	42	45
	5	9	4	9	441	9	9
	6	1	1	1	449	1	1
(81, 6, 4, 4)	0	1	19	20	1	401	615
	1	10	16	26	10	170	210
	2	51	10	51	51	51	55
	3	10	4	10	170	10	10
	4	1	1	1	401	1	1
(81, 7, 4, 4)	0	1	10	11	1	1793	4917
	1	11	16	27	11	1243	2277
	2	62	19	81	62	622	880
	3*	231	16	231	231	231	275
	4	62	10	62	622	62	66
	5	11	4	11	1243	11	11
	6	1	1	1	1793	1	1

we have $2m(p-1) = 8$. At $d = 0$, the dimensions of $\langle M \rangle_8$ and $R_8^{(2)}$ are given by the theoretical values $T(4,2,2) = 6$ and $T(10,2,8) = 45$, respectively. From our experiments, at $d = 0$, we obtained that

$$\dim\langle P \rangle_8 = 1, \quad \dim\langle P, M \rangle_8 = 7, \quad \dim(R^{(2)}/I)_0 = 1.$$

For most parameters, the same values were obtained in all 5 trials. However, only for the parameter set $(q, v, o, m) = (81, 7, 4, 4)$ at $d = 3$ (denoted as 3^* in Table 1), the dimension of $\langle P \rangle_{d+2m(p-1)}$ was 230 in one trial, while it was 231 in the other 4 trials.

Finally, we investigate the structure of the ideals $\langle P \rangle$ and $\langle P, M \rangle$ based on the experimental results in Table 1. Our experiments suggest the following observations:

Observation 1. Equality holds in (11). Moreover, $\dim\langle P \rangle_{d+2m(p-1)}$ has a symmetric pattern.

Observation 2. As the degree $d' = d+2m(p-1)$ increases, $\dim\langle P, M \rangle_{d'}$ changes from $\dim\langle P \rangle_{d'} + \dim\langle M \rangle_{d'}$ to $\dim\langle P \rangle_{d'}$.

From these observations, we formulate the following conjecture, which provides a precise description of the algebraic structure of the ideals $\langle P \rangle$ and $\langle P, M \rangle$.

Conjecture 1. Let the parameters and ideals be defined as above. Then, the following assertions generically hold:

(i) The relation in (11) holds with equality:

$$\dim\langle P \rangle_{d+2m(p-1)} = \min\left\{ \dim(R^{(p)}/I)_d,\ \dim(R^{(p)}/I)_{(n-2m)(p-1)-d} \right\}.$$

(ii) More precisely, the dimension of $\langle P \rangle_{d+2m(p-1)}$ is given by

$$\dim\langle P \rangle_{d+2m(p-1)} = \begin{cases} \dim(R^{(p)}/I)_d & \text{if } d < \left\lceil \frac{n-2m}{2}(p-1) \right\rceil, \\ \dim(R^{(p)}/I)_{(n-2m)(p-1)-d} & \text{if } d \geq \left\lceil \frac{n-2m}{2}(p-1) \right\rceil. \end{cases}$$

(iii) Assume that $d + 2m(p-1) \geq v(p-1)$, namely, $\langle M \rangle_{d+2m(p-1)} \neq 0$. Then

$$\langle P, M \rangle_{d+2m(p-1)} = \begin{cases} \langle P \rangle_{d+2m(p-1)} \oplus \langle M \rangle_{d+2m(p-1)}, & \text{if } d < \left\lceil \frac{n-2m}{2}(p-1) \right\rceil, \\ \langle P \rangle_{d+2m(p-1)}, & \text{if } d \geq \left\lceil \frac{n-2m}{2}(p-1) \right\rceil, \end{cases}$$

where the first case is equivalent to

$$\langle P, M \rangle_{d+2m(p-1)} \neq \langle P \rangle_{d+2m(p-1)}.$$

Remark 5. The above conjecture is expected not to hold when $o > v$. For example, we experimentally verified that assertion (i) fails for the parameter set $(q, v, o, m) = (16, 5, 8, 3)$.

4.3 Complexity analysis

In this subsection, we estimate the smallest integer D such that our attack succeeds under Conjecture 1. Moreover, using such D, we give a complexity estimation of our attack.

From the above discussion, our attack needs the following conditions to succeed:

$$\begin{aligned}
&(a)\ I_D^{\perp} = \langle P, M\rangle_{n(p-1)-D},\\
&(b)\ \langle P, M\rangle_{n(p-1)-D} \neq \langle P\rangle_{n(p-1)-D},\\
&(c)\ \langle P, M\rangle_{n(p-1)-D+1} \neq \langle P\rangle_{n(p-1)-D+1},\\
&(d)\ D \leq o(p-1),\ \text{i.e.,}\ \langle M\rangle_{n(p-1)-D} \neq 0.
\end{aligned}$$

We derive a method for estimating the smallest integer D satisfying the above conditions under Conjecture 1. We then discuss whether our attack succeeds whenever such an integer D exists.

First, we discuss the condition of D such that $I_D^{\perp} = \langle P, M\rangle_{n(p-1)-D}$ using the Hilbert series. If the public key $p_1(\mathbf{x}), \ldots, p_m(\mathbf{x})$ are semi-regular in $R^{(p)}$, the Hilbert series of $R^{(p)}/I$ is given by

$$\sum_{d=0}^{n(p-1)} H_d \cdot z^d = \left[\frac{(1+z+\cdots+z^{p-1})^n}{(1+z^2+\cdots+z^{2(p-1)})^m}\right]. \tag{12}$$

Since $I_D^{\perp}$ is the annihilator of I_D with respect to the non-degenerate bilinear form Φ_D in Lemma 2, we have

$$\dim I_D^{\perp} = \dim(R^{(p)}/I)_D = H_D.$$

Hence, we expect that if

$$H_D \leq \dim\langle P, M\rangle_{n(p-1)-D}, \tag{13}$$

then the equality $I_D^{\perp} = \langle P, M\rangle_{n(p-1)-D}$ holds.

The following theorem provides a sufficient condition for the success of the proposed attack and the resulting complexity estimation.

Theorem 1. *We consider the UOV with the parameter $(q = p^e, v, o, m)$. We assume $v > o$ and $n := v + o \geq 2m$. We also assume Conjecture 1.*

(i) The above conditions (a),(b),(c) and (d) are satisfied if

$$n(p-1) - \left\lceil \frac{n+2m}{2}(p-1)\right\rceil + 2 \leq D \leq o(p-1),$$

and

$$H_D \leq H_{(n-2m)(p-1)-D} + T(o, o(p-1)-D, p).$$

(ii) Assume that (a),(b),(c) and (d) are satisfied and $h \notin \langle P \rangle$. Then the subspace $\mathcal{L}$ in Step 3 of the attack contains $y_1, \ldots, y_v$ and is a proper subspace in $R_1^{(p)}$. Thus, in Step 4, a nonzero element of the oil subspace $\mathcal{O}$ is recovered.

(iii) Let D be the smallest integer satisfying the above conditions in (i). The complexity of Step 2 using the Wiedemann XL algorithm [17] is given by

$$3\binom{n+1}{2}\left(T(n,D,p) - H_{(n-2m)(p-1)-D} - T(o, o(p-1)-D, p) + 1\right)^2.$$

(iv) Moreover, the complexity of Step 3 using Gaussian elimination is at most

$$O\Big(\big(T\left(n, (n-2m)(p-1)-D+1, p\right)+n\big)^3\Big).$$

Proof. (i) Since $D \leq o(p-1)$, it is clear that condition (d) holds. Set

$$d := (n-2m)(p-1) - D.$$

By the first inequality in Theorem 1 (i), we have

$$d + 2m(p-1) + 1 < \left\lceil \frac{n+2m}{2}(p-1) \right\rceil.$$

Hence,

$$d < \left\lceil \frac{n-2m}{2}(p-1) \right\rceil - 1$$

also holds. Therefore, since $n(p-1)-D = d+2m(p-1)$, Conjecture 1(iii) yields

$$\langle P, M \rangle_{n(p-1)-D} \neq \langle P \rangle_{n(p-1)-D},$$

and

$$\langle P, M \rangle_{n(p-1)-D+1} \neq \langle P \rangle_{n(p-1)-D+1}.$$

Thus, (b) and (c) are satisfied. Furthermore, by Conjecture 1(ii),

$$\begin{aligned}
\dim\langle P, M\rangle_{n(p-1)-D} &= \dim\langle P, M\rangle_{d+2m(p-1)} \\
&= \dim\langle P\rangle_{d+2m(p-1)} + \dim\langle M\rangle_{d+2m(p-1)} \\
&= H_d + T(o, d+2m(p-1)-v(p-1), p) \\
&= H_{(n-2m)(p-1)-D} + T\big(o, o(p-1)-D, p\big).
\end{aligned}$$

Condition (a) follows from the second inequality in Theorem 1 (i) and (13).

(ii) We explained in Step 3 that $\mathcal{L}$ contains $y_1, \ldots, y_v$. If $\mathcal{L} = R_1^{(p)}$, then $L \cdot g_2 M \in \langle P \rangle_{n(p-1)-D+1} \cap \langle M \rangle_{n(p-1)-D+1}$ for all linear polynomial L, where $g_2 M$ is in Step 2. From condition (c) and Conjecture 1 (iii), we have

$$\langle P, M \rangle_{n(p-1)-D+1} = \langle P \rangle_{n(p-1)-D+1} \oplus \langle M \rangle_{n(p-1)-D+1},$$

namely, $\langle P \rangle_{n(p-1)-D+1} \cap \langle M \rangle_{n(p-1)-D+1} = 0$. Thus, we have $L \cdot g_2 M = 0$ for all linear polynomial L, which means $g_2 M = 0$, i.e., $h \in \langle P \rangle$. As a result, we have

$\mathrm{Span}\{y_1, \ldots, y_v\} \subset \mathcal{L} \subsetneq R_1^{(p)}$. Therefore, in Step 4, we can obtain a nonzero element of $\mathcal{O}$.

(iii) When (i) holds, the dimension of Ker $\mathcal{M}_D^{(p)}$ is $H_{(n-2m)(p-1)-D} - T(o, o(p-1)-D, p)$. Therefore, (iii) follows immediately.

(iv) In Step 3, we solve (10) to compute $\mathcal{L}$. The number of unknowns is $T(n, (n-2m)(p-1)-D+1)+n$. Since we need to compute the solution space, we use Gaussian elimination. Thus, the complexity of Step 3 is at most

$$O\Big(\big(T\left(n, (n-2m)(p-1)-D+1, p\right)+n\big)^3\Big).$$

□

Remark 6. If we find that $h \in \langle P \rangle$, we simply repeat Step 2 with another choice of h.

The overall complexity of our attack is given by the sum of the costs in Step 2 and Step 3. However, for practical parameter sets, the dominant part of our attack is typically given by that of Step 2. Therefore, the complexity of our attack can be estimated by the complexity given in Step 2, i.e., Theorem 1 (iii).

If $D > (n-2m)(p-1)$, then we can use Jin et al.'s attack [8] since P does not appear in $I_D^{\perp}$. Namely, in that case, for $h = g_2 M$ obtained in Step 2, we only need to compute its permanent minor as in [8].

As is well known, one can reduce a UOV scheme with parameters (v, o, m) to one with parameters $(v, o-k, m)$ by fixing k variables to random values. By taking such a reduction, our method is sometimes more effective.

5 Experimental results for our attack

In this subsection, we experimentally evaluate the proposed attack for the following two parameter sets (q, v, o, m):

$$\text{(A) } (16, 8, 7, 3) \qquad \text{(B) } (81, 6, 5, 3)$$

In our experiments, we choose parameter sets so that it satisfies $D \leq (n-2m)(p-1)$, which are outside the range where the attacks of Ran [14] and Jin et al. [8] are expected to work.

(A) $(q, v, o, m) = (16, 8, 7, 3)$
For this parameter set, we first compute the coefficients H_d of the Hilbert series

$$\left[\frac{(1+z)^{15}}{(1+z^2)^3}\right] = \sum_{d=0}^{7} H_d z^d = 1+15z+102z^2+410z^3+1056z^4+1728z^5+1530z^6+6z^7.$$

Then $p = 2$ and $D = 7$ is the smallest integer satisfying the condition (i) in Theorem 1. In fact, the first inequality is $6 \leq D \leq 7$ and the second one is $H_D \leq H_{9-D} + T(7, 7-D, 2)$. Since $T(7,1,2) = 7, T(7,0,2) = 1$, we have $D = 7$. So our attack is considered to succeed as $D = 7$ from Theorem 1.

For the estimated degree $D = 7$, we experimented our attack in 10 times. In every trial, the attack successfully recovered a nonzero element of the oil subspace $\mathcal{O}$.

(B) $(q, v, o, m) = (81, 6, 5, 3)$
For this parameter set, the Hilbert series is given by

$$\left[\frac{(1+z+z^2)^n}{(1+z^2+z^4)^m}\right] = \sum_{d=0}^{9} H_d z^d$$
$$= 1 + 11z + 63z^2 + 242z^3 + 685z^4 + 1485z^5 + 2477z^6 + 3058z^7 + 2367z^8 + 11z^9.$$

Then $p = 3$ and $D = 9$ is the smallest integer satisfying the condition (i) in Theorem 1. In fact, the first inequality is $7 \leq D \leq 10$ and the second one is $H_D \leq H_{10-D} + T(5, 10-D, 3)$. Since $T(5,3,3) = 30, T(5,2,3) = 15, T(5,1,2) = 5, T(5,0,2) = 1$, we have $D = 9$. So our attack is considered to succeed as $D = 9$ from Theorem 1.

We performed our attack with $D = 9$ on 10 randomly generated instances. In every trial, the attack successfully recovered a nonzero element of the oil subspace $\mathcal{O}$.

6 Security Analysis of NIST PQC Additional Signature Candidates

In this section, we evaluate the complexity of our attack on the parameter sets of the multivariate signature schemes UOV [3], MAYO [2], QR-UOV [7], and SNOVA [16] in the second round of the NIST PQC standardization process [13].

First we note that if $2m \geq n$, our attack is already covered by the attacks of Ran [14] and Jin et al. [8]. Since both UOV and MAYO satisfy $2m \geq n$, they fall outside the scope of our analysis. Furthermore, the lifted version of QR-UOV can be regarded as an ordinary UOV instance satisfying $2m \geq n$, and is therefore also covered by the attacks of Ran and Jin et al. Consequently, we do not consider UOV, MAYO, or QR-UOV.

It remains to consider SNOVA. By the lifting technique of Nakamura et al. [11], a SNOVA instance with parameters (v, o, q, l) can be regarded as a plain UOV instance over the extension field $\mathbb{F}_{q^l}$ with parameters (v, o, o). Since these parameters satisfy $n = v + o \geq 2o = 2m$, SNOVA is a potential target of our attack. Table 2 summarizes the complexity of our attack on the SNOVA parameter sets proposed in the second round of NIST PQC standardization process for additional signatures [16]. The symbol "–" indicates that the corresponding parameter set does not admit a valid value of D for the attack. Note that, for the parameter sets to which our attack applies, the complexity shown in Table 2 is that of Step 2, since the complexity of Step 3 is smaller. In fact, the complexity of Step 3 is 2^{61}, 2^{100}, and 2^{139} gate operations, respectively.

For the three parameter sets to which our method applies, it achieves the same complexity as Bros et al.'s attack [4]. On the other hand, Bros et al.'s attack [4] is designed specifically for SNOVA by exploiting its block-ring structure,

Table 2. Complexities of our attack and existing estimations [4, 16] on the SNOVA parameter sets submitted to the second round of the NIST PQC standardization process for additional digital signatures [16]. The complexity is expressed as $\log_2$ of the number of gates. Thus it is given by multiplying the complexity in Theorem 1 (iii) by $2(\log_2(q^l))^2 + \log_2 q^l$. Also, k denotes the number of fixed variables, resulting in a plain UOV instance with the parameter $(q^l, v, o-k, o)$.

Security Level	(v, o, q, l)	Our Attack	[4]	[16]
I	$(37, 17, 16, 2)$	103 ($k = 2$)	103	153
	$(25, 8, 16, 3)$	–	110	166
	$(24, 5, 16, 4)$	–	155	180
III	$(56, 25, 16, 2)$	140 ($k = 5$)	140	221
	$(49, 11, 16, 3)$	–	246	220
	$(37, 8, 16, 4)$	–	214	257
	$(24, 5, 16, 5)$	–	155	257
V	$(75, 33, 16, 2)$	180 ($k = 7$)	180	288
	$(66, 15, 16, 3)$	–	313	293
	$(60, 10, 16, 4)$	–	–	343
	$(29, 6, 16, 5)$	–	181	310

whereas our method extends the applicability of Ran's [14] and Jin et al.'s [8] attacks against UOV beyond their original limitation. Notably, for the three parameter sets to which our method applies, the attacks of Ran and Jin et al. are not applicable.

Note that the above discussion concerns the parameter sets of SNOVA submitted to the second round of the NIST PQC standardization process for additional signatures. Following earlier cryptanalytic results, these parameter sets are already planned to be updated for the third round.

Remark 7. Although our method can be combined with the intersection attack for the parameter sets submitted to the second round of the NIST PQC standardization process, the resulting system is handled by the attacks of Ran [14] and Jin et al. [8], since the resulting system has fewer than twice as many variables as polynomials.

7 Conclusion

In this paper, we improved one of the main limitations of the line of attacks against the UOV signature scheme initiated by Ran. More precisely, we proposed a method for recovering the oil subspace even in the presence of the additional kernel element arising from the public key. We also derived conditions under which the proposed method succeeds and analyzed its complexity. Furthermore, for some small parameters, our experimental results confirmed that the proposed method successfully recovers the oil subspace even when such a additional kernel element exists. As an application, we showed that our method extends the

applicability of this line of attacks to several parameter sets of SNOVA in the second round to which Ran's attack cannot be applied.

Acknowledgements

This work was supported by JST K Program Grant Number JPMJKP24U2, Japan, JSPS KAKENHI Grant Number JP25K00140, JP24K02939 and JP26K23821, Japan, and Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University (FY2025 Short-term Joint Research "Speeding up of symbolic computation and its application to solving industrial problems 3" (Reference No.2025a012)).

References

1. W. Beullens. Improved cryptanalysis of UOV and Rainbow. In *EUROCRYPT 2021*, volume 12696 of *LNCS*, pages 348–373. Springer, 2021.
2. W. Beullens, F. Campos, S. Celi, B. Hess, and M. Kannwischer. MAYO specification document - round 2. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/mayo-spec-round2-web.pdf`, 2025.
3. W. Beullens, M.-S. Chen, J. Ding, B. Gong, M. J. Kannwischer, J. Patarin, B.-Y. Peng, D. Schmidt, C.-J. Shih, C. Tao, and B.-Y. Yang. UOV specification document - round 2. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/uov-spec-round2-web.pdf`, 2025.
4. M. Bros, T.-H. Le, J. Lichtinger, B. Minaud, R. Perlner, D. Smith-Tone, and C. Valenzuela. Exploiting SNOVA's structure in the wedge product attack. Cryptology ePrint Archive, Paper 2026/237, 2026.
5. J. Ding, B. Yang, C.-O. Chen, M. Chen, and C. Cheng. New differential-algebraic attacks and reparametrization of Rainbow. In *ACNS 2008*, volume 5037 of *LNCS*, pages 242–257. Springer, 2008.
6. H. Furue and Y. Ikematsu. Key recovery attacks on UOV using p^ℓ-truncated polynomial rings. Cryptology ePrint Archive, Paper 2026/298, 2026.
7. H. Furue, Y. Ikematsu, F. Hoshino, T. Takagi, H. Kosuge, K. Yamakoshi, R. Akiyama, S. Nakamura, S. Orihara, and K. Kinjo. QR-UOV specification document - round 2. `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/qruov-spec-round2-web.pdf`, 2025.
8. Y. Jin, Y. Pan, X. He, B. Gong, and J. Ding. Security analysis on UOV families with odd characteristics: Using symmetric algebra. In *PKC 2026*, volume 16551 of *LNCS*, pages 428–454. Springer, 2026.
9. A. Kipnis, J. Patarin, and L. Goubin. Unbalanced oil and vinegar signature schemes. In *EUROCRYPT 1999*, volume 1592 of *LNCS*, pages 206–222. Springer, 1999.
10. A. Kipnis and A. Shamir. Cryptanalysis of the oil and vinegar signature scheme. In *CRYPTO 1998*, volume 1462 of *LNCS*, pages 257–266. Springer, 1998.
11. S. Nakamura, Y. Tani, and H. Furue. Lifting approach against the SNOVA scheme. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 108(10):1373–1381, 2025.

12. NIST. NIST: 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, 2022.
13. NIST. Status report on the second round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. NIST Internal Report 8610, 2026.
14. L. Ran. Wedges, oil, and vinegar – an analysis of UOV in the exterior algebra. In *EUROCRYPT 2026*, volume 16544 of *LNCS*, pages 363–388. Springer, 2026.
15. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.
16. L.-C. Wang, C.-Y. Chou, J. Ding, Y.-L. Kuan, J. A. Leegwater, M.-S. Li, B.-S. Tseng, P.-E. Tseng, and C.-C. Wang. SNOVA specification document - round 2. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-2/spec-files/snova-spec-round2-web.pdf, 2025.
17. D. H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theor.*, 32(1):54–62, 1986.