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

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

Abstract: Unbalanced oil and vinegar signature scheme (UOV) is known as one of the securest multivariate signature schemes, but a disadvantage of UOV is its large public key. 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 generating the quotient ring affects the security of our proposed scheme. Furthermore, we investigate secure parameters of our proposed scheme against the previously known and possible attacks. As a result, our proposed scheme is able to reduce public key size without increasing signature size comparing with other variants of UOV. For example, the public key of our proposed scheme is 66.7 KB in security level IV of NIST PQC project, whereas that of cyclic Rainbow is 252.3 KB.

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

1. Introduction

The problems relied on by current public key cryptosystems are known to be solved in polynomial time using a quantum computer. Therefore, in recent years, the research on the post-quantum cryptography (PQC), which is secure against attacks by a quantum computer, has been accelerating and NIST proceeds with PQC standardization project. Multivariate public key cryptography (MPKC), which is based on the difficulty of the problem solving a multivariate quadratic polynomial system over a finite field ($\mathcal{MQ}$-problem), is regarded as one of the prominent candidates of PQC. The $\mathcal{MQ}$-problem is known to be NP-complete [10] and hence is considered to be secure in the post-quantum world.

Unbalanced Oil and Vinegar signature scheme (UOV) [11], as one of the multivariate signature schemes, has withstood various attacks for about twenty years and been considered as one of the securest multivariate signature schemes. In particular, Rainbow [6], which is one of the variants of UOV using a multi-layer construction for efficiency, was selected as the third round finalists of NIST PQC project [14].

UOV is highly evaluated for its short signature and small execution time, but has a problem that its public key size is much larger than other candidates of PQC, e.g. lattice based signature schemes. Actually, Rainbow has the largest public key among the third round finalists, and the NIST's report [14] states that Rainbow is not suitable as a general-purpose signature scheme. Hence, the research to shorten the public key size of UOV is important in MPKC and PQC.

There are three main researches to realize a variant of UOV with small public key size. First one is Petzoldt et al.'s compression technique [15]. This technique can be applied to all existing variants of UOV and is based on the fact that a part of a public key can be chosen arbitrarily independent of the choice of the secret key. Thus the part of a public key can be generated using a seed and a pseudo random number generator. This technique can significantly reduce the public key size and the variant of Rainbow using this technique is called "cyclic Rainbow".

Second one is the Lifted Unbalanced Oil and Vinegar (LUOV) [5], which uses polynomials over a small field as its public key, whereas the signature and message space are defined over an extension field. This variant realizes its small public key size and was selected as one of the candidates in the second round of NIST PQC project. However, Ding et al. [8] proposed a new attack on LUOV that breaks the security of proposed parameter sets.

Third one is block-anti-circulant UOV (BAC-UOV) which was proposed by Szepieniec et al. in 2019 [17]. The public key of BAC-UOV is represented by block-anti-circulant matrices, which are block matrices whose every block is an anti-circulant matrix. Since such a matrix is recovered by its first row vector, BAC-UOV succeeded in reducing the size of the public key. However, since such a matrix can be transformed into the diagonal concatenation of two smaller matrices, BAC-UOV can be reduced to a smaller UOV scheme. As a result, BAC-UOV is broken in smaller complexity than asserted one. (See [9] for more detail).

In BAC-UOV, circulant matrices and anti-circulant matri-

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

ces are used. As is well known, any element of the quotient ring $\mathbb{F}_q[x]/(x^\ell - 1)$ is represented by a circulant matrix of size ℓ, where $\mathbb{F}_q$ is a finite field. More generally, for a polynomial $f \in \mathbb{F}_q[x]$, an element g of the quotient ring $\mathbb{F}_q[x]/(f)$ can be represented by an $\ell \times \ell$ matrix Φ_g^f, which is called a polynomial matrix. Since the polynomial matrix Φ_g^f is determined by the ℓ coefficients of g, we can compress the ℓ^2 components in Φ_g^f to ℓ elements in $\mathbb{F}_q$. This implies that there is a possibility of constructing a new variant of UOV using the quotient ring $\mathbb{F}_q[x]/(f)$ to shorten public key size.

Our Contribution

In this paper, we propose a new variant of UOV (QR-UOV) using a quotient ring $\mathbb{F}_q[x]/(f)$ to shorten public key size. In QR-UOV, a public key is represented by block matrices whose every component is written using Φ_g^f for elements g of the quotient ring $\mathbb{F}_q[x]/(f)$. This can be considered as a generalization of BAC-UOV.

However, there are some problems to be solved. In general, since Φ_g^f is not symmetric for any g, we cannot directly use polynomial matrices Φ_g^f to construct a variant of UOV. In order to solve this problem, we introduce the concept of an invertible $\ell \times \ell$ matrix W such that $W\Phi_g^f$ is symmetric for any g. Then, we prove that there exist such W for a lot of quotient ring $\mathbb{F}_q[x]/(f)$ (see in Proposition 1). Moreover, since BAC-UOV has a vulnerableness coming from the reducibility of $x^\ell - 1$, we must study a relation with the irreducibility of f. In particular, if f is irreducible, then polynomial matrices Φ_g^f can not be transformed into the diagonal concatenation of two smaller matrices as BAC-UOV, which implies such an f is suitable to construct a variant of UOV. (See Theorem 2.)

By using these results, we propose quotient ring UOV (QR-UOV) by using a quotient ring $\mathbb{F}_q[x]/(f)$ generated by an irreducible polynomial f. Moreover, we investigate the previously known attacks of UOV and possible attacks using the structure of the quotient ring $\mathbb{F}_q[x]/(f)$. Finally, we propose three parameter sets of QR-UOV which satisfy the security level II, IV and VI of the NIST PQC project. As a result, QR-UOV reduces the public key size about $50 \sim 70\%$ from Rainbow. For example, the public key of our proposed scheme is 66.7 KB in security level IV of NIST PQC project, whereas that of cyclic Rainbow is 252.3 KB.

Organizations

Our paper is organized as follows. In Section 2, we explain the construction of multivariate signature schemes, UOV, BAC-UOV and an attack on BAC-UOV. In Section 3, we discuss a way of generalizing circulant matrices and its property. In Section 4, we give the details of our proposed signature scheme QR-UOV. In Section 5, we analyze the security of our proposed scheme. Finally, we propose the parameter sets and compare our proposed scheme with Rainbow in Section 6, and conclude the paper in Section 7.

2. Preliminaries

In this section, we first explain the $\mathcal{MQ}$-problem and general signature schemes that are based on the $\mathcal{MQ}$-problem. Next, we recall the construction of the Unbalanced Oil and Vinegar signature scheme (UOV) [11]. Thirdly, we describe the construction of block-anti-circulant UOV (BAC-UOV) [17], and finally explain the attack [9] on BAC-UOV.

2.1 Multivariate Signature Scheme

Let $\mathbb{F}_q$ be a finite field with q elements and n and m be two positive integers. Given 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 $\mathcal{MQ}$-problem. Garey and Johnson [10] proved that the $\mathcal{MQ}$-problem is NP-complete if $n \approx m$, and hence it is considered to have the potential to resist quantum computer attacks.

Now, we briefly explain the construction of general multivariate signature schemes. First, we generate 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*. Next, randomly choose two invertible linear maps $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ in order to hide the structure of $\mathcal{F}$. Then, the public key $\mathcal{P}$ is given as a polynomial map as follows:

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

The secret key consists of $\mathcal{T}$, $\mathcal{F}$ and $\mathcal{S}$. The signature generation is done 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 $\mathcal{F}(\mathbf{x}) = \mathbf{m}_1$. Then, $\mathbf{s} = \mathcal{S}^{-1}(\mathbf{m}_2) \in \mathbb{F}_q^n$ is a signature for the message $\mathbf{m}$. The verification process is done by confirming whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$ or not.

2.2 Unbalanced Oil and Vinegar Signature Scheme

Let v, o be two positive integers and $n = v + o$ and we assume that $v > o$. 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 $\mathcal{F} = (f_1, \ldots, f_o) : \mathbb{F}_q^n \to \mathbb{F}_q^o$ is designed such that each f_k is a quadratic polynomial of the following form:

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

where $\alpha_{i,j}^{(k)} \in \mathbb{F}_q$. Furthermore, we randomly choose a linear map $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. Then, the public key map $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^o$ is computed by $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$. Here, $\mathcal{T}$ of (1) is not needed since it does not affect to hide the structure of $\mathcal{F}$. The secret key consists of $\mathcal{F}$ and $\mathcal{S}$.

Subsequently, we explain a way of inverting the central map $\mathcal{F}$. Given $\mathbf{y} \in \mathbb{F}_q^o$, we first choose random values $a_1, \ldots, a_v$ in $\mathbb{F}_q$ to the vinegar variables. Then, we can 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 o equations in o oil variables. If there is no solution to this equation, then we choose new random values $a'_1, \ldots, a'_v$ and repeat the previous procedure. As a result, we obtain a solution $\mathbf{x} = (a_1, \ldots, a_v, a_{v+1}, \ldots, a_n)$ to $\mathcal{F}(\mathbf{x}) = \mathbf{y}$. By using this way, we can execute the signing process as explained in Subsection 2.1.

We assume the characteristic of $\mathbb{F}_q$ is odd. For each $1 \leq i \leq o$, there exists $n \times n$ symmetric matrices F_i such that $f_i(\mathbf{x}) = \mathbf{x} \cdot F_i \cdot \mathbf{x}^\top$. Then, from (2), this F_i has the following form:

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

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

$$P_i = S^\top F_i S, \;\; (i = 1, \ldots, o)$$

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

Block-anti-circulant (BAC) UOV [17] is a variant of UOV, designing the public key to be represented by block-anti-circulant matrices to shorten the public key. In this subsection, we describe the construction of BAC-UOV.

A circulant matrix is a matrix whose each row vector is rotated one element to the right relative to the preceding row vector. On the other hand, an anti-circulant matrix is a matrix whose each row vector is rotated one element to the left relative to the preceding row vector. In addition, a matrix is called a block-circulant matrix or a block-anti-circulant matrix with block size ℓ if every $\ell \times \ell$ block is a circulant matrix or an anti-circulant matrix. For a block-circulant matrix A and a block-anti-circulant matrix B, the products AB and BA become block-anti-circulant matrices.

In BAC-UOV, the number of vinegar variables v and the number of oil variables o are set to be divisible by the block size ℓ. The representation matrices $F_1, \ldots, F_o$ 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, respectively. Then, the representation matrices $P_1, \ldots, P_o$ for the public key $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$ are computed by $P_i = S^\top F_i S\ (i = 1, \ldots, o)$, and become block-anti-circulant matrices.

Due to the block-anti-circulant construction, the n-by-n matrices $P_1, \ldots, P_o$ can be represented by using only the first row of every block. Therefore, these matrices $P_1, \ldots, P_o$ can be represented by using only n^2/ℓ elements, which is one ℓ-th of a plain matrix. This makes the size of the public key shorter compared to the original UOV.

2.4 An Attack on BAC-UOV

In 2020, a new attack on BAC-UOV that breaks the security of proposed parameter sets was proposed [9]. The attack utilizes the property of the anti-circulant matrix that the sum of the elements of one row is the same as those of other rows.

We define an $\ell \times \ell$ matrix L_ℓ such that $(L_\ell)_{1i} = (L_\ell)_{j1} = 1\,(1 \leq i, j \leq \ell)$, $(L_\ell)_{ii} = -1\,(2 \leq i \leq \ell)$ and the other elements are equal to 0. Then, for an $\ell \times \ell$ anti-circulant matrix Y, we have:

$$L_\ell^\top Y L_\ell = \begin{pmatrix} *_{1\times 1} & 0_{1\times(\ell-1)} \\ 0_{(\ell-1)\times 1} & *_{(\ell-1)\times(\ell-1)} \end{pmatrix}. \tag{4}$$

Let $L_\ell^{(n)}$ be an $n \times n$ block diagonal matrix such that every diagonal submatrix is L_ℓ. Then, for an $n \times n$ block-anti-circulant matrix Z with block size ℓ, the matrix ${L_\ell^{(n)}}^\top Z L_\ell^{(n)}$ becomes a block matrix whose every block is in the form of (4). Furthermore, there exists a permutation matrix L' such that

$$(L_\ell^{(n)} L')^\top Z (L_\ell^{(n)} L') = \left(\begin{array}{c|c} *_{N\times N} & 0_{N\times(\ell-1)N} \\ \hline 0_{(\ell-1)N\times N} & *_{(\ell-1)N\times(\ell-1)N} \end{array}\right), \tag{5}$$

where $N := n/\ell$.

The representation matrices $P_1, \ldots, P_o$ for the public key $\mathcal{P}$ of BAC-UOV can all be transformed into the form of (5) by $L_\ell^{(n)} L'$. Subsequently, we execute the UOV attack [12] on the upper-left $N \times N$ submatrices of the obtained matrices, which only requires very little complexity. By this operation, we can reduce the number of variables that appear in the public equations $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ for a message $\mathbf{m}$. As a result, the complexity of the attack decreases by about 20% compared with the best existing attack on UOV.

3. Generalization of Circulant Matrices

In this section, we generalize circulant matrices and anti-circulant matrices used in BAC-UOV [17], and prepare a condition to apply them to the UOV scheme. Furthermore, we discuss whether generalized matrices can be transformed as stated in (4).

3.1 Matrix Representation of a Quotient Ring

Let $q, \ell \in \mathbb{N}$ 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 define an $\ell \times \ell$ matrix Φ_g^f over $\mathbb{F}_q$ uniquely, such that

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

We call such a matrix Φ_g^f *the 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*

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

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. Furthermore, 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 be also represented by only ℓ elements in $\mathbb{F}_q$.

As seen in Subsection 2.2, the transposition is appeared in the computation of the public matrices P_i. Thus, in order to use polynomial matrices Φ_g^f in the UOV scheme, we need that WA_f is stable under the transposition for some W.

A simple example is from BAC-UOV [17]. An $\ell \times \ell$ circulant matrix, which is used in BAC-UOV, is an element in $A_{x^\ell-1}$, and an anti-circulant matrix is an element in $J_\ell A_{x^\ell-1}$, where J_ℓ is anti-identity matrix with size ℓ:

$$J_\ell := \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

Moreover, any matrix in $J_\ell A_{x^\ell-1}$ is symmetric, that is, $J_\ell A_{x^\ell-1}$ is stable under the transposition.

For our purpose in this paper, we need other examples. The following proposition shows that there exist infinitely many examples.

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

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

Then, for any $X \in A_f$, WX becomes a symmetric matrix.

3.2 Effect of Irreducibility of f

As stated in Subsection 2.4, the proposed parameters of BAC-UOV were broken by using the transformation (4) on anti-circulant matrices. This transformation is obtained from the reducibility of $x^\ell - 1$. Therefore, we discuss a relationship between the irreducibility of the polynomial f generating the quotient ring $\mathbb{F}_q[x]/(f)$ and the existence of such a transformation for $W\Phi_g^f$.

Theorem 1. *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 becomes a symmetric matrix. Then there exist an invertible matrix $L \in \mathbb{F}_q^{\ell\times\ell}$ and $i, j \in \{1, \ldots, \ell\}$ such that for any $X \in WA_f$,*

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

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 becomes a symmetric matrix. 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 $X \in WA_f$,*

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

(Proofs will be in full paper.)

From these theorems, we will choose an irreducible polynomial as f of A_f used in our variant proposed in Section 4.

Remark. For $\mathbb{F}_q = \mathbb{F}_3, \mathbb{F}_7$ and $\mathbb{F}_{31}$, we checked that for almost all $30 \ge \ell \ge 2$, there exists an irreducible polynomial $f \in \mathbb{F}_q[x]$ with the form of $x^\ell - ax^i - 1$ described in Proposition 1.

4. Quotient Ring UOV (QR-UOV)

In this section, we propose a new variant of UOV, QR-UOV, which is constructed by applying polynomial matrices to UOV.

4.1 Description of QR-UOV

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

Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial 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 by Proposition 1 and the remark in Subsection 3.2. We define two subspaces B_f^N and C_f^N in $\mathbb{F}_q^{n\times n}$ as follows:

$$\begin{aligned} B_f^N &:= \{X \in \mathbb{F}_q^{n\times n} \mid \forall i, j \in \{0, \ldots, N-1\}, \\ &\quad X[i\ell+1 : (i+1)\ell,\ j\ell+1 : (j+1)\ell] \in WA_f\}, \\ C_f^N &:= \{X \in \mathbb{F}_q^{n\times n} \mid \forall i, j \in \{0, \ldots, N-1\}, \\ &\quad X[i\ell+1 : (i+1)\ell,\ j\ell+1 : (j+1)\ell] \in A_fW^{-1}\}, \end{aligned}$$

where $X[a : b,\ c : d]$ denotes a $(b-a) \times (d-c)$ submatrix of X whose upper left element has index (a, b), which means every $\ell \times \ell$ block are elements of WA_f or A_fW^{-1}. Due to the symmetry of WA_f, we obtain the following proposition:

Proposition 2. *For $X \in B_f^N$ and $Y \in C_f^N$, we have*

$$X^\top YX \in B_f^N.$$

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 of WA_f is symmetric.
- Choose F_i ($i = 1, \ldots, o$) from C_f^N such that lower right $o \times o$ sub matrices are zero matrices.
- Choose an invertible matrix S from B_f^N randomly.
- Compute $P_i = S^\top F_i S$ ($i = 1, \ldots, o$).

Then, we obtain that P_i ($i = 1, \ldots, o$) are elements of B_f^N from Proposition 2. The signing and verification process are same as that of plain UOV.

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

4.2 Optimized QR-UOV

We use the same optimization techniques as that used in Rainbow. In the plain UOV, the matrix S of the linear map $\mathcal{S}$ can be restricted to a special form as follows:

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

since this does not affect the security. In QR-UOV, we replace the upper-left and lower-right identity matrices to block diagonal matrices whose every diagonal block is $W\Phi_1^f$ since S is chosen in B_f^N.

Subsequently, we introduce Petzoldt et al.'s compression technique [15] used in Rainbow as *cyclic Rainbow*. The representation matrices P_i $(i = 1, \ldots, o)$ of the public key map are written as in the following form:

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

Here, $P_{i,1}$, $P_{i,2}$ and $P_{i,3}$ are $v \times v$, $v \times o$ and $o \times o$ matrices, respectively, and $P_{i,1}$ and $P_{i,3}$ are symmetric matrices. Then, the representation matrices F_i, P_i $(i = 1, \ldots, o)$ and S hold the following equation:

$$F_i = \begin{pmatrix} I_{v\times v} & 0_{v\times o} \\ -S'^\top & I_{v\times v} \end{pmatrix} \begin{pmatrix} P_{i,1} & P_{i,2} \\ P_{i,2}^\top & P_{i,3} \end{pmatrix} \begin{pmatrix} I_{v\times v} & -S' \\ 0_{o\times v} & I_{v\times v} \end{pmatrix} = \begin{pmatrix} P_{i,1} & -P_{i,1}S' + P_{i,2} \\ -S'^\top P_{i,1} + P_{i,2}^\top & S'^\top P_{i,1}S' - P_{i,2}^\top S' - S'^\top P_{i,2} + P_{i,3} \end{pmatrix}.$$

In the optimized key generation step, we first generate $P_{i,1}$, $P_{i,2}$ $(i = 1, \ldots, o)$ and S' from a seed to the pseudo random number generator (PRNG). Second, $P_{i,3}$ $(i = 1, \ldots, o)$ are computed by the following equation:

$$P_{i,3} = -S'^\top P_{i,1}S' + P_{i,2}^\top S' + S'^\top P_{i,2}. \tag{6}$$

Then, the representation matrices F_i $(i = 1, \ldots, o)$ have the form of (3). As a result, the public key is composed by $o \times o$ matrices $P_{i,3}$ $(i = 1, \ldots, o)$ and the seed for $P_{i,1}$, $P_{i,2}$ $(i = 1, \ldots, o)$. This compression technique significantly reduces the public key size of the UOV scheme. We apply Petzoldt et al.'s compression technique to QR-UOV.

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

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

and that of the optimized QR-UOV is

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

5. Security Analysis

In this section, we first explain the existing attacks on UOV. Subsequently, we discuss how the block structure of QR-UOV affects the existing attacks.

5.1 Plain Attacks on UOV

Direct Attack

Given a quadratic polynomial system $\mathcal{P} = (p_1, \ldots, p_o)$ in n variables over $\mathbb{F}_q$ and $\mathbf{m} \in \mathbb{F}_q^o$, the direct attack algebraically solves the system $\mathcal{P}(\mathbf{x}) = \mathbf{m}$. In the case of UOV, the number of variables n is larger than the number of equations o, but $n - o$ variables can be specified with random values without disturbing the existence of the solution. One of the best-known approaches solving the quadratic system is the hybrid approach [4]. The complexity of this approach by a classical adversary is estimated to be

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

where d_{reg} is the *degree of regularity*, which is the highest polynomial degree appeared during a Gröbner basis computation for the components of the highest degree (quadratic) of these polynomials.

If $n \leq o$, then for a certain class of polynomial systems called *semi-regular systems* [1], [2], [3], their d_{reg} can be estimated by the degree of the first non-positive term in the following series [3]:

$$\frac{(1-z^2)^o}{(1-z)^n}.$$

Empirically, a random polynomial system with very high probability is a semi-regular system, and hence the aforementioned formula can be used to estimate its degree of regularity.

Furthermore, Thomae and Wolf [18] proposed a technique for reducing the number of variables and equations if $n > o$. In this technique, we assume that the order of the finite field q is even. For the $n \times n$ matrices P_i representing the quadratic parts of p_i, the technique chooses a new matrix S' such that $S'^\top P_i S'$ $(i = 1, \ldots, \alpha)$ become diagonal for their first α variables where $\alpha = \lfloor \frac{n}{o} \rfloor - 1$. Then, we can reduce $(n - o + \alpha)$ variables and α equations, and obtain an $\mathcal{MQ}$-system with $o - \alpha$ variables and equations.

UOV Attack

UOV attack [12] 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 (2). Such an $\mathcal{S}'$ is called an *equivalent key*. In the UOV attack, we find the subspace $\mathcal{S}^{-1}(\mathcal{O})$ of $\mathbb{F}_q^n$, where $\mathcal{O}$ is the oil subspace defined as follows:

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

This subspace $\mathcal{S}^{-1}(\mathcal{O})$ can induce an equivalent key. To obtain $\mathcal{S}^{-1}(\mathcal{O})$, in the UOV attack, we choose two invertible matrices W_i, W_j from the set of linear combinations of $P_1, \ldots, P_o$. Then, we can probabilistically recover a part of the subspace $\mathcal{S}^{-1}(\mathcal{O})$ by computing the invariant subspace of $W_i^{-1}W_j$. The complexities of the UOV attack is estimated to be

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

Reconciliation Attack

The reconciliation attack [7] is executed by treating elements of the matrix S as variables and solving the system of equations obtained by $(S^{-\top}P_iS^{-1})[v+1:n,\ v+1:n] = O$ $(i = 1,\ldots,o)$. This attack is known to be decomposed into a series of steps and the first step solves a system of o quadratic equations in v variables. If $v \leq o$, then the complexity of the reconciliation attack is the same as that of solving a quadratic system of o equations in v variables. On the other hand, in the case of UOV where $v > o$, the complexity is estimated to be larger than that of solving a quadratic system of v equations in v variables.

5.2 An Attack using the Quotient Ring

In this subsection, we explain a way of attacking on QR-UOV by regarding every $\ell \times \ell$ submatrix over $\mathbb{F}_q$ as an element of $\mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^\ell}$. We define two maps $G_1 : B_f^N \to (\mathbb{F}_q[x]/(f))^{N\times N}$ such that given $X \in B_f^N$, $(G_1(X))_{ij}$ is $g \in \mathbb{F}_q[x]/(f)$ if ij-block of X is $W\Phi_g^f$. Furthermore, we define $G_2 : C_f^N \to (\mathbb{F}_q[x]/(f))^{N\times N}$ similarly.

If we attack on QR-UOV by finding the equivalent key S', then we can also attack on matrices $G_1(P_1),\ldots,G_1(P_o)$ over $\mathbb{F}_q[x]/(f)$ by executing UOV attack or reconciliation attack. If we obtain an equivalent key S' over $\mathbb{F}_q[x]/(f)$, then $G_2^{-1}(S') \in \mathbb{F}_q^{n\times n}$ becomes an equivalent key over $\mathbb{F}_q$.

This attacking way changes the complexity of UOV attack and reconciliation attack. The complexities of UOV attack over $\mathbb{F}_q[x]/(f)$ become as follows:

$$q^{v-o-\ell}\cdot(o/\ell)^4.$$

In terms of reconciliation attack, the first step of the reconciliation attack solves the quadratic system of o equations in v/ℓ variables over $\mathbb{F}_q[x]/(f)$. By using the discussion in Subsection 5.1, the complexity is estimated to be larger than that of solving a quadratic system of $\max\{o, v/\ell\}$ equations in v/ℓ variables over $\mathbb{F}_q[x]/(f)$.

We consider that the manipulation on $\mathbb{F}_q[x]/(f)$ does not change the complexity of the direct attack, since the two vectors $\mathbf{x}$ and $\mathbf{m}$ of $\mathcal{P}(\mathbf{x}) = \mathbf{m}$ can not be represented over the quotient ring $\mathbb{F}_q[x]/(f)$. Furthermore, we experimentally confirmed that the degree of regularity obtained by executing the direct attack on QR-UOV is same as the degree obtained theoretically by the way described in Subsection 5.1.

5.3 Linear Transformation Over an Extension Field

Due to the discussion in Subsection 3.2, there does not exist a linear transformation over $\mathbb{F}_q$ such that it transforms the representation matrices $P_1,\ldots,P_o$ of QR-UOV into a special form. Then, in this subsection, we discuss a linear transformation over extension field $\mathbb{F}_{q^\ell}$.

First, we show that the plain polynomial matrix can be diagonalized over $\mathbb{F}_{q^\ell}$. (Proof will be in full paper).

Lemma 2. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial with $\deg f = \ell$. Then, for any $g \in \mathbb{F}_q[x]/(f)$, there exists an $\ell\times\ell$ matrix L over $\mathbb{F}_{q^\ell}$ such that $L^{-1}\Phi_g^f L$ is diagonal.*

By using this L, we prove two theorems about the congruent transformation on $W\Phi_g^f$ used in QR-UOV over $\mathbb{F}_{q^\ell}$ (Proofs will be in full paper).

Theorem 3. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial with $\deg f = \ell$ and W be an invertible matrix over $\mathbb{F}_q^{\ell\times\ell}$ such that for any $g \in \mathbb{F}_q[x]/(f)$, $W\Phi_g^f$ becomes a symmetric matrix. Then, for any $g \in \mathbb{F}_q[x]/(f)$, $L^\top W\Phi_g^f L$ is diagonal, where L is described in Lemma 2.*

Theorem 4. *Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial with $\deg f = \ell$ and W be an invertible matrix over $\mathbb{F}_q^{\ell\times\ell}$ such that for any $g \in \mathbb{F}_q[x]/(f)$, $W\Phi_g^f$ becomes a symmetric matrix. If for any $g \in \mathbb{F}_q[x]/(f)$, there exists $\mathbf{x} \in \mathbb{F}_{q^\ell}^\ell$ such that $\mathbf{x}^\top W\Phi_g^f\mathbf{x} = 0$, then $\mathbf{x} = \mathbf{0}$.*

Theorem 3 indicates that $P_1,\ldots,P_o$ of QR-UOV are transformed into block diagonal matrices whose block size are $N\times N$ by executing a change of variables. Let L_N be an $n\times n$ $(n = \ell\cdot N)$ block matrix whose N diagonal blocks are L and other blocks are zero matrices. Then, $L_N^\top P_i L_N$ $(i = 1,\ldots,o)$ become the block matrices whose every $\ell\times\ell$ block is of the diagonal form. Then, there exists a permutation matrix L' such that $(L_NL')^\top P_i(L_NL')$ becomes a block diagonal matrix whose every block size is $N\times N$, and let $\bar{L} := L_NL'$. On the other hand, Theorem 4 indicates that there does not exist a change of variables over $\mathbb{F}_{q^\ell}$ such that it recovers the structure of UOV directly.

We consider the complexity of each attack on $\bar{L}^\top P_i\bar{L}$ $(i = 1,\ldots,o)$. 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

$$L^{-1}(\Phi_g^fW^{-1})L^{-\top} = (L^{-1}\Phi_g^fL)(L^\top WL)^{-1},$$

where $L^\top WL$ is diagonal (Proof will be in full paper). Then, due to the structure of F_i, every diagonal block of $\bar{L}^{-1}F_i\bar{L}^{-\top}$ has $o/\ell\times o/\ell$ zero block as similar to F_i. By using these facts, the complexity of UOV attack on each block over $\mathbb{F}_{q^\ell}$ is $O(q^{v-o-\ell}\cdot(o/\ell)^4)$. Moreover, the complexity of reconciliation attack on each block is estimated to be larger than that of solving a quadratic system of $\max\{o, v/\ell\}$ equations in v/ℓ variables over $\mathbb{F}_{q^\ell}$. These complexities are same as that of UOV attack and reconciliation attack over $\mathbb{F}_q[x]/(f)$ discussed in Subsection 5.2.

Finally, we consider the direct attack on $\bar{L}^\top P_i\bar{L}$ $(i = 1,\ldots,o)$. In subsection 5.1, we use the technique proposed by Thomae and Wolf to reduce the size of a quadratic system to be solved. However, if we first use Thomae and Wolf's technique, then we cannot diagonalize the representation matrices, since the linear transformation executed in Thomae and Wolf's technique breaks the block structure. Then, we suppose that we use Thomae and Wolf's technique, after diagonalizing over $\mathbb{F}_{q^\ell}$. In the case where $n > o$, the

dimension of the solution space is generally $\mathbb{F}_q^v$. But now, since we try to solve the system over $\mathbb{F}_{q^\ell}$, the dimension of the solution space changes into $\mathbb{F}_{q^\ell}^v$. Therefore, in this way, the probability that the obtained solution is in $\mathbb{F}_q^n$ is very low and this way is not efficient. In conclusion, we consider that there does not exist an effective way of executing the direct attack with Thomae and Wolf's technique on $\bar{L}^\top P_i \bar{L}$.

Subsequently, we suppose that we fix v values randomly before diagonalizing over $\mathbb{F}_{q^\ell}$ without using Thomae and Wolf's technique. Then, we will obtain the solution in $\mathbb{F}_q^n$, since the solution is thought to be uniquely determined. By executing an experiment on the degree of regularity of the system represented by $n \times n$ block diagonal matrices whose every block is $(n/\ell) \times (n/\ell)$ $(\ell = 2, 3)$, we confirmed that the obtained degree of regularity is smaller than the theoretical value by at most one. Then, the complexity of the direct attack on the diagonalized system over $\mathbb{F}_{q^\ell}$ becomes larger than that of the plain direct attack due to the large order of the extension field q^ℓ. Consequently, we consider that the direct attack on the block diagonalized system over $\mathbb{F}_{q^\ell}$ is not effective when we compared it with the plain direct attack.

6. Parameter and Comparison

In this section, we propose concrete parameters of each security level of NIST PQC project and compare the size of public key and signature of QR-UOV with that of Rainbow [16].

6.1 Parameter

We propose the following parameter sets for QR-UOV:

- II: $(q, v, o, \ell) = (7, 122, 68, 2)$,
- IV: $(q, v, o, \ell) = (7, 276, 102, 3)$,
- VI: $(q, v, o, \ell) = (31, 210, 108, 2)$.

The indices II, IV and VI denote the corresponding security levels of the NIST security categories. The security level II, IV and VI mean that any classical attacker breaking the parameter needs more than 2^{146}, 2^{210} and 2^{274} classical gates, and any quantum attacker needs more than 2^{74}, 2^{137} and 2^{202} quantum gates, respectively [13]. These parameters aim to realize small public key compared with Rainbow and reasonable signature size.

6.2 Security of Proposed Parameters

In this subsection, we show the complexity of each attack on our proposed parameters. Table 1 shows the complexity of plain attacks on UOV. Moreover, Table 2 shows the complexity of the UOV attack and the reconciliation attack using the structure of $\mathbb{F}_q[x]/(f)$ described in Subsection 5.2. For each parameter set, each upper entry shows the number of classical gates, while each lower entry shows the number of quantum gates. For example, in Table 1, the complexity of the direct attack for level (II) are 149.2 classical gates and 102.2 quantum gates, respectively.

Table 1 Complexity of the plain attacks in Subsection 5.1 on QR-UOV. Each upper entry is the number of classical gates and each lower entry is the number of quantum gates.

Security category	parameters (q, v, o, ℓ)	$\log_2$(#gates)		
		direct	UOV	Rec
II	$(7, 122, 68, 2)$	**149.2** **102.2**	177.4 103.0	250.8 170.9
IV	$(7, 276, 102, 3)$	**210.4** **143.8**	516.6 273.7	528.2 353.7
VI	$(31, 210, 108, 2)$	**274.3** **212.5**	533.1 283.0	504.9 388.5

Table 2 Complexity of the attacks UOV* and Rec* which are UOV attack and reconciliation attack using the structure of $\mathbb{F}_q[x]/(f)$ in Subsection 5.2. Each upper entry is the number of classical gates and each lower entry is the number of quantum gates.

Security category	parameters (q, v, o, ℓ)	$\log_2$(#gates)	
		UOV*	Rec*
II	$(7, 122, 68, 2)$	172.4 **99.4**	**150.3** 133.8
IV	$(7, 276, 102, 3)$	507.6 267.6	**217.6** **209.0**
VI	$(31, 210, 108, 2)$	526.1 278.4	**283.8** **262.5**

These tables show that our proposed parameter sets satisfy the condition of each security level.

6.3 Comparison of Public Key and Signature Size

Table 3 compares public key and signature size of cyclic Rainbow [16], which is a variant of Rainbow using Petzoldt et al.'s compression technique [15] described in Subsection 4.2, and optimized QR-UOV in each security level. We suppose that the secret key can be compressed to a seed of 512 bits, public keys include a seed of 256 bits, and signatures include a 128 bit *salt*, which is a random binary vector for the EUF-CMA security. As a result, optimized QR-UOV enables us to reduce the size of the public key about $50 \sim 70\%$ from the optimized Rainbow with a small loss of the signature size. Note that our proposed scheme is worse than Rainbow in terms of execution time, since the number of variables of our scheme generally becomes larger than that of Rainbow.

7. Conclusion

In this paper, we proposed a new variant of UOV (QR-UOV) using a quotient ring $\mathbb{F}_q[x]/(f)$ to reduce the public key size. To do so, we defined the polynomial matrix Φ_g^f and introduced the concept of a matrix W such that $W\Phi_g^f$ is symmetric. As a result, we are able to construct QR-UOV which utilizes polynomial matrices Φ_g^f in block matrices. Moreover, we proved that if f is irreducible, then QR-UOV is resistant to the attack breaking BAC-UOV. We also analyzed the security of QR-UOV against the previously known attacks of UOV and possible attacks using the quotient ring. Our new variant QR-UOV realizes small public key and reasonable signature size. In particular, for our proposed parameter sets, the optimized

Table 3 Comparing public key and signature size of Cyclic Rainbow and QR-UOV (1KB=1024B)

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

QR-UOV enables us to reduce the size of the public key about 50 $\sim$ 70% from the optimized Rainbow and their signature sizes are almost same.

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**, 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] Ding, J., Schmidt, D.: Rainbow, a New Multivariable Polynomial Signature Scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005)
[7] Ding, J., Yang, B., Chen, C.-O., Chen, M., Cheng, C.: New differential-algebraic attacks and reparametrization of Rainbow. In: ACNS 2008, LNCS, vol. 5037, pp. 242–257. Springer (2008)
[8] Ding, J., Zhang, Z., Deaton, J., Schmidt, K., Vishakha, FNU.: New attacks on lifted unbalanced oil vinegar. In: Second PQC Standardization Conference 2019, National Institute of Standards and Technology (2019)
[9] 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)
[10] Garey, M.-R., Johnson, D.-S.: Computers and intractability: a guide to the theory of NP-completeness. W. H. Freeman (1979)
[11] Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999)
[12] Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998)
[13] 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)
[14] NIST: Status report on the second round of the NIST post-quantum cryptography standardization process. `https://csrc.nist.gov/publications/detail/nistir/8309/final` (2020)
[15] Petzoldt, A., Buchmann, J. A.: A multivariate signature scheme with an almost cyclic public key. IACR Cryptology ePrint Archive 2009, 440, `http://eprint.iacr.org/2009/440` (2009)
[16] 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://sites.google.com/site/jintaiding/nist-papers` (2020)
[17] Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced oil and vinegar. In: SAC 2019 (2019)
[18] Thomae, E., Wolf, C.: Solving underdetermined systems of multivariate quadratic equations revisited. In: PKC 2012, LNCS, vol. 7293, pp. 156–171. Springer (2012)