SCIS 2025 2025 Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 28 – 31, 2025
The Institute of Electronics,
Information and Communication Engineers

NIST PQC Additional Signatures Second Round Candidate: QR-UOV

Hiroki Furue [*] Yasuhiko Ikematsu [†] Fumitaka Hoshino [‡] Tsuyoshi Takagi [§]
Haruhisa Kosuge [*] Kimihiro Yamakoshi [*] Rika Akiyama [*] Satoshi Nakamura [*]
Shingo Orihara [*] Koha Kinjo [*]

Abstract: The multivariate-based unbalanced oil and vinegar signature scheme (UOV) is one of the candidates for post-quantum cryptography (PQC). UOV is a well-established signature scheme owing to its short signature and fast performance, but 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 PQC standardization of additional digital signature schemes and recently selected as a second round candidate. In this work, we discuss the security points mentioned in the first round report of NIST. Furthermore, we provide a new method of the key recovery attacks on QR-UOV over the base fields utilizing the QR structure. We show that this proposed method is corresponding to existing attacks performed over the extension fields and does not reduce the security of QR-UOV compared with the previous estimation.

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 [26] 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 [21].

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 [14] and is 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) [17], 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. UOV is a well-established signature scheme owing to its short signature and fast performance. 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)* [12]. 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 $\mathbb{F}_q[t]/(f)$ with $f \in \mathbb{F}_q[t]$ 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 [27], which is the case for $f = t^\ell - 1$.

In 2022, NIST initiated the additional call for digital signature proposals [23] to be considered in the PQC standardization process. We submitted QR-UOV to this additional call in 2023 [11]. In this call, NIST expressed particular interest in signature schemes with short signatures and fast verification such as UOV. Indeed, NIST accepted 40 first-round candidates including 7 UOV-based schemes. In October 2024, NIST announced the selection of 14 signature algorithms as second-round candidates [24]. Among these 14 candidates, 4 schemes are UOV variants, UOV, QR-UOV, MAYO [5], SNOVA [28]. In the first round status re-

[*] NTT Social Informatics Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo, 180-8585, Japan. ({hiroki.furue, hrhs.kosuge, kimihiro.yamakoshi, rika.akiyama, satoshi.nakamura, shingo.orihara, kouha.kinjo}@ntt.com)

[†] 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)

[§] Department of Mathematical Informatics, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan. (takagi@g.ecc.u-tokyo.ac.jp)

port [24], they provide some comments to QR-UOV especially about its security and implementation. In this work, we discuss the security point mentioned in the report and show that QR-UOV is sufficiently secure against some cryptoanalysis methods recently proposed. Further, we show brief results of our new implementation.

Moreover, we provide a new method for key recovery attacks on QR-UOV. This method utilizes the QR structure used in QR-UOV, but it is performed over the base fields $\mathbb{F}_q$. By using this method, we can increase the number of public key matrices utilized in the key recovery attacks to $m \cdot \ell$ from the original m matrices. We also show that this proposed method is equivalent to the existing attacks on QR-UOV over the extension fields, called the pull-back and lifting methods. For this reason, the proposed method does not reduce the security of QR-UOV compared with the previous estimation.

Organization The rest of this paper is organized as follows: Section 2 recalls the construction of the plain UOV and QR-UOV. Section 3 explains the NIST PQC standardization of additional signatures and discusses the security and implementation of QR-UOV mentioned in the status report. Section 4 provides a new cryptoanalysis of QR-UOV and shows that it does not weaken the scheme. Finally, Section 5 is devoted to the conclusion.

2 Preliminaries

This section recalls the description of UOV [17] and QR-UOV [12] and some cryptoanalysis of these schemes.

2.1 UOV

This subsection describes the structure of UOV. 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 $\mathbf{x} = (x_1, \dots, x_n)$ over $\mathbb{F}_q$, we call $x_1, \dots, x_v$ *vinegar variables* and $x_{v+1}, \dots, x_n$ *oil variables.*

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

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

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 $a_1, \dots, a_v$ in $\mathbb{F}_q$ as the values of the vinegar variables. We can then easily solve the equation $\mathcal{F}(a_1, \dots, a_v, x_{v+1}, \dots, x_n) = \mathbf{y}$ for the oil variables $x_{v+1}, \dots, x_n$, because this is a linear system of m equations in m variables from the construction of the central map (1). If there is no solution to this equation, we choose new random values $a'_1, \dots, a'_v$, 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 some 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

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

2.2 Key Recovery Attacks on UOV

This subsection recalls some existing key recovery attacks on UOV, the Kipnis-Shamir [18], reconciliation [7], intersection [4], and rectangular MinRank [4] attacks. In this subsection, we describe the behavior of the key recovery attacks on 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

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

Kipnis-Shamir Attack The attack proposed by Kipnis and Shamir [18] chooses two invertible matrices W_i, W_j from the set of linear combinations of the representation matrices $P_1, \dots, P_m$ for the public key. Then, it probabilistically recovers an element 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 $y_1, \dots, y_k$ 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 $L_1, \dots, L_k$ be k invertible matrices randomly chosen from a set of linear combinations of the representation matrices $P_1, \dots, P_m$ for the public key. This attack then solves the following equations for $\mathbf{y} \in \mathbb{F}_q^n$:

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

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 $\mathcal{S}^{-1}(\mathcal{O})$.

Rectangular MinRank Attack The rectangular MinRank attack was originally proposed for the Rainbow scheme [6] by Beullens [4], and it tries to solve a new MinRank problem obtained by transforming the public key matrices of Rainbow. In [10], they show that the rectangular MinRank is applicable to UOV(q, v, o, m) with $v < m$ which is the case of the transformed QR-UOV over the extension fields.

Before describing the rectangular MinRank attack, we introduce a way of transforming sets of matrices used in the attack. Let $(G_1, \dots, G_m)$ be a set of n-by-n matrices over $\mathbb{F}_q$, and $\mathbf{g}_i^{(j)}$ denotes the j-th column vector of G_i, namely,

$$G_i = \begin{pmatrix} \mathbf{g}_i^{(1)} & \mathbf{g}_i^{(2)} & \cdots & \mathbf{g}_i^{(n)} \end{pmatrix} \in M_n(\mathbb{F}_q).$$

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

$$\begin{aligned} \tilde{G}_1 &:= \begin{pmatrix} \mathbf{g}_1^{(1)} & \mathbf{g}_2^{(1)} & \cdots & \mathbf{g}_m^{(1)} \end{pmatrix}, \\ \tilde{G}_2 &:= \begin{pmatrix} \mathbf{g}_1^{(2)} & \mathbf{g}_2^{(2)} & \cdots & \mathbf{g}_m^{(2)} \end{pmatrix}, \\ &\vdots \\ \tilde{G}_n &:= \begin{pmatrix} \mathbf{g}_1^{(n)} & \mathbf{g}_2^{(n)} & \cdots & \mathbf{g}_m^{(n)} \end{pmatrix}. \end{aligned}$$

Then, when we apply this deformation to $(P_1, \dots, P_m)$ and $(F_1, \dots, F_m)$, we have

$$(\tilde{P}_1, \dots, \tilde{P}_n) = (S^\top \tilde{F}_1, \dots, S^\top \tilde{F}_n) \cdot S.$$

For parameters with $v < m$, it is easily seen that the deformation matrices $\tilde{F}_{v+1}, \dots, \tilde{F}_n \in \mathbb{F}_q^{n \times m}$ are of rank $\le v$ since they have the following form:

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

Then, there exists a linear combination of $\tilde{P}_1, \dots, \tilde{P}_n \in \mathbb{F}_q^{n \times m}$ whose rank is $\le v$, and thus, as in Rainbow, the rectangular MinRank attack can be applied to UOV with $v < m$. As a result, the rectangular MinRank attack tries to find the vector $\mathbf{a} = (a_1, \dots, a_n)$ as a common solution to the following problems:

$$\begin{aligned} &\text{(i) Rank} \left(\sum_{i=1}^{n} a_i \tilde{P}_i \right) \le v, \\ &\text{(ii) } p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0. \end{aligned}$$

2.3 Description of QR-UOV

This subsection recalls the construction of QR-UOV mainly following the notation and description for the plain UOV in Subsection 2.1. 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 $\mathbb{F}_q[t]$ with $\deg f = \ell$. For any element g of the quotient ring $\mathbb{F}_q[t]/(f)$, we can uniquely define an $\ell \times \ell$ matrix Φ_g^f over $\mathbb{F}_q$ such that

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

For any $g \in \mathbb{F}_q[t]/(f)$, the matrix Φ_g^f can be represented by only ℓ elements in $\mathbb{F}_q$. We let the algebra of the matrices $A_f := \left\{ \Phi_g^f \in \mathbb{F}_q^{\ell \times \ell} \;\middle|\; g \in \mathbb{F}_q[t]/(f) \right\}$, 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 [12] 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 $t^\ell - at^i - 1$ with $a \neq 0$ and $1 \le i < \ell$, 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

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

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 $W^{(N)}A_f^{N,N} := \{A \cdot B \mid A \in W^{(N)}, B \in A_f^{N,N}\}$. Note that we here represent the public and secret keys by matrices as described in Subsection 2.1. We prepare an irreducible polynomial $f \in \mathbb{F}_q[t]$ with degree ℓ and $W \in \mathbb{F}_q^{\ell \times \ell}$ that symmetrizes every element of A_f. 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 $W^{(N)}A_f^{N,N}$ from Proposition 1 in [12]. The signing and verification processes are performed in the same way as the plain UOV.

2.4 Cryptoanalysis of QR-UOV

This subsection recalls the pull-back method which applies the key recovery attacks over the extension fields. Another way of performing the attacks over the extension fields is called the lifting method. It is shown that these two methods are equivalent in [11].

We here introduce a one-to-one map representing the keys of QR-UOV as those of the plain UOV over $\mathbb{F}_q[t]/(f) \cong \mathbb{F}_{q^\ell}$. In the pull-back method, after applying this transformation, we perform 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 $\bar{P}_k^{(0)}, \ldots, \bar{P}_k^{(\ell-1)} \in \mathbb{F}_q^{N \times N}$ satisfying

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

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:

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

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

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

$$S = \sum_{i=0}^{\ell-1} \left(\bar{S}^{(i)} \otimes \Phi_{t^i}^f \right) \Rightarrow \bar{S} = \sum_{i=0}^{\ell-1} t^i \bar{S}^{(i)}.$$

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 $\mathbb{F}_{q^\ell}$.

3 NIST PQC Second Round Selection

This section confirms comments to QR-UOV given in the NIST status report [24] and discusses the security and implementation mentioned in the report.

3.1 NIST PQC Additional Call

This subsection roughly summarizes the NIST PQC additional call for digital signatures [23], to which the QR-UOV scheme is submitted.

NIST has initiated a PQC standardization project [21] since 2016, and in 2022 they selected some algorithms to be standardized [22]. 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. In 2022, NIST has called for additional digital signature proposals [23] to select schemes based on different mathematical problems, and NIST announced that 40 submissions were accepted as first round candidates in July 2023. NIST recently announced the selection of 14 signature schemes as second round candidates [24].

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 performance. Indeed, 7 schemes out of the 40 accepted first-round submissions are UOV variants, and 4 schemes, UOV, QR-UOV, MAYO, and SNOVA, out of the 14 second round candidates are UOV variants. Among these UOV-based schemes, QR-UOV is considered to be a promising candidate due to its small public key and simple construction.

In the status report of NIST [24], they provide the following comments to QR-UOV:

> *A previous attempt that relied on quotient rings was broken [13], and another candidate in the Additional Call for Digital Signatures that incorporated the same technique was also attacked [9, 15].*
>
> *NIST maintains interest in QR-UOV for its competitive performance, but the structure of QR-UOV requires further study. NIST anticipates that the performance could be improved and encourages the designers to further optimize their implementation.*

The subsections below discuss the security and implementation of QR-UOV pointed out in the above comments.

3.2 Security Analysis of QR Structure

As mentioned in Subsection 3.1, NIST's report to the first round candidates expresses their concerns about the security of the quotient ring structure of QR-UOV. As seen in [11], the security of QR-UOV can be reduced to the following two problems, the UOV and QR-MQ problems. The UOV problem asks to distinguish randomized quadratic systems and UOV public key systems. The QR-MQ problem asks to find a solution to the MQ problem with the quotient ring structure. Indeed, most of attacks [9, 15, 16, 19] recently proposed to some UOV-based candidates are key-recovery attacks. We clearly reveal that the key recovery attacks on QR-UOV can be reduced to those on the plain UOV with specific parameters. Therefore, we think that the proposed parameters of QR-UOV will be secure against key recovery attacks unless a new efficient attack on the plain UOV is proposed. Note that our proposed parameter sets of the first round remain secure up to the present time, and this fact indicates the reliability of our parameter sets of QR-UOV.

In the following, we claim that QR-UOV is secure against some attacks mentioned in the status report.

Attack on BAC-UOV [13] Block Anti Circulant (BAC) UOV [27] is a UOV variant using BAC matrices as public key. Furue et al. [13] show that the public key matrices of BAC-UOV can be decomposed into two smaller parts, and we can apply some existing attacks on smaller UOV public keys. We proposed our QR-UOV by generalizing this BAC-UOV. Indeed, we can regard BAC-UOV as a variant of QR-UOV with $f = t^\ell - 1$. As mentioned in [12], we can apply the decomposition used in [13] to QR-UOV in the case of f is a reducible polynomial. On the other hand, we prove that there exists no such a decomposition in the case where f is irreducible (See [12]), and thus QR-UOV is secure against the attack on BAC-UOV.

Comment on VOX [9] In [10], they show that the rectangular MinRank attack originally proposed on Rainbow is applicable to some UOV variants such as QR-UOV and MAYO. In the above comment on the security of VOX [25] in PQC forum, it is pointed out that the rectangular MinRank attack is also applicable to the first round parameter sets of VOX and it significantly reduces the security level of the parameters. For QR-UOV, we originally chose our parameter sets considering the rectangular MinRank attack. Thus, this attack does not affect the parameters of QR-UOV.

Attack on VOX [15] After the above comment on VOX is announced, the parameters of VOX are revised such that the rectangular MinRank attack cannot be applied to the new parameters [20]. However, Guo et al. [15] proposed a new MinRank attack on VOX and showed that the revised parameter sets of VOX can be broken with smaller complexities than the claimed security levels. This attack is constructed by improving the original rectangular MinRank attack and enables us to apply the MinRank attack to VOX by padding the target matrices. On the other hand, we can apply the original rectangular MinRank attack to QR-UOV and it does not weaken the security as mentioned above. We can also use the padding method against QR-UOV, but it will not make the MinRank attack more efficient. This is the reason that the attack proposed by Guo et al. does not weaken the security of the parameters of QR-UOV.

Table 1: Comparison of timing data on the NIST reference platform (Mcycles) of the parameter $(q, v, m, \ell) = (127, 156, 54, 3)$ with the security level I between the first round version and our new implementation

parameters	keygen	sign	verify
First Round	16.700	13.419	10.575
New	10.061	1.920	1.589

3.3 Performance Improvements

As seen in Subsection 3.1, the report of NIST [24] also mentioned the implementation of QR-UOV. In response to this comment, we improve our implementation from the first round versions. Indeed, Table 1 shows that the timing data can be significantly reduced from the original implementation.

4 Key Recovery Attacks on QR-UOV

This section proposes a new method applying the key recovery attacks on QR-UOV using the QR structure over the base fields. Further, we compare the efficiency of the proposed method with the existing attacks over the extension fields.

4.1 Attacks Using Quotient-Ring Structure

This subsection provides a new way of recovering the secret key of QR-UOV over the base fields $\mathbb{F}_q$. This method is mainly derived from the technique used in the attack on SNOVA [16].

We here provide a way of increasing the number of public key equations. When we multiply $(\Phi_t^f)^{(N)} \in \mathbb{F}_q^{n\times n}$ to public key matrices P_i with $1 \leq i \leq m$ from the right side, then we have

$$\begin{aligned} P_i(\Phi_t^f)^{(N)} &= S^\top F_i S(\Phi_t^f)^{(N)} \\ &= S^\top F_i(\Phi_t^f)^{(N)} S, \end{aligned}$$

due to the commutativity of Φ_g^f with $g \in \mathbb{F}_q[t]/(f)$. Since $(\Phi_t^f)^{(N)}$ is a block diagonal matrix, $F_i(\Phi_t^f)^{(N)}$ also has the secret key structure, i.e., the lower-right $m \times m$ submatrix of $F_i(\Phi_t^f)^{(N)}$ is a zero matrix as in the original F_i. Note that if we multiply ${(\Phi_t^f)^{(N)}}^\top$ from the left side, then we have the same matrix as $P_i(\Phi_t^f)^{(N)}$

as follows:

$$\begin{aligned}(\Phi_t^f)^{(N)^\top} P_i &= (\Phi_t^f)^{(N)^\top} S^\top W^{(N)} \bar{F}_i S \\ &= S^\top (\Phi_t^f)^{(N)^\top} W^{(N)} \bar{F}_i S \\ &= S^\top W^{(N)} (\Phi_t^f)^{(N)} \bar{F}_i S \\ &= S^\top W^{(N)} \bar{F}_i (\Phi_t^f)^{(N)} S,\end{aligned}$$

where $F_i = W^{(N)} \bar{F}_i \in W^{(N)} A_f^{(N)}$.

From these discussions, we can use $m \cdot \ell$ matrices $P_i(\Phi_{t^j}^f)^{(N)}$ with $1 \leq i \leq m$ and $0 \leq j \leq \ell - 1$ as public key matrices when we apply the key recovery attacks. Here, for each P_i with $1 \leq i \leq m$, we can only utilize ℓ matrices $P_i(\Phi_{t^j}^f)^{(N)}$ with $0 \leq j \leq \ell - 1$. This is because $\Phi_{t^\ell}^f$ can be seen as an element of the $\mathbb{F}_q$-space spanned by $\{\Phi_{t^j}^f\}_{0 \leq j \leq \ell-1}$ and we have

$$(\Phi_{t^a}^f)^{(N)^\top} P_i (\Phi_{t^b}^f)^{(N)} = P_i (\Phi_{t^{a+b}}^f)^{(N)}.$$

By applying this method, we can use more equations to recover the secret key than the original attack on the base field. In Subsection 4.2 below, we will discuss its efficiency.

4.2 Relation with Attacks over Extension Fields

As mentioned in Subsection 2.4, we can apply the key recovery attacks over extension fields $\mathbb{F}_{q^\ell}$ on QR-UOV. This subsection shows that the proposed method in Subsection 4.1 can be seen as attacks obtained by naturally transforming the attack over $\mathbb{F}_{q^\ell}$ to the base field $\mathbb{F}_q$.

In the attack over $\mathbb{F}_{q^\ell}$ in Subsection 2.4, we use public key matrices $\bar{P}_i$ $(1 \leq i \leq m)$ with size N-by-N over the extension field $\mathbb{F}_{q^\ell}$. For variables $\bar{\mathbf{x}} \in \mathbb{F}_{q^\ell}^N$, these public key matrices bring us m equations

$$\bar{\mathbf{x}}^\top \bar{P}_i \bar{\mathbf{x}} = 0 \quad (1 \leq i \leq m). \tag{6}$$

We can clearly transform these equations into equations with n variables and $m \cdot \ell$ equations over the base field $\mathbb{F}_q$. More specifically, for $\mathbf{x} \in \mathbb{F}_q^n$ obtained by naturally transforming $\bar{\mathbf{x}}$, there exist ℓ matrices $P_i^{(1)}, \ldots, P_i^{(\ell)} \in \mathbb{F}_q^{n \times n}$ satisfying

$$\bar{\mathbf{x}}^\top \bar{P}_i \bar{\mathbf{x}} = \sum_{j=1}^{\ell} t^{j-1} \mathbf{x}^\top P_i^{(j)} \mathbf{x}. \tag{7}$$

In the following theorem, we show the equivalency between the space spanned by equations obtained from $P_i^{(j)}$ described in the above equation and obtained from $P_i(\Phi_{t^j}^f)^{(N)}$ described in Subsection 4.1.

Theorem 1. *For each public key matrix P_i of QR-UOV with $1 \leq i \leq m$, the $\mathbb{F}_q$-space spanned by ℓ equations over $\mathbb{F}_q$ naturally obtained from equation* (6) *as above is equal to the $\mathbb{F}_q$-space spanned by equations $\left\{\mathbf{x}^\top P_i (\Phi_{t^j}^f)^{(N)} \mathbf{x} = 0\right\}_{0 \leq j \leq \ell-1}$.*

Proof. *The above space obtained from equation* (6) *is equal to the space spanned by*

$$\left\{(\bar{x}_{\mathrm{mat}}^\top P_i \bar{x}_{\mathrm{mat}})_{1,j} = 0\right\}_{1 \leq j \leq \ell},$$

where $\bar{x}_{\mathrm{mat}} \in \mathbb{F}_q^{n \times \ell}$ is obtained by transforming each element $\bar{x}_i$ of $\bar{\mathbf{x}}$ into $\Phi_{\bar{x}_i}^f$. This is because

$$\bar{x}_{\mathrm{mat}}^\top P_i \bar{x}_{\mathrm{mat}} = W \Phi_{\bar{\mathbf{x}}^\top \bar{P}_i \bar{\mathbf{x}}}^f,$$

and $W \Phi_{\bar{\mathbf{x}}^\top \bar{P}_i \bar{\mathbf{x}}}^f$ is symmetric. We then have

$$(\bar{x}_{\mathrm{mat}}^\top P_i \bar{x}_{\mathrm{mat}})_{1,j} = \mathbf{x}^\top P_i (\Phi_{t^j}^f)^{(N)} \mathbf{x},$$

with $1 \leq j \leq \ell$ from the definition of Φ_*^f, and thus we have the above statement. □

From the above theorem, we confirm that $m \cdot \ell$ matrices used in the proposed method in Subsection 4.1 can be seen as the base field version of the public key matrices over $\mathbb{F}_q^\ell$ used in the method in Subsection 2.4. This fact indicates that the proposed method is not more effective than the original pull-back method against QR-UOV.

We here do not discuss the details, but in the framework of each key recovery attack, the proposed method can be seen as a variant of the method over the extension field. For example, in the case of the reconciliation attack, this statement is directly derived from the above theorem. In general, solving quadratic systems over extension fields after transforming them into base fields is not more efficient than the original case. This is because we cannot utilize the structure of extension fields if we transform the systems into base fields. As a result, the proposed method does not weaken the security of QR-UOV from the previous analysis.

5 Conclusion

QR-UOV is a UOV variant with the quotient ring structure reducing the public key size and has been selected as a second round candidate for the NIST PQC standardization of additional signatures. In this work, we first check comments to QR-UOV given by NIST and discuss the security and implementation mentioned in the first round report. We recall that the security of QR-UOV against key recovery attacks can be reduced to that of the plain UOV with specific parameters. Thus, we claim that the proposed parameters of QR-UOV are secure against some key recovery attacks on UOV variants recently proposed. Furthermore, we provide a new method of the key recovery attacks on QR-UOV over the base fields utilizing the QR structure. We show that this proposed method is equivalent to the previous attacks performed over the extension fields and thus does not reduce the security of QR-UOV compared with the previous estimation.

Acknowledgements

This work was supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Numbers JP22K17889, JP24K02939.

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., et al.: 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.: MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In: SAC 2021, LNCS, vol. 13203, pp. 355–376. Springer (2021)

[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] Round 1 (Additional Signatures) OFFICIAL COMMENT: VOX. NIST PQC Forum. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/VOX-round1-dig-sig-official-comment.pdf (2023)

[10] 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)

[11] Furue, H., Ikematsu, Y., Hoshino, F., Takagi, T., Yasuda, K., Miyazawa, T., Saito, T., Nagai, A.: Name of proposal: QR-UOV. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/qruov-spec-web.pdf

[12] 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)

[13] Furue, H., Kinjo, K., Ikematsu, Y., Wang, Y., Takagi, T.: A structural attack on block-anti-circulant UOV at SAC 2019. In: PQCrypto 2020, LNCS, vol. 12100, pp. 323–339. Springer (2020)

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

[15] Guo, H., Jin, Y., Pan, Y., He, X., Gong, B., Ding, J.: Practical and theoretical cryptanalysis of VOX. In: PQCrypto 2024: LNCS, vol. 14772, pp. 186–208. Springer (2024)

[16] Ikematsu, Y., Akiyama, R.: Revisiting the security analysis of SNOVA. In: APKC@AsiaCCS 2024, pp. 54–61. ACM (2024)

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

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

[19] Li, P., Ding, J.: Cryptanalysis of the SNOVA signature scheme. In: PQCrypto 2024, LNCS, vol. 14772, pp. 79–91. Springer (2024)

[20] 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)

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

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

[23] 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)

[24] NIST: Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8528.pdf (2024)

[25] 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)

[26] 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)

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

[28] Wang L.-C., Chou, C.-Y., Ding, J., Kuan, Y.-L., Li, M.-S., Tseng, B.-S., Tseng, P.-E., Wang, C.-C.: SNOVA: Proposal for NISTPQC: Digital signature schemes project. https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/SNOVA-spec-web.pdf (2023)