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
{furue-hiroki261,takagi}@g.ecc.u-tokyo.ac.jp
[2] Kyushu University, Fukuoka, Japan
ikematsu@imi.kyushu-u.ac.jp
[3] NTT Secure Platform Laboratories, Tokyo, Japan
yutaro.kiyomura.vs@hco.ntt.co.jp

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; thus, various methods have been proposed to reduce its size. In this paper, we propose a new variant of UOV with a public key represented by block matrices whose components correspond to an element of a quotient ring. We discuss how this affects the security of our proposed scheme, whether the quotient ring is a field. Furthermore, we discuss their security against currently known and newly possible attacks and propose parameters for our scheme. We demonstrate that our proposed scheme can achieve a small public key size without significantly increasing the signature size compared to 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 compressed Rainbow is 252.3 KB, where Rainbow is a variant of the UOV and one of the third-round finalists of the NIST PQC project.

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

1 Introduction

Currently used public key cryptosystems such as RSA and ECC can be broken in polynomial time using a quantum computer executing Shor's algorithm [31]. Thus, there has 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 [23].

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 ($\mathcal{MQ}$) problem), is regarded to be a strong candidate for PQC. The $\mathcal{MQ}$ problem is NP-complete [18] and is thus likely to be secure in the post-quantum era.

The unbalanced oil and vinegar signature scheme (UOV) [20], a multivariate signature scheme proposed by Kipnis et al. at EUROCRYPT 1999, has withstood various types of attacks for approximately 20 years. UOV is a well-established signature scheme owing to its short signature and short execution time. Rainbow [12]—a multilayer UOV variant—was selected as a third-round finalist in the NIST PQC project [26]. However, both UOV and Rainbow have public keys much larger than those of other PQC candidates, for example, lattice-based signature schemes. Indeed, Rainbow has the largest public key among the third-round-finalist signature schemes, and NIST's report [26] states that Rainbow is unsuitable as a general-purpose signature scheme owing to this problem.

The CRYSTALS-DILITHIUM [22] 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 [8]. As is well known, LWE [29] is a confidential hard problem in cryptography, and the MLWE problem is a generalization of it using a module comprising 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. [27]. This technique can be applied to various UOV variants and is based on the fact that a part of a public key can be arbitrarily chosen before determining the secret key. This indicates that a part of a public key can be generated using a seed of a pseudo random number generator. The version of Rainbow using this technique and a secret key compression technique is called "compressed Rainbow" in the third-round finalist NIST PQC project [11]. The second approach is to use the lifted unbalanced oil and vinegar (LUOV) [6] that uses polynomials over a small field as a public key, whereas the signature and message spaces are defined over an extension field. This results in a small public key. LUOV was thus selected as a candidate in the second round of the NIST PQC project [25]. However, several of its parameters were broken using the new attack proposed by Ding et al. [14]. The third approach is to use the block-anti-circulant UOV (BAC-UOV) developed by Szepieniec et al. and presented at SAC 2019 [32]. Its public key is represented by block-anti-circulant matrices, wherein every block is an anti-circulant matrix. As 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, block-anti-circulant-matrices can be transformed into the diagonal concatenation of two smaller matrices. This enabled Furue et al. [17] 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 of 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 called QR-UOV. In 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 study, 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 of $\mathbb{F}_q$ because the polynomial matrix Φ_g^f is determined by the ℓ coefficients of g. This can be considered as a generalization of BAC-UOV [32], which is the case for $f = x^\ell - 1$. Utilizing the elements of a quotient ring in block matrices is similar to the MLWE problem [8] because the MLWE problem uses elements of a ring in vectors. Namely, we can consider that the research undertaken to obtain from UOV to QR-UOV (including BAC-UOV) corresponds to that obtained from LWE to MLWE. Therefore, as with the MLWE problem, this type of research deserves more attention than passing notice.

To construct the QR-UOV, we must consider the symmetry of the polynomial matrices Φ_g^f. In UOV, the public key $\mathcal{P} = (p_1, \ldots, p_m)$, which comprises 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 wherein 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. Polynomial matrices Φ_g^f are generally unstable under the transpose operation, 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 Theorem 1 herein, we prove that there exists such W for any quotient rings $\mathbb{F}_q[x]/(f)$. Therefore, from equations

$$(W\Phi_{g_1}^f)^\top(\Phi_{g_2}^f W^{-1})W\Phi_{g_3}^f = (W\Phi_{g_1}^f)(\Phi_{g_2}^f W^{-1})W\Phi_{g_3}^f = W\Phi_{g_1g_2g_3}^f,$$

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 with $W\Phi_g^f$.

Moreover, we should consider how the choice of f affects the security of the QR-UOV. Furue et al. [17] 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 relation 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 2 herein, we show that if f is irreducible (*i.e.,* $\mathbb{F}_q[x]/(f)$ is a field), then there does not exist such a transformation for matrices $W\Phi_g^f$, indicating that such an f is resistant to Furue et al.'s structural attack [17].

Based on these considerations regarding 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 [17]. We investigated its performance against both currently known and possible attacks. The currently known attacks include the direct attack, the UOV attack [21], the reconciliation attack [13], and the intersection attack [5]. Possible attacks are derived from (1) pull-back techniques and (2) lifting techniques. In (1), the UOV, reconciliation, and intersection attacks are executed over the quotient-ring $\mathbb{F}_q[x]/(f)$ by pulling $W\Phi_g^f$ back to g. In (2), we prove that by lifting the base field $\mathbb{F}_q$ to the extension field $\mathbb{F}_{q^\ell}$, the QR-UOV public key can be transformed into the diagonal concatenation of some smaller matrices: as is done in the structural attack on BAC-UOV. After applying such a transformation over $\mathbb{F}_{q^\ell}$, we execute the four currently known attacks.

Finally, by considering these currently known and possible attacks, we can select the appropriate parameters for the QR-UOV. In accordance with the I, III, and V security levels of the NIST PQC project [24], we propose three parameters for QR-UOV. These parameters achieve a small public key, and the sizes of the public keys are approximately 30%–50% of those of compressed Rainbow [11]. For example, the public key size is 66.7 KB for security level III, whereas that of compressed 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 The remainder of this 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 the polynomial matrices of a quotient ring as a generalization of the circulant matrices. In Section 4, we describe the proposed signature scheme, QR-UOV. In Section 5, we analyze the security of the 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 based on this problem. Subsequently, we review the construction of the UOV [20]. We then describe the construction of the BAC-UOV [32] and finally explain Furue et al.'s structural attack [17] on BAC-UOV.

2.1 Multivariate Signature Schemes

Let $\mathbb{F}_q$ be a finite field with q elements, and let 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 obtaining 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 [18] 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 the 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 to hide the structure of $\mathcal{F}$. The public key $\mathcal{P}$ is then provided 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 comprises $\mathcal{T}$, $\mathcal{F}$, 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 obtain a solution $\mathbf{m}_2$ to the equation $\mathcal{F}(\mathbf{x}) = \mathbf{m}_1$. This gives the signature $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{m}_2) \in \mathbb{F}_q^n$ for the message. Verification is performed by confirming whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$.

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 required because it does not help hide the structure of $\mathcal{F}$. Thus, the secret key comprises $\mathcal{F}$ and $\mathcal{S}$.

Next, we explain the inversion 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 $\mathbb{F}_q$ as the vinegar variables. We can then efficiently obtain a solution $(a_{v+1}, \ldots, a_n)$ for the equation $\mathcal{F}(a_1, \ldots, a_v, x_{v+1}, \ldots, x_n) = \mathbf{y}$ because 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 the 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 as follows. For each $1 \leq i \leq m$, 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), 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 an $n \times n$ symmetric matrix 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 [32] is a variant of the UOV. The public key is shortened by representing it using block-anti-circulant matrices. In this subsection, we describe the construction of BAC-UOV.

A circulant matrix is a matrix wherein each row vector is rotated by one element to the right relative to the preceding row vector. An anti-circulant matrix is a matrix wherein each row vector is rotated by 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 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 the 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 the 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.

Owing 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 the plain UOV. That is, the public key was smaller than that of the 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 [17]. The attack utilizes the property of the anti-circulant matrix, wherein 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-component of A, namely

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

Subsequently, 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 wherein each block is in the form of equation (5). Furthermore, a permutation matrix L' exists 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 [21] can then be executed on only the upper-left $N \times N$ submatrices of the obtained matrices with little complexity. By using the transformed public key, we can reduce the number of variables appearing in the public equations $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ for a message $\mathbf{m}$. This reduces the complexity of the attack by approximately 20% compared with the best existing attack on the UOV. This attack can be executed only if there exists a transformation on the public key, as 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 [32] and describe a method for converting polynomial matrices into symmetric matrices 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

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

From this equation, we have

$$x^{j-1}g = \sum_{i=1}^{\ell} \left(\Phi_g^f\right)_{ij} \cdot x^{i-1} \quad (1 \le j \le \ell),$$

and $\left(\Phi_g^f\right)_{ij}$ is the coefficient of x^{i-1} in $x^{j-1}g$. We call such a matrix Φ_g^f the *polynomial matrix* of g. The following lemma can be easily derived from this definition:

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

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

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

An $\ell \times \ell$ polynomial matrix Φ_g^f can be represented by only ℓ elements in $\mathbb{F}_q$, because Φ_g^f is determined by the ℓ coefficients of $g \in \mathbb{F}_q[x]/(f)$. We let the algebra of the matrices $A_f := \left\{\Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} \mid g \in \mathbb{F}_q[x]/(f)\right\}$. 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 shown 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. Thus, to construct our proposed scheme, we need an explicit family of f and W such that WA_f is stable under the transpose operation. In the following theorem, we prove that there exists an invertible matrix W for any f.

Theorem 1. *Let $f \in \mathbb{F}_q[x]$ with $\deg f = \ell$. Then, there exists an invertible matrix $W \in \mathbb{F}_q^{\ell\times\ell}$ such that WX is a symmetric matrix for any $X \in A_f$.*

Proof. Let $\phi : \mathbb{F}_q[x]/(f) \to \mathbb{F}_q$ be a non-zero linear map. We define W such that the ij-component of W is equal to $\phi(x^{i+j-2})$. Then, for any $g \in \mathbb{F}_q[x]/(f)$, we have the following:

$$\begin{aligned}
(W\Phi_g^f)_{ij} &= \sum_{k=1}^{\ell} \phi(x^{i+k-2})(\Phi_g^f)_{kj} \\
&= \phi\left(\sum_{k=1}^{\ell} x^{i+k-2}(\Phi_g^f)_{kj}\right) \\
&= \phi\left(x^{i-1}\left(\sum_{k=1}^{\ell} x^{k-1}(\Phi_g^f)_{kj}\right)\right) \\
&= \phi(x^{i-1}x^{j-1}g) \qquad (\because (7)) \\
&= \phi(x^{i+j-2}g) \\
&= (W\Phi_g^f)_{ji}.
\end{aligned}$$

This equation shows that $W\Phi_g^f$ is symmetric.

If we define ϕ such that $\phi(a_0 + a_1 x + \cdots + a_{\ell-1}x^{\ell-1}) = a_{\ell-1}$, then W is of the following form:

$$\begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & * \end{pmatrix},$$

and hence W is invertible. This indicates that there exists one invertible matrix W constructed using the above method. $\square$

As stated in Subsection 3.2 below, from a security perspective, f must be irreducible in our scheme. Furthermore, from the perspective of efficiency, f should have only a few non-zero terms. As there are no irreducible binomials f with $\deg f = \ell$ for many ℓ, trinomials f are considered suitable for our scheme. The following example shows that there are some trinomials f and suitable W for symmetrization purposes.

Example 1. We assume that $f = x^\ell - ax^i - 1$ $(a \in \mathbb{F}_q, 1 \leq i \leq \ell - 1)$. If $W \in \mathbb{F}_q^{\ell\times\ell}$ is constructed using a linear map $\phi : \mathbb{F}_q[x]/(f) \to \mathbb{F}_q$ such that $\phi(a_0 + a_1 x + \cdots + a_{\ell-1}x^{\ell-1}) = a_{i-1}$, then we can represent the matrix W as

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

where $J_i := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}$ denotes the anti-identity matrix of size i. From Theorem 1, WX becomes a symmetric matrix for any $X \in A_f$.

The polynomial f needs to be irreducible in our scheme; thus, we conducted several experiments to confirm the irreducibility of $x^\ell - ax^i - 1$. We treated the

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 $\mathbb{F}_q = \mathbb{F}_7$.

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

finite field $\mathbb{F}_q = \mathbb{F}_7$, which is used for our proposed scheme as described below, and checked whether there exists an irreducible polynomial $f \in \mathbb{F}_q[x]$ in 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.

Finally, if we choose $f = x^\ell - 1$ and a linear map $\phi : \mathbb{F}_q[x]/(f) \to \mathbb{F}_q$ such that $\phi(a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1}) = a_{\ell-1}$, then $W = J_\ell$ and $W\Phi_g^f$ is an anti-circulant matrix. Thus, this choice corresponds exactly to BAC-UOV [32], and Theorem 1 can be regarded as describing the generalization of anti-circulant matrices.

3.2 Effect of Irreducibility of f

In this subsection, we discuss the relation between the irreducibility of the polynomial f used to generate the 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 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 2. *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. Subsequently, there is no invertible matrix $L \in \mathbb{F}_q^{\ell\times\ell}$ and $i, j \in \{1, \ldots, \ell\}$ such that, for any $X \in WA_f$,*

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

Proof. We assume that there exists 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, we have $L_i^\top \Phi_h^f L_j = 0$ for any $h \in \mathbb{F}_q[x]/(f)$.

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

$$V_1(a_0 + a_1x + \cdots + a_{\ell-1}x^{\ell-1}) = (a_0, a_1, \ldots, a_{\ell-1})^\top,$$

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. Because A_f is a field, Φ_g^f is the zero matrix, namely $g = 0$. As a result, V_2 is an isomorphism.

Let $g_i := V_2^{-1}(L_i)$ and $g_j := V_1^{-1}(L_j)$. Clearly, $(\Phi^f_{g_i}\Phi^f_h\Phi^f_{g_j})_{11} = L_i^\top \Phi^f_h L_j = 0$ 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 2 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 of elements of WA_f with reducible f by using Theorems 4 and 5 in Appendix A. Theorem 4 shows that if f is decomposed into distinct irreducible polynomials, WA_f are transformed into a concatenation of two smaller submatrices. In fact, the transformation, as in equation (5) in the structural attack on BAC-UOV, corresponds to the transformation described in Theorem 4. If f is divisible by a squared polynomial, Theorem 5 shows that the representation matrices can be transformed by executing a change of variables into a special form wherein 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.

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. There exist f and W satisfying the above condition for many ℓ, as shown by Theorem 1 and the discussion in Subsection 3.1. We define 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 1. *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 $Y := \Phi_{g_2}^f W^{-1}$. Owing 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. □

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

Remark 2. We can apply the polynomial matrices of a quotient ring to both UOV and Rainbow.

4.2 Improved QR-UOV

In this subsection, we explain two improved methods used in the NIST third-round proposal of Rainbow [11]. First, the secret key $\mathcal{S}$ is limited to a specific compact form. The second replaces a large part of the public key with a small seed for pseudo random number generation (PRNG).

In the plain UOV, the matrix S of the secret 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 because it does not affect the security. In QR-UOV, the upper-left and lower-right identity submatrices in S are replaced with block diagonal matrices in which every diagonal block is $W\Phi_1^f = W$ because S is chosen in $W^{(N)}A_f^{(N)}$. Namely, S is written as

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

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 [27]. The version of Rainbow using this technique and a secret key compression technique is called "compressed Rainbow" in the third-round finalist NIST PQC project [11]. The representation matrices P_i $(i = 1, \dots, m)$ 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 $(i = 1, \dots, m)$ 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, as we have

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

where $S'' := -(W^{-1})^{(v/\ell)} S' (W^{-1})^{(m/\ell)}$, the representation matrices F_i, P_i $(i = 1, \dots, m)$, 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, $P_{i,1}$, $P_{i,2}$ $(i = 1, \dots, m)$, and S' are first generated from seeds $\mathbf{s}_{pk}$ and $\mathbf{s}_{sk}$, respectively, using PRNG. Next, $P_{i,3}$ $(i = 1, \dots, m)$ is 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 $\mathbf{s}_{pk}$ for $P_{i,1}$, $P_{i,2}$ ($i = 1, \ldots, m$). This compression technique significantly reduced the public key size of the 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 by $P_{i,1}$, $P_{i,2}$, and $P_{i,3}$ ($i = 1, \ldots, m$), and that of the improved QR-UOV uses a seed $\mathbf{s}_{pk}$ and $P_{i,3}$ ($i = 1, \ldots, m$). Thus, the number of elements in $\mathbb{F}_q$ needed to represent the public key of the 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 four 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 consider QR-UOV as the plain UOV described in Subsection 2.2 and describe the execution of four currently known attacks on UOV—the direct attack, UOV attack [21], reconciliation attack [13], and intersection attack [5].

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 with high probability.

One of the best-known approaches for algebraically solving the quadratic system is the hybrid approach [4] that randomly guesses k ($k = 0, \ldots, n$) variables before computing a Gröbner basis [9]. The guessing was repeated until a solution was obtained. Well-known algorithms for computing Gröbner bases include F4 [15], F5 [16], and XL [10]. The complexity of this approach for a classical adversary is estimated as follows:

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

Table 2. Theoretical and experimental degree of regularity of public key system of QR-UOV obtained using the Magma algebra system [7].

(q, v, m, ℓ, k)	theoretical d_{reg}	experimental d_{reg}
$(7, 24, 12, 3, 0)$	13	13
$(7, 24, 12, 3, 1)$	7	7
$(7, 24, 12, 3, 2)$	6	6
$(7, 30, 15, 3, 0)$	16	16
$(7, 30, 15, 3, 1)$	8	9
$(7, 30, 15, 3, 2)$	7	7

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 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 the UOV is considered to be a semi-regular system. Therefore, this series (10) can be used to estimate the degree of regularity.

However, the complexity of a quantum direct attack is estimated to be

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

by using Grover's algorithm [19].

Thomae and Wolf [33] 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. This technique can be fully applied only to 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 cases and empirically makes the direct attack faster on quadratic systems over finite fields of odd characteristics. Therefore, from a security perspective, it is not extreme that we consider this technique to be applicable to odd characteristic cases.

In Table 2, for a QR-UOV public key system, we compare the theoretical d_{reg} and experimental d_{reg}. The theoretical d_{reg} is the degree of regularity obtained by equation (10), assuming that the system is semi-regular. The experimental d_{reg} is the highest degree among the step degrees, where non-zero polynomials are generated in experiments of the direct attack using the Magma algebra system [7]. In our experiment, m was set to sufficiently large values so that our computation for one parameter was performed within one day, and v is set equal to $2m$, while q and ℓ are set to the values given in Subsection 6.1. For the public key of the QR-UOV with $(v + m)$ variables and m equations, we fix the last v variables and execute the hybrid approach by fixing k variables additionally. These results demonstrate that the degrees of regularity obtained experimentally were the same as those obtained theoretically.

Remark 3. In the case of $(q, v, m, \ell, k) = (7, 30, 15, 3, 1)$ in Table 2, the experimental d_{reg} is larger than the theoretical d_{reg}. However, our experiment shows that the experimental d_{reg} of the same size randomized quadratic system of m equations in $(m - k)$ variables over $\mathbb{F}_7$ is not different from our experimental d_{reg} of $(q, v, m, \ell, k) = (7, 30, 15, 3, 1)$.

UOV Attack The UOV attack [21] obtains 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). This $\mathcal{S}'$ is called the *equivalent key*. The UOV attack obtains 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

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

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

$$O\left(q^{\frac{v-m-1}{2}} \cdot m^4\right).$$

Reconciliation Attack The reconciliation attack [13] also obtains, similar to the UOV attack, an equivalent key $\mathcal{S}'$. The reconciliation attack treats every component of the matrix S' as a variable and solves the quadratic system of equations obtained 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, where the upper-left component has index (a, b). This attack can be decomposed into a series of steps; 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 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 a quadratic system with v variables and v equations, which are obtained by (9) and (11) as $n = v$. If $v \leq m$, 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.

Intersection Attack In [5], Beullens proposed a new attack against UOV, called the intersection attack.

The intersection attack attempts to obtain an equivalent key by recovering the subspace $S^\top(\mathcal{V})$ of $\mathbb{F}_q^n$, where S is the representation matrix for the secret key $\mathcal{S}$ and $\mathcal{V}$ is the vinegar subspace defined as the orthogonal subspace of the oil subspace. The intersection attack solves the following equations for $\mathbf{y} \in \mathbb{F}_q^n$:

$$\begin{cases} (W_i\mathbf{y})^\top P_k (W_i\mathbf{y}) = 0 \\ (W_j\mathbf{y})^\top P_k (W_j\mathbf{y}) = 0 \\ (W_i\mathbf{y})^\top P_k (W_j\mathbf{y}) = 0 \end{cases} \tag{12}$$

where W_i, W_j are two invertible matrices chosen from a set of linear combinations of the public key $P_1, \ldots, P_m$. In the case where $n < 3m$, the solution space obtained from equations (12) is of the $(3m-n)$ dimensions. Thus, its complexity is equivalent to that of solving the quadratic system with $n-(3m-n) = 2n-3m$ variables and $(3m-2)$ equations. In contrast, in the case where $n \geq 3m$, the intersection attack becomes a probabilistic algorithm for solving the system (12) with n variables and $(3m-2)$ equations with a probability of approximately $q^{-n+3m-1}$. Therefore, its complexity is estimated by q^{n-3m+1} times the complexity of solving the quadratic system with n variables and $(3m-2)$ equations.

Remark 4. In [5], Beullens proposed a new attack against Rainbow, called the rectangular MinRank attack. This attack uses non-full-rank property of Rainbow and thus does not affect the security of our proposed scheme.

5.2 Pull-back Attacks over Quotient Ring

In this subsection, we explain a technique for executing four currently known attacks on QR-UOV by utilizing the block structure derived 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 [21], reconciliation attack [13], and intersection attack [5] in the quotient-ring $\mathbb{F}_q[x]/(f)$ by replacing $W\Phi_g^f$ with g.

For this, 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 $G_2 : A_f^{(N)}(W^{(N)})^{-1} \to (\mathbb{F}_q[x]/(f))^{N\times N}$. In the following, we consider the execution of the four currently known attacks described in Subsection 5.1 on $G_1(P_1), \ldots, G_1(P_m)$, which is called the pull-back technique.

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 obtain an equivalent key S' for the transformed matrices by executing the UOV attack over $\mathbb{F}_q[x]/(f)$, then $G_2^{-1}(S') \in \mathbb{F}_q^{n\times n}$ is an equivalent key over $\mathbb{F}_q$. The complexities of the pull-back UOV attack for a classical and quantum attacker are

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

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

Second, the pull-back reconciliation attack is 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 $\mathbb{F}_q[x]/(f)$.

Third, we discuss applying the pull-back technique to the intersection attack. The pull-back intersection attack can also be seen as the intersection attack on the UOV with v/ℓ vinegar variables and m equations in $\mathbb{F}_q[x]/(f)$. From the discussion in Subsection 5.1, When $n < 3m$, the complexity of the pull-back intersection attack is equivalent to that of solving the quadratic system with $(2n-3m)/\ell$ variables and $(3m-2)$ equations in $\mathbb{F}_q[x]/(f)$. On the contrary, in the case where $n \geq 3m$, the complexity of the pull-back intersection attack is estimated by $q^{n-3m+\ell}$ times the complexity of solving the quadratic system with n/ℓ variables and $(3m-2)$ equations.

Finally, for the direct attack, as 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 2, 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, such as 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, such a transformation exists in the public key of QR-UOV over the extension field $\mathbb{F}_{q^\ell}$. In this subsection, we explain a technique for transforming the public key over $\mathbb{F}_{q^\ell}$ and how this affects the four currently known attacks on the UOV.

Theorem 3. *With the same notation as in Theorem 2,*

(i) There exists an invertible matrix $L \in \mathbb{F}_{q^\ell}^{\ell \times \ell}$ such that $L^{-1}\Phi_g^f L$ is diagonal for any $g \in \mathbb{F}_q[x]/(f)$.
(ii) The matrix L described in (i) satisfies the condition that $L^\top X L$ is diagonal for any $X \in WA_f$.
(iii) If there exists $\mathbf{y} \in \mathbb{F}_{q^\ell}^{\ell}$ such that $\mathbf{y}^\top X \mathbf{y} = 0$ for any $X \in WA_f$, then $\mathbf{y} = \mathbf{0}$.

(The proof is provided in the appendix.)

First, Theorem 3 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 $n \times n$ block diagonal matrix with block size ℓ ($n = \ell \cdot N$), for which the N diagonal blocks are L. Then, $(L^{(N)})^\top P_i L^{(N)}$ ($i = 1, \ldots, m$) become block matrices wherein every component is in a 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, and let

$\bar{L} := L^{(N)}L'$. Finally, this theorem states that there does not exist a change of variables over $\mathbb{F}_{q^\ell}$ such that it directly recovers the structure of the central map of the UOV.

Next, we consider the complexities of the lifting UOV, reconciliation, and intersection attacks which are the UOV attack [21], the reconciliation attack [13], and the intersection attack [5] 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 as $(\bar{L}^\top S \bar{L})^\top (\bar{L}^{-1} F_i \bar{L}^{-\top})\ (\bar{L}^\top S \bar{L})$. Then, $\bar{L}^\top S \bar{L}$ is the diagonal concatenation of ℓ smaller matrices, similar to $\bar{L}^\top P_i \bar{L}$. Furthermore, $\bar{L}^{-1} F_i \bar{L}^{-\top}$ is a diagonal block matrix because

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

where $L^{-1}\Phi_g^f L$ and $L^\top W L$ are diagonal from (i) and (ii) in Theorem 3. Then, owing 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. Therefore, each diagonal block of $\bar{L}^\top P_i \bar{L}$ has the same form as the matrix representing the public key of the UOV with v/ℓ vinegar variables and m/ℓ oil variables over $\mathbb{F}_{q^\ell}$. The lifting technique executes currently known attacks on one of such diagonal blocks. Consequently, the complexity of the lifting UOV attack on each block over $\mathbb{F}_{q^\ell}$ is $O(q^{v-m-\ell} \cdot (m/\ell)^4)$, and 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 $\mathbb{F}_{q^\ell}$. Furthermore, we can apply the lifting technique to the intersection attack. In the case where $n < 3m$, the complexity of the lifting intersection attack on each block over $\mathbb{F}_{q^\ell}$ is estimated to be the complexity of solving the quadratic system with $(2n - 3m)/\ell$ variables and $(3m - 2)$ equations over $\mathbb{F}_{q^\ell}$. In contrast, in the case where $n \geq 3m$, the complexity is estimated by $q^{n-3m+\ell}$ times the complexity of solving the quadratic system with n/ℓ variables and $(3m - 2)$ equations over $\mathbb{F}_{q^\ell}$.

Note that the complexities of the lifting UOV, reconciliation, and intersection attacks in this subsection are the same as those of the pull-back UOV, reconciliation, and intersection attacks in Subsection 5.2, respectively.

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 [33] 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 because 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, because the system is solved 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; therefore, this technique is inefficient. In conclusion, there is no effective way to execute 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 $\mathbb{F}_q^n$ because the solution is considered to be

Table 3. Theoretical and experimental degree of regularity obtained by executing the lifting direct attack using the Magma algebra system [7].

(q, v, m, ℓ, k)	theoretical d_{reg}	experimental d_{reg}
$(7, 24, 12, 3, 0)$	13	13
$(7, 24, 12, 3, 1)$	7	7
$(7, 24, 12, 3, 2)$	6	5
$(7, 30, 15, 3, 0)$	16	15
$(7, 30, 15, 3, 1)$	8	8
$(7, 30, 15, 3, 2)$	7	7

uniquely determined. This means that we can execute the direct attack on a block-diagonalized system without reducing the probability of obtaining a solution in $\mathbb{F}_q^n$. Table 3 summarizes the results of experiments investigating the degree of regularity of the block-diagonalized public key system of QR-UOV using the Magma algebra system [7]. In our experiment, v is set to be equal to $2m$. For the representation matrices $P_1, \ldots, P_m$ of the public key of the QR-UOV with $(v+m)$ variables and 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 by fixing k variables additionally. In Table 3, the theoretical d_{reg} is the degree of regularity obtained by equation (10), assuming that the system is semi-regular, and the experimental d_{reg} is the highest degree among the step degrees, where non-zero polynomials are generated in experiments of the direct attack using the Magma algebra system [7]. The results show that the experimental d_{reg} was smaller than the theoretical d_{reg} 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) with 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 [24] and compare the performance of the improved QR-UOV with that of compressed Rainbow [11].

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 [24] to enable comparison with the performance of compressed Rainbow [11]. The parameters for the improved QR-UOV are the number of finite fields q, number of vinegar variables v, number of oil variables, number of equations m, block size of the representation matrices ℓ, and polynomial used to generate the quotient-ring f. We set q odd from a security perspective. The integer v is mainly determined by the

Table 4. The complexity of the plain attacks in Subsection 5.1, the pull-back attacks in Subsection 5.2, and lifting attacks in Subsection 5.3 on the proposed parameters of QR-UOV in Subsection 6.1. Here, "dir", "UOV", "rec", and "int" denote the direct attack, UOV attack, reconciliation attack, and intersection attack, respectively. The bold font indicates the lowest complexity among all attacks at the same security level.

parameter (q, v, m, ℓ)	attack model	$\log_2(\#\text{gates})$										
		plain				pull-back			lifting			
		dir	UOV	rec	int	UOV	rec	int	dir	UOV	rec	int
QR-UOV I	classical	149	346	361	663	337	**148**	241	203	337	**148**	241
(7,183,69,3)	quantum	**102**	187	244	401	181	146	174	175	181	146	174
QR-UOV III	classical	**210**	517	528	991	508	218	351	287	508	218	351
(7,276,102,3)	quantum	**144**	274	354	593	268	209	245	247	268	209	245
QR-UOV V	classical	298	713	736	1364	704	**279**	453	410	704	**279**	453
(7,393,150,3)	quantum	**202**	373	490	819	367	275	318	350	367	275	318

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 $\ell = 3$ because a large ℓ increases the signature and execution time. From Theorem 2, we choose irreducible polynomials f in the form of $x^\ell - ax^i - 1$ described in Example 1. In summary, we propose the following parameters for improved QR-UOV:

$$\begin{aligned}
\text{QR-UOV I}: &\quad (q, v, m, \ell, f) = (7, 183, 69, 3, x^3 - 3x - 1),\\
\text{QR-UOV III}: &\quad (q, v, m, \ell, f) = (7, 276, 102, 3, x^3 - 3x - 1),\\
\text{QR-UOV V}: &\quad (q, v, m, \ell, f) = (7, 393, 150, 3, x^3 - 3x - 1).
\end{aligned}$$

Next, we show that these parameters of QR-UOV I, III, and V satisfy the security levels I, III, and V of the NIST PQC project, respectively. Here, security levels I, III, and V indicate that a classical attacker needs more than 2^{143}, 2^{207}, and 2^{272} classical gates to break the parameters, whereas a quantum attacker needs more than 2^{74}, 2^{137}, and 2^{202} quantum gates, respectively [24]. The number of gates required for an attack against the NIST third-round proposal version of Rainbow [11] can be computed using

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

Next, we consider the complexity of each attack described in Section 5 on the proposed parameters. Table 4 shows the complexity of the plain direct, UOV, reconciliation, and intersection attacks described in Subsection 5.1, the pull-back UOV, reconciliation, and intersection attacks described in Subsection 5.2, and the lifting direct, UOV, reconciliation, and intersection attacks described in Subsection 5.3. (See each subsection for a concrete way of estimating the complexity of each attack). This table does not include the complexity of "the pull-back direct attack" because we cannot execute the direct attack on the pulled back public key system, as stated in Subsection 5.2. For each parameter

Table 5. Comparison of public key and signature size of compressed Rainbow with those of QR-UOV. We use parameters for compressed Rainbow in [11], 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	Compressed Rainbow I	$(q, v_1, o_1, o_2) = (16, 36, 32, 32)$	57.4	66.0
	QR-UOV I	$(q, v, m, \ell) = (7, 183, 69, 3)$	**21.0**	**110.5**
III	Compressed 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	Compressed Rainbow V	$(q, v_1, o_1, o_2) = (256, 96, 36, 64)$	511.2	212.0
	QR-UOV V	$(q, v, m, \ell) = (7, 393, 150, 3)$	**210.1**	**219.6**

set, the upper entry shows the number of classical gates, whereas the lower entry shows the number of quantum gates. For example, the complexity of the direct attack for level I is 149 classical gates and 102 quantum gates. Furthermore, the values in bold indicate the complexity of the best attack against each parameter set. The lowest complexity among all attacks is the direct attack, except for the classical attacks on QR-UOV I and V. As a result, this table shows that the proposed parameters satisfy the requirements for each security level.

Remark 5. Similar to the proposed parameters for Rainbow [11], our proposed parameters for security levels I, III, and V also satisfy security levels II, IV, and VI of the NIST PQC project [24].

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 compressed Rainbow [11] for security levels I, III, and V. As for compressed Rainbow in the third-round proposal [11], 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 [30]. 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 approximately half that of compressed Rainbow. As a result, the public key size of the improved QR-UOV can be reduced by approximately 50%–70% compared with that of compressed Rainbow at the cost of a small increase in signature size. We stress that the Rainbow team [28] did not update the parameters of compressed Rainbow by considering the intersection attack and the rectangular MinRank attack proposed by Beullens [5].

Although the public key size could be further reduced by setting the block size ℓ larger, enlarging the block size would likely increase the signature size and increase 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 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, is that they have a large public key. Research on reducing the size of the UOV public key is important for post-quantum cryptography. In this paper, we present 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, using the proposed parameters, the public key size of the improved QR-UOV can be reduced approximately 50%–70% compared with that of compressed Rainbow, a third-round finalist in the NIST PQC project, without significantly increasing the signature size. To construct QR-UOV, we defined polynomial matrices 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, then QR-UOV is resistant to attacks that can break the block-anti-circulant UOV. We also analyzed the security of QR-UOV against four 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, a generalization of the LWE using a module comprising vectors over a ring.

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

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.: Improved cryptanalysis of UOV and Rainbow. IACR Cryptology ePrint Archive: Report 2020/1343 (2020)
6. Beullens, W., Preneel, B.: Field lifting for smaller UOV public keys. In; INDOCRYPT 2017, LNCS, vol. 10698, pp. 227–246. Springer (2017)
7. 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)
8. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012, pp. 309-325. ACM, January 2012.
9. Buchberger, B.: Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. PhD thesis, Universität Innsbruck (1965)
10. 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)
11. Ding, J., Chen, M.-S., Kannwischer, M., Patarin, J., Petzoldt, A., Schmidt, D., Yang, B.-Y.: Rainbow signature schemes proposal for NIST PQC project (round 3 version).
12. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005)
13. 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)
14. 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)
15. 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)
16. Faugère, J.-C.: A new efficient algorithm for computing Gröbner bases without reduction In: ISSAC 2002, pp. 75–83. ACM (2002)
17. 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)
18. Garey, M.-R., Johnson, D.-S.: Computers and intractability: a guide to the theory of NP-completeness. W. H. Freeman (1979)
19. Grover, L.-K.: A fast quantum mechanical algorithm for database search. In: STOC 1996, pp. 212–219. ACM (1996)
20. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999)
21. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998)
22. 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).

23. NIST: Post-quantum cryptography CSRC. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
24. 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)
25. NIST: Status report on the first round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8240, NIST (2019)
26. NIST: Status report on the second round of the NIST post-quantum cryptography standardization process. NIST Internal Report 8309, NIST (2020)
27. 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)
28. Rainbow Team: Response to Ward Beullens' new Rainbow attacks. https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/NVeyXz8wmIo/m/TEXgW8qOBQAJ (2020)
29. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC 2005, pp. 84–93, ACM (2005)
30. 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)
31. 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)
32. Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced oil and vinegar. In: SAC 2019, LNCS, vol. 11959, pp. 574–588. Springer (2019)
33. 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 wherein f is reducible and decomposed into distinct irreducible polynomials.

Theorem 4. *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 $f_1, \ldots, f_k$ are distinct, irreducible, and $\deg f_1 \leq \cdots \leq \deg f_k$, then there exists an invertible matrix $L \in \mathbb{F}_q^{\ell \times \ell}$ and $i \in \{1, \ldots, \ell-1\}$ such that for any $X \in WA_f$,*

$$L^\top XL = \begin{pmatrix} *_{i\times i} & 0_{i\times(\ell-i)} \\ 0_{(\ell-i)\times i} & *_{(\ell-i)\times(\ell-i)} \end{pmatrix}. \tag{13}$$

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.

As 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 assume 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 (13) 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 2. From equation (7), for any $c \in \mathbb{F}_q[x]/(f)$,

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

As 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, as $\Phi_a^f \cdot V_1(b) = \mathbf{0}, \Phi_a^f \cdot V_1(xb) = \mathbf{0}, \ldots, \Phi_a^f \cdot V_1(x^{\deg a - 1} b) = \mathbf{0}$, we have $\operatorname{rank} \Phi_a^f = \deg b$. Similarly, it is 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, i.e., the column vector spaces of Φ_a^f and Φ_b^f have no intersection. If this statement holds, then 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 $\Phi_a^f \mathbf{x} = \Phi_b^f \mathbf{y}$ because 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 intersections. □

Next, we discuss another case where f is reducible.

Theorem 5. *With the same notation as in Theorem 4, 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 this 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 wherein the ℓ-th column vector is chosen from the column vectors of $\Phi_a^f W^{-1}$. From the above equation, the (ℓ,ℓ) component of $L^\top(W\Phi_g^f)L$ is zero for any $g \in \mathbb{F}_q[x]/(f)$. □

Appendix B: Proof of Theorem 3 in Subsection 5.3

Theorem 3. *With the same notation as in Theorem 2,*

(i) There exists an invertible matrix $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ such that $L^{-1}\Phi_g^f L$ is diagonal for any $g \in \mathbb{F}_q[x]/(f)$.
(ii) The matrix L described in (i) satisfies the condition that $L^\top XL$ is diagonal for any $X \in WA_f$.
(iii) If there exists $\mathbf{y} \in \mathbb{F}_{q^\ell}^{\ell}$ such that $\mathbf{y}^\top X\mathbf{y} = 0$ for any $X \in WA_f$, then $\mathbf{y} = \mathbf{0}$.

Proof. First, we prove statement 1. The characteristic polynomial of Φ_x^f is equal to f for $x \in \mathbb{F}_q[x]/(f)$. As 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 $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ 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 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 because 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 2, for $L \in \mathbb{F}_{q^\ell}^{\ell\times\ell}$ described in Theorem 3, $L^\top WL$ 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, because Φ_1^f is the identity matrix, W is symmetric. As a result, we have

$$(\Phi_g^f)^\top = W\Phi_g^f W^{-1}. \tag{14}$$

As $L^{-1}\Phi_g^f L$ is symmetric,

$$\begin{aligned} L^{-1}\Phi_g^f L &= L^\top (\Phi_g^f)^\top L^{-\top} \\ &= L^\top W\Phi_g^f W^{-1} L^{-\top} \quad (\because (14)) \\ &= (L^\top W L)(L^{-1}\Phi_g^f L)(L^\top W L)^{-1}. \end{aligned}$$

Then, $L^\top W L$ and $L^{-1}\Phi_g^f L$ are commutative. As $L^{-1}\Phi_g^f L$ is diagonal, and the diagonal components are distinct, $L^\top W L$ is diagonal. □

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

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

From statement 1 and Lemma 2, $L^\top W\Phi_g^f L$ are diagonal.

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

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

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

$$\begin{aligned} & \mathbf{y}^\top (L^\top W L)(L^{-1}\Phi_g^f L)\mathbf{y} = 0 \\ \Leftrightarrow & \left(g(\theta_1) \cdots g(\theta_\ell)\right)(L^\top W L)\mathbf{y}' = 0 \end{aligned} \tag{15}$$

since $L^\top W L$ is diagonal.

Let $g_1, \ldots, g_\ell$ be the basis of $\mathbb{F}_q[x]/(f)$ over $\mathbb{F}_q$, then, satisfying equation (15) for any $g \in \mathbb{F}_q[x]/(f)$ is equivalent to

$$\begin{pmatrix} g_1(\theta_1) & \ldots & g_1(\theta_\ell), \\ \vdots & \ddots & \vdots \\ g_\ell(\theta_1) & \ldots & g_\ell(\theta_\ell) \end{pmatrix} (L^\top W L)\mathbf{y}' = \mathbf{0}. \tag{16}$$

In addition, $g_1, \ldots, g_\ell$ form the 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

$$\begin{aligned} (16) &\Leftrightarrow \mathbf{y}' = \mathbf{0} \\ &\Leftrightarrow \mathbf{y} = \mathbf{0} \\ &\Leftrightarrow \mathbf{x} = \mathbf{0}. \end{aligned}$$

□

Table 6. Performance of QR-UOV in Subsection 4.2 in Magma algebra system [7].

parameter	(q, v, m, ℓ)	key generation	signature generation	verification
QR-UOV I	$(7, 183, 69, 3)$	0.08 s	0.04 s	0.01 s
QR-UOV III	$(7, 276, 102, 3)$	0.21 s	0.12 s	0.04 s
QR-UOV V	$(7, 393, 150, 3)$	0.55 s	0.30 s	0.10 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 the Magma algebra system (V2.24-82) [7]. 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; however, we herein use two 32-bit seeds because the size of the input for `SetSeed` is at most 32 bits.) Next, we generate a secret key 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. The signature is generated in the same manner as a signature is generated in the compressed Rainbow [11]. In the verification step, we generate the public key from the $\mathbf{s}_{pk}$ seed and follow the procedure explained in Subsection 2.1. In the signature generation and verification steps, we need to compute the product of a vector and matrices $W\Phi_g^f$ or $\Phi_g^f W^{-1}$, which 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 0.08 s, 0.04 s, and 0.01 s, respectively.