A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV

Hiroki Furue[1], Yasuhiko Ikematsu[2], Yutaro Kiyomura[3], and Tsuyoshi Takagi[1]

[1] The University of Tokyo, Tokyo, Japan
[2] Kyushu University, Fukuoka, Japan
[3] NTT Secure Platform Laboratories, Tokyo, Japan

Abstract. The unbalanced oil and vinegar signature scheme (UOV) is a multivariate signature scheme that has essentially not been broken for over 20 years. However, it requires the use of a large public key, so various methods have been proposed to reduce its size. In this paper, we propose a new variant of UOV with the public key represented by block matrices whose components are represented as an element of a quotient ring. We discuss how the irreducibility of the polynomial used to generate the quotient ring affects the security of our proposed scheme. Furthermore, we propose parameters for our proposed scheme and discuss their security against currently known and possible attacks. We show that our proposed scheme can reduce the public key size without significantly increasing the signature size compared with other UOV variants. For example, the public key size of our proposed scheme is 66.7 KB for NIST's Post-Quantum Cryptography Project (security level 3), while that of cyclic Rainbow is 252.3 KB, where Rainbow is a variant of UOV and one of the third round finalists of NIST PQC project.

Keywords: post-quantum cryptography, multivariate public key cryptography, unbalanced oil and vinegar, quotient ring.

1 Introduction

Currently used public key cryptosystems, e.g., RSA and ECC, can be broken in polynomial time using a quantum computer executing Shor's algorithm [30]. There has thus been growing interest in post-quantum cryptography (PQC), which is secure against quantum computing attacks. Research on PQC has thus been accelerating, and the U.S. National Institute for Standards and Technology (NIST) has initiated a PQC standardization project [22].

Multivariate public key cryptography (MPKC), which is based on the difficulty of solving a system of multivariate quadratic polynomial equations over a finite field (the multivariate quadratic ($\mathcal{MQ}$) problem), is regarded as a strong candidate for PQC. The $\mathcal{MQ}$ problem is NP-complete [17] and is thus likely to be secure in the post-quantum era.

The unbalanced oil and vinegar signature scheme (UOV) [19], a multivariate signature scheme proposed by Kipnis et al. at EUROCRYPT 1999, has withstood various types of attacks for about 20 years. UOV is a well-established signature scheme due to its short signature and short execution time. Rainbow [11], a multi-layer UOV variant, was selected as a third-round finalist in the NIST PQC project [25]. However, both UOV and Rainbow have public keys that are much larger than those of other PQC candidates, e.g., lattice-based signature schemes. Indeed, Rainbow has the largest public key among the third-round-finalist signature schemes, and NIST's report [25] states that Rainbow is not suitable as a general-purpose signature scheme due to this problem.

On the other hand, the CRYSTALS-DILITHIUM [21] lattice-based signature scheme is also a third-round finalist in the NIST PQC project. It is based on the hardness of the module learning with errors (MLWE) problem [7]. As is well known, LWE [28] is a confidential hard problem in cryptography, and the MLWE problem is a generalization of it using a module consisting of vectors over a ring. This illustrates that a natural way to develop an efficient multivariate scheme with a small public key is to improve confidential schemes such as UOV and Rainbow in MPKC by investigating further algebraic theory.

There are three main research approaches to developing a UOV variant with a small public key. One is to use the compression technique developed by Petzoldt et al. [26]. This technique can be applied to various UOV variants and is based on the fact that part of a public key can be chosen arbitrarily before determining the secret key. This means that part of a public key can be generated using a seed of a pseudo random number generator. This reduces the size of the public key substantially. The version of Rainbow using this technique is called "cyclic Rainbow." The second approach is to use the lifted unbalanced oil and vinegar (LUOV) [5], which uses polynomials over a small field as a public key, whereas the signature and message space are defined over an extension field. This results in a small public key. LUOV was thus selected as one of the candidates in the second round of the NIST PQC project [24]. However, several of its parameters were broken using a new attack proposed by Ding et al. [13]. The third approach is to use the block-anti-circulant UOV (BAC-UOV) developed by Szepieniec et al. and presented at SAC 2019 [31]. Its public key is represented by block-anti-circulant matrices in which every block is an anti-circulant matrix. Since such a matrix can be constructed by its first-row vector, BAC-UOV has a smaller public key. However, the public key has a special structure; that is, the block-anti-circulant-matrices can be transformed into the diagonal concatenation of two smaller matrices. This enabled Furue et al. [16] to devise a structural attack on BAC-UOV that has less complexity than the asserted one. The attack is based on the fact that the anti-circulant matrices with size ℓ used in BAC-UOV can be represented using an element of the quotient ring $\mathbb{F}_q[x]/(x^\ell - 1)$, where $\mathbb{F}_q$ is a finite field, and $x^\ell - 1$ is reducible.

Our Contribution In this paper, we present a new UOV variant using an arbitrary quotient ring that is called QR-UOV. In the QR-UOV, a public key is represented by block matrices in which every component corresponds to an element of a quotient ring $\mathbb{F}_q[x]/(f)$. More precisely, we use an injective ring homomorphism from the quotient ring $\mathbb{F}_q[x]/(f)$ to the matrix ring $\mathbb{F}_q^{\ell\times\ell}$, where $f \in \mathbb{F}_q[x]$ is a polynomial with $\deg f = \ell$. In this paper, the image Φ_g^f of the homomorphism for $g \in \mathbb{F}_q[x]/(f)$ is called the *polynomial matrix* of g. From this homomorphism, we can compress the ℓ^2 components in Φ_g^f to ℓ elements in $\mathbb{F}_q$ since the polynomial matrix Φ_g^f is determined by the ℓ coefficients of g. Note that this can be considered as a generalization of BAC-UOV [31], which is the case of $f = x^\ell - 1$. Utilizing elements of a quotient ring in block matrices is similar to the MLWE problem [7] since the MLWE problem uses elements of a ring in vectors. Namely, we can consider that the research undertaken to get from UOV to QR-UOV (including BAC-UOV) corresponds to that to get from LWE to MLWE. Therefore, as with the MLWE problem, this kind of research deserves more than passing notice.

To construct the QR-UOV, we need to consider the symmetry of polynomial matrices Φ_g^f. In UOV, the public key $\mathcal{P} = (p_1, \ldots, p_m)$, which consists of quadratic polynomials p_i, is obtained by composing a central map $\mathcal{F} = (f_1, \ldots, f_m)$ and a linear map $\mathcal{S}$; that is, $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$. Then the corresponding matrices $P_1, \ldots, P_m$ of the public key $\mathcal{P}$ are given by $P_i = S^\top F_i S$, where $F_1, \ldots, F_m$ and S are matrices corresponding to $\mathcal{F}$ and $\mathcal{S}$, respectively. If we choose $F_1, \ldots, F_m$ and S as block matrices in which the components are polynomial matrices Φ_g^f, the polynomial matrices must be stable under the transpose operation; namely $(\Phi_g^f)^\top = \Phi_{g'}^f$ for some g'. Otherwise $P_1, \ldots, P_m$ are not block matrices of Φ_g^f, and we cannot reduce the public key size using them. Note that polynomial matrices Φ_g^f are not stable under the transpose operation in general, so we cannot directly use polynomial matrices Φ_g^f to construct an efficient UOV variant. To solve this problem, we introduce the concept of an $\ell \times \ell$ invertible matrix W such that $W\Phi_g^f$ is symmetric for any $g \in \mathbb{F}_q[x]/(f)$; that is, $W\Phi_g^f$ is stable under the transpose operation. In Proposition 1, we prove that there exist such W for various quotient rings $\mathbb{F}_q[x]/(f)$. Therefore, from equations

$$(W\Phi_{g_1}^f)^\top (\Phi_{g_2}^f W^{-1}) W\Phi_{g_3}^f = (W\Phi_{g_1}^f)(\Phi_{g_2}^f W^{-1}) W\Phi_{g_3}^f = W\Phi_{g_1 g_2 g_3}^f,$$

we can construct a UOV variant using the quotient ring $\mathbb{F}_q[x]/(f)$ by choosing $F_1, \ldots, F_m$ as block matrices using $\Phi_g^f W^{-1}$ and S as a block matrix using $W\Phi_g^f$.

Moreover, we need to consider how the choice of f affects the security of QR-UOV. Furue et al. [16] broke BAC-UOV by transforming its anti-circulant matrices into diagonal concatenations of two smaller matrices. This transformation is obtained from the decomposition $x^\ell - 1 = (x-1)(x^{\ell-1} + \cdots + 1)$. Therefore, we investigate the relationship between the irreducibility of the polynomial f used to generate the quotient ring $\mathbb{F}_q[x]/(f)$ and the existence of such a transformation for symmetric matrices $W\Phi_g^f$. In Theorem 1, we show that, if f is irreducible, there does not exist such a transformation for matrices $W\Phi_g^f$, which means that such an f has resistance against Furue et al.'s structural attack [16].

On the basis of these considerations about the symmetry of $W\Phi_g^f$ and the choice of f, we derive our quotient-ring UOV (QR-UOV). It uses $\mathbb{F}_q[x]/(f)$ generated by an irreducible polynomial f, which is resistant to Furue et al.'s structural attack [16]. We investigate its performance against both currently known and possible attacks. The currently known attacks include the direct attack, the UOV attack [20], and the reconciliation attack [12]. The possible attacks include pull-back attacks and lifting attacks. In the pull-back attacks, the UOV attack and the reconciliation attack are executed over the quotient ring $\mathbb{F}_q[x]/(f)$ by pulling $W\Phi_g^f$ back to g. In the lifting attacks, we use an extension field $\mathbb{F}_{q^\ell}$. We prove that the QR-UOV public key can be transformed into the diagonal concatenation of some smaller matrices over the extension field $\mathbb{F}_{q^\ell}$ as is done in the structural attack on BAC-UOV. After applying the above transformation over $\mathbb{F}_{q^\ell}$, we can execute the three currently known attacks.

Finally, by considering these currently known and possible attacks, we can select appropriate parameters for QR-UOV. In accordance with the I, III, and V security levels of the NIST PQC project [23], we propose three parameters for QR-UOV. Using these parameters reduces the size of the QR-UOV public key size about 50–70% compared to that of cyclic Rainbow with updated parameters [27]. For example, the public key size is 66.7 KB for security level III, whereas that of cyclic Rainbow is 252.3 KB. The signature sizes with the proposed parameters are almost the same as those of Rainbow except for security level I.

Organization Our paper is organized as follows. In Section 2, we explain the construction of multivariate signature schemes, plain UOV, BAC-UOV, and an attack on BAC-UOV. In Section 3, we introduce polynomial matrices of a quotient ring as a generalization of circulant matrices. In Section 4, we describe our proposed signature scheme, QR-UOV. In Section 5, we analyze the security of our proposed scheme. We present our proposed parameters and compare the performance of our scheme with that of Rainbow in Section 6. We conclude the paper in Section 7 by summarizing the key points and suggesting possible future work.

2 Preliminaries

In this section, we first explain the $\mathcal{MQ}$ problem and general signature schemes that are based on this problem. Next, we review the construction of the UOV [19]. We then describe the construction of the BAC-UOV [31] and finally explain Furue et al.'s structural attack [16] on BAC-UOV.

2.1 Multivariate Signature Schemes

Let $\mathbb{F}_q$ be a finite field with q elements and n and m be two positive integers. For a system of quadratic polynomials $\mathcal{P} = (p_1(x_1,\ldots,x_n),\ldots,p_m(x_1,\ldots,x_n))$ in n variables over $\mathbb{F}_q$ and $\mathbf{y} \in \mathbb{F}_q^m$, the problem of finding a solution $\mathbf{x} \in \mathbb{F}_q^n$ to $\mathcal{P}(\mathbf{x}) = \mathbf{y}$ is called the $\mathcal{MQ}$ problem. Garey and Johnson [17] proved that this problem is NP-complete if $n \approx m$, so it is considered to have the potential to resist quantum computer attacks.

Next, we briefly explain the construction of general multivariate signature schemes. First, an easily invertible quadratic map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, called a *central map* is generated. Next, two invertible linear maps $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ are randomly chosen in order to hide the structure of $\mathcal{F}$. The public key $\mathcal{P}$ is then given as a polynomial map:

$$\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m. \tag{1}$$

The secret key consists of $\mathcal{T}$, $\mathcal{F}$, and $\mathcal{S}$. The signature is generated as follows: Given a message $\mathbf{m} \in \mathbb{F}_q^m$ to be signed, compute $\mathbf{m}_1 = \mathcal{T}^{-1}(\mathbf{m})$ and find a solution $\mathbf{m}_2$ to the equation $\mathcal{F}(\mathbf{x}) = \mathbf{m}_1$. This gives a signature $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{m}_2) \in \mathbb{F}_q^n$ for the message. Verification is done by confirming whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$ or not.

2.2 Unbalanced Oil and Vinegar Signature Scheme

Let v be a positive integer 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*. In the UOV scheme, a central map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is designed such that each f_k $(k = 1, \ldots, m)$ is a quadratic polynomial of the form

$$f_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{v} \alpha_{i,j}^{(k)} x_i x_j\,, \tag{2}$$

where $\alpha_{i,j}^{(k)} \in \mathbb{F}_q$. A linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is then randomly chosen. Next, the public key map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is computed using $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$. The linear map $\mathcal{T}$ in equation (1) is not needed since it does not help to hide the structure of $\mathcal{F}$. The secret key thus consists of $\mathcal{F}$ and $\mathcal{S}$.

Next, we explain the inverting of the central map $\mathcal{F}$. Given $\mathbf{y} \in \mathbb{F}_q^m$, we first choose random values $a_1, \ldots, a_v$ in $\mathbb{F}_q$ to be the vinegar variables. Then, we can efficiently obtain a solution $(a_{v+1}, \ldots, a_n)$ for the equation $\mathcal{F}(a_1, \ldots, a_v, x_{v+1}, \ldots, x_n) = \mathbf{y}$ since this is a linear system of m equations in m oil variables. If there is no solution to this equation, we choose new random values $a_1', \ldots, a_v'$ and repeat the procedure. Eventually, we obtain a solution $\mathbf{x} = (a_1, \ldots, a_v, a_{v+1}, \ldots, a_n)$ to $\mathcal{F}(\mathbf{x}) = \mathbf{y}$. In this manner, we execute the signing process explained in Subsection 2.1.

We assume that the characteristic of $\mathbb{F}_q$ is odd in the following. For each $1 \le i \le m$, there exists an $n \times n$ symmetric matrix F_i such that $f_i(\mathbf{x}) = \mathbf{x} \cdot F_i \cdot \mathbf{x}^\top$. From equation (2), this F_i has the form

$$\begin{pmatrix} *_{v\times v} & *_{v\times m} \\ *_{m\times v} & 0_{m\times m} \end{pmatrix}. \tag{3}$$

Let P_i $(i = 1, \ldots, m)$ be $n \times n$ symmetric matrices P_i such that $p_i(\mathbf{x}) = \mathbf{x} \cdot P_i \cdot \mathbf{x}^\top$. Then, taking the $n \times n$ matrix S such that $\mathcal{S}(\mathbf{x}) = S \cdot \mathbf{x}^\top$, we have

$$P_i = S^\top F_i S, \ \ (i = 1, \ldots, m) \tag{4}$$

from $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$. We call F_i and P_i the representation matrices of f_i and p_i, respectively.

2.3 Block-Anti-Circulant UOV

As mentioned above, the block-anti-circulant (BAC) UOV [31] is a variant of UOV. The public key is shortened by representing it with block-anti-circulant matrices. In this subsection, we describe the construction of BAC-UOV.

A circulant matrix is a matrix in which each row vector is rotated one element to the right relative to the preceding row vector. An anti-circulant matrix is a matrix in which each row vector is rotated one element to the left relative to the preceding row vector. A circulant matrix X and an anti-circulant matrix Y with size ℓ take the following forms:

$$X = \begin{pmatrix} a_0 & a_1 & \dots & a_{\ell-2} & a_{\ell-1} \\ a_{\ell-1} & a_0 & \dots & a_{\ell-3} & a_{\ell-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \dots & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{\ell-1} & a_0 \end{pmatrix}, Y = \begin{pmatrix} a_0 & a_1 & \dots & a_{\ell-2} & a_{\ell-1} \\ a_1 & a_2 & \dots & a_{\ell-1} & a_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{\ell-2} & a_{\ell-1} & \dots & a_{\ell-4} & a_{\ell-3} \\ a_{\ell-1} & a_0 & \dots & a_{\ell-3} & a_{\ell-2} \end{pmatrix}.$$

In addition, a matrix is called a block-circulant matrix A or a block-anti-circulant matrix B with block size ℓ if every $\ell \times \ell$ block in A or B is a circulant matrix or an anti-circulant matrix, as follows ($N \in \mathbb{N}$):

$$A = \begin{pmatrix} X_{11} & \dots & X_{1N} \\ \vdots & \ddots & \vdots \\ X_{N1} & \dots & X_{NN} \end{pmatrix}, B = \begin{pmatrix} Y_{11} & \dots & Y_{1N} \\ \vdots & \ddots & \vdots \\ Y_{N1} & \dots & Y_{NN} \end{pmatrix},$$

where X_{ij} is an $\ell \times \ell$ circulant matrix, and Y_{ij} is an $\ell \times \ell$ anti-circulant matrix. For these block matrices, it holds that the products AB and BA are block-anti-circulant matrices.

In BAC-UOV, the number of vinegar variables v and the number of equations m are set to be divisible by block size ℓ. The representation matrices $F_1, \dots, F_m$ for the central map $\mathcal{F}$ are chosen as block-anti-circulant matrices with block size ℓ, and the matrix S for the linear map $\mathcal{S}$ is chosen as a block-circulant matrix with block size ℓ. The representation matrices $P_1, \dots, P_m$ for the public key $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$ are computed using $P_i = S^\top F_i S$ ($i = 1, \dots, m$) and are block-anti-circulant matrices.

Due to the structure of block-anti-circulant matrices, the $n \times n$ matrices $P_1, \dots, P_m$ can be represented by using only the first row of each block. Therefore, they can be represented by using only mn^2/ℓ elements in the finite field $\mathbb{F}_q$, which is one ℓ-th the size of the public key of plain UOV. That is, the public key is smaller than that of plain UOV.

2.4 Structural Attack on BAC-UOV

In 2020, Furue et al. proposed an attack on BAC-UOV that breaks the security of the proposed parameter sets [16]. The attack utilizes the property of the anti-circulant matrix that the sum of the elements of one row (column) is the same as those of the other rows (columns).

We define an $\ell \times \ell$ matrix L_ℓ such that $(L_\ell)_{1i} = (L_\ell)_{i1} = 1\,(1 \leq i \leq \ell)$, $(L_\ell)_{ii} = -1\,(2 \leq i \leq \ell)$ and the other elements are equal to 0, where for a matrix A, $(A)_{ij}$ denotes the ij-element of A, namely:

$$L_\ell := \ell \left\{ \overbrace{\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & -1 & & \\ \vdots & & \ddots & \\ 1 & & & -1 \end{pmatrix}}^{\ell} \right. .$$

Then, for an $\ell \times \ell$ anti-circulant matrix Y, we have

$$L_\ell^\top Y L_\ell = \begin{pmatrix} *_{1\times 1} & 0_{1\times(\ell-1)} \\ 0_{(\ell-1)\times 1} & *_{(\ell-1)\times(\ell-1)} \end{pmatrix}. \tag{5}$$

Let $L_\ell^{(N)}$ be an $n \times n$ block diagonal matrix constructed by concatenating L_ℓ diagonally N times:

$$L_\ell^{(N)} := N \left\{ \overbrace{\begin{pmatrix} L_\ell & & \\ & \ddots & \\ & & L_\ell \end{pmatrix}}^{N} \right. ,$$

where $N := n/\ell$. Then, for an $n \times n$ block-anti-circulant matrix B with block size ℓ, the matrix $(L_\ell^{(N)})^\top B L_\ell^{(N)}$ is a block matrix in which every block is in the form of equation (5). Furthermore, there exists a permutation matrix L' such that

$$(L_\ell^{(N)} L')^\top B (L_\ell^{(N)} L') = \left(\begin{array}{c|c} *_{N\times N} & 0_{N\times(\ell-1)N} \\ \hline 0_{(\ell-1)N\times N} & *_{(\ell-1)N\times(\ell-1)N} \end{array}\right). \tag{6}$$

Therefore, the representation matrices $P_1, \dots, P_m$ for the public key $\mathcal{P}$ of BAC-UOV can all be transformed into the form of (6) by using $L_\ell^{(N)} L'$. The UOV attack [20] can then be executed on only the upper-left $N \times N$ submatrices of the obtained matrices, a manipulation with very little complexity. By using the transformed public key, we can reduce the number of variables that appear in the public equations $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ for a message $\mathbf{m}$. This reduces the complexity of the attack by about 20% compared with the best existing attack on UOV. Note that this attack can be executed only if there exists a transformation on the public key like that given by equation (6).

3 Polynomial Matrices of Quotient Ring

In this section, we introduce polynomial matrices as a generalization of the circulant and anti-circulant matrices used in BAC-UOV [31] and describe a method for converting polynomial matrices into symmetric ones that can be applied to the UOV scheme. Furthermore, we discuss whether such generalized matrices can be transformed as shown in equation (5).

3.1 Polynomial Matrices and Their Symmetrization

Let ℓ be a positive integer and $f \in \mathbb{F}_q[x]$ 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

$$\left(1\ x\ \cdots\ x^{\ell-1}\right) \Phi_g^f = \left(g\ xg\ \cdots\ x^{\ell-1} g\right). \tag{7}$$

We call such a matrix Φ_g^f a *polynomial matrix* of g. The following lemma can be easily derived from the definition.

Lemma 1. *For any $g_1, g_2 \in \mathbb{F}_q[x]/(f)$, we have*

$$\Phi_{g_1}^f + \Phi_{g_2}^f = \Phi_{g_1+g_2}^f,\ \Phi_{g_1}^f \Phi_{g_2}^f = \Phi_{g_1 g_2}^f.$$

Namely, the map $g \mapsto \Phi_g^f$ is an injective ring homomorphism from $\mathbb{F}_q[x]/(f)$ to matrix ring $\mathbb{F}_q^{\ell\times\ell}$.

Note that an $\ell\times\ell$ polynomial matrix Φ_g^f can be represented by only ℓ elements in $\mathbb{F}_q$ since Φ_g^f is determined by the ℓ coefficients of $g \in \mathbb{F}_q[x]/(f)$. We let the algebra of such matrices $A_f := \left\{\Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} \;\middle|\; g \in \mathbb{F}_q[x]/(f)\right\}$. This is a subalgebra in the matrix algebra $\mathbb{F}_q^{\ell\times\ell}$ from Lemma 1. Similarly, for a matrix $W \in \mathbb{F}_q^{\ell\times\ell}$, any matrix in $WA_f := \{W\Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} \mid g \in \mathbb{F}_q[x]/(f)\}$ can also be represented by only ℓ elements in $\mathbb{F}_q$.

As seen in equation (4) in Subsection 2.2, the transpose appears in the computation of the public matrices P_i. Thus, to use polynomial matrices Φ_g^f in the UOV scheme, we need WA_f to be stable under the transpose operation for some W. That means that, to construct our proposed scheme, we need an explicit family of f and W such that WA_f is stable under the transpose operation. As stated in Subsection 3.2 below, from the perspective of security, f needs to be irreducible in our scheme. Furthermore, from the perspective of efficiency, f should have only a few non-zero terms. Since there are no irreducible binomials f with $\deg f = \ell$ for many ℓ, trinomials f are thought to be suitable for our scheme. The following proposition shows that there are an infinite number of trinomials f and W.

Proposition 1. *Let $f = x^\ell - ax^i - 1$ $(a \in \mathbb{F}_q, 1 \le i \le \ell - 1)$ and W be in the form*

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

where $J_i := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ stands for an anti-identity matrix with size i. Then, for any $X \in A_f$, WX is a symmetric matrix.

If we set $a = 0$ and $W = J_\ell$, then $f = x^\ell - 1$ holds, and $W\Phi_g^f$ is an anti-circulant matrix. Thus, this case corresponds exactly to BAC-UOV [31], and Proposition 1 can be regarded as describing a generalization of anti-circulant matrices.

Table 1. Degree ℓ such that there exist no irreducible trinomials of the form $x^\ell - ax^i - 1$ among $2 \le \ell \le 30$ for $\mathbb{F}_q = \mathbb{F}_7$ and $\mathbb{F}_{31}$.

$\mathbb{F}_q$	$\mathbb{F}_7$	$\mathbb{F}_{31}$
ℓ	$6, 15, 30$	$6, 25, 30$

As stated in Subsection 3.2 below, from the perspective of security, f needs to be irreducible in our scheme. Since f with the form $x^\ell - ax^i - 1$ is not always irreducible, we conducted several experiments. We treated finite fields $\mathbb{F}_q = \mathbb{F}_7$ and $\mathbb{F}_{31}$, which are used for our proposed scheme as described below, and checked whether there exists an irreducible polynomial $f \in \mathbb{F}_q[x]$ with the form $x^\ell - ax^i - 1$ for $2 \le \ell \le 30$. We found an irreducible polynomial $x^\ell - ax^i - 1$ for sufficiently many $2 \le \ell \le 30$. Table 1 shows the degree ℓ such that there exists *no* irreducible polynomials of the above form.

3.2 Effect of Irreducibility of f

In this subsection, we discuss the relationship between the irreducibility of the polynomial f used to generate quotient ring $\mathbb{F}_q[x]/(f)$ and the existence of transformation on symmetric matrices $W\Phi_g^f$ into the diagonal concatenation of smaller matrices. This is because, as stated in Subsection 2.4, the proposed parameters of BAC-UOV were broken by using the transformation of equation (5) on anti-circulant matrices, and this transformation is obtained from the decomposition $x^\ell - 1 = (x-1)(x^{\ell-1} + \cdots + 1)$.

In the following theorem, we show that, if f is irreducible, there does not exist a transformation such as equation (5) on symmetric matrices $W\Phi_g^f$.

Theorem 1. *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. Then, there do not exist an invertible matrix $L \in \mathbb{F}_q^{\ell \times \ell}$ and $i, j \in \{1, \ldots, \ell\}$ such that, for any $X \in WA_f$,*

$$(L^\top X L)_{ij} = 0.$$

Proof. We assume that there exist a matrix $L \in \mathbb{F}_q^{\ell \times \ell}$ and $i, j \in \{1, \ldots, \ell\}$ satisfying the above condition. Let L_i be the i-th column vector of $W^\top L$, and L_j be the j-th column vector of L. Then, for any $h \in \mathbb{F}_q[x]/(f)$, we have $L_i^\top \Phi_h^f L_j = 0$.

Now, we define a linear isomorphism $V_1 : \mathbb{F}_q[x]/(f) \to \mathbb{F}_q^\ell$ such that

$$V_1(a_0 + a_1 x + \cdots + a_{\ell-1} x^{\ell-1}) = (a_0, a_1, \ldots, a_{\ell-1})^\top,$$

and $V_1(g)$ is equal to the first column vector of Φ_g^f. Furthermore, we define a linear map $V_2 : \mathbb{F}_q[x]/(f) \to \mathbb{F}_q^\ell$ such that $V_2(g)$ is equal to the first column vector of $(\Phi_g^f)^\top$. If $V_2(g) = \mathbf{0}$, then Φ_g^f is not invertible by the definition of V_2. Since A_f is a field, Φ_g^f is the zero-matrix, namely $g = 0$. As a result, V_2 is isomorphic.

Let $g_i := V_2^{-1}(L_i)$ and $g_j := V_1^{-1}(L_j)$. It is clear that $(\Phi^f_{g_i}\Phi^f_h\Phi^f_{g_j})_{11} = L_i^\top \Phi^f_h L_j = 0$ for any $h \in \mathbb{F}_q[x]/(f)$. If we take $h = (g_i g_j)^{-1}$, then

$$0 = (\Phi^f_{g_i}\Phi^f_{(g_i g_j)^{-1}}\Phi^f_{g_j})_{11} = I_{11} = 1.$$

This is a contradiction. Therefore, Theorem 1 holds. □

From this theorem, we choose an irreducible polynomial as the f of A_f used in our proposed variant, which is described in Section 4.

Remark 1. In this remark, we discuss the transformation on elements of WA_f with reducible f by using Theorems 3 and 4 in Appendix A. Theorem 3 shows that, if f is decomposed into distinct irreducible polynomials, the WA_f are transformed into a concatenation of two smaller submatrices. In fact, the transformation, like equation (5) in the structural attack on BAC-UOV, corresponds to the transformation described in Theorem 3. If f is divisible by a squared polynomial, Theorem 4 shows that the representation matrices can be transformed by executing a change of variables into a special form in which the lower-right $(n/\ell) \times (n/\ell)$ block is a zero block, similar to the representation matrices of the central map (equation (3)).

4 Our Proposal: Quotient-Ring UOV (QR-UOV)

In this section, we present our proposed UOV variant, QR-UOV, which is constructed by applying the polynomial matrices described in Subsection 3.1 to UOV.

4.1 Description

Let ℓ be a positive integer and v, m be multiples of ℓ such that $v > m$. Set $n := v + m$ and $N := n/\ell$.

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 symmetric. Note that there exist f and W satisfying the above condition for many ℓ, as shown by Proposition 1 and the discussion in Subsection 3.1. We define a subspace $A_f^{(N)}$ in $\mathbb{F}_q^{n\times n}$ containing $n \times n$ matrices as

$$\begin{pmatrix} X_{11} & \dots & X_{1N} \\ \vdots & \ddots & \vdots \\ X_{N1} & \dots & X_{NN} \end{pmatrix},$$

where every $X_{ij} \in \mathbb{F}_q^{\ell\times\ell}$ $(i, j \in \{1, \dots, N\})$ is an element of A_f. Furthermore, we define an $n \times n$ block diagonal matrix $W^{(N)}$ constructed by concatenating W diagonally N times:

$$W^{(N)} := \begin{pmatrix} W & & \\ & \ddots & \\ & & W \end{pmatrix}.$$

For these matrices, we obtain the following proposition:

Proposition 2. *For $X \in W^{(N)} A_f^{(N)}$ and $Y \in A_f^{(N)} (W^{(N)})^{-1}$, we have*

$$X^\top Y X \in W^{(N)} A_f^{(N)}.$$

Proof. We prove this proposition for $N = 1$. Let $X := W\Phi_{g_1}^f$ and $Y := \Phi_{g_2}^f W^{-1}$. Due to the symmetry of WA_f,

$$\begin{aligned} X^\top Y X &= (W\Phi_{g_1}^f)^\top (\Phi_{g_2}^f W^{-1})(W\Phi_{g_1}^f) \\ &= (W\Phi_{g_1}^f)(\Phi_{g_2}^f W^{-1})(W\Phi_{g_1}^f) \\ &= W\Phi_{g_1}^f \Phi_{g_2}^f \Phi_{g_1}^f \\ &= W\Phi_{g_1 \cdot g_2 \cdot g_1}^f. \end{aligned}$$

For $N \geq 2$, the statement is proven similarly. $\square$

By using this proposition, we can construct a quotient-ring UOV (QR-UOV), which is a variant of UOV using polynomial matrices.

Key Generation

- Choose an irreducible polynomial $f \in \mathbb{F}_q[x]$ with $\deg f = \ell$ and $W \in \mathbb{F}_q^{\ell \times \ell}$ such that every element in WA_f is symmetric.
- Choose F_i $(i = 1, \ldots, m)$ from $A_f^{(N)} (W^{(N)})^{-1}$ such that the lower-right $m \times m$ submatrices are zero matrices.
- Choose an invertible matrix S from $W^{(N)} A_f^{(N)}$ randomly.
- Compute $P_i = S^\top F_i S$ $(i = 1, \ldots, m)$.

We then obtain that P_i $(i = 1, \ldots, m)$ are elements of $W^{(N)} A_f^{(N)}$ from Proposition 2. The signing and verification processes are the same as those of plain UOV. Note that, in QR-UOV, the cardinality of the finite field q is set to be odd since, if q is even, the coefficients corresponding to the non-diagonal elements of every diagonal block are zero due to the symmetry of every block $W\Phi_g^f$.

Remark 2. We can apply the polynomial matrices of a quotient ring to not only UOV but also Rainbow.

4.2 Improved QR-UOV

In this subsection, we explain two improved methods used in the NIST second-round proposal of Rainbow [10]. The first one limits the secret key $\mathcal{S}$ to a specific compact form. The second one replaces a large part of the public key with a small seed for pseudo random number generation (PRNG).

In plain UOV, matrix S of linear map $\mathcal{S}$ can be restricted to a special form:

$$S = \begin{pmatrix} I_{v \times v} & S' \\ 0_{m \times v} & I_{m \times m} \end{pmatrix},$$

where S' is a $v \times m$ matrix since it does not affect security. In QR-UOV, the upper-left and lower-right identity matrices are replaced with block diagonal matrices in which every diagonal block is $W\Phi_1^f = W$ since S is chosen in $W^{(N)} A_f^{(N)}$:

$$S = \begin{pmatrix} W^{(v/\ell)} & S' \\ 0_{m \times v} & W^{(m/\ell)} \end{pmatrix},$$

where S' is a block matrix in which every component is an element of WA_f. This limits the secret key to a specific compact form.

The second method is based on Petzoldt et al.'s compression technique [26], which is used to convert Rainbow into *cyclic Rainbow*. The representation matrices P_i $(i = 1, \ldots, m)$ of the public key map are written in the form

$$P_i = \begin{pmatrix} P_{i,1} & P_{i,2} \\ P_{i,2}^\top & P_{i,3} \end{pmatrix},$$

where $P_{i,1}$, $P_{i,2}$, and $P_{i,3}$ are $v \times v$, $v \times m$, and $m \times m$ matrices, respectively, and $P_{i,1}$ and $P_{i,3}$ are symmetric matrices. Similarly, the representation matrices F_i $(i = 1, \ldots, m)$ of the central map in equation (3) are written in the form

$$F_i = \begin{pmatrix} F_{i,1} & F_{i,2} \\ F_{i,2}^\top & 0_{m \times m} \end{pmatrix},$$

where $F_{i,1}$ and $F_{i,2}$ are $v \times v$ and $v \times m$ matrices, respectively, and $F_{i,1}$ is a symmetric matrix. Then, since S^{-1} is

$$S^{-1} = \begin{pmatrix} (W^{-1})^{(v/\ell)} & S'' \\ 0_{m \times v} & (W^{-1})^{(m/\ell)} \end{pmatrix},$$

where $S'' := -(W^{-1})^{(v/\ell)} S' (W^{-1})^{(m/\ell)}$, the representation matrices F_i, P_i $(i = 1, \ldots, m)$ and S hold the following equation:

$$\begin{pmatrix} F_{i,1} & F_{i,2} \\ F_{i,2}^\top & 0_{m \times m} \end{pmatrix} = \begin{pmatrix} (W^{-1})^{(v/\ell)} & 0_{v \times m} \\ S''^\top & (W^{-1})^{(m/\ell)} \end{pmatrix} \begin{pmatrix} P_{i,1} & P_{i,2} \\ P_{i,2}^\top & P_{i,3} \end{pmatrix} \begin{pmatrix} (W^{-1})^{(v/\ell)} & S'' \\ 0_{m \times v} & (W^{-1})^{(m/\ell)} \end{pmatrix}.$$

By computing the right-hand side, we obtain

$$\begin{aligned} F_{i,1} &= (W^{-1})^{(v/\ell)} P_{i,1} (W^{-1})^{(v/\ell)}, \\ F_{i,2} &= (W^{-1})^{(v/\ell)} P_{i,1} S'' + (W^{-1})^{(v/\ell)} P_{i,2} (W^{-1})^{(m/\ell)}, \\ 0_{m \times m} &= S''^\top P_{i,1} S'' + (W^{-1})^{(m/\ell)} P_{i,2}^\top S'' + S''^\top P_{i,2} (W^{-1})^{(m/\ell)} \\ &\quad + (W^{-1})^{(m/\ell)} P_{i,3} (W^{-1})^{(m/\ell)}. \end{aligned} \tag{8}$$

In the improved key generation step, $P_{i,1}$, $P_{i,2}$ $(i = 1, \ldots, m)$, and S' are first generated from seeds $\mathbf{s}_{pk}$ and $\mathbf{s}_{sk}$, respectively, using PRNG. Next, $P_{i,3}$ $(i = 1, \ldots, m)$ are computed using

$$P_{i,3} = -W^{(m/\ell)} S''^\top P_{i,1} S'' W^{(m/\ell)} - P_{i,2}^\top S'' W^{(m/\ell)} - W^{(m/\ell)} S''^\top P_{i,2}$$

from equation (8). As a result, the public key is composed of $m \times m$ matrices $P_{i,3}$ ($i = 1, \ldots, m$) and the seed for $P_{i,1}$, $P_{i,2}$ ($i = 1, \ldots, m$). This compression technique significantly reduces the public key size of QR-UOV.

Finally, we compare the public key size of plain QR-UOV with that of the improved QR-UOV. The public key of plain QR-UOV is represented using $P_{i,1}$, $P_{i,2}$, and $P_{i,3}$ ($i = 1, \ldots, m$) and that of the improved QR-UOV uses a seed and $P_{i,3}$ ($i = 1, \ldots, m$). Thus, the number of elements in $\mathbb{F}_q$ needed to mainly represent the public key of plain QR-UOV is

$$mn(n + \ell)/2\ell,$$

whereas that of the improved QR-UOV is

$$m^2(m + \ell)/2\ell.$$

5 Security Analysis

In this section, we first analyze the security of QR-UOV against three currently known attacks on plain UOV. We then discuss possible attacks on the quotient ring obtained by pulling submatrices $W\Phi_g^f$ back to g in the quotient ring. Finally, we consider the execution of possible attacks obtained by lifting the base field $\mathbb{F}_q$ to an extension field $\mathbb{F}_{q^\ell}$ and transforming the public key system over the extension field.

5.1 Currently Known Attacks on Plain UOV

In this subsection, we regard QR-UOV as the plain UOV described in Subsection 2.2, and describe the execution of three currently known attacks on UOV, the direct attack, the UOV attack [20], and the reconciliation attack [12].

Direct Attack Given a quadratic polynomial system $\mathcal{P} = (p_1, \ldots, p_m)$ in n variables over $\mathbb{F}_q$ and $\mathbf{m} \in \mathbb{F}_q^m$, the direct attack algebraically solves the system $\mathcal{P}(\mathbf{x}) = \mathbf{m}$. For UOV, the number of variables n is larger than the number of equations m; therefore, $n - m$ variables can be specified with random values without disturbing the existence of a solution.

One of the best-known approaches for algebraically solving the quadratic system is the hybrid approach [4], which randomly guesses k ($k = 0, \ldots, n$) variables before computing a Gröbner basis [8]. The guessing is repeated until a solution is obtained. Well-known algorithms for computing Gröbner bases include F4 [14], F5 [15], and XL [9]. The complexity of this approach for a classical adversary is estimated to be

$$\min_k \left(q^k \cdot 3 \cdot \binom{m-k}{2} \cdot \binom{d_{reg} + m - k}{d_{reg}}^2 \right), \tag{9}$$

Table 2. Theoretical and experimental degree of regularity of public key system of QR-UOV obtained using Magma algebra system [6].

(q, v, m, ℓ)	theoretical d_{reg}	experimental d_{reg}
$(7, 28, 14, 2)$	15	15
$(7, 32, 16, 2)$	17	17
$(7, 24, 12, 3)$	13	13
$(7, 30, 15, 3)$	16	16
$(31, 28, 14, 2)$	15	15
$(31, 32, 16, 2)$	17	17

where d_{reg} is the so called degree of regularity of the system. The degree of regularity d_{reg} for a certain class of polynomial systems called *semi-regular systems* [1–3] is known to be estimated to be the degree of the first non-positive term in the following series [3]:

$$\frac{\left(1-z^2\right)^m}{\left(1-z\right)^{m-k}}. \tag{10}$$

Empirically, the public key system of UOV is considered to be a semi-regular system, so this formula can be used to estimate its degree of regularity.

On the other hand, the complexity of a quantum direct attack is estimated to be

$$\min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k}{2} \cdot \binom{d_{reg}+m-k}{d_{reg}}^2 \right), \tag{11}$$

by using Grover's algorithm [18].

Furthermore, Thomae and Wolf [32] proposed a technique for reducing the number of variables and equations when $n > m$. For the $n \times n$ representation matrices P_i of the public key, the technique chooses a new matrix S' such that every upper-left $m \times m$ submatrix of $S'^{\top} P_i S'$ $(i = 1, \ldots, \alpha)$ is diagonal, where $\alpha = \lfloor \frac{n}{m} \rfloor - 1$. We can then reduce the $(n-m+\alpha)$ variables and α equations and thereby obtain a quadratic system with $m-\alpha$ variables and equations. Note that, this technique can be fully applied only for quadratic systems that are over finite fields of even characteristics. However, Thomae and Wolf show that a part of the technique can be applied to odd characteristic case and empirically makes the direct attack faster on quadratic systems over finite fields of odd characteristic. Therefore, from a security perspective, it is not extreme that we consider this technique can be applied to odd characteristic case.

In Table 2, for a QR-UOV public key system, we compare the degree of regularity (theoretical d_{reg}) obtained by equation (10) assuming that the system is semi-regular and the degree (experimental d_{reg}) obtained by executing the direct attack on the system as calculated using the Magma algebra system [6]. In our experiment, m was set to enough large values so that our computation for one parameter is done within one day, and v was set to be equal to $2m$, while

q and ℓ were set to the values given in Subsection 6.1. For the public key of QR-UOV with $(v+m)$ variables, m equations, we fix the last v variables and execute the hybrid approach with $k=0$ in Subsection 5.1. These results show that the degrees of regularity obtained experimentally were the same as those obtained theoretically.

UOV Attack The UOV attack [20] finds a linear map $\mathcal{S}' : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that every component of $\mathcal{F}' := \mathcal{P} \circ \mathcal{S}'$ has the form of equation (2). Such an $\mathcal{S}'$ is called an *equivalent key*. The UOV attack finds the subspace $\mathcal{S}^{-1}(\mathcal{O})$ of $\mathbb{F}_q^n$, where $\mathcal{O}$ is the oil subspace defined as

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

This subspace $\mathcal{S}^{-1}(\mathcal{O})$ can induce an equivalent key. To obtain $\mathcal{S}^{-1}(\mathcal{O})$, the UOV attack chooses two invertible matrices W_i, W_j from the set of linear combinations of $P_1, \ldots, P_m$. 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 UOV attack is estimated to be

$$q^{v-m-1} \cdot m^4.$$

Grover's algorithm can be used to reduce the complexity for a quantum adversary to

$$q^{\frac{v-m-1}{2}} \cdot m^4.$$

Reconciliation Attack The reconciliation attack [12] also finds, similarly to the UOV attack, an equivalent key $\mathcal{S}'$. The reconciliation attack treats every element of the matrix S' as a variable and solves the quadratic system of equations obtained by using $({S'}^\top P_i S')[v+1:n,\, v+1:n] = 0_{m\times m}$ $(i=1,\ldots,m)$, where $X[a:b,\, c:d]$ denotes a $(b-a)\times(d-c)$ submatrix of X in which the upper-left element has index (a,b). This attack can be decomposed into a series of steps, and in the first step, a system of m quadratic equations in v variables is solved. In the case of the plain UOV where $v>m$, the complexity is considered to be greater than that of solving a quadratic system of v equations in v variables. Therefore, we estimate the complexity of the reconciliation attack as that of the direct attack on the quadratic system with v variables, v equations, which is obtained by (9) and (11) as $n=v$. Note that if $v \le m$, then the complexity of the reconciliation attack is the same as that of solving a quadratic system of m equations in v variables. As a result, we estimate the complexity of the reconciliation attack as the direct attack on the quadratic system with v variables and $\max\{m,v\}$ equations.

5.2 Pull-back Attacks over Quotient Ring

In this subsection, we explain a method for executing three currently known attacks on QR-UOV by utilizing the block structure from the quotient ring. For every block submatrix $W\Phi_g^f$ of the representation matrices of the public key, we can execute the UOV attack and the reconciliation attack in the quotient ring $\mathbb{F}_q[x]/(f)$ by replacing $W\Phi_g^f$ to g.

To do so, we define a map $G_1 : W^{(N)}A_f^{(N)} \to (\mathbb{F}_q[x]/(f))^{N\times N}$ such that given $X \in W^{(N)}A_f^{(N)}$, $(G_1(X))_{ij}$ is equal to $g \in \mathbb{F}_q[x]/(f)$ if the ij-block of X is $W\Phi_g^f$. Furthermore, we define $G_2 : A_f^{(N)}(W^{(N)})^{-1} \to (\mathbb{F}_q[x]/(f))^{N\times N}$ similarly. In the following, we consider the execution of the three currently known attacks described in Subsection 5.1 on $G_1(P_1), \ldots, G_1(P_m)$.

First, we consider the complexity of the pull-back UOV attack which is the UOV attack on the transformed representation matrices $G_1(P_1), \ldots, G_1(P_m)$. If we find an equivalent key S' for the transformed matrices by executing the UOV attack over $\mathbb{F}_q[x]/(f)$, $G_2^{-1}(S') \in \mathbb{F}_q^{n\times n}$ is an equivalent key over $\mathbb{F}_q$. The complexities of the pull-back UOV attack for a classical and quantum attacker are

$$q^{v-m-\ell} \cdot (m/\ell)^4, \quad q^{\frac{v-m-\ell}{2}} \cdot (m/\ell)^4,$$

which are basically the same values as for the plain UOV attack.

The pull-back reconciliation attack can be seen as the reconciliation attack on the UOV with v/ℓ vinegar variables and m equations. As we stated in the last paragraph of Subsection 5.1, the complexity is estimated to be that of the direct attack on a quadratic system with v/ℓ variables and $\max\{m, v/\ell\}$ equations over $\mathbb{F}_q[x]/(f)$.

For the direct attack, since vectors $\mathbf{x}$ and $\mathbf{m}$ of $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ cannot be represented over the quotient ring $\mathbb{F}_q[x]/(f)$, the direct attack cannot be executed on $G_1(P_1), \ldots, G_1(P_m)$.

5.3 Lifting Attacks over Extension Field

As stated in Theorem 1, there does not exist a transformation on the representation matrices $P_1, \ldots, P_m$ of QR-UOV into the diagonal concatenation of smaller matrices like the form of equation (6) used in the structural attack on BAC-UOV by executing a change of variables over $\mathbb{F}_q$. However, as we prove below, there exists such a transformation on the public key of QR-UOV over the extension field $\mathbb{F}_{q^\ell}$. In this subsection, we explain a method for transforming the public key over $\mathbb{F}_{q^\ell}$ and how this affects the three currently known attacks on UOV.

Theorem 2. *With the same notation as in Theorem 1,*

1. *there exists an invertible matrix $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ such that, for any $g \in \mathbb{F}_q[x]/(f)$, $L^{-1}\Phi_g^f L$ is diagonal,*
2. *for any $X \in WA_f$, $L^\top XL$ is diagonal,*
3. *if, for any $X \in WA_f$, there exists $\mathbf{y} \in \mathbb{F}_{q^\ell}^\ell$ such that $\mathbf{y}^\top X\mathbf{y} = 0$, then $\mathbf{y} = \mathbf{0}$.*

(The proof is in the appendix.)

First, Theorem 2 shows that the polynomial matrix can be diagonalized over $\mathbb{F}_{q^\ell}$. Subsequently, it indicates that $P_1, \ldots, P_m$ of QR-UOV can be transformed into block diagonal matrices for which the block size is $N \times N$ by executing a change of variables over $\mathbb{F}_{q^\ell}$. Let $L^{(N)}$ be an $n \times n$ ($n = \ell \cdot N$) block diagonal matrix with block size ℓ, for which the N diagonal blocks are L. Then, $(L^{(N)})^\top P_i L^{(N)}$ ($i = 1, \ldots, m$) become block matrices in which every component is of the diagonal form. Furthermore, there exists a permutation matrix L' such that $(L^{(N)}L')^\top P_i (L^{(N)}L')$ is a block diagonal matrix with block size N; let $\bar{L} := L^{(N)}L'$. This theorem finally states that there does not exist a change of variables over $\mathbb{F}_{q^\ell}$ such that it recovers the structure of the central map of UOV directly.

We next consider the complexities of the lifting UOV and reconciliation attacks which are the UOV and reconciliation attacks on $\bar{L}^\top P_i \bar{L}$ ($i = 1, \ldots, m$). The transformed matrices $\bar{L}^\top P_i \bar{L}$ can be represented by $(\bar{L}^\top S \bar{L})^\top (\bar{L}^{-1} F_i \bar{L}^{-\top})$ $(\bar{L}^\top S \bar{L})$. Then, $\bar{L}^\top S \bar{L}$ explicitly has the same form as $\bar{L}^\top P_i \bar{L}$. Furthermore, $\bar{L}^{-1} F_i \bar{L}^{-\top}$ is also a diagonal block matrix since

$$L^{-1}(\Phi_g^f W^{-1})L^{-\top} = (L^{-1}\Phi_g^f L)(L^\top W L)^{-1},$$

where $L^{-1}\Phi_g^f L$ and $L^\top W L$ are diagonal. Then, due to the structure of F_i, every diagonal block of $\bar{L}^{-1} F_i \bar{L}^{-\top}$ has an $m/\ell \times m/\ell$ zero block, similar to F_i. Consequently, the complexity of the lifting UOV attack on each block over $\mathbb{F}_{q^\ell}$ is $O(q^{v-m-\ell} \cdot (m/\ell)^4)$. Moreover, the complexity of the lifting reconciliation attack on each block is estimated to be that of the direct attack on a quadratic system with v/ℓ variables and $\max\{m, v/\ell\}$ equations over $\mathbb{F}_{q^\ell}$. These complexities are the same as those of the pull-back UOV attack and reconciliation attack described in Subsection 5.2.

Next, we consider the direct attack on $\bar{L}^\top P_i \bar{L}$ ($i = 1, \ldots, m$). Although in Subsection 5.1 we use the technique proposed by Thomae and Wolf [32] in the plain direct attack, we cannot use this technique in the lifting direct attack. If we use this technique before the linear transformation using $\bar{L}$ over $\mathbb{F}_{q^\ell}$, we cannot diagonalize the representation matrices since the linear transformation executed in this technique breaks the block structure of QR-UOV. We thus use the technique after block-diagonalizing over $\mathbb{F}_{q^\ell}$. If $n > m$, the cardinality of the solution is generally $\mathbb{F}_q^v$. However, since we are solving the system over $\mathbb{F}_{q^\ell}$, the cardinality of the obtained solution changes to $\mathbb{F}_{q^\ell}^v$. Therefore, the probability that the obtained solution is in $\mathbb{F}_q^n$ is very low, so this technique is not efficient. In conclusion, there does not exist an effective way of executing the direct attack on $\bar{L}^\top P_i \bar{L}$ using Thomae and Wolf's technique.

Therefore we consider the lifting direct attack without using Thomae and Wolf's technique, in which we fix the v values before block-diagonalizing over $\mathbb{F}_{q^\ell}$. We then obtain a solution in $\mathbb{F}_q^n$ since the solution is thought to be uniquely determined. This means that we can execute the direct attack on a block-diagonalized system without reducing the probability of finding a solution in $\mathbb{F}_q^n$. Table 3 summarizes the results of an experiment investigating the degree of regularity of the block-diagonalized public key system of QR-UOV using the Magma algebra sys-

Table 3. Theoretical and experimental degree of regularity obtained by executing the lifting direct attack using the Magma algebra system [6].

(q, v, m, ℓ)	theoretical d_{reg}	experimental d_{reg}
$(7, 24, 12, 2)$	13	13
$(7, 28, 14, 2)$	15	14
$(7, 24, 12, 3)$	13	13
$(7, 30, 15, 3)$	16	15
$(31, 24, 12, 2)$	13	13
$(31, 28, 14, 2)$	15	14

tem [6]. In our experiment, v is set to be equal to $2m$. For representation matrices $P_1, \dots, P_m$ of the public key of QR-UOV with $(v + m)$ variables, m equations, after transforming the system like $\bar{L}^\top P_i \bar{L}$, we fix the last v variables and execute the hybrid approach with $k = 0$ in Subsection 5.1. As a result, it shows that the degree of regularity was smaller than the theoretical value obtained by equation (10) assuming the system is semi-regular by at most one. Therefore, we estimate the complexity of the lifting direct attack by replacing q and d_{reg} in equations (9) and (11) to q^ℓ and $d_{reg} - 1$, respectively. In this estimation, the degree of regularity becomes one degree smaller, but the base field $\mathbb{F}_q$ is lifted to the extension field $\mathbb{F}_{q^\ell}$.

6 Proposed Parameters and Comparison

In this section, we propose specific parameters for three security levels of the NIST PQC project [23] and compare the performance of the improved QR-UOV with that reported for cyclic Rainbow [27].

6.1 Proposed Parameters

In this subsection, we describe the parameters selected for the improved QR-UOV described in Subsection 4.2. Our proposed parameters are set to satisfy security levels I, III, and V of the NIST PQC project [23] to enable comparison with the performance of cyclic Rainbow [27]. The parameters for the improved QR-UOV are the number of finite fields q, the number of vinegar variables v, the number of oil variables, the number of equations m, the block size of the representation matrices ℓ, and the polynomial used to generate the quotient ring f. We set q to be odd from the perspective of security. The v is mainly determined by the complexity of the pull-back and lifting reconciliation attacks described in Subsections 5.2 and 5.3, and m is determined by that of the plain direct attack. We use $\ell = 2$ or 3 since a large ℓ makes the signature and execution time larger. From Theorem 1, we choose irreducible polynomials f with the form of $x^\ell - ax^i - 1$ described in Proposition 1. In summary, we propose the following

Table 4. Complexity of the plain attacks in Subsection 5.1, the pull-back attacks in Subsection 5.2, and the lifting attacks in Subsection 5.3 on the proposed parameters of QR-UOV in Subsection 6.1. Here, "direct", "UOV" and "Rec" stand for the direct attack, UOV attack, and reconciliation attack, respectively. The bold fonts indicate the lowest complexity among all attacks in the same security level.

parameter (q,v,m,ℓ)	attack model	$\log_2(\#\text{gates})$							
		plain			pull-back		lifting		
		direct	UOV	Rec	UOV	Rec	direct	UOV	Rec
QR-UOV I (7,122,68,2)	classical	**149.2**	177.4	250.8	172.4	150.3	184.9	172.4	150.3
	quantum	102.2	103.0	170.9	**99.4**	133.8	148.4	**99.4**	133.8
QR-UOV III (7,276,102,3)	classical	**210.4**	516.6	528.2	507.6	217.6	287.2	507.6	217.6
	quantum	**143.8**	273.7	353.7	267.6	209.0	246.7	267.6	209.0
QR-UOV V (31,210,108,2)	classical	**274.3**	533.1	504.9	526.1	283.8	310.1	526.1	283.8
	quantum	**212.5**	283.0	388.5	278.4	262.5	273.0	278.4	262.5

parameters for the improved QR-UOV:

$$\begin{aligned}
\text{QR-UOV I}: &\quad (q,v,m,\ell,f) = (7,122,68,2,x^2-x-1),\\
\text{QR-UOV III}: &\quad (q,v,m,\ell,f) = (7,276,102,3,x^3-3x-1),\\
\text{QR-UOV V}: &\quad (q,v,m,\ell,f) = (31,210,108,2,x^2-3x-1).
\end{aligned}$$

Next, we show that these parameters of QR-UOV I, III, and V satisfy the security levels I, III, and V of NIST PQC project, respectively. Here, security levels I, III, and V mean that a classical attacker needs more than 2^{143}, 2^{207}, and 2^{272} classical gates to break the parameters while a quantum attacker needs more than 2^{74}, 2^{137}, and 2^{202} quantum gates, respectively [23]. The number of gates required for an attack against the NIST second round proposal version of Rainbow [10] can be computed using

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

We next consider the complexity of each currently known attack described in Section 5 on our proposed parameters. Table 4 shows the complexity of the plain direct, UOV, and reconciliation attacks described in Subsection 5.1, the pull-back UOV and reconciliation attacks described in Subsection 5.2, and the lifting direct, UOV, and reconciliation attacks described in Subsection 5.3. (See each subsection for the concrete way of estimating the complexity of each attack.) This table does not include the complexity of "the pull-back direct attack", since we cannot execute the direct attack on the pulled back public key system as we sated in Subsection 5.2. For each parameter set, the upper entry shows the number of classical gates while the lower entry shows the number of quantum gates. For example, the complexity of the direct attack for level I is 149.2 classical gates and 102.2 quantum gates, respectively. Furthermore, the values in bold show the complexity of the best attack against each parameter set. The lowest complexity of among all attacks is the direct attack except the quantum direct

Table 5. Comparison of public key and signature size of cyclic Rainbow with those of QR-UOV. We use parameters for cyclic Rainbow updated in [27], and parameters for the improved QR-UOV in Subsection 4.2. The unit of the public key size is kilobyte (KB), but that of the signature size is byte (B).

security level	scheme	parameters	public key size (KB)	signature size (B)
I	Cyclic Rainbow I	$(q, v_1, o_1, o_2) = (16, 36, 32, 32)$	57.4	66.0
	QR-UOV I	$(q, v, m, \ell) = (7, 122, 68, 2)$	**29.7**	**87.3**
III	Cyclic Rainbow III	$(q, v_1, o_1, o_2) = (256, 68, 32, 48)$	252.3	164.0
	QR-UOV III	$(q, v, m, \ell) = (7, 276, 102, 3)$	**66.7**	**157.8**
V	Cyclic Rainbow V	$(q, v_1, o_1, o_2) = (256, 96, 36, 64)$	511.2	212.0
	QR-UOV V	$(q, v, m, \ell) = (31, 210, 108, 2)$	**195.8**	**214.8**

attack of 102.2 gates on QR-UOV I, while the quantum pull-back and lifting UOV attacks on QR-UOV I have a little lower complexity of 99.4 gates. As a result, this table shows that our proposed parameters satisfy the requirement for each security level.

Remark 3. As with the proposed parameters for Rainbow [27], our proposed parameters for security levels I, III, and V also respectively satisfy security levels II, IV, and VI of the NIST PQC project [23].

6.2 Comparison with Rainbow

In Table 5, we compare the public key and signature size for our proposed improved QR-UOV parameters with those for cyclic Rainbow [27] for security levels I, III, and V. As for cyclic Rainbow in the second round proposal [10], the public key includes a 256 bit seed $\mathbf{s}_{pk}$, and the signature includes a 128 bit *salt*, which is a random binary vector for EUF-CMA security [29]. The secret key can be generated from two 256 bit seeds $\mathbf{s}_{sk}$ and $\mathbf{s}_{pk}$. For example, the public key size of the improved QR-UOV for level I is 29.7 KB, which is about half that of cyclic Rainbow. As a result, the public key size of the improved QR-UOV can be reduced about 50–70% compared with that of cyclic Rainbow at the cost of a small increase in signature size.

Although the public key size could be further reduced by setting block size ℓ larger, enlarging the block size would likely increase the signature size and lengthen the execution time.

7 Conclusion

We have proposed a new variant of the unbalanced oil and vinegar (UOV), which is a well-established multivariate signature scheme that has essentially not been broken for over 20 years. Our proposed QR-UOV scheme uses a quotient ring ($\mathbb{F}_q[x]/(f)$) to reduce the public key size. Although multivariate signature schemes are promising candidates for post-quantum cryptography, and a UOV variant called Rainbow was selected as a third-round finalist in the NIST Post-Quantum Cryptography (PQC) project, a disadvantage of UOV variants including Rainbow in general is that they have a large public key. Research on reducing UOV public key size is important for post-quantum cryptography. In this paper, we have presented a new approach to achieving such a reduction.

Our proposed QR-UOV scheme features a small public key and a reasonable signature size. In particular, with our proposed parameters, the public key size of the improved QR-UOV can be reduced about 50–70% compared with that of cyclic Rainbow, a third-round finalist in the NIST PQC project, without significantly increasing the signature size. To construct QR-UOV, we defined polynomial matrix Φ_g^f ($g \in \mathbb{F}_q[x]/(f)$) and introduced the concept of a matrix W such that $W\Phi_g^f$ is symmetric. QR-UOV utilizes polynomial matrices Φ_g^f in block matrices. Moreover, we proved that, if the polynomial f used to generate the quotient ring is irreducible, QR-UOV is resistant to attacks that are able to break block-anti-circulant UOV. We also analyzed the security of QR-UOV against three currently known attacks on plain UOV and possible attacks on the quotient ring. We stress that utilizing the elements of a quotient ring in block matrices is similar to the MLWE problem which is a generalization of LWE using a module consisting of vectors over a ring.

An important open problem is improving the efficiency of QR-UOV. The Rainbow UOV variant has a multi-layer structure and is efficient and secure. Extending QR-UOV to a comparable efficient and secure multi-layer version of QR-Rainbow will be a challenging task. We need to carefully analyze the security of QR-Rainbow against various attacks by considering its multi-layer structure. Another possible way to improve efficiency is to exploit a better choice of polynomial f. In this paper, we simply used a simple trinomial for the first construction of QR-UOV; we expect to find another family of polynomials that can produce more efficient operations.

Acknowledgments: This work was supported by JST CREST Grant Number JPMJCR14D6 and JSPS KAKENHI Grant Number JP19K20266.

References

1. Bardet, M.: Étude des systèms algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. PhD thesis, Université Pierre et Marie Curie-Paris VI (2004)

2. Bardet, M., Faugère, J.-C., Salvy, B.: Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. Research Report, INRIA (2003)
3. Bardet, M., Faugère, J.-C., Salvy, B., Yang, B.-Y.: Asymptotic behavior of the index of regularity of quadratic semi-regular polynomial systems. In: 8th International Symposium on Effective Methods in Algebraic Geometry (2005)
4. Bettale, L., Faugère, J.-C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology **3**, pp. 177–197 (2009)
5. Beullens, W., Preneel, B.: Field lifting for smaller UOV public keys. In; INDOCRYPT 2017, LNCS, vol. 10698, pp. 227–246. Springer (2017)
6. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. Journal of Symbolic Computation **24**(3-4), pp. 235–265 (1997)
7. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012, pp. 309-325. ACM, January 2012.
8. Buchberger, B.: Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. PhD thesis, Universität Innsbruck (1965)
9. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: EUROCRYPT 2000, LNCS, vol. 1807, pp. 392–407. Springer (2000)
10. Ding, J., Chen, M.-S., Petzoldt, A., Schmidt, D., Yang, B.-Y.: Rainbow signature schemes proposal for NIST PQC project (round 2 version).
11. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005)
12. 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)
13. Ding, J., Zhang, Z., Deaton, J., Schmidt, K., Vishakha, FNU.: New attacks on lifted unbalanced oil vinegar. In: Second PQC Standardization Conference 2019, NIST (2019)
14. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra **139**(1-3), pp. 61–88 (1999)
15. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction In: ISSAC 2002, pp. 75–83. ACM (2002)
16. 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)
17. Garey, M.-R., Johnson, D.-S.: Computers and intractability: a guide to the theory of NP-completeness. W. H. Freeman (1979)
18. Grover, L.-K.: A fast quantum mechanical algorithm for database search. In: STOC 1996, pp. 212–219. ACM (1996)
19. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999)
20. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998)
21. Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P., Seiler, G., Stehle, D.: CRYSTALS-DILITHIUM signature schemes proposal for NIST PQC project (round 2 version).
22. NIST: Post-quantum cryptography CSRC. `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`

23. NIST: Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf` (2016)
24. NIST: Status report on the first round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8240, NIST (2019)
25. NIST: Status report on the second round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8309, NIST (2020)
26. Petzoldt, A., Bulygin, S., Buchmann, J.-A.: CyclicRainbow - a multivariate signature scheme with a partially cyclic public key. In: INDOCRYPT 2010, LNCS, vol. 6498, pp. 33–48. Springer (2010)
27. Rainbow Team: Modified parameters of rainbow in response to a refined analysis of the rainbow band separation attack by the NIST team and the recent new minrank attacks. `https://drive.google.com/file/d/1tcGC38SSkF_csxpzJpkM3qzfsWJq1ywL/view` (2020)
28. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005, pp. 84–93, ACM (2005)
29. Sakumoto, K., Shirai, T., Hiwatari, H.: On provable security of UOV and HFE signature schemes against chosen-message attack. In: PQCrypto 2011, LNCS, vol. 7071, pp. 68–82 (2011)
30. 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)
31. Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced oil and vinegar. In: SAC 2019, LNCS, vol. 11959, pp. 574–588. Springer (2019)
32. Thomae, E., Wolf, C.: Solving underdetermined systems of multivariate quadratic equations revisited. In: PKC 2012, LNCS, vol. 7293, pp. 156–171. Springer (2012)

Appendix A: Transformation on Polynomial Matrix from a Reducible Polynomial

First, we discuss the case in which f is reducible and decomposed into distinct irreducible polynomials.

Theorem 3. *Let $f \in \mathbb{F}_q[x]$ be a reducible polynomial with $\deg f = \ell$ and W be an invertible matrix such that every element of WA_f is a symmetric matrix. If $f = f_1 \cdots f_k$ ($k \in \mathbb{N}$), where $f_1, \dots, f_k$ are distinct, irreducible, and $\deg f_1 \leq \cdots \leq \deg f_k$, then there exist an invertible matrix $L \in \mathbb{F}_q^{\ell \times \ell}$ and $i \in \{1, \dots, \ell-1\}$ such that, for any $X \in WA_f$,*

$$L^\top XL = \begin{pmatrix} *_{i\times i} & 0_{i\times(\ell-i)} \\ 0_{(\ell-i)\times i} & *_{(\ell-i)\times(\ell-i)} \end{pmatrix}. \tag{12}$$

Proof. We first prove that every element of $A_f W^{-1}$ is symmetric. For any $g \in \mathbb{F}_q[x]/(f)$,

$$\begin{aligned}
(\Phi_g^f W^{-1})^\top &= W^{-\top}(\Phi_g^f)^\top \\
&= W^{-\top}(\Phi_g^f)^\top W W^{-1} \\
&= W^{-\top}(W\Phi_g^f)^\top W^{-1} \quad (\because W \text{ is symmetric.}) \\
&= W^{-\top} W \Phi_g^f W^{-1} \\
&= \Phi_g^f W^{-1}.
\end{aligned}$$

Therefore, every element of $A_f W^{-1}$ is symmetric.

Since f is reducible, there exist $a, b \in \mathbb{F}_q[x]/(f)$ such that $a \cdot b = 0$. Then, for any $g \in \mathbb{F}_q[x]/(f)$,

$$\begin{aligned}
(\Phi_a^f W^{-1})^\top (W\Phi_g^f)(\Phi_b^f W^{-1}) &= \Phi_{a\cdot g\cdot b}^f W^{-1} \\
&= \Phi_0^f W^{-1} = 0_{\ell\times\ell}.
\end{aligned}$$

We suppose that $L \in \mathbb{F}_q^{\ell\times\ell}$ is designed such that the first i column vectors of L are chosen from the column vector space of $\Phi_a^f W^{-1}$ and the other $(\ell - i)$ column vectors of L are chosen from the column vector space of $\Phi_b^f W^{-1}$. Then, equation (12) explicitly holds from the above equation.

We next show that there exists an invertible such a L. We suppose that $a := f_1$ and $b := f_2 \cdots f_k$ and prove that $\operatorname{rank} \Phi_a^f = \deg b$ ($\operatorname{rank} \Phi_b^f = \deg a$). We use the bijective map V_1 used in the proof of Theorem 1. From equation (7), for any $c \in \mathbb{F}_q[x]/(f)$,

$$a \cdot c = 0 \Leftrightarrow \Phi_a^f \cdot V_1(c) = \mathbf{0}.$$

Since there does not exist $c \in \mathbb{F}_q[x]/(f)$ such that $a \cdot c = 0$ and $\deg c < \deg b$, the first $\deg b$ column vectors are linearly independent. Furthermore, since $\Phi_a^f \cdot V_1(b) = \mathbf{0}, \Phi_a^f \cdot V_1(xb) = \mathbf{0}, \ldots, \Phi_a^f \cdot V_1(x^{\deg a - 1} b) = \mathbf{0}$, we have $\operatorname{rank} \Phi_a^f = \deg b$. It is similarly proved that $\operatorname{rank} \Phi_b^f = \deg a$.

Next, we design $L \in \mathbb{F}_q^{\ell\times\ell}$ such that the first $\deg b$ column vectors of L are bases of the column vector space of $\Phi_a^f W^{-1}$ and the other $(\ell - \deg b)$ $(= \deg a)$ column vectors of L are bases of the column vector space of $\Phi_b^f W^{-1}$.

Finally, we prove that the column vector spaces of $\Phi_a^f W^{-1}$ and $\Phi_b^f W^{-1}$ have no intersection; that is, the column vector spaces of Φ_a^f and Φ_b^f have no intersection. If this statement holds, L constructed using this approach is invertible. We assume that the column vector spaces of Φ_a^f and Φ_b^f have an intersection. Then, there exist two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^\ell$ such that the last $(\ell - \deg b)$ elements of $\mathbf{x}$ and the last $(\ell - \deg a)$ elements of $\mathbf{y}$ are zero, and $\Phi_a^f \mathbf{x} = \Phi_b^f \mathbf{y}$ since the first $\deg b$ $(\deg a)$ vectors of Φ_a^f (Φ_b^f) are linearly independent. From the definition of Φ_g^f, $aV_1^{-1}(\mathbf{x}) = bV_1^{-1}(\mathbf{y})$, $\deg(V_1^{-1}(\mathbf{x})) < \deg b$, and $\deg(V_1^{-1}(\mathbf{y})) < \deg a$. However, this contradicts that $f_1, \ldots, f_k$ are distinct and irreducible. Therefore, the column vector spaces of Φ_a^f and Φ_b^f have no intersection. $\square$

Next, we discuss another case where f is reducible.

Theorem 4. *With the same notation as in Theorem 3, if there exists $f' \in \mathbb{F}_q[x]$ such that ${f'}^2 \mid f$, there exists an invertible matrix $L \in \mathbb{F}_q^{\ell\times\ell}$ such that, for any $X \in WA_f$,*

$$(L^\top XL)_{\ell\ell} = 0.$$

Proof. From the assumption, there exists $a \in \mathbb{F}_q[x]/(f)$ such that $a^2 = 0$. Therefore, for any $g \in \mathbb{F}_q[x]/(f)$,

$$\begin{aligned}(\Phi_a^f W^{-1})^\top (W\Phi_g^f)(\Phi_a^f W^{-1}) &= \Phi_{a\cdot g\cdot a}^f W^{-1}\\ &= 0_{\ell\times\ell},\end{aligned}$$

and $\Phi_a^f W^{-1}$ is symmetric. We suppose that $L \in \mathbb{F}_q^{\ell\times\ell}$ is an invertible matrix in which the ℓ-th column vector is chosen from the column vectors of $\Phi_a^f W^{-1}$. Then, from the above equation, for any $g \in \mathbb{F}_q[x]/(f)$, the (ℓ,ℓ) element of $L^\top(W\Phi_g^f)L$ is zero. □

Appendix B: Proof of Theorem 2 in Subsection 5.3

Theorem 2. *With the same notation as in Theorem 1,*

1. *there exists an invertible matrix $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ such that, for any $g \in \mathbb{F}_q[x]/(f)$, $L^{-1}\Phi_g^f L$ is diagonal,*
2. *for any $X \in WA_f$, $L^\top XL$ is diagonal,*
3. *if, for any $X \in WA_f$, there exists $\mathbf{y} \in \mathbb{F}_{q^\ell}^{\ell}$ such that $\mathbf{y}^\top X\mathbf{y} = 0$, $\mathbf{y} = \mathbf{0}$.*

Proof. First, we prove statement 1. For $x \in \mathbb{F}_q[x]/(f)$, the characteristic polynomial of Φ_x^f is equal to f. Since f is irreducible over $\mathbb{F}_q[x]$, f is separable, and its roots are distinct in $\mathbb{F}_{q^\ell}[x]$. Therefore, the eigenvalues of Φ_x^f are distinct in $\mathbb{F}_{q^\ell}$, and there exists $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ such that $L^{-1}\Phi_x^f L$ is diagonal. Furthermore, Φ_1^f is the identity matrix, and $\Phi_{x^i}^f$ $(i = 2,\ldots,\ell-1)$ can be diagonalized by using L:

$$\begin{aligned}L^{-1}\Phi_{x^i}^f L &= L^{-1}(\Phi_x^f \cdots \Phi_x^f)L\\ &= (L^{-1}\Phi_x^f L)\cdots(L^{-1}\Phi_x^f L).\end{aligned}$$

Then, for any $g \in \mathbb{F}_q[x]/(f)$, $L^{-1}\Phi_g^f L$ becomes diagonal since A_f is spanned by $\{\Phi_1^f, \Phi_x^f, \ldots, \Phi_{x^{\ell-1}}^f\}$ over $\mathbb{F}_q$.

Next, we prove statement 2 by using the following lemma.

Lemma 2. *With the same notation as in Theorem 1, for $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ described in Theorem 2, $L^\top WL$ is diagonal.*

Proof. Since $W\Phi_g^f$ is symmetric,

$$W\Phi_g^f = (W\Phi_g^f)^\top = (\Phi_g^f)^\top W^\top.$$

Furthermore, since Φ^f_1 is the identity matrix, W is symmetric. As a result, we have

$$(\Phi^f_g)^\top = W\Phi^f_g W^{-1}. \tag{13}$$

As $L^{-1}\Phi^f_g L$ is symmetric,

$$\begin{aligned} L^{-1}\Phi^f_g L &= L^\top(\Phi^f_g)^\top L^{-\top} \\ &= L^\top W\Phi^f_g W^{-1}L^{-\top} \quad (\because (13)) \\ &= (L^\top WL)(L^{-1}\Phi^f_g L)(L^\top WL)^{-1}. \end{aligned}$$

Then, $L^\top WL$ and $L^{-1}\Phi^f_g L$ are commutative. As $L^{-1}\Phi^f_g L$ is diagonal and diagonal elements are distinct, $L^\top WL$ is diagonal. □

For any $g \in \mathbb{F}_q[x]/(f)$, we can transform $L^\top W\Phi^f_g L$:

$$L^\top W\Phi^f_g L = (L^\top WL)(L^{-1}\Phi^f_g L).$$

From statement 1 and Lemma 2, $L^\top W\Phi^f_g L$ is diagonal.

Finally, we prove statement 3. Let $\mathbf{y} := L^{-1}\mathbf{x}$; then

$$\begin{aligned} \mathbf{x}^\top W\Phi^f_g\mathbf{x} &= (L\mathbf{y})^\top W\Phi^f_g(L\mathbf{y}) \\ &= \mathbf{y}^\top(L^\top WL)(L^{-1}\Phi^f_g L)\mathbf{y}. \end{aligned}$$

If we define the diagonal elements of $L^{-1}\Phi^f_x L$ as $\theta_1,\ldots,\theta_\ell$ (the roots of f in $\mathbb{F}_{q^\ell}$), the diagonal elements of $L^{-1}\Phi^f_g L$ are equal to $g(\theta_1),\ldots,g(\theta_\ell)$. If $\mathbf{y}' := \left(y_1^2 \ldots y_\ell^2\right)^\top$,

$$\begin{aligned} &\mathbf{y}^\top(L^\top WL)(L^{-1}\Phi^f_g L)\mathbf{y} = 0 \\ \Leftrightarrow &\left(g(\theta_1) \cdots g(\theta_\ell)\right)(L^\top WL)\mathbf{y}' = 0 \end{aligned} \tag{14}$$

since $L^\top WL$ is diagonal.

Let $g_1,\ldots,g_\ell$ be a basis of $\mathbb{F}_q[x]/(f)$ over $\mathbb{F}_q$; then satisfying equation (14) for any $g \in \mathbb{F}_q[x]/(f)$ is equivalent to

$$\begin{pmatrix} g_1(\theta_1) & \ldots & g_1(\theta_\ell) \\ \vdots & \ddots & \vdots \\ g_\ell(\theta_1) & \ldots & g_\ell(\theta_\ell) \end{pmatrix}(L^\top WL)\mathbf{y}' = \mathbf{0}. \tag{15}$$

In addition, $g_1,\ldots,g_\ell$ are also a basis of $\mathbb{F}_{q^\ell}[x]/(f)$ over $\mathbb{F}_{q^\ell}$, and

$$\begin{aligned} \mathbb{F}_{q^\ell}[x]/(f) &\cong \mathbb{F}_{q^\ell}[x]/(x-\theta_1) \oplus \mathbb{F}_{q^\ell}[x]/(x-\theta_2) \oplus \cdots \oplus \mathbb{F}_{q^\ell}[x]/(x-\theta_\ell) \\ &\cong \mathbb{F}_{q^\ell}^\ell. \end{aligned}$$

Therefore, $(g_i(\theta_1)\cdots g_i(\theta_\ell))$ $(i = 1,\ldots,\ell)$ are linearly independent, and

$$\begin{aligned} (15) &\Leftrightarrow \mathbf{y}' = \mathbf{0} \\ &\Leftrightarrow \mathbf{y} = \mathbf{0} \\ &\Leftrightarrow \mathbf{x} = \mathbf{0}. \end{aligned}$$

□

Table 6. Performance of QR-UOV in Subsection 4.2 in Magma algebra system [6].

parameter	(q, v, m, ℓ)	key generation	signature generation	verification
QR-UOV I	$(7, 122, 68, 2)$	0.05 s	0.03 s	0.01 s
QR-UOV III	$(7, 276, 102, 3)$	0.54 s	0.23 s	0.04 s
QR-UOV V	$(31, 210, 108, 2)$	0.79 s	0.28 s	0.04 s

Appendix C: Performance in Magma

Here we present the execution times for key generation, signature generation, and verification of QR-UOV in Subsection 4.2. All experiments were performed on a MacBook Pro with a 2.4-GHz quad-core, Intel Core i5 CPU and running the Magma algebra system (V2.24-82) [6]. Table 6 shows the average times for 100 runs using QR-UOV scheme described in Subsection 4.2 and our proposed parameters for levels I, III, and V of the NIST PQC project. All timings are in second. These are not optimized implementations.

In the key generation step, we first generate two 32-bit seeds ($\mathbf{s}_{sk}$ and $\mathbf{s}_{pk}$) by using the Magma `Random` command. We then use the Magma `SetSeed` command as a pseudo random number generator to generate part of the public and secret keys. (In Subsection 6.2 we stated that the size of the two seeds is 256 bits, but here we use two 32-bit seeds since the size of the input for `SetSeed` is at most 32 bits.) Next, we generate a secret key by using the method described in Subsection 4.2. In the signature generation step, we recover the public and secret keys from the two seeds and perform the procedure explained in Subsection 2.2. Note that the signature is generated in the same manner that a signature is generated in compressed Rainbow [10]. In the verification step, we generate the public key from the $\mathbf{s}_{pk}$ seed and follow the procedure explained in Subsection 2.1. Note that, in the signature generation and verification steps, we need to compute the product of a vector and matrices $W\Phi_g^f$ or $\Phi_g^f W^{-1}$, and this computation is efficient only if the coefficients of g without the matrix structure of Φ_g^f are used.

For example, in Table 6, the execution times of the key generation, signature generation, and verification steps of QR-UOV for level I are 0.05 s, 0.03 s, and 0.01 s, respectively.