SCIS 2024 2024 Symposium on
Cryptography and Information Security
Nagasaki, Japan, Jan. 23 – 26, 2024
The Institute of Electronics,
Information and Communication Engineers

Further Security Analysis for Multivariate Polynomial Signature Scheme QR-UOV

Hiroki Furue * Yasuhiko Ikematsu † Fumitaka Hoshino ‡ Tsuyoshi Takagi *
Kan Yasuda § Toshiyuki Miyazawa § Akira Nagai § Rika Akiyama §
Koha Kinjo §

Abstract: The multivariate-based unbalanced oil and vinegar signature scheme (UOV) is expected to be one of the candidates for post-quantum cryptography (PQC). UOV is a well-established signature scheme owing to its short signature and execution time. However, its public key is much larger than that of other PQC candidates. At ASIACRYPT 2021, Furue et al. proposed quotient ring UOV (QR-UOV) as a new variant of UOV, which reduces the public key size compared to the plain UOV. This QR-UOV has been submitted to the NIST additional call for digital signature schemes. For the QR-UOV scheme, there have been proposed two methods of recovering the secret key by using the quotient ring structure. In this paper, we show that these two methods are essentially the same and the key recovery attacks using the quotient ring structure are more efficient than the plain key recovery attacks.

Keywords: PQC, MPKC, unbalanced oil and vinegar (UOV), quotient ring UOV (QR-UOV)

1 Introduction

Currently used public key cryptosystems such as RSA and ECC can be broken in polynomial time using Shor's algorithm [22] on a quantum computer. Thus, research on post-quantum cryptography (PQC), which is secure against quantum computing attacks, has been attracting much attention. Indeed, the U.S. National Institute for Standards and Technology (NIST) has initiated a PQC standardization project since 2016 [16].

Multivariate public key cryptography (MPKC), based on the difficulty of solving a system of multivariate quadratic polynomial equations over a finite field (the multivariate quadratic (MQ) problem), is regarded as a strong candidate for PQC. The MQ problem is NP-complete [12] and is thus expected to be secure in the post-quantum era. Furthermore, this MPKC is known to be specifically suitable for building digital signature schemes.

The unbalanced oil and vinegar signature scheme (UOV) [13], proposed by Kipnis et al. at EUROCRYPT 1999, is a well-known multivariate signature scheme and has withstood various types of attacks for over 20 years. Indeed, a multilayer UOV variant Rainbow [6], which is weakened by an attack proposed by Beullens at CRYPTO 2022 [5], was selected as a third-round finalist in the NIST PQC project [17]. UOV is a well-established signature scheme owing to its short signature and execution time. By contrast, UOV has public keys much larger than those of other PQC candidates, for example, lattice-based signature schemes. Thus, developing a UOV variant with a small public key is an important task.

At ASIACRYPT 2021, Furue et al. presented a new UOV variant using a quotient ring structure called *quotient ring UOV (QR-UOV)* [11]. In QR-UOV, a public key is represented by block matrices in which every $\ell \times \ell$ component corresponds to an element of a quotient ring $\mathbb{F}_q[x]/(f)$ with $f \in \mathbb{F}_q[x]$ and $\deg f = \ell$. From this construction, we can compress ℓ^2 components in each block to ℓ coefficients in $\mathbb{F}_q$, and thus QR-UOV can reduce the public key size from the plain UOV. Note that this QR-UOV can be considered as a generalization of BAC-UOV [23], which is the case for $f = x^\ell - 1$. Furthermore, this QR-UOV has been recently submitted to the call for additional digital signature schemes for NIST PQC standardization [19], and in this submission, four parameters have been selected from nine parameters proposed in SCIS 2023 [10] for each security level. Thus, the detailed analysis of the security of QR-UOV is our important task.

* Department of Mathematical Informatics, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan. ({furue-hiroki261, takagi}@g.ecc.u-tokyo.ac.jp)
† Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan. (ikematsu@imi.kyushu-u.ac.jp)
‡ Faculty of Information Systems, University of Nagasaki, 1-1-1, Manabino, Nagayo-cho, Nishisonogi-gun, Nagasaki, 851-2195, Japan. (hoshino@sun.ac.jp)
§ NTT Social Informatics Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo, 180-8585, Japan. ({kan.yasuda, toshiyuki.miyazawa, akira.nagai, rika.akiyama, kouha.kinjo}@ntt.com)

Our Contributions For the QR-UOV, there have been proposed two methods of recovering the secret key by using the quotient ring structure. One is the pull-back method which directly transforms block matrices with QR-structure into smaller matrices over extension fields. Another one is the lifting method which transforms block matrices with QR-structure into diagonal block matrices over extension fields. In this paper, we show that these two methods are essentially the same. Furthermore, we show that the key recovery attacks using the quotient ring structure are more efficient than the plain key recovery attacks over the base field.

Organization The rest of this paper is organized as follows: Section 2 and 3 recalls the plain UOV and QR-UOV, respectively. Section 4 recalls two methods for transforming the public and secret key maps of QR-UOV into extension fields and shows their equivalence. Finally, Section 5 is devoted to the conclusion.

2 Unbalanced Oil and Vinegar (UOV)

This subsection recalls the description of UOV and some known attacks on the scheme.

2.1 Description

This section describes the structure of the unbalanced oil and vinegar signature scheme (UOV) [13]. Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Furthermore, let v and m be positive integers and $n = v + m$. For variables $\mathbf{x} = (x_1, \ldots, x_n)$ over $\mathbb{F}_q$, we call $x_1, \ldots, x_v$ *vinegar variables* and $x_{v+1}, \ldots, x_n$ *oil variables*.

We first recall the key generation of UOV as follows: We design $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, called a *central map*, such that each f_k $(k = 1, \ldots, m)$ is a quadratic polynomial of the form

$$f_k(x_1, \ldots, x_n) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{i,j}^{(k)} x_i x_j \tag{1}$$

where $\alpha_{i,j}^{(k)} \in \mathbb{F}_q$. Next, we choose a random linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to hide the structure of $\mathcal{F}$. The public key $\mathcal{P}$ is then provided as a polynomial map,

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

and the secret key comprises $\mathcal{F}$ and $\mathcal{S}$.

Next, we describe the inversion of the central map $\mathcal{F}$. When we try to find $\mathbf{x} \in \mathbb{F}_q^n$ satisfying $\mathcal{F}(\mathbf{x}) = \mathbf{y}$ for a given $\mathbf{y} \in \mathbb{F}_q^m$, we first choose random values $a_1, \ldots, a_v$ in $\mathbb{F}_q$ as the values of the vinegar variables. We can then easily obtain a solution for the equation $\mathcal{F}(a_1, \ldots, a_v, x_{v+1}, \ldots, x_n) = \mathbf{y}$, because this is a linear system of m equations in m oil variables from the construction of the central map (1). If there is no solution to this equation, we choose new random values $a_1', \ldots, a_v'$, and repeat the above procedure.

By using this inversion approach, the signature is generated as follows: Given a message $\mathbf{m} \in \mathbb{F}_q^m$ to be signed, find a solution $\mathbf{m}_1$ to the equation $\mathcal{F}(\mathbf{x}) = \mathbf{m}$, and this gives the signature $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{m}_1) \in \mathbb{F}_q^n$ for the message $\mathbf{m}$. Then, the verification step is performed by confirming whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$.

Finally, we introduce matrices representing the public and secret keys of UOV. For each polynomial p_i of the public key $\mathcal{P}$, there exists an $n \times n$ matrix P_i such that $p_i(\mathbf{x}) = \mathbf{x}^\top \cdot P_i \cdot \mathbf{x}$. Similarly, an $n \times n$ matrix F_i can be taken for each f_i with $1 \le i \le m$, and an $n \times n$ matrix S is defined to satisfy $\mathcal{S}(\mathbf{x}) = S \cdot \mathbf{x}$. In general, these matrices P_i and F_i are taken as symmetric matrices if q is odd, and are taken as upper triangular matrices if q is even. For these representation matrices, based on equation (1), F_i has the following form

$$\begin{pmatrix} *_{v\times v} & *_{v\times m} \\ *_{m\times v} & 0_{m\times m} \end{pmatrix}, \tag{2}$$

in the case where q is odd. Furthermore, from $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$, we have

$$P_i = S^\top F_i S, \ \ (i = 1, \ldots, m).$$

2.2 Key Recovery Attacks on UOV

This subsection recalls some existing key recovery attacks on UOV, the Kipnis-Shamir [14], reconciliation [7], and intersection [4] attacks. In this subsection, we describe the behavior of the key recovery attacks on $\mathrm{UOV}(q, v, o, m)$ which denotes the plain UOV with v vinegar variables, o oil variables, and m equations over $\mathbb{F}_q$. Given the public key map, these attacks try to recover the corresponding secret key. More specifically, the key recovery attacks aim to obtain the subspace $\mathcal{S}^{-1}(\mathcal{O})$ of $\mathbb{F}_q^n$, where $\mathcal{O}$ is the oil subspace defined as

$$\mathcal{O} := \left\{ (0, \ldots, 0, \alpha_1, \ldots, \alpha_o)^\top \;\middle|\; \alpha_i \in \mathbb{F}_q \right\}.$$

Kipnis-Shamir Attack The Kipnis-Shamir attack [14] chooses two invertible matrices W_i, W_j from the set of linear combinations of the representation matrices $P_1, \ldots, P_m$ for the public key. Then, it probabilistically recovers a part of the subspace $\mathcal{S}^{-1}(\mathcal{O})$ by computing the invariant subspace of $W_i^{-1} W_j$. The complexity of the Kipnis-Shamir attack is estimated as

$$O\left(q^{v-o-1} \cdot o^4\right).$$

Reconciliation Attack The reconciliation attack [7] treats a vector y of $\mathcal{S}^{-1}(\mathcal{O})$ as variables and solves the quadratic system $y^\top P_i y = 0$ $(i \in [m])$. Here, the dimension of $\mathcal{S}^{-1}(\mathcal{O})$ is o, and thus if we impose affine constraints, we then solve a system of m equations in $n - o = v$ variables. Parameters of UOV are generally set to satisfy $v > m$ for the security against the Kipnis-Shamir attack, and in this case, the system of $y^\top P_i y = 0$ has a large number of solutions. Therefore, to determine a solution uniquely, we need to solve the following system to find multiple vectors $y_1, \ldots, y_k$ of $\mathcal{S}^{-1}(\mathcal{O})$:

$$\begin{cases} y_j^\top P_i y_j = 0 & (1 \le i \le m, 1 \le j \le k), \\ y_j^\top P_i y_\ell = 0 & (1 \le i \le m, 1 \le j < \ell \le k). \end{cases}$$

On the other hand, if the number v of the vinegar variables is smaller than the number m of equations, then the complexity of the reconciliation attack is estimated as that of solving a quadratic system of m equations in v variables.

Intersection Attack In [4], Beullens proposed a new key recovery attack against UOV, called an intersection attack. In the case of $v < 2o$, for an integer $k \geq 2$ satisfying $k < \frac{v}{v-o}$, let $L_1, \ldots, L_k$ be k invertible matrices randomly chosen from a set of linear combinations of the representation matrices $P_1, \ldots, P_m$ for the public key. This attack then solves the following equations for $\mathbf{y} \in \mathbb{F}_q^n$:

$$\begin{cases} (L_j^{-1}\mathbf{y})^\top P_i (L_j^{-1}\mathbf{y}) = 0 & (1 \leq i \leq m, 1 \leq j \leq k), \\ (L_j^{-1}\mathbf{y})^\top P_i (L_\ell^{-1}\mathbf{y}) = 0 & (1 \leq i \leq m, 1 \leq j < \ell \leq k). \end{cases} \tag{3}$$

Note that a solution $\mathbf{z}$ for this system is not a vector in $\mathcal{S}^{-1}(\mathcal{O})$, but $L_j^{-1}\mathbf{z}$ is an element of $\mathcal{S}^{-1}(\mathcal{O})$, unlike the Kipnis-Shamir and reconciliation attacks. The solution space obtained from the above equation has $ko - (k-1)v$ dimensions. Thus, its complexity is equivalent to that of solving the quadratic system with $n - (ko - (k-1)v) = kv - (k-1)o$ variables and $\binom{k+1}{2}m - 2\binom{k}{2}$ equations owing to its linear dependency. The value of k is generally chosen such that the complexity of solving the above system takes the minimum value under the condition of $k < \frac{v}{v-o}$. On the other hand, in the case of $v \geq 2o$, the intersection attack becomes a probabilistic attack, which solves the system of equation (3) as $k = 2$ with n variables and $(3m-2)$ equations and one of the solutions is a target vector with a probability of approximately $q^{-v+2o-1}$. Therefore, its complexity is estimated by q^{v-2o+1} times the complexity of solving the quadratic system with n variables and $(3m-2)$ equations.

3 QR-UOV

This section first recalls the description of the quotient ring UOV (QR-UOV) [11]. Then, we summarize the NIST PQC additional call for digital signatures [19], to which the QR-UOV scheme is submitted.

3.1 Basic Scheme

This subsection recalls the construction of QR-UOV mainly following the notation and description for the plain UOV in Section 2. Let ℓ be a positive integer and take v and m as multiples of ℓ. We then define $N := n/\ell$, $V := v/\ell$, and $M := m/\ell$.

Before explaining the key generation, we prepare some notations for QR-UOV. Let f be a polynomial in $\mathbb{F}_q[x]$ with $\deg f = \ell$. For any element g of the quotient ring $\mathbb{F}_q[x]/(f)$, we can uniquely define an $\ell \times \ell$ matrix Φ_g^f over $\mathbb{F}_q$ such that

$$\begin{pmatrix} 1 & x & \cdots & x^{\ell-1} \end{pmatrix} \Phi_g^f = \begin{pmatrix} g & xg & \cdots & x^{\ell-1}g \end{pmatrix}.$$

For any $g \in \mathbb{F}_q[x]/(f)$, the matrix Φ_g^f can be represented by only ℓ elements in $\mathbb{F}_q$. We let the algebra of the matrices $A_f := \left\{ \Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} \;\middle|\; g \in \mathbb{F}_q[x]/(f) \right\}$, and this A_f is a subalgebra in the matrix algebra $\mathbb{F}_q^{\ell\times\ell}$. For such matrices corresponding to elements of a quotient ring, Theorem 1 in [11] shows that there exists an invertible matrix $W \in \mathbb{F}_q^{\ell\times\ell}$ such that for any $X \in A_f$, WX is symmetric. Specifically, if f has a form of $x^\ell - ax^i - 1$ with $a \neq 0$ and $1 \leq i < \ell$, then the above symmetrization is realized by

$$W = \begin{pmatrix} J_i & \\ & J_{\ell-i} \end{pmatrix}, \tag{4}$$

where $J_i := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} \in \mathbb{F}_q^{i\times i}$. For the subalgebra A_f, we define a subspace $A_f^{a,b}$ with $a, b \in \mathbb{N}$ in $\mathbb{F}_q^{a\ell\times b\ell}$ containing matrices of the following form

$$\begin{pmatrix} X_{11} & \cdots & X_{1b} \\ \vdots & \ddots & \vdots \\ X_{a1} & \cdots & X_{ab} \end{pmatrix},$$

where every $X_{ij} \in \mathbb{F}_q^{\ell\times\ell}$ is an element of A_f. Furthermore, $W^{(a)}$ denotes an $a\ell \times a\ell$ block diagonal matrix concatenating $W \in \mathbb{F}_q^{\ell\times\ell}$ diagonally a times.

From these notations, we can construct a quotient-ring UOV (QR-UOV) representing public and secret keys by elements of $A_f^{N,N}$ and $W^{(N)}A_f^{N,N} := \{A \cdot B \,|\, A \in W^{(N)}, B \in A_f^{N,N}\}$. Note that we here represent the public and secret keys by matrices as described in Subsection 2.1. Before generating the public and secret keys, we prepare an irreducible polynomial $f = x^\ell - ax^i - 1 \in \mathbb{F}_q[x]$ with $a \neq 0$ and $1 \leq i < \ell$ and $W \in \mathbb{F}_q^{\ell\times\ell}$ like equation (4). We here take f as an irreducible polynomial for the security of the resulting scheme. Then, the key generation of QR-UOV is described as follows:

1. Choose F_i $(i = 1, \ldots, m)$ from $W^{(N)}A_f^{N,N}$ as a symmetric matrix with the lower-right $m \times m$ zero-block like equation 2.
2. Choose an invertible matrix S from $A_f^{N,N}$ randomly.
3. Compute the public key $P_i = S^\top F_i S$ $(i = 1, \ldots, m)$.

Then, P_i $(i = 1, \ldots, m)$ representing the public key map are elements of $W^{(N)}A_f^{(N)}$ from Proposition 1 in [11]. The signing and verification processes are performed in the same way as the plain UOV.

3.2 NIST PQC Additional Call

This subsection roughly summarizes the NIST PQC additional call for digital signatures [19], to which the QR-UOV scheme is submitted.

NIST has initiated a PQC standardization project [16] since 2016, and in 2022 they selected some algorithms to be standardized [18]. Indeed, CRYSTALS-Kyber [2] is chosen as a standardized public key encryption scheme. Further, CRYSTALS-Dilithium [3], FALCON [8], and

SPHINCS+ [1] are chosen as standardized digital signature schemes. Except for SPHINCS+, all these schemes are based on the computational hardness of problems involving structured lattices, whereas SPHINCS+ is a hash-based scheme. Currently, NIST has called for additional digital signature proposals [19] to be considered in the PQC standardization process, and NIST announced that 40 submissions were accepted in July 2023.

In this call, NIST is specifically interested in schemes with short signatures and fast verification. Thus, UOV and its variants have been attracting much interest due to their short signatures and fast implementations. Indeed, 10 schemes out of the 40 accepted submissions are multivariate signatures, and 7 schemes, UOV, QR-UOV, MAYO, PROV, SNOVA, TUOV, and VOX, out of the 10 multivariate candidates are UOV variants. Among these UOV variants, QR-UOV is considered to be a promising candidate due to its small public key and simple construction. It has been pointed out in pqc-forum [21] that there are some issues with the security of all three multivariate schemes other than UOV variants. Furthermore, in pqc-forum [21], Furue and Ikematsu pointed out that the proposed parameters of VOX [20], which is a variant of UOV with (+) and QR techniques, is broken by the rectangular MinRank attack [4] originally proposed on Rainbow. (See [15] for more details.) Note that the proposed parameters of QR-UOV were selected by considering the effect of this rectangular MinRank attack.

4 Key Recovery Attacks over Extension Field

In this section, we first recall two methods for transforming the public key map of QR-UOV into the extension field. Subsection 4.3 then shows that these two methods are essentially the same, and Subsection 4.4 theoretically compares the complexity of the key recovery attacks over the base field and the extension field. Note that we here suppose that the polynomial f used in QR-UOV is taken as an irreducible polynomial as mentioned in Subsection 3.1.

4.1 Pull-back Method

We here construct a one-to-one map representing the keys of QR-UOV as those of the plain UOV over $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^\ell}$. Note that, after applying this transformation, the pullback method performs the key recovery attacks on the UOV over the extension field.

For each representation matrix $P_k \in W^{(N)}A_f^{N,N}$ of the public key of QR-UOV, we can take ℓ matrices $\bar{P}_k^{(0)}, \dots, \bar{P}_k^{(\ell-1)} \in \mathbb{F}_q^{N\times N}$ satisfying

$$P_k = \sum_{i=0}^{\ell-1} \left(\bar{P}_k^{(i)} \otimes W\Phi_{x^i}^f\right), \tag{5}$$

due to the structure of the QR-UOV public key. We then can define an $N\times N$ matrix $\bar{P}_k$ over $\mathbb{F}_{q^\ell}$ as follows:

$$\bar{P}_k = \sum_{i=0}^{\ell-1} x^i \bar{P}_k^{(i)}.$$

By using the same way, we can construct $\bar{F}_1, \dots, \bar{F}_m$ and $\bar{S}$ corresponding to the secret key $F_1, \dots, F_m$ and S as follows:

$$F_k = \sum_{i=0}^{\ell-1} \left(\bar{F}_k^{(i)} \otimes W\Phi_{x^i}^f\right) \;\Rightarrow\; \bar{F}_k = \sum_{i=0}^{\ell-1} x^i \bar{F}_k^{(i)},$$
$$S = \sum_{i=0}^{\ell-1} \left(\bar{S}^{(i)} \otimes \Phi_{x^i}^f\right) \;\Rightarrow\; \bar{S} = \sum_{i=0}^{\ell-1} x^i \bar{S}^{(i)}.$$

Then, it holds $\bar{P}_k = \bar{S}^\top \bar{F}_k \bar{S}$ from $P_k = S^\top F_k S$, and $\bar{F}_k$ has the form as in (2). Thus, these set of $\bar{P}_k$, $\bar{F}_k$, and $\bar{S}$ can be seen as the keys of the plain UOV with N variables and m equations over the extension field $\mathbb{F}_{q^\ell}$. This transformation is clearly a bijective map from the key space $\left(\{P_k\}_{k\in[m]}, \{F_k\}_{k\in[m]}, S\right)$ of QR-UOV into the key space $\left(\{\bar{P}_k\}_{k\in[m]}, \{\bar{F}_k\}_{k\in[m]}, \bar{S}\right)$ of the plain UOV over the extension field $\mathbb{F}_{q^\ell}$.

4.2 Lifting Method

The lifting method is a method of attacking QR-UOV by diagonalizing the matrices in A_f over the extension field $\mathbb{F}_{q^\ell}$ and was proposed in [11]. To explain it, we prepare some results.

Theorem 1 (Theorem 3 in [11]) *Let $f \in \mathbb{F}_q[x]$ be an **irreducible** polynomial with $\deg f = \ell$ and W be an invertible matrix such that every element of WA_f is a symmetric matrix.*

(i) There exists an invertible matrix $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ such that

$$L^{-1}\Phi_x^f L = \begin{pmatrix} x & & & & \\ & x^q & & & \\ & & x^{q^2} & & \\ & & & \ddots & \\ & & & & x^{q^{\ell-1}} \end{pmatrix}.$$

In particular, this L diagonalizes any matrix in A_f.

(ii) The matrix L described in (i) satisfies the condition that $L^\top WL$ is diagonal. Therefore, we can write

$$L^\top WL = \begin{pmatrix} \alpha_0 & & & \\ & \alpha_1 & & \\ & & \ddots & \\ & & & \alpha_{\ell-1} \end{pmatrix}.$$

The first and second statements in the theorem show that for any $g \in \mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^\ell}$ the matrix $L^\top W\Phi_g^f L$ is diagonal. This indicates that $P_1, \dots, P_m$ of QR-UOV can be transformed into block diagonal matrices for

which the block size is $N \times N$. Let $L^{(N)} = I_N \otimes L$ be an $n \times n$ block diagonal matrix with block size ℓ ($n = \ell \cdot N$), for which the N diagonal blocks are L. Then, $(L^{(N)})^\top P_i L^{(N)}$ ($i \in [m]$) become block matrices wherein every component is in a diagonal form. Furthermore, there exists a permutation matrix A such that $(L^{(N)}A)^\top P_i (L^{(N)}A)$ is a block diagonal matrix with block size N, and we here denote $\bar{L} := L^{(N)}A$. The transformed matrices $\bar{L}^\top P_i \bar{L}$ can be represented by $(\bar{L}^{-1}S\bar{L})^\top(\bar{L}^\top F_i \bar{L})$ $(\bar{L}^{-1}S\bar{L})$. Then, $\bar{L}^\top F_i \bar{L}$ is the diagonal concatenation of ℓ smaller matrices, similar to $\bar{L}^\top P_i \bar{L}$. Furthermore, $\bar{L}^{-1}S\bar{L}$ is also the diagonal concatenation of ℓ smaller matrices from (i) in Theorem 1. Then, owing to the structure of F_i, every diagonal block of $\bar{L}^\top F_i \bar{L}$ has an $M \times M$ zero block, similar to F_i. Therefore, each diagonal block of $\bar{L}^\top P_i \bar{L}$ has the same form as the matrix representing the public key of UOV with V vinegar variables and M oil variables over $\mathbb{F}_{q^\ell}$. The lifting method proposed in [11] executes the key recovery attacks on one of such diagonal blocks.

4.3 Equivalence of These Two Methods

In this subsection, we show that the pull-back method given in Subsection 4.1 is essentially the same as the lifting method in Subsection 4.2.

Let $A \in \mathbb{F}_q^{n\times n}$ be a permutation matrix such that

$$A^\top (X \otimes Y) A = Y \otimes X$$

for any $X \in \mathbb{F}_q^{N\times N}$ and $Y \in \mathbb{F}_q^{\ell\times\ell}$. Also, from equation (5), the transformation in the above lifting method can be described as follows:

$$\begin{aligned}
&A^\top (L^{(N)})^\top P_k L^{(N)} A \\
=&A^\top (L^{(N)})^\top \left(\sum_{i=0}^{\ell-1} \bar{P}_k^{(i)} \otimes W\Phi^f_{x^i} \right) L^{(N)} A \\
=&A^\top \left(\sum_{i=0}^{\ell-1} \bar{P}_k^{(i)} \otimes L^\top W\Phi^f_{x^i} L \right) A \\
=&\sum_{i=0}^{\ell-1} L^\top W\Phi^f_{x^i} L \otimes \bar{P}_k^{(i)} \\
=&\sum_{i=0}^{\ell-1} L^\top WL \cdot L^{-1}\Phi^f_{x^i} L \otimes \bar{P}_k^{(i)} \\
=&\sum_{i=0}^{\ell-1} \mathrm{diag}(\alpha_0 x^i, \alpha_1 x^{qi}, \ldots, \alpha_{\ell-1} x^{q^{\ell-1}i}) \otimes \bar{P}_k^{(i)} \\
=&\mathrm{diag}\left(\alpha_0 \sum_{i=0}^{\ell-1} \bar{P}_k^{(i)} x^i, \ldots, \alpha_{\ell-1} \sum_{i=0}^{\ell-1} \bar{P}_k^{(i)} x^{q^{\ell-1}i} \right) \\
=&\mathrm{diag}\left(\alpha_0 \bar{P}_k, \alpha_1 \bar{P}_{k,q}, \ldots, \alpha_{\ell-1} \bar{P}_{k,q^{\ell-1}} \right),
\end{aligned}$$

where $\mathrm{diag}(A_1, \ldots, A_k)$ denotes a block diagonal matrix whose diagonal blocks are given square matrices $A_1, \ldots, A_k$. Further, we have set $\bar{P}_{k,q^a} := (p_{i,j}^{q^a})_{i,j}$, where $\bar{P}_k = (p_{i,j})$. Then, $\bar{P}_{k,q}, \ldots, \bar{P}_{k,q^{\ell-1}}$ are easily recovered from $\bar{P}_k$. Thus, when we consider a key recovery attack using the lifting method, it is enough to treat only $\bar{P}_k$ ($k \in [m]$). Since the pull-back method is also to execute a key recovery attack on $\bar{P}_k$, we conclude that a key recovery attack using the pull-back method is the same as that using the lifting method. The only difference from the pull-back method is that we can apply the direct attack on the system of $\bar{L}^\top P_i \bar{L}$ ($i = 1, \ldots, m$) obtained by applying the lifting method. However, for most cases, this lifting direct attack is not more efficient than the plain direct attack, since the large finite field $\mathbb{F}_{q^\ell}$ disturbs guessing some variables in the hybrid approach.

4.4 Comparison of Complexity

For QR-UOV, the key recovery attacks can be performed on the following two problems:

- $\mathrm{UOV}(q, v, m, m)$,
- $\mathrm{UOV}(q^\ell, v/\ell, m/\ell, m)$,

where $\mathrm{UOV}(q, v, o, m)$ denotes the plain UOV with v vinegar variables, o oil variables, and m equations over $\mathbb{F}_q$. The first one is clearly enabled by ignoring the quotient ring structure of QR-UOV, and the second one is obtained by applying the transformations described in Subsection 4.1 and 4.2. This subsection theoretically compares the complexity of the key recovery attacks on $\mathrm{UOV}(q, v, m, m)$ and $\mathrm{UOV}(q^\ell, v/\ell, m/\ell, m)$.

From the complexity estimation in Subsection 2.2, the dominant part of the complexity estimation of the Kipnis-Shamir attack is q^{v-o}, and thus the complexities of the Kipnis-Shamir attack on $\mathrm{UOV}(q, v, m, m)$ and $\mathrm{UOV}(q^\ell, v/\ell, m/\ell, m)$ are asymptotically the same. Furthermore, in [9], they show that the rectangular MinRank attack originally proposed on Rainbow is applicable to QR-UOV. However, the rectangular MinRank attack is only applicable to $\mathrm{UOV}(q^\ell, v/\ell, m/\ell, m)$, not $\mathrm{UOV}(q, v, m, m)$, and thus we do not consider the rectangular MinRank attack here. From these points, in the following, we discuss the complexity of the reconciliation and intersection attacks.

Before comparing the complexity of the key recovery attacks, we prepare some assumptions for the following comparison. If we denote by $MQ(q, n, m)$ the complexity of solving the MQ problem of m equations in n variables over the finite field $\mathbb{F}_q$, we assume the following two points:

- If $n \le m_1 \le m_2$, then $MQ(q, n, m_1) \ge MQ(q, n, m_2)$.
- If $n \le m$ and $\ell \,|\, n$, m, then $MQ(q, n, m) \ge MQ(q^\ell, n/\ell, m/\ell)$.

The first statement holds because the MQ problem with parameters (q, n, m_2) can be reduced to the one with parameters (q, n, m_1) by simply ignoring $m_2 - m_1$ equations, and it does not affect the solutions with high probability. Further, we have the second statement because we can clearly solve the MQ problem with parameters $(q^\ell, n/\ell, m/\ell)$ as the one with parameters (q, n, m) by decomposing the given system into the base field $\mathbb{F}_q$.

Reconciliation Attack From the discussion in Subsection 2.2, the complexity of the reconciliation attack on UOV(q, v, m, m) can be given as $MQ\left(q, kv, \binom{k}{2}m\right)$ where this $k \geq 1$ is the minimum integer satisfying $kv \leq \binom{k}{2}m$. Similarly, the complexity of the reconciliation attack on UOV$(q^\ell, v/\ell, m/\ell, m)$ is estimated as $MQ\left(q^\ell, k'v/\ell, \binom{k'}{2}m\right)$ where this $k' \geq 1$ is the minimum integer satisfying $k'v/\ell \leq \binom{k'}{2}m$. Then, we clearly have $k \geq k'$ and thus

$$MQ\left(q^\ell, kv/\ell, \binom{k}{2}m\right) \geq MQ\left(q^\ell, k'v/\ell, \binom{k'}{2}m\right).$$

From the second assumption, we have

$$MQ\left(q, kv, \binom{k}{2}m\right) \geq MQ\left(q^\ell, kv/\ell, \binom{k}{2}m/\ell\right).$$

Then, from the first assumption, we have

$$MQ\left(q^\ell, kv/\ell, \binom{k}{2}m/\ell\right) \geq MQ\left(q^\ell, kv/\ell, \binom{k}{2}m\right).$$

In conclusion, from the above equations, we have

$$MQ\left(q, kv, \binom{k}{2}m\right) \geq MQ\left(q^\ell, k'v/\ell, \binom{k'}{2}m\right).$$

This indicates that the reconciliation attack is more efficient on UOV$(q^\ell, v/\ell, m/\ell, m)$ than on UOV(q, v, m, m). In practice, if $k, k' \geq 2$, then we can utilize the bilinear structure of the system to perform the attack efficiently. Even in the case where we utilize the bilinear structure, the reconciliation attack on UOV$(q^\ell, v/\ell, m/\ell, m)$ is more efficient from the same discussion.

Intersection Attack From the discussion in Subsection 2.2, if $v < 2m$, then the complexity of the reconciliation attack on UOV(q, v, m, m) can be given as $MQ\left(q, kv-(k-1)m, \binom{k+1}{2}m - 2\binom{k}{2}\right)$ where $k \leq v/(v-m)$. Similarly, the complexity of the reconciliation attack on UOV$(q^\ell, v/\ell, m/\ell, m)$ can be given as $MQ\left(q^\ell, kv/\ell-(k-1)m/\ell, \binom{k+1}{2}m - 2\binom{k}{2}\right)$ where $k \leq v/(v-m)$ in the case of $v < 2m$. Note that the conditions for the value k are the same between the above two settings. Then from a similar discussion as the case of the reconciliation attack, we have

$$\begin{aligned} &MQ\left(q, kv-(k-1)m, \binom{k+1}{2}m - 2\binom{k}{2}\right) \\ &\geq MQ\left(q^\ell, kv/\ell-(k-1)m/\ell, \binom{k+1}{2}m - 2\binom{k}{2}\right), \end{aligned}$$

and thus the intersection attack is more efficient on UOV$(q^\ell, v/\ell, m/\ell, m)$ than on UOV(q, v, m, m). For the case of $v \geq 2m$, we have the same conclusion from the same discussion.

5 Conclusion

In this paper, we analyze the security of the quotient ring UOV (QR-UOV) proposed at ASIACRYPT 2021. QR-UOV is a variant of UOV reducing the public key size compared with the plain UOV and has recently been submitted to the NIST additional call for digital signature schemes. For the QR-UOV scheme, there have been proposed two methods of recovering the secret key by using the quotient ring structure, the pull-back and lifting methods. In this study, we first prove that these two methods are essentially the same. More specifically, we show that smaller matrices over extension fields obtained by applying these two methods on block matrices with the QR-structure are the essentially same. Furthermore, we show that the key recovery attacks with these two methods over the extension field $\mathbb{F}_{q^\ell}$ are more efficient than the plain key recovery attacks over the base field $\mathbb{F}_q$.

Acknowledgements

This work was supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Number 22KJ0554 and 22K17889, Japan.

References

[1] Aumasson, J.-P., Bernstein, D. J., Beullens, W., Dobraunig, C., Eichlseder, M., Fluhrer, S., Gazdag, S.-L., Hülsing, A., Kampanakis, P., Kölbl, S., Lange, T., Lauridsen, M. M., Mendel, F., Niederhagen, R., Rechberger, C., Rijneveld, J., Schwabe, P., Westerbaan, B.: SPHINCS+ submission to the NIST post-quantum project, v.3. `https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022` (2020)

[2] Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Kyber algorithm specifications and supporting documentation (version 3.0). `https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022` (2020)

[3] Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium algorithm specifications and supporting documentation. `https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022` (2020)

[4] Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: EUROCRYPT 2021, LNCS, vol. 12696, pp. 348–373. Springer (2021)

[5] Beullens, W.: Breaking Rainbow takes a weekend on a laptop. In: CRYPTO 2022, LNCS, vol. 13508, pp. 464–479. Springer (2022)

[6] Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005)

[7] Ding, J., Yang, B., Chen, C.-O., Chen, M., Cheng, C.: New differential-algebraic attacks and reparametrization of Rainbow. In: ACNS 2008, LNCS, vol. 5037, pp. 242–257. Springer (2008)

[8] Fouque P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON: Fast-fourier lattice-based compact signatures over NTRU. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022 (2020)

[9] Furue, H., Ikematsu, Y.: A new security analysis against MAYO and QR-UOV using rectangular MinRank attack. In: IWSEC 2023, LNCS, vol. 14128, pp. 101–116. Springer (2021)

[10] Furue, H., Ikematsu, Y., Hoshino, F., Kiyomura, Y., Saito, T., Takagi, T.: Secure parameters for multivariate polynomial signature scheme QR-UOV. In: SCIS 2023, 1A1-4. http://crypto.mist.i.u-tokyo.ac.jp/publications/1A1-4.pdf (2023)

[11] Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T.: A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. In: ASIACRYPT 2021, LNCS, vol. 13093, pp. 187–217. Springer (2021)

[12] Garey, M.-R., Johnson, D.-S.: Computers and intractability: A guide to the theory of NP-completeness. W. H. Freeman (1979)

[13] Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999)

[14] Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998)

[15] Macario-Rat, G., Patarin, J., Cogliati, B., Faugère, J.-C., Fouque, P.-A., Gouin L., Larrieu, R., Minaud, B.: Rectangular attack on VOX. Cryptology ePrint Archive, Paper 2023/1822 (2023)

[16] NIST: Post-quantum cryptography CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[17] NIST: Status report on the second round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8309, NIST (2020)

[18] NIST: Status report on the third round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8413, NIST (2022)

[19] 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)

[20] Patarin, J., Cogliati, B., Faugère, J.-C., Fouque, P.-A., Gouin L., Larrieu, R., Macario-Rat, G., Minaud, B.: VOX specification v1.0. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/vox-spec-web.pdf (2023)

[21] PQC-forum. https://groups.google.com/a/list.nist.gov/g/pqc-forum?pli=1

[22] Shor, P. W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing **26**(5), pp. 1484–1509 (1997)

[23] Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced oil and vinegar. In: SAC 2019, LNCS, vol. 11959, pp. 574–588. Springer (2019)