SCIS 2023 2023 Symposium on
Cryptography and Information Security
Fukuoka, Japan, Jan. 24 – 27, 2023
The Institute of Electronics,
Information and Communication Engineers

Secure Parameters for Multivariate Polynomial Signature Scheme QR-UOV

Hiroki Furue * Yasuhiko Ikematsu † Fumitaka Hoshino ‡ Yutaro Kiyomura §
Tsunekazu Saito § Tsuyoshi Takagi *

Abstract: The multivariate-based unbalanced oil and vinegar signature scheme (UOV) is expected to be one of the candidates for post-quantum cryptography (PQC). UOV is a well-established signature scheme owing to its short signature and execution time. However, its public key is much larger than that of other PQC candidates. At ASIACRYPT 2021, Furue et al. proposed quotient ring UOV (QR-UOV) as a new variant of UOV, which reduces the public key size compared to the plain UOV. However, there has not been a formal security proof and detailed parameter analysis for QR-UOV. In this paper, one of our contributions is that we present the formal definitions of two assumptions and prove the EUF-CMA security of QR-UOV based on these assumptions. Furthermore, we propose various parameter sets of QR-UOV with different security levels, the orders of the finite field, and the purposes, and estimate the public key and signature size of these parameters. By comparing the public key and signature size of these parameter sets with that of other PQC candidates, we discuss the (dis)advantages of each parameter set.

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

1 Introduction

The public key cryptosystems such as RSA and ECC, which are being widely used in recent times, can be broken in polynomial time using Shor's algorithm [21] on a quantum computer. Thus, research on post-quantum cryptography (PQC), which is secure against quantum computing attacks, is accelerating. Indeed, the U.S. National Institute for Standards and Technology (NIST) has initiated a standardization project on it since 2016 [16].

Multivariate public key cryptography (MPKC) is based on the difficulty of solving a system of multivariate quadratic polynomial equations over a finite field (the multivariate quadratic (MQ) problem), and it is regarded as a strong candidate for PQC. The MQ problem is NP-complete [13] and is thus likely to be secure in the post-quantum era.

The unbalanced oil and vinegar signature scheme (UOV) [14], a multivariate signature scheme proposed by Kipnis et al. at EUROCRYPT 1999, has withstood various types of attacks for approximately 20 years. Indeed, a multilayer UOV variant Rainbow [9], which is significantly weakened by an attack proposed by Beullens at CRYPTO 2022 [7], was selected as a third-round finalist in the NIST PQC project [18]. UOV is a well-established signature scheme owing to its short signature and execution time. By contrast, UOV has public keys much larger than those of other PQC candidates, such as lattice-based signature schemes. Thus, it is important to develop a UOV variant with a small public key.

At ASIACRYPT 2021, Furue et al. presented a new UOV variant using an arbitrary quotient ring called *quotient ring UOV (QR-UOV)* [12]. In QR-UOV, a public key is represented by block matrices in which every $\ell \times \ell$ component corresponds to an element of a quotient ring $\mathbb{F}_q[x]/(f)$ with $f \in \mathbb{F}_q[x]$ and $\deg f = \ell$. From this construction, we can compress ℓ^2 components in each block to ℓ coefficients in $\mathbb{F}_q$, and thus QR-UOV can reduce the public key size from the plain UOV. Note that this QR-UOV can be considered as a generalization of the block-anti-circulant UOV [22], which is the case for $f = x^\ell - 1$.

In [12], the authors show the security of QR-UOV only by evaluating the complexity of considerable attacks on QR-UOV and propose only one parameter set for each of the security levels I, III, V for the NIST PQC standardization project [17]. Therefore, constructing a formal security proof and analyzing various parameter sets have been the remaining tasks for QR-UOV.

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

Our Contributions Our two main contributions to the QR-UOV signature scheme are the following:

- Formally proving the existential unforgeability under adaptive chosen message attacks (EUF-CMA) security of a modified version of QR-UOV based on two assumptions.
- Giving various parameter sets for QR-UOV and analyzing their public key and signature size.

In the first point, we give the first formal security proof of QR-UOV. This proof is based on two assumptions: One is derived from the plain UOV, whereas another one is a new assumption derived from QR-UOV. Thus, this security proof is not enough to guarantee the security of QR-UOV but is valuable for cryptoanalysis. In the second point, we propose three types of parameters with different purposes for each order of the finite field and security level. For these proposed parameter sets, we analyze their public key and signature size and compare them with those of other post-quantum signature schemes.

Organization The rest of this paper is organized as follows: Section 2 recalls the plain UOV signature scheme. Section 3 recalls QR-UOV and proposes a new modification for the security proof. Section 4 gives some assumptions and a security definition, and then theoretically proves the security of QR-UOV. Section 5 proposes some parameter sets for QR-UOV and analyzes their public key and signature size. Finally, Section 6 is devoted to the conclusion.

2 Unbalanced Oil and Vinegar (UOV)

This section describes the structure of the unbalanced oil and vinegar signature scheme (UOV) [14]. Let q be a prime power and $\mathbb{F}_q$ be the field with q elements. Furthermore, let v and m be positive integers and $n = v + m$. For variables $\mathbf{x} = (x_1, \ldots, x_n)$ over $\mathbb{F}_q$, we call $x_1, \ldots, x_v$ *vinegar-variables* and $x_{v+1}, \ldots, x_n$ *oil-variables*.

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

$$f_k(x_1, \ldots, x_n) = \sum_{i=1}^{v} \sum_{j=i}^{n} \alpha_{i,j}^{(k)} x_i x_j \tag{2.1}$$

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

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

and the secret key comprises $\mathcal{F}$ and $\mathcal{S}$. We here omit linear and constant terms of $\mathcal{F}$ for simplicity.

Next, we describe the inversion of the central map $\mathcal{F}$. When we find $\mathbf{x} \in \mathbb{F}_q^n$ satisfying $\mathcal{F}(\mathbf{x}) = \mathbf{y}$ for a given $\mathbf{y} \in \mathbb{F}_q^m$, we first choose random values $a_1, \ldots, a_v$ in $\mathbb{F}_q$ as the values of the vinegar-variables. We then can easily obtain a solution for the equation $\mathcal{F}(a_1, \ldots, a_v, x_{v+1}, \ldots, x_n) = \mathbf{y}$ because this is a linear system of m equations in m oil-variables from the construction of the central map (2.1). If no solution exists for this equation, we choose new random values $a'_1, \ldots, a'_v$, and repeat the above procedure.

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

Finally, we introduce matrices representing the public and secret keys of UOV. For each polynomial p_i of the public key $\mathcal{P}$, there exists an $n \times n$ matrix P_i such that $p_i(\mathbf{x}) = \mathbf{x}^\top \cdot P_i \cdot \mathbf{x}$. Similarly, an $n \times n$ matrix F_i can be taken for each f_i with $1 \le i \le m$, and an $n \times n$ matrix S is defined to satisfy $\mathcal{S}(\mathbf{x}) = S \cdot \mathbf{x}$. In general, these matrices P_i and F_i are taken as symmetric matrices if q is odd, and are taken as upper triangular matrices if q is even. For these representation matrices, based on equation (2.1), F_i has the following form

$$\begin{pmatrix} *_{v\times v} & *_{v\times m} \\ *_{m\times v} & 0_{m\times m} \end{pmatrix}. \tag{2.2}$$

Furthermore, from $\mathcal{P} = \mathcal{F} \circ \mathcal{S}$, we have

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

3 QR-UOV

This section first recalls the basic version of the QR-UOV and the method reducing its public key size [12]. Then, we explain a way of modifying the signature generation step to prove its security in Section 4.

3.1 Basic Scheme

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

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

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

For any $g \in \mathbb{F}_q[x]/(f)$, the matrix Φ_g^f can be represented by only ℓ elements in $\mathbb{F}_q$. We let the algebra of the matrices $A_f := \left\{ \Phi_g^f \in \mathbb{F}_q^{\ell\times\ell} \;\middle|\; g \in \mathbb{F}_q[x]/(f) \right\}$, and this A_f is a subalgebra in the matrix algebra $\mathbb{F}_q^{\ell\times\ell}$. For such matrices corresponding to elements of a quotient ring, Theorem 1 in [12] shows that there exists an invertible matrix $W \in \mathbb{F}_q^{\ell\times\ell}$ such that for any $X \in A_f$, WX is symmetric. Specifically, if f has a form of

$x^\ell - ax^i - 1$ with $a \neq 0$ and $1 \leq i < \ell$, then the above symmetrization is realized by

$$W = \begin{pmatrix} J_i & \\ & J_{\ell-i} \end{pmatrix}, \tag{3.1}$$

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

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

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

From these notations, we can construct a QR-UOV representing public and secret keys by elements of $A_f^{N,N}$ and $W^{(N)}A_f^{N,N} := \{A \cdot B \,|\, A \in W^{(N)}, B \in A_f^{N,N}\}$. Note that we here represent the public and secret keys by matrices as described in Section 2. Before generating the public and secret keys, we prepare an irreducible polynomial $f = x^\ell - ax^i - 1 \in \mathbb{F}_q[x]$ with $a \neq 0$ and $1 \leq i < \ell$ and $W \in \mathbb{F}_q^{\ell\times\ell}$ like equation (3.1), We here take f as an irreducible polynomial for the security of the resulting scheme. Then, the key generation of QR-UOV is described as follows:

(1) Choose F_i $(i = 1, \dots, m)$ from $W^{(N)}A_f^{N,N}$ as a symmetric matrix with the lower-right $m \times m$ zero-block like equation (2.2).

(2) Choose an invertible matrix S from $A_f^{N,N}$ randomly.

(3) Compute the public key $P_i = S^\top F_i S$ $(i = 1, \dots, m)$.

Then, P_i $(i = 1, \dots, m)$ representing the public key map are elements of $W^{(N)}A_f^{(N)}$ from Proposition 1 in [12]. The signing and verification processes are performed in the same way as the plain UOV.

3.2 Reducing Public Key Size

In this subsection, we apply an improved method restricting the secret key $\mathcal{S}$ to a specific compact form, which was first proposed by Czypek et al. [8].

Before describing the improved method, we prepare some notations: For the public key P_i $(i = 1, \dots, m)$ and the secret key F_i $(i = 1, \dots, m)$, we define submatrices as follows

$$P_i = \begin{pmatrix} P_{i,1} & P_{i,2} \\ P_{i,2}^\top & P_{i,3} \end{pmatrix},$$
$$F_i = \begin{pmatrix} F_{i,1} & F_{i,2} \\ F_{i,2}^\top & 0_{m\times m} \end{pmatrix},$$

where $P_{i,1}$ and $F_{i,1}$ are symmetric $v \times v$ matrices, $P_{i,2}$ and $F_{i,2}$ are $v \times m$ matrices, and $P_{i,3}$ is a symmetric $m \times m$ matrix.

We then aim at limiting the secret key S to the following compact form

$$\begin{pmatrix} I_v & S' \\ O & I_m \end{pmatrix},$$

where S' is a $v \times m$ matrix. Then, from $P_i = S^\top F_i S$ $(i = 1, \dots, m)$, we obtain

$$\begin{aligned} F_{i,1} &= P_{i,1}, \\ F_{i,2} &= -P_{i,1}S' + P_{i,2}, \\ 0_{m\times m} &= S'^\top P_{i,1} S' - P_{i,2}^\top S' - S'^\top P_{i,2} + P_{i,3}. \end{aligned} \tag{3.2}$$

By using this equation, in the improved key generation step, $P_{i,1}$, $P_{i,2}$ $(i = 1, \dots, m)$, and S' are first generated from random seeds, and $P_{i,3}$ $(i = 1, \dots, m)$ is computed by

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

Thus, the public key is composed of $m \times m$ matrices $P_{i,3}$ $(i = 1, \dots, m)$ and the small seed for $P_{i,1}$, $P_{i,2}$ $(i = 1, \dots, m)$. The security of QR-UOV is not weakened by this optimization because this does not affect the distribution of the public and secret keys.

3.3 EUF-CMA Secure Variant

This subsection introduces a modification of the signature generation of QR-UOV for the security proof. Its construction is mainly based on the method proposed by Sakumoto et al. [20].

We here describe the inversion of the central map $\mathcal{F}$ in our modified signature generation. We first choose values for the vinegar-variables $y_1, \dots, y_v$ randomly. We then choose λ-bit random salt r and compute $\mathbf{t} \in \mathbb{F}_q$ by applying a hash function on the input concatenating a given message $\mathbf{M}$ and the salt r. If the linear system for the oil-variables $x_{v+1}, \dots, x_n$

$$\mathcal{F}(y_1, \dots, y_v, x_{v+1}, \dots, x_n) = \mathbf{t} \tag{3.3}$$

has solutions, then we obtain the signature by applying $\mathcal{S}^{-1}$ into $(y_1, \dots, y_v, y_{v+1}, \dots, y_n)$ where $(y_{v+1}, \dots, y_n)$ is a randomly chosen solution of equation (3.3). If there exists no solution of equation (3.3), then we choose a new salt and update $\mathbf{t}$ until equation (3.3) has solutions.

The main difference from the standard signature generation algorithm is that if equation (3.3) has no solution, then we choose a new random salt instead of choosing new vinegar-variables. By doing so, the signature $\mathbf{s}$ satisfying $\mathcal{P}(\mathbf{s}) = \mathrm{Hash}(\mathbf{M}||r)$ is uniformly distributed in $\mathbb{F}_q^n$, and this fact enables us to prove the EUF-CMA security of QR-UOV in Section 4. For the efficiency, we confirm that the expected number of computing $\mathbf{t} = \mathrm{Hash}(\mathbf{M}||r)$ until equation (3.3) has solutions is approximately 2.0 for any parameter sets by assuming that equation (3.3) is a randomized system for $x_{v+1}, \dots, x_n$.

See Algorithm $1 \sim 3$ for more details of the key generation, signature generation, and verification of QR-UOV with the improvement in Subsection 3.2 and the modification in this subsection.

Algorithm 1 KeyGen()

$\mathsf{seed}_{\mathsf{pk}}, \mathsf{seed}_{\mathsf{sk}} \leftarrow \{0,1\}^{2\lambda}$
$P_{1,1}, \ldots, P_{m,1}, P_{1,2}, \ldots, P_{m,2} \leftarrow \mathsf{Hash}(\mathsf{seed}_{\mathsf{pk}})$
$S' \leftarrow \mathsf{Hash}(\mathsf{seed}_{\mathsf{sk}})$
for i form 1 to m **do**
  $P_{i,3} \leftarrow -{S'}^{\top} P_{i,1} S' + P_{i,2}^{\top} S' + {S'}^{\top} P_{i,2}$
end for
return $(\mathsf{pk}, \mathsf{sk}) = \left(\left(\mathsf{seed}_{\mathsf{pk}}, \{P_{i,3}\}_{i\in\{1,\ldots,m\}}\right), \mathsf{seed}_{\mathsf{sk}}\right)$

Algorithm 2 Sign($\mathbf{M}, \mathsf{pk}, \mathsf{sk}$)

$\left(\mathsf{seed}_{\mathsf{pk}}, \{P_{i,3}\}_{i\in\{1,\ldots,m\}}\right) \leftarrow \mathsf{pk}$
$\mathsf{seed}_{\mathsf{sk}} \leftarrow \mathsf{sk}$
$P_{1,1}, \ldots, P_{m,1}, P_{1,2}, \ldots, P_{m,2} \leftarrow \mathsf{Hash}(\mathsf{seed}_{\mathsf{pk}})$
$S' \leftarrow \mathsf{Hash}(\mathsf{seed}_{\mathsf{sk}})$
Generate $\mathcal{F}$ following equation (3.2).
$(y_1, \ldots, y_v) \leftarrow \mathbb{F}_q^v$
repeat
  $r \leftarrow \{0,1\}^{\lambda}$
  $\mathbf{t} \leftarrow \mathsf{Hash}(\mathbf{M}||r)$
until $\mathcal{F}(y_1, \ldots, y_v, x_{v+1}, \ldots, x_n) = \mathbf{t}$ has solutions for $(x_{v+1}, \ldots, x_n)$.
Choose one solution $(y_{v+1}, \ldots, y_n) \in \mathbb{F}_q^m$ randomly.
$\mathbf{s} \leftarrow \mathcal{S}^{-1}(y_1, \ldots, y_v, y_{v+1}, \ldots, y_n)$
return $\sigma = (r, \mathbf{s})$

Algorithm 3 Verify($\mathbf{M}, \mathsf{pk}, \sigma$)

$\left(\mathsf{seed}_{\mathsf{pk}}, \{P_{i,3}\}_{i\in\{1,\ldots,m\}}\right) \leftarrow \mathsf{pk}$
$(r, \mathbf{s}) \leftarrow \sigma$
$P_{1,1}, \ldots, P_{m,1}, P_{1,2}, \ldots, P_{m,2} \leftarrow \mathsf{Hash}(\mathsf{seed}_{\mathsf{pk}})$
$\mathbf{t} \leftarrow \mathsf{Hash}(\mathbf{M}||r)$
$\mathbf{t}' \leftarrow \mathcal{P}(\mathbf{s})$
return accept if $\mathbf{t} = \mathbf{t}'$ and reject otherwise.

4 Security Proof

This section discusses the security of QR-UOV with the modified signature generation in Subsection 3.3. After introducing two assumptions, based on which the security proof of QR-UOV can be constructed, and the standard security definition, we show the statement of the EUF-CMA security of QR-UOV. We here omit the proof of the security statement, and our discussion is mainly following [6].

We first introduce two assumptions for the security proof of QR-UOV as follows:

Definition 1 (UOV problem) *We let $\mathsf{MQ}_{q,n,m}$ denote the set of random quadratic maps with n variables and m equations over $\mathbb{F}_q$ and let $\mathsf{UOV}_{q,v,o,m}$ denote the set of public key maps of UOV with v vinegar-variables, o oil-variables, and m equations over $\mathbb{F}_q$. The UOV problem asks to distinguish a random quadratic system from a UOV public key.*

Let $\mathcal{A}$ be a UOV distinguisher algorithm. We say the distinguishing advantage of $\mathcal{A}$ is

$$\begin{aligned}\mathsf{Adv}^{\mathsf{UOV}}_{q,v,o,m}(\mathcal{A}) =& |\Pr[\mathcal{A}(\mathcal{P}) = 1 | \mathcal{P} \leftarrow \mathsf{MQ}_{q,(v+o),m}] \\ &- \Pr[\mathcal{A}(\mathcal{P}) = 1 | \mathcal{P} \leftarrow \mathsf{UOV}_{q,v,o,m}]|.\end{aligned}$$

Definition 2 (QR-MQ problem) *Let $\mathsf{QR}_{q,n,m,\ell}$ be the set of quadratic maps constructed from m matrices in $W^{(N)}A_f^{N,N}$ where f is an irreducible polynomial with $\deg f = \ell$ and $N = n/\ell$. For a random $\mathcal{P} \in \mathsf{QR}_{q,n,m,\ell}$ and $\mathbf{t} \in \mathbb{F}_q^m$, the QR-MQ problem asks to compute $\mathbf{s}$ such that $\mathcal{P}(\mathbf{s}) = \mathbf{t}$.*

Let $\mathcal{A}$ be an adversary. We say that the advantage of $\mathcal{A}$ against the QR-MQ problem is

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{QRMQ}}_{q,n,m,\ell}(\mathcal{A}) = \\ &\Pr[\mathcal{P}(\mathbf{s}) = \mathbf{t} | \mathcal{P} \leftarrow \mathsf{QR}_{q,n,m,\ell}, \mathbf{t} \leftarrow \mathbb{F}_q^m, \mathbf{s} \leftarrow \mathcal{A}(\mathcal{P}, \mathbf{t})].\end{aligned}$$

The first assumption is originally utilized for the security of the plain UOV and thus seems relatively well understood. By contrast, the second assumption is inherent in QR-UOV. Therefore, it is one of the important tasks to correctly evaluate the difficulty of the QR-MQ problem.

Subsequently, we give the definition of the EUF-CMA security, which is the standard security definition for digital signature schemes.

Definition 3 (EUF-CMA security) *Let $\mathcal{O}$ be a random oracle and let $\mathcal{A}$ be an adversary. We say the advantage of $\mathcal{A}$ against the EUF-CMA game of a signature scheme $\mathrm{DSS} = (\mathrm{KeyGen}, \mathrm{Sign}^{\mathcal{O}}, \mathrm{Verify}^{\mathcal{O}})$ in the random oracle model is*

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{EUF\text{-}CMA}}_{\mathrm{DSS}}(\mathcal{A}) = \\ &\Pr[\mathrm{Verify}^{\mathcal{O}}(\mathsf{pk}, m, \sigma) = 1 | (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KeyGen}(), \\ &\quad (m, \sigma) \leftarrow \mathcal{A}^{\mathcal{O}, \mathrm{Sign}^{\mathcal{O}}(\mathsf{sk}, \cdot)}(\mathsf{pk})],\end{aligned}$$

where $\mathsf{Sign}^{\mathcal{O}}(\mathsf{sk}, \cdot)$ was not queried on input m.

We then show the EUF-CMA security of the QR-UOV signature scheme with the modified signature generation.

Theorem 1 *Let $\mathcal{A}$ be an EUF-CMA adversary that runs in time T against QR-UOV in the random oracle model with parameters (q, v, m, ℓ) and which makes Q_s signing queries and Q_h random oracle queries. Then there exist adversaries $\mathcal{B}$ and $\mathcal{B}'$ against the UOV and QR-MQ problems respectively, that run in time $T + O((Q_s + Q_h) \cdot poly(q, n, m, \ell))$ such that*

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{EUF-CMA}}_{q,v,m,\ell}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{UOV}}_{q^\ell,v/\ell,o/\ell,m}(\mathcal{B}) \\ &+ Q_h \mathsf{Adv}^{\mathsf{QRMQ}}_{q,(v+m),m,\ell}(\mathcal{B}') + (Q_h + Q_s) Q_s 2^{-\lambda} + q^m.\end{aligned}$$

The proof for this theorem is based on the proof for Lemma 7 and 8 in [6] and Theorem 1 in [20]. The reason that the security of QR-UOV is reduced into the

UOV problem with the parameters $(q^\ell, v/\ell, o/\ell, m)$ is that the public and secret keys of QR-UOV are equivalent to those of the plain UOV over the extension field as follows:

Lemma 1 *For any parameters (q, v, m, ℓ) of QR-UOV and an irreducible polynomial f with $\deg f = \ell$, there exists a one-to-one mapping from the set of the public and secret keys of QR-UOV with parameter (q, v, m, ℓ) into that of the plain UOV with v/ℓ vinegar-variables, m/ℓ oil-variables, and m equations over $\mathbb{F}_{q^\ell}$.*

We here show a way of constructing such a one-to-one map representing the keys of QR-UOV as those of the plain UOV over $\mathbb{F}_q[x]/(f) \approx \mathbb{F}_{q^\ell}$. For the representation matrix P_k of the public key of QR-UOV, we here define an $N \times N$ matrix $\bar{P}_k$ over $\mathbb{F}_q[x]/(f)$ as follows:

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

where $\bar{P}_k^{(i)} \in \mathbb{F}_q^{N\times N}$ with $0 \le i \le \ell - 1$ satisfies

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

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

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

Then, it holds $\bar{P}_k = \bar{S}^\top \bar{F}_k \bar{S}$ from $P_k = S^\top F_k S$, and $\bar{F}_k$ has the form like equation (2.2). Thus, these sets $\bar{P}_k$, $\bar{F}_k$, and $\bar{S}$ can be seen as the keys of the plain UOV with N variables and m equations over the extension field $\mathbb{F}_q[x]/(f)$.

5 Parameter Analysis

We first propose various parameters for QR-UOV satisfying the security level I, III, and V of NIST PQC standardization project [17]. We then analyze the public key and signature size of the proposed parameters and compare with that of other post-quantum signature schemes.

5.1 Proposed Parameters

We propose some parameter sets of QR-UOV. These parameter sets are proposed in accordance with the security level I, III, and V of the NIST PQC project. We take 7, 31, and 127 as the number q of the finite field. The reason that we do not use a finite field with even characteristics is as follows: If q is even, in a polynomial obtained as $\mathbf{x}A\mathbf{x}^\top$, where $A \in W^{(N)} A_f^{N,N}$, the coefficients corresponding to the non-diagonal components of every diagonal block are zero owing to the symmetry of $W\Phi_g^f$. For each security level and q, we choose three parameter sets denoted by (a), (b), and (c), which are chosen for the following respective purposes:

(a) to make the signature size small ($\ell = 3$),

(b) to make the sum of the signature and public key sizes small ($\ell > 10$),

(c) to obtain intermediate results of the above two conditions ($\ell = 10$).

These types are determined according to the fact that if we take larger ℓ, then the signature size becomes larger and the public key size becomes smaller. In the following, we denote each parameter set by the security level, q, and the type described above. (e.g., (I, 7, a) denotes a parameter with the security level I, $q = 7$, and the type (a).) We then propose some parameter sets in Table 1 $\sim$ 3. Here, we do not specify f because any irreducible trinomial with degree ℓ over $\mathbb{F}_q$ can be taken as f. We further confirmed that there exists such a polynomial for every proposed parameter set.

Table 1: **Security level I parameters**: parameters for QR-UOV satisfying the security level I for the NIST PQC standardization project (q; the order of the finite field, v: the number of vinegar-variables, o: the number of oil-variables and equations, ℓ: block size)

(v, m, ℓ)	(a)	(b)	(c)
$q = 7$	$(189, 72, 3)$	$(2409, 99, 33)$	$(650, 80, 10)$
$q = 31$	$(165, 60, 3)$	$(1664, 78, 26)$	$(600, 70, 10)$
$q = 127$	$(156, 54, 3)$	$(1440, 72, 24)$	$(550, 60, 10)$

Table 2: **Security level III parameters**

(v, m, ℓ)	(a)	(b)	(c)
$q = 7$	$(291, 111, 3)$	$(4640, 160, 40)$	$(1050, 130, 10)$
$q = 31$	$(246, 87, 3)$	$(3783, 117, 39)$	$(890, 100, 10)$
$q = 127$	$(228, 78, 3)$	$(3348, 108, 36)$	$(830, 90, 10)$

Table 3: **Security level V parameters**

(v, m, ℓ)	(a)	(b)	(c)
$q = 7$	$(411, 162, 3)$	$(7335, 225, 45)$	$(1450, 180, 10)$
$q = 31$	$(324, 114, 3)$	$(4699, 148, 37)$	$(1120, 120, 10)$
$q = 127$	$(306, 105, 3)$	$(6000, 144, 48)$	$(1120, 120, 10)$

We then present a method of evaluating the security of the proposed parameters. The security levels I, III, and V indicate that a classical attacker needs more than 2^{143}, 2^{207}, and 2^{272} classical gates, and a quantum attacker needs more than 2^{74}, 2^{137}, and 2^{202} quantum gates, respectively, to break the parameters. For the security of QR-UOV, we confirm that the complexities of the existing four attacks, the direct, Kipnis-Shamir [15], reconciliation [10], and intersection attacks [5], are larger than the claimed criteria. To evaluate the complexity of the direct attack, we assume

that the difficulty of solving quadratic systems from the public key of QR-UOV is equivalent to that of solving randomized quadratic systems. This assumption is not theoretically proven, but the fact confirmed in [12] that the experimental degree of regularity of the public key system of QR-UOV was the same as the theoretical one of the semi-regular systems [2, 3, 4] indicates the correctness of this assumption. On the other hand, the other three attacks, the Kipnis-Shamir, reconciliation, and intersection attacks, are key recovery attacks, which find the secret key given the public key. These three key recovery attacks can be performed by seeing the public key of QR-UOV not only as one of the plain UOV with n variables over $\mathbb{F}_q$ but also as one of the plain UOV with N variables over $\mathbb{F}_q^\ell$ as described in Lemma 1. In general, the complexity of the key recovery attacks on UOV with fewer variables on the extension field is smaller than or equal to that on UOV over the base field. Therefore, we estimate the complexity of the key recovery attacks on QR-UOV as that on the plain UOV with N variables over $\mathbb{F}_q^\ell$. See [12] for specific formulae to estimate the complexity of the four attacks on QR-UOV. We show the complexity of the classical and quantum versions of the four attacks on the parameter (I, 7, a) in Table 4.

Table 4: The complexity ($\log_2$ of the number of gates) of the direct, Kipnis-Shamir, reconciliation, intersection attacks on QR-UOV with the parameter (I, 7, a)

attacks	over $\mathbb{F}_q$	over $\mathbb{F}_{q^\ell}$		
	direct	KS	recon.	inter.
classical	152	346	149	242
quantum	91	186	148	175

5.2 Comparison

This subsection analyzes the public key and signature size of the proposed parameter sets in Subsection 5.1 and compares with that of other post-quantum signature schemes.

For each one of the proposed parameter sets, we estimate the public key and signature size. From the same discussion in [12], the public key size of QR-UOV is given as $\lceil \log q \rceil \cdot \left(\frac{m^3}{2\ell} + \frac{m^2}{2} \right) + 256$ bits, and the signature size is given as $\lceil \log q \rceil \cdot n + 128$ bits. We suppose that the public key and signature of QR-UOV include a 256-bit seed and a 128-bit salt, respectively, as described in Algorithm 1 $\sim$ 3. Indeed, Table 5 computes the public key and signature size of the proposed parameter sets according to the above formulae. We can confirm that parameters of type (a), (b), and (c) behave according to their purposes described in Subsection 5.1, respectively.

Further, we compare the size of the public key and signature of QR-UOV with that of other post-quantum signature schemes. To compare with QR-UOV, we choose two multivariate signature schemes, UOV and MAYO [6], and two lattice-based signature schemes, CRYSTALS-DILITHIUM [1] and FALCON [11], the selected algorithms in the NIST PQC standardization project [19]. Figure 1 displays the public key and signature size of the security level I parameters of these signature schemes. We omit one of the selected algorithms, SPHINCS+, because its public key size is much smaller, and its signature size is much larger than other schemes. In Figure 1, we can confirm that our proposed parameters of type (a) have smaller public keys than UOV, and smaller signatures than MAYO and the lattice-based signatures. Therefore, we consider that the type (a) parameters are superior than the other two types (b) and (c).

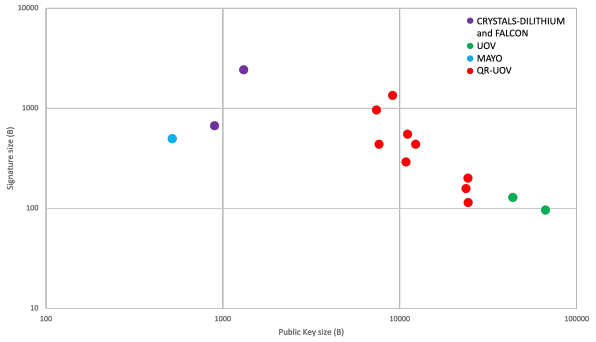

Figure 1: Comparison of the public key and signature size between some candidates of PQC and QR-UOV

6 Conclusion

In this paper, we discussed the security proof and parameter sets of the QR-UOV. QR-UOV was proposed at ASIACRYPT 2021 as a variant of the UOV signature scheme. Because QR-UOV reduces its public key size compared with the plain UOV, it is considered to be one of the strong candidates for post-quantum cryptography.

One of our contributions is that we gave the first formal EUF-CMA security proof for QR-UOV. Our security proof is essentially based on the proof by Beullens for the MAYO signature scheme, and the proof is based on two assumptions: the UOV problem and the QR-MQ problem. This QR-MQ problem is a new assumption generated by us to construct the security proof, and thus, further cryptoanalysis for this problem is necessary to guarantee its security. Another contribution is that we proposed various parameter sets for QR-UOV with different security levels, the orders of the finite field, and the purposes. For these proposed parameter sets, we estimated their public key and signature size in Table 5. Furthermore, we compared our proposed parameters with some lattice-based signatures, the plain UOV, and MAYO, and we considered that type (a) parameters with block size $\ell = 3$ have an advantage compared with other schemes.

As stated above, one of our future works is to analyze the difficulty of solving the QR-MQ problem. For the security of QR-UOV, it would be desirable to theoret-

Table 5: The public key and signature size of the parameter sets of QR-UOV proposed in Subsection 5.1

parameter	(I, 7, a)	(I, 7, b)	(I, 7, c)	(I, 31, a)	(I, 31, b)	(I, 31, c)	(I, 127, a)	(I, 127, b)	(I, 127, c)
public key (B)	24332	7383	10832	23657	7637	12282	24271	9104	11057
signature (B)	114	957	290	157	1105	435	200	1339	550

parameter	(III, 7, a)	(III, 7, b)	(III, 7, c)	(III, 31, a)	(III, 31, b)	(III, 31, c)	(III, 127, a)	(III, 127, b)	(III, 127, c)
public key (B)	87819	24032	44395	70991	17143	34407	71899	20444	35470
signature (B)	167	1816	459	224	2454	635	284	3040	821

parameter	(V, 7, a)	(V, 7, b)	(V, 7, c)	(V, 31, a)	(V, 31, b)	(V, 31, c)	(V, 127, a)	(V, 127, b)	(V, 127, c)
public key (B)	270673	56985	115457	158421	34257	58532	173676	36320	81932
signature (B)	231	2851	627	290	3045	791	376	5392	1101

ically reduce the difficulty of the QR-MQ problem to that of the plain MQ problem. Furthermore, obtaining the performance data of QR-UOV and comparing with the performance of other PQC candidates is also our remaining task.

Acknowledgements

This work was supported by JST CREST Grant Number JPMJCR2113, Japan, and JSPS KAKENHI Grant Number 21J20391 and 22K17889, Japan.

References

[1] Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium. Supporting documentation for NIST PQC project (2020)

[2] 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)

[3] 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)

[4] 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)

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

[6] Beullens, W.: MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In: SAC 2021, LNCS, vol. 13203, pp. 355–376. Springer (2021)

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

[8] Czypek, P., Heyse, S., Thomae, E.: Efficient implementations of MQPKS on constrained devices. In: CHES 2012, LNCS, vol. 7428, pp. 374–389. Springer (2012)

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

[10] 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)

[11] Fouque P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: FALCON: Fast-fourier lattice-based compact signatures over NTRU. Supporting documentation for NIST PQC project (2020)

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

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

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

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

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

[17] 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)

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

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

[20] 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. Springer (2011)

[21] 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)

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