NOVA, a Noncommutative-ring Based Unbalanced Oil and Vinegar Signature Scheme with Key-randomness Alignment

Lih-Chung Wang [*†] Po-En Tseng [‡] Yen-Liang Kuan [§]
Chun-Yen Chou [¶]

Abstract

In this paper, we propose a noncommutative-ring based unbalanced oil and vinegar signature scheme with key-randomness alignment: NOVA (Noncommutative Oil and Vinegar with Alignment). Instead of fields or even commutative rings, we show that noncommutative rings can be used for algebraic cryptosystems. At the same or better level of security requirement, NOVA has a much smaller public key than UOV (Unbalanced Oil and Vinegar), which makes NOVA practical in most situations. We use Magma to actually implement and give a detailed security analysis against known major attacks. [1]

1 Introduction

All known multivariate cryptosystems are systems of nonlinear polynomial equations in several variables over a finite field. The security of these multivariate schemes is based on the MQ problem: for m quadratic polynomials $p_1(x_1, \ldots, x_n)$, $p_2(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n)$ in n variables $x_1, x_2, \ldots, x_n$ over a finite field $\mathbb{F}_q$ of order q, to find a vector

[*]Corresponding author: Lih-Chung Wang
[†]Lih-Chung Wang, Email: lcwang@gms.ndhu.edu.tw Address: Department of Applied Mathematics, National Donghwa University, No. 1, Sec. 2, Da Hsueh Rd., Shoufeng, Hualien 974301, Taiwan, R.O.C.
[‡]Po-En Tseng, Email: briantseng0320@gmail.com Address: Department of Applied Mathematics, National Donghwa University, No. 1, Sec. 2, Da Hsueh Rd., Shoufeng, Hualien 974301, Taiwan, R.O.C.
[§]Yen-Liang Kuan, Email: ylkuan@gms.ndhu.edu.tw Address: Department of Applied Mathematics, National Donghwa University, No. 1, Sec. 2, Da Hsueh Rd., Shoufeng, Hualien 974301, Taiwan, R.O.C.
[¶]Chun-Yen Chou, Email: choucy@gms.ndhu.edu.tw Address: Department of Applied Mathematics, National Donghwa University, No. 1, Sec. 2, Da Hsueh Rd., Shoufeng, Hualien 974301, Taiwan, R.O.C.
[1]2020 Mathematics Subject Classification. Primary:94A62, 12E20, 03D15, 13P10, 13P15

$(a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ such that $p_1(a_1, \ldots, a_n) = p_2(a_1, \ldots, a_n) = \cdots = p_m(a_1, \ldots, a_n) = 0$. The MQ problem is proven to be NP-hard [19]. The private key of a usual multivariate scheme consists of three maps: $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $F : \mathbb{F}_q^m \to \mathbb{F}_q^n$, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ where F is a plausibly invertible polynomial map (called the central map) and S, T are easily invertible maps (usually linear maps) to hide the structure of the central map F. The public key is the composite map $S \circ F \circ T$. Since 1988, many multivariate schemes such as C^* [26], HFE [31], MFE [22], UOV [23], Rainbow [12], TRMS [41], TRMC [40], ABC [37] and other applications [15, 36] are presented.

However, why the polynomials used in multivariate cryptosystems must be over fields or even over commutative rings? If we can overcome difficulties in computation over noncommutative rings, we end up with cryptosystems of the same or better security. Well-known noncommutative rings include matrix rings, group rings and quoternion rings. Note that a finite group ring can be viewed as a subring of some matrix ring, and a finite quoternion ring can be viewed as a quotient ring of some subring of a matrix ring. In this paper, we choose the noncommutative matrix ring $\mathcal{R}$ of $l \times l$ matrices over $\mathbb{F}_q$ to be the coefficient ring. We construct a UOV-like scheme with coefficients in $\mathcal{R}$ and overcome difficulties in computation and thus show that we can have multivariate cryptosystems of nonlinear polynomial equations in several variables over a noncommutative ring.

For cryptanalysis, because of the noncommutative structure of the coefficient ring $\mathcal{R}$, it will be very difficult for the attacker to directly attack the system at the ring level due to the lack of commutativity, hence powerful computation tools such as F_4 [16], F_5 [17] and XL variants [10, 42] as in the case of fields. On the other hand, it is possible to attack the system at the level of the field $\mathbb{F}_q$ since $\mathcal{R}$ is the matrix ring of $l \times l$ matrices over $\mathbb{F}_q$. However, since each element in $\mathcal{R}$ consists of l^2 elements in $\mathbb{F}_q$, thus m equations with n variables in $\mathcal{R}$ will result in $l^2 \cdot m$ equations with $l^2 \cdot n$ variables in $\mathbb{F}_q$, thus making the corresponding attack at the field level computationally infeasible. And, from this point of view, we see that the reduction of key-size is tremendous at the same or even better security level by using the noncommutative ring.

Also, multivariate cryptosystems are now getting more attention as number theory based cryptosystems losing ground under the attack of quantum computing power that executing Shor's algorithm [35]. However, straightforward multivariate cryptosystems suffer from huge key sizes as the private key keeping the records of random choices and the public key keeping the records of all coefficients in all polynomials in the public key. A known way to downsize the private key is to use a seed and a pseudo random number generator (PRNG). That is, use the randomness of the seed to generate the randomness of the private key while reducing the key size. Ironically, for the purpose of practical use of public key cryptosystems, the focus of downsizing keys should be on the public key rather than the private key since it is the public key should be known and transmitted over public channels.

In [32, 33], Petzoldt *et al.* proposed a new technique that realign the randomness of the central map F to a part of the public key, and then downsizing of the public key is

possible without sacrificing the randomness of the composite map. That is, to realign part of the source of randomness from the private key to a part of the public key. Note that this randomness alignment technique is applicable to UOV-alike systems. In [11], they apply this technique on Rainbow scheme. We will also use this technique to help reducing the public key size. Thus we name our noncommutative-ring based unbalanced oil and vinegar signature schemes with key-randomness alignment: NOVA (Noncommutative Oil and Vinegar with Alignment).

In Section 2, we first briefly introduce the notations used in this paper and the construction of usual multivariate signature schemes. We then describe UOV in details, including original key generation and key generation with key-randomness alignment in Section 3.

In Section 4, we give a full introduction of our signature scheme NOVA, first using key generation without key-randomness alignment, then using key generation with key-randomness alignment.

A detailed security analysis of NOVA is given in Section 5. After briefly introducing NIST levels I, III, and V, we thoroughly discuss known major attacks including Direct attack, Min-Rank alike attacks, K-S attack (UOV attack), Intersection attack, and algebraic attack for matrix $[T^{-1}]$ we called equivalent key attack.

We carefully pick several sets of parameters for NOVA so that it meets the requirements of National Institute for Standards and Technology (NIST) level I, III, and V in its PQC standardization project [28], respectively. An actual comparison with NIST final candidates is given in the analysis below.

Section 6 gives our proposed parameter settings for actual implementation of NOVA using Magma, including tables showing complexity in $\log_2(\sharp\text{gates})$ and key-sizes and lengths of the signature with these proposed parameter settings.

A conclusion is given in Section 7. A brief introduction of a variant of NOVA scheme is given in Appendix using whipping technique proposed by Beullens [5].

2 Preliminaries

2.1 Notation Used in The Paper

Symbol	Description
$\mathbb{F}_q$	finite field of order q
$\mathcal{R}$	noncommutative ring
v	number of vinegar variables
o	number of oil variables
s	symmetric matrix used in NOVA
$n = v + o$	number of variables
$m = o$	number of equations
$F = [F_1 \cdots F_m]$	central map of the signature scheme
$[F_i]$	matrix corresponding to F_i in F
T	invertible linear map in signature scheme
$[T]$	matrix corresponding to T
$[T^{-1}]$	matrix corresponding to the map T^{-1}
$P = [P_1 \cdots P_m]$	public key of the signature scheme
D	document to be signed
$Hash(D)$	hash value of the document D
$\mathcal{O}$	oil space of the central map F
$T^{-1}(\mathcal{O})$	oil space of the public key P
$MQ(N, M, q)$	complexity of solving MQ system of M equations in N variables

2.2 Construction of Multivariate Quadratic (MQ) Signature

Usual multivariate signature schemes are constructed as follows. Let $\mathbb{F}_q$ denote the finite field of order q. Let n and m are two positive integers. A usual multivariate signature scheme consists of three maps, S, F, T where $F = [F_1, \cdots, F_m] : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is an easily invertible quadratic map (trapdoor map) called the central map, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ are two invertible linear maps randomly chosen in order to hide the specific structure of F.

Public key. The public key of the multivariate signature scheme is the multivariate polynomial map $P = S \circ F \circ T : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Secret key. The three maps $S,\ F$ and T.

Signature. Let $z = Hash(D) \in \mathbb{F}_q^m$ be the hash value of the document to be signed. Compute $y = S^{-1}(z)$ and then solve $x = F^{-1}(y)$. Therefore, the signature of document D is $u = T^{-1}(x)$.

Verification. Accept the signature $u \in \mathbb{F}_q^n$ if $P(u) = Hash(D)$, and reject it otherwise.

3 Unbalanced Oil and Vinegar Signature Scheme

The Oil and Vinegar (OV) digital signature scheme, proposed by Patarin [30], is a MQ digital signature scheme. The central map of OV is an MQ-based trapdoor function with $n = 2m$. The K-S attack, also called the UOV attack, given by Kipnis and Shamir [24] reveals that OV scheme is insecure. However, with slight modification in the setting of OV scheme, i.e., to set $n > 2m$, then it can resist the attack in [24]. This modified version of OV is known as Unbalanced Oil and Vinegar (UOV) signature scheme [23].

Being an MQ signature scheme, in practical aspect, UOV scheme still face the problem: to meet the security requirement proposed by NIST level I, III, and V, the size of the public key is too large if nothing is done.

A UOV signature scheme is associated with a triple of positive integers $(v,\ o,\ q)$ with $v > o$ so that the number of variables $n = v + o$, the number of equations $m = o$, and q is the order of the finite field $\mathbb{F}_q$.

Central map. We described the central map of UOV scheme $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ as below.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{v}\sum_{k=j}^{n} f_{1,jk}x_jx_k \\ \vdots \\ \sum_{j=1}^{v}\sum_{k=j}^{n} f_{i,jk}x_jx_k \\ \vdots \\ \sum_{j=1}^{v}\sum_{k=j}^{n} f_{m,jk}x_jx_k \end{bmatrix}$$

where $f_{i,jk}$'s are the coefficients chosen randomly from $\mathbb{F}_q$. Thus F consists of m homogeneous quadratic polynomials in n variables over $\mathbb{F}_q$ and $F_i = x^t\,[F_i]\,x$ with $x = (x_1, \cdots, x_n)^t$. Note that, for $j, k = v+1, \cdots, n$, each F_i does not contain x_jx_k terms. This kind of phenomenon is analogous to that oil and vinegar won't mix completely and this enables us to invert F easily.

We called the variables $x_1, \cdots, x_v$ the vinegar variables, and $x_{v+1}, \cdots, x_n$ the oil variables. It is also required that $v > o$ in order to resist the K-S attack. This is the reason

why the scheme is called Unbalanced Oil and Vinegar (UOV).

Private key. The design of UOV chooses S in the usual private key (S, F, T) to be the identity map. Thus, for UOV, the private key is only the pair (F, T) where F is the central map above, and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is an invertible linear map which is randomly chosen.

Public key. The composite map $P = F \circ T : \mathbb{F}_q^n \to \mathbb{F}_q^m$ consisting of m homogeneous quadratic polynomials in n variables over $\mathbb{F}_q$ is the public key. Note that the i-th public polynomial P_i can be written in a quadratic form, that is, $P_i = u^t [P_i] u$ where $u = (u_1, \cdots, u_n)^t$ and $[P_i] = [T]^t [F_i] [T]$ where $[T]$ is the matrix corresponding to T.

Oil space of the public key. By the construction of UOV scheme, we know that P vanishes on a subspace of $\mathbb{F}_q^n$ denoted by $T^{-1}(\mathcal{O})$ with $\mathcal{O} = \{(x_1, \cdots x_n)^t \in \mathbb{F}_q^n : x_1 = \cdots = x_v = 0\}$, which is called the oil space of public key P. In other words, $P(\tilde{o}) = 0$ for all $\tilde{o} \in T^{-1}(\mathcal{O})$.

Signature. Let D be the document to be signed. We first solve $x = (x_1, \cdots, x_n)^t \in \mathbb{F}_q^n$ such that $F(x) = Hash(D) \in \mathbb{F}_q^m$ where $Hash(D)$ is the hash value of D. The strategy is to randomly assign values to vinegar variables $x_1, \cdots, x_v$, then the resulting system becomes linear in oil variables $x_{v+1}, \cdots, x_n$ only since there is no $x_j x_k$ where $j, k = v+1, \cdots, n$, in each F_i. Hence, with a very high probability, it can be solved, e.g., using Gaussian elimination. If the resulting linear system cannot be solved uniquely, we simply randomly assign another set of values to vinegar variables $x_1, \cdots, x_v$. The signature of UOV scheme is $u = T^{-1}(x) \in \mathbb{F}_q^n$.

Verification. First, we compute the hash value $Hash(D)$. Secondly, we verify whether $P(u) = Hash(D)$ or not. If so then the signature is accepted, otherwise rejected.

Public key generation. Choose all coefficients in (F, T) randomly and then compute the composite map $P = F \circ T$.

3.1 Original Key Generation of UOV

Notice that according to the congruence relation $[P_i] = [T]^t [F_i] [T]$ we can do the following to speed up the generation of the public key of UOV scheme without sacrificing security.

1. The matrix representation $[T]$ of the invertible linear map T can be chosen in the form (see [32]).

$$[T] = \begin{bmatrix} I^{11} & T^{12} \\ 0 & I^{22} \end{bmatrix}$$

where I^{11}, I^{22} are identity matrices of size $v \times v$ and $o \times o$, respectively, and T^{12} is a

$v \times o$ matrix over $\mathbb{F}_q$. We also denote

$$\left[T^{-1}\right] = \begin{bmatrix} I^{11} & (T^{-1})^{12} \\ 0 & I^{22} \end{bmatrix}.$$

2. We can represent the map F as a set of $n \times n$ matrices $[F_i]$ for $i = 1, \cdots, m$. By the design of F, we can write these $[F_i]$ in the form

$$[F_i] = \begin{bmatrix} F_i^{11} & F_i^{12} \\ 0 & 0 \end{bmatrix},$$

where F_i^{11} is a $v \times v$ upper triangular matrix and F_i^{12} is a $v \times o$ matrix.

3. The map P can be represented as a set of $n \times n$ upper triangular matrices $[P_i]$.

Now we can go through the following steps to obtain public key $[P_i]$ for $i = 1, \cdots, m$.

First Step: Generate the private key (F, T) from a seed.

First, choose a seed $\mathbf{s_{private}}$ and use pseudo random number generator(PRNG) to generate the coefficients of the invertible linear map T and the coefficients of central map F, namely the matrix T^{12} and the components of the matrices $[F_i]$'s.

Second Step: Compute the matrices $[P_i]$'s corresponding to the public key P.

Since the public key $P = F \circ T$, it follows that each matrix

$$\begin{aligned}
[P_i] = Upper\left([T]^t [F_i] [T]\right) &= Upper\left(\begin{bmatrix} F_i^{11} & F_i^{11}T^{12} + F_i^{12} \\ (T^{12})^t F_i^{11} & (T^{12})^t F_i^{11} T^{12} + (T^{12})^t F_i^{12} \end{bmatrix}\right) \\
&= \begin{bmatrix} Upper(F_i^{11}) & (F_i^{11} + (F_i^{11})^t)T^{12} + F_i^{12} \\ 0 & Upper\left((T^{12})^t F_i^{11} T^{12} + (T^{12})^t F_i^{12}\right) \end{bmatrix} \\
&= \begin{bmatrix} P_i^{11} & P_i^{12} \\ 0 & P_i^{22} \end{bmatrix}
\end{aligned}$$

where $Upper(\cdot)$ is the map that expresses how the public key of UOV assembles its terms. Hence $Upper(\cdot)$ sends a matrix to its equivalent upper triangular matrix in the sense when applying as a quadratic form. That is, in the case of UOV, for a matrix $\hat{A} = [a_{ij}]$, $Upper(\hat{A}) = [\tilde{a}_{ij}]$ with

$$\tilde{a}_{ij} = \begin{cases} a_{ij} + a_{ji} & , \ i < j \\ a_{ij} & , \ i = j \\ 0 & , \ \text{otherwise.} \end{cases}$$

Remark 3.1. The use of a seed $\mathbf{s_{private}}$ is to save the cost of storing the private key (F, T). One may choose not to record the coefficients in the generated private key (F, T), but only the seed $\mathbf{s_{private}}$. It can be regarded as a trade off of increasing the cost of time in exchange for the cost of key size. However, the private key is only stored

in the private device of the user. Thus the cost of the private key size is acceptable. Although such saving is not extremely necessary, the idea of only recording the seed to reduce size is still valuable. In combinations of other ideas as in [32] and [11], it is used to solve the problem that the public key size of a multivariate cryptosystem is too large as below.

3.2 Key Generation of UOV with Key-Randomness Alignment

A. Petzoldt [32] and Rainbow [11] of the third-round of NIST proposal indicate that the number of coefficients in the original randomly generated private key can be regarded as the degree of freedom for determining the coefficients in the key generation process. Part of the degree of freedom of the private key can be transferred to the public key by another seed (key-randomness alignment) and thus reducing the public key size. Thus it solves the essential problem of the public key of original UOV being too large.

First Step: Generate a part of the public key P and the private key T from two seeds respectively.

First, [32] use a seed $\mathbf{s_{private}}$ and PRNG to generate a component of the private key T^{12}. Use another seed $\mathbf{s_{public}}$ to generate the coefficients of part of the public key P: $P_i^{11},\ P_i^{12}$ for $i = 1, \cdots, m$.

Second Step: Compute the matrices F_i's corresponding to the central map F.

From the relation $[P_i] = Upper([T]^t\,[F_i]\,[T])$ and $[T]$ is an invertible matrix, it follows that the matrix

$$[F_i] = ([T]^t)^{-1}\,[P_i]\,[T]^{-1} = \left[T^{-1}\right]^t\,[P_i]\,\left[T^{-1}\right]$$

and hence we have that

$$F_i^{11} = P_i^{11},$$
$$F_i^{12} = (P_i^{11} + (P_i^{11})^t)(T^{-1})^{12} + P_i^{12}.$$

Third Step: Compute the remaining parts of the public key P:

$$P_i^{22} = Upper\left((T^{12})^t F_i^{11} T^{12} + (T^{12})^t F_i^{12}\right).$$

4 Noncommutative Oil and Vinegar with Alignment

In this section, we introduce our signature scheme over a noncommutative ring, NOVA. The core idea behind our scheme is to use noncommutative structure to resist attacks with fewer ring variables at or above the same level of security requirement, thereby reducing the size of the public key.

4.1 Description

Let v, o be positive integers with $v > o$ and q a power of a prime. For implementation, we choose our noncommutative ring $\mathcal{R}$ be the ring consisting of $l \times l$ matrices over the finite field $\mathbb{F}_q$. A NOVA signature scheme is associated with a quadruple of positive integers (v, o, q, l). Let $n = v + o$ and $m = o$.

The space $\mathbb{F}_q[\mathrm{s}]$. First, we randomly choose an $l \times l$ symmetric matrix with irreducible characteristic polynomial over $\mathbb{F}_q$, say s. Let $\mathbb{F}_q[\mathrm{s}] = \{a_0 + a_1 s + \cdots + a_{l-1}s^{l-1} : a_0, a_1, \cdots, a_{l-1} \in \mathbb{F}_q\}$. Note that the elements in $\mathbb{F}_q[\mathrm{s}]$ are symmetric and commute with each others.

Central map. The central map of NOVA scheme $F = [F_1, \cdots, F_m] : \mathcal{R}^n \to \mathcal{R}^m$ is constructed as below. Let $\Omega = \{(j, k) : 1 \leq j, k \leq n\}$ and $\tilde{\Omega} = \{(j, k) : m+1 \leq j, k \leq n\}$ For $i = 1, \cdots, m$, F_i is of the form

$$F_i = \sum_{\alpha=1}^{l^2} \sum_{\Omega \setminus \tilde{\Omega}} A_{\alpha 1} \cdot x_j^t (Q_{\alpha 1} F_{i,jk} Q_{\alpha 1}^{-1} - Q_{\alpha 2} F_{i,jk} Q_{\alpha 2}^{-1}) x_k \cdot A_{\alpha 2}$$

where $F_{i,jk}$'s, $A_{\alpha 1}$ and $A_{\alpha 2}$ are the elements chosen randomly from $\mathcal{R}$, and $Q_{\alpha 1}$, $Q_{\alpha 2}$ are invertible matrices chosen randomly from $\mathbb{F}_q[\mathrm{s}]$.

The matrix over $\mathcal{R}$ corresponding to F_i is

$$[F_i] = \begin{bmatrix} F_i^{11} & F_i^{12} \\ F_i^{21} & 0 \end{bmatrix},$$

where F_i^{11}, F_i^{12} and F_i^{21} are matrices over $\mathcal{R}$ of size $v \times v$, $v \times o$ and $o \times v$, respectively.

We can see that the central map of NOVA keep the spirit of UOV, that is, F_i does not contain the terms $A_{\alpha 1} \cdot x_j^t (Q_{\alpha 1} F_{i,jk} Q_{\alpha 1}^{-1} - Q_{\alpha 2} F_{i,jk} Q_{\alpha 2}^{-1}) x_k \cdot A_{\alpha 2}$ for $j, k = v + 1, \cdots, n$. It follows that NOVA generalize the notion of oil and vinegar variables from $\mathbb{F}_q$ to $\mathcal{R}$. That is, NOVA scheme behaves like a UOV scheme over a noncommutative ring.

Remark 4.1. The key formulation in matrices and the technique using key randomness alignment in the key generation process of UOV are also applicable to NOVA.

Ivertible linear map. Let $T : \mathcal{R}^n \to \mathcal{R}^n$ be the map corresponding to the matrix

$$[T] = \begin{bmatrix} I^{11} & T^{12} \\ 0 & I^{22} \end{bmatrix},$$

where T^{12} is a $v \times o$ matrix consisting of nonzero elements t_{ij} we choose randomly from $\mathbb{F}_q[\mathrm{s}]$. Note that elements in $\mathbb{F}_q[\mathrm{s}]$ can commute with each other. I^{11}, I^{22} are the diagonal matrices with all diagonal entries being the unity in $\mathcal{R}$ (i.e. identity matrix). Thus, $[T]$ is invertible and hence T.

The map $\tilde{F}$. Let $\tilde{F} = F \circ T$. For $i = 1, 2, \ldots, m$, each component map $\tilde{F}_i$ is the composition of F_i and T, that is, $\tilde{F}_i = F_i \circ T$. According to the relation $\tilde{F}_i = F_i \circ T$ and $x = [T] \cdot u$ we get

$$\tilde{F}_i(u) = F_i(T(u)) = \sum_{\alpha=1}^{l^2} \sum_{d_j=1}^{n} \sum_{d_k=1}^{n} A_{\alpha 1} \cdot u_{d_j}^t (Q_{\alpha 1} \tilde{F}_{i,d_j d_k} Q_{\alpha 1}^{-1} - Q_{\alpha 2} \tilde{F}_{i,d_j d_k} Q_{\alpha 2}^{-1}) u_{d_k} \cdot A_{\alpha 2}$$

where $\tilde{F}_{i,d_j d_k} = \sum_{\Omega \setminus \tilde{\Omega}} t_{j,d_j} \cdot F_{i,jk} \cdot t_{k,d_k}$ and $u = (u_1, \cdots, u_n)$. Note that t_{ij} commutes with $Q_{\alpha 1}$ and $Q_{\alpha 2}$ since they all are in $\mathbb{F}_q[\mathrm{s}]$.

Perturbation on the map $\tilde{F}_i$. Different from the original UOV map $P = F \circ T$, we introduce a technique we called perturbation to the map $\tilde{F}_i$ to form the public key of NOVA scheme. First, we randomly choose $\varepsilon_{i,d_j d_k} \in \mathbb{F}_q[\mathrm{s}]$. We denote the matrix corresponding to perturbations $\varepsilon_{i,d_j d_k}$ by $[\varepsilon_i]$. Secondly, we let $P_{i,d_j d_k} = \tilde{F}_{i,d_j d_k} + \varepsilon_{i,d_j d_k}$. Therefore, we have

$$\begin{aligned} P_i(u) &= \sum_{\alpha=1}^{l^2} \sum_{d_j=1}^{n} \sum_{d_k=1}^{n} A_{\alpha 1} \cdot u_{d_j}^t \left(Q_{\alpha 1} \Big(P_{i,d_j d_k} \Big) Q_{\alpha 1}^{-1} - Q_{\alpha 2} \Big(P_{i,d_j d_k} \Big) Q_{\alpha 2}^{-1} \right) u_{d_k} \cdot A_{\alpha 2} \\ &= \tilde{F}_i(u). \end{aligned}$$

Note that P can not be regarded as a UOV over $\mathcal{R}$. Therefore, this will make it more difficult for the attacker to attack NOVA, in general. The matrix over $\mathcal{R}$ corresponding to P_i has the form of

$$[P_i] = \begin{bmatrix} P_i^{11} & P_i^{12} \\ P_i^{21} & P_i^{22} \end{bmatrix}.$$

Public key. The public key are the map $P : \mathcal{R}^n \to \mathcal{R}^m$, i.e., the corresponding matrices $[P_i]$ for $i = 1, \cdots, m$, and the matrices $A_{\alpha k}$ and $Q_{\alpha k}$ for $k = 1, 2$. Note that, without key-randomness alignment, the verifier will receive matrices $[P_i]$ and a seed $\mathbf{s_{public}}$ which is used to generate $A_{\alpha k}$ and $Q_{\alpha k}$ for $k = 1, 2$. On the other hand, with alignment technique, the signer distributes the part of $[P_i]$, namely P_i^{22}, for $i = 1, \cdots, m$ and a seed $\mathbf{s_{public}}$ that is used to generate $P_i^{11}, P_i^{12}, P_i^{21}, A_{\alpha k}$ and $Q_{\alpha k}$. In other words, the matrices do not incur any additional costs on public key size with using randomness-alignment.

Private key. The private key of NOVA is (F, T), i.e., the matrices $[T]$ and the matrices $[F_i]$.

Structure of NOVA. According to the perturbation on P in NOVA scheme, there does not exist an oil space of P of NOVA scheme over R similar to the space $T^{-1}(\mathcal{O})$ as in the case of UOV. However, an equation over $\mathcal{R}$ gives $l \times l$ equations over $\mathbb{F}_q$ which means a NOVA scheme can not only be regarded as a UOV scheme in $\mathcal{R}$ variables, but also a UOV scheme in $\mathbb{F}_q$ variables. Therefore, a (v, o, q, l) NOVA over $\mathcal{R}$ scheme

can be regard as an (l^2v, l^2o, q) UOV scheme over $\mathbb{F}_q$. In fact, they are the same when considered as only over $\mathbb{F}_q$. However, the noncommutativity of $\mathcal{R}$ and the perturbation on P still create differences between NOVA and UOV when NOVA is also considered over $\mathcal{R}$. These differences are also reasons that NOVA can resist the attacks against UOV.

Signature. Note that for the signer it is unaffected by the perturbation, that is, the process of signing is the same as for UOV. Let $Hash(D) = (y_1, \cdots, y_m) \in \mathcal{R}^m$ be the hash value of document D. First, we solve $x = (x_1, \cdots, x_n) \in \mathcal{R}^n$ such that $F_i(x) = y_i$ for $i = 1, \cdots, m$. For this, we assign values to vinegar variables $x_1, \cdots, x_v$ randomly and then, as mentioned above, we can regard the resulting system as a linear system over $\mathbb{F}_q$. Hence with a high probability, we can solve the system using Gaussian elimination over $\mathbb{F}_q$. Therefore, the signature is $u = T^{-1}(x) \in \mathcal{R}^n$.

Verification. Similarly, the verification of a signature is not affected by perturbation. Let $u = (u_1, \cdots, u_n) \in \mathcal{R}^n$ be the signature to be verified. We compute the hash value $Hash(D)$ of the document and the value $P(u)$. If $Hash(D) = P(u)$ then the signature is accepted, otherwise rejected.

Remark 4.2. Due to the structure of P_i and that $\mathcal{R}$ is noncommutative, it is impossible to write the public key in quadratic form over $\mathcal{R}$, namely $P_i(u) = u^t [P_i] u$. However, it is possible to write the public key in quadratic form over $\mathbb{F}_q$, i.e. regards NOVA as a UOV scheme over $\mathbb{F}_q$, but with the explosion of the number of equations and the number of variables.

4.2 Key Generation without Key-Randomness Alignment

We can obtain the public key $[P_i]$ of NOVA by following steps.

First Step: Generate the private key $[T]$, $[F_i]$ and $[\varepsilon_i]$ from a seed.

We use PRNG to generate $[T]$, $[F_i]$ and $[\varepsilon_i]$ from a seed $\mathbf{s_{private}}$.

Second Step: Compute matrices $\left[\tilde{F}_i\right]$ by the formulas above.

Since for ring variables $x = (x_1, \cdots, x_n)$ we have $x = T(u)$, we write

$$x_j = \sum_{d_j=1}^{n} t_{j,d_j} u_{d_j}, \ j = 1, \cdots n.$$

Since $\tilde{F} = F \circ T$ and t_{ij} commutes with $Q_{\alpha 1}$ and $Q_{\alpha 2}$ we have

$$\tilde{F}_i(u) = \sum_{\alpha=1}^{l^2} \sum_{d_j=1}^{n} \sum_{d_k=1}^{n} A_{\alpha 1} \cdot u_{d_j}^t (Q_{\alpha 1} \tilde{F}_{i,d_j d_k} Q_{\alpha 1}^{-1} - Q_{\alpha 2} \tilde{F}_{i,d_j d_k} Q_{\alpha 2}^{-1}) u_{d_k} \cdot A_{\alpha 2}$$

where $\tilde{F}_{i,d_jd_k} = \sum_{\Omega\setminus\tilde{\Omega}} t_{j,d_j} \cdot F_{i,jk} \cdot t_{k,d_k}$. Therefore, the matrices corresponding to $\tilde{F}_i$ are obtained by

$$\begin{aligned}\left[\tilde{F}_i\right] &= \begin{bmatrix} \tilde{F}_i^{11} & \tilde{F}_i^{12} \\ \tilde{F}_i^{21} & \tilde{F}_i^{22} \end{bmatrix} \\ &= [T]^t \, [F_i] \, [T] \\ &= \begin{bmatrix} F_i^{11} & F_i^{11}T^{12} + F_i^{12} \\ (T^{12})^t F_i^{11} + F_i^{21} & (T^{12})^t F_i^{11} T^{12} + F_i^{21} T^{12} + (T^{12})^t F_i^{12} \end{bmatrix}.\end{aligned}$$

Third Step: Compute the public key of NOVA, i.e., matrices $[P_i]$.

To obtain the matrix $[P_i]$, for each component in $[P_i]$, we let $P_{i,d_jd_k} = \tilde{F}_{i,d_jd_k} + \varepsilon_{i,d_jd_k}$ for $d_j, d_k = 1, \cdots, n$, i.e., apply the perturbation on $\tilde{F}_i$. Therefore, public key

$$\begin{aligned}[P_i] &= \left[\tilde{F}_i\right] + [\varepsilon_i] \\ &= \begin{bmatrix} \tilde{F}_i^{11} + \varepsilon_i^{11} & \tilde{F}_i^{12} + \varepsilon_i^{12} \\ \tilde{F}_i^{21} + \varepsilon_i^{21} & \tilde{F}_i^{22} + \varepsilon_i^{22} \end{bmatrix}\end{aligned}$$

where $[\varepsilon_i] = \begin{bmatrix} \varepsilon_i^{11} & \varepsilon_i^{12} \\ \varepsilon_i^{21} & \varepsilon_i^{22} \end{bmatrix} \in \mathrm{Mat}_n(\mathbb{F}_q[s])$.

Key size of the public key: The key size of the public key is

$$\mathrm{Size}_{\mathrm{pk}} = m \cdot n^2 \cdot l^2$$

field elements of $\mathbb{F}_q$.

4.3 Key Generation with Key-Randomness Alignment

First Step: Generate P_i^{11}, P_i^{12} and P_i^{21} for $i = 1, \cdots, m$, and $[T]$ from two seeds $\mathbf{s_{public}}$ and $\mathbf{s_{private}}$ respectively. Moreover, we also generate $[\varepsilon_i]$ from $\mathbf{s_{private}}$.

Second Step: Compute the matrices $\tilde{F}_i^{11}$, $\tilde{F}_i^{12}$ and $\tilde{F}_i^{21}$ corresponding to the map $\tilde{F}_i$.

From the formulas above, we see that once we generate P_i^{11}, P_i^{12} and P_i^{21}, then $\tilde{F}_i^{11}$, $\tilde{F}_i^{12}$ and $\tilde{F}_i^{21}$ can be solved. Note that $\tilde{F}_i^{11} = P_i^{11} - \varepsilon_i^{11}$ and so on.

Third Step: Compute matrices F_i^{11}, F_i^{12} and F_i^{21}

Note that

$$\left[T^{-1}\right] = \begin{bmatrix} I^{11} & -T^{12} \\ 0 & I^{22} \end{bmatrix},$$

where T^{12} is the top right corner submatrix of $[T]$.

From the relation

$$[F_i] = \left([T]^t\right)^{-1} \left[\tilde{F}_i\right] [T]^{-1} = \left([T]^{-1}\right)^t \left[\tilde{F}_i\right] [T]^{-1},$$

we can obtain F_i^{11}, F_i^{12} and F_i^{21} as in the key generation process of UOV. Namely,we have

$$\begin{aligned}
[F_i] &= \begin{bmatrix} F_i^{11} & F_i^{12} \\ F_i^{21} & 0 \end{bmatrix} \\
&= \left([T]^{-1}\right)^t \left[\tilde{F}_i\right] [T]^{-1} \\
&= \begin{bmatrix} \tilde{F}_i{}^{11} & \left(\tilde{F}_i{}^{11}(-T^{12}) + \tilde{F}_i{}^{12}\right) \\ (-T^{12})^t \tilde{F}_i{}^{11} + \tilde{F}_i{}^{21} & (T^{12})^t \tilde{F}_i{}^{11}(T^{12}) + \tilde{F}_i{}^{21}(-T^{12}) + (-T^{12})^t \tilde{F}_i{}^{12} + \tilde{F}_i{}^{22} \end{bmatrix}
\end{aligned}$$

Fourth Step: Compute the remaining part of $\left[\tilde{F}_i\right]$'s, that is, $\tilde{F}_i{}^{22}$.

From the last step, F_i^{11}, F_i^{12} and F_i^{21} are obtained. Thus we can compute

$$\tilde{F}_i{}^{22} = (T^{12})^t F_i^{11} T^{12} + F_i^{21} T^{12} + (T^{12})^t F_i^{12}.$$

Final Step: Compute the remaining part of public key P_i^{22} by

$$P_i^{22} = \tilde{F}_i{}^{22} + \varepsilon_i^{22}.$$

Reduced size of the public key. The reduced size of the public key of NOVA using alignment is

$$\text{Size}_{\text{rpk}} = m \cdot m^2 \cdot l^2$$

field elements of $\mathbb{F}_q$.

5 Security Analysis

In this section, we first introduce several currently known attacks against UOV scheme and then discuss their corresponding complexity analysis and consider the situation of these attacks against our NOVA scheme. Notice that since NOVA is a signature scheme over the matrix ring $\mathcal{R}$ with entries in $\mathbb{F}_q$ and it can be regarded as a UOV over $\mathbb{F}_q$. We will analyze the complexity from two different aspects, i.e., over the ring $\mathcal{R}$ and over the field $\mathbb{F}_q$.

5.1 Complexity and NIST Security Level

Given a homogeneous multivariate quadratic map $P : \mathbb{F}_q^N \to \mathbb{F}_q^M$, we use $MQ(N, M, q)$ to denote the complexity of finding a non-trivial solution u such that $P(u) = 0$ if that such a solution exists. There are several algorithms to solve a quadratic system of M equations in N variables over finite fields such as F_4 [16], F_5 [17] and XL variants [10, 42].

In this paper, our complexity estimation follows from [3, 7]. The complexity of solving M homogeneous quadratic equations in N variables can be estimated by

$$3 \cdot \binom{N - 1 + d_{reg}}{d_{reg}}^2 \cdot \binom{N+1}{2}$$

field multiplications where d_{reg} is the degree of regularity of a semi-regular polynomial system and it is equal to the degree of the first non-positive term in the series generated by

$$\frac{(1-t^2)^M}{(1-t)^N}.$$

The hybrid approach [2], which randomly guesses a small amount of variables, say k variables, before solving the system with the Gröbner basis techniques. The complexity of using this approach can be estimated by $q^k \cdot MQ(N-k, M, q)$ field multiplications for the classical case and $q^{k/2} \cdot MQ(N-k, M, q)$ field multiplications when applying Grover's algorithm [20] for the quantum case.

Methods solving underdetermined MQ. Recently, Thomae and Wolf [39], Furue, Nakamura and Takagi [18], Hashimoto [21] provide several methods to solve an underdetermined multivariate quadratic system P of M equations in N variables over a finite field, that is, N is larger than M. The main idea of these methods is to find a particular invertible linear map S converting the first α_k equations into a special form where k is the number of guessing in the hybrid approach. We can then remove $(N-M)+\alpha_k$ variables and α_k equations from system P. Therefore, an underdetermined $MQ(N,\ M,\ q)$ problem is reduced to an $MQ(M-k-\alpha_k,\ M-\alpha_k,\ q)$ problem and hence can by solved using the hybrid approach [2]. Note that different methods obtain different optimal values α_k due to how they convert P into different forms. Therefore, the formulas for estimation of complexity of [39, 18, 21] are the same but with different optimal values α_k. We denote the optimal values α_k of [39, 18] by α_{TW}, α_{F}, respectively and α_{HMa}, α_{HMb} corresponding to two algorithms in [21] respectively. Therefore, the main term of complexity of NOVA under this technique is given by, take the classical case for example,

$$\min_k\ q^k \cdot MQ(M-k-\alpha_k,\ M-\alpha_k,\ q)$$

field multiplications with different optimal values α_k corresponding to different methods. They are given by $\alpha_{\mathrm{TW}} = \lfloor \frac{N}{M} \rfloor - 1$, $\alpha_{\mathrm{F}} = \lfloor \frac{N-k}{M-k} \rfloor - 1$, $\alpha_{\mathrm{HMa}} = \lfloor \frac{N}{M-k} \rfloor - 1$ and α_{HMb} is the optimal value such that $N \geq M - (\alpha_k + k - M)\alpha_k$ holds. So far, the attack in [21] would be the sharpest among [39, 18, 21].

Algorithms for super-underdetermined MQ. There are also several algorithms indicating that if the number of variables N is sufficiently larger than the number of equations M in a MQ problem then it can be solved in polynomial time. Please refer to [24, 9, 27, 8] for more information. Note that these four algorithms are not applicable to the parameter settings of NOVA.

Generally speaking, a scheme can be attacked in several ways. The different attacks will construct different MQ systems and then solve them. Therefore, each attack will have a corresponding complexity which is the difficulty of executing the attack. To enable the system satisfies the required level of security means that to choose parameter settings so that the lowest complexity among all known attacks is beyond the security requirement. There are five security levels in the NIST PQC project [28].

NIST security level. Herein, We focus on level I, III, and V. Security levels I, III and V aim that a classical attacker needs 2^{143}, 2^{207} and 2^{272} classical gates to break the scheme, and 2^{74}, 2^{137} and 2^{202} quantum gates for a quantum attacker, respectively.

Note that the formulas in this section give complexity estimations of attacks in terms of field multiplications. And the number of gates required for an attack against digital signature scheme can be computed by

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

with the assumption that one field multiplication in the field $\mathbb{F}_q$ needs about $(\log_2 q)^2$ bit multiplications and same for bit additions. On the other hand, for each field multiplication in the process of the attack, it also needs an addition of field elements, each takes $\log_2 q$ bit additions.

5.2 Direct Attack

Given a quadratic multivariate polynomial system P consisting of m equations in n variables over $\mathbb{F}_q$ and $y \in \mathbb{F}_q^m$. The direct attack here is the straightforward method to attack a scheme that trying to solve the solution u of the system $P(u) = y$ algebraically as explained below. In the case of UOV, the system is underdetermined, that is, the number of variables n is larger than the number of equations m. Therefore we can assign the values to $n - m$ variables in the system $P(u) = y$ randomly and then the resulting system consisting of m equations of m variables can be solved in high probability.

Note that the public key of UOV is considered to be a semi-regular system [1]. Therefore, the complexity of direct attack can estimated by

$$\text{Comp}_{\text{Direct; Classical}}\text{UOV} = \min_k \; q^k \cdot MQ(m - k + 1,\; m,\; q)$$

field multiplications and the complexity of the quantum direct attack is given by

$$\text{Comp}_{\text{Direct; Quantum}}\text{UOV} = \min_k \; q^{k/2} \cdot MQ(m - k + 1,\; m,\; q)$$

field multiplications when applying Grover's algorithm [20].

In the case of NOVA, if the attacker wants to solve a quadratic system over the ring $\mathcal{R}$ directly then he will face a fundamental problem, that is, there is no efficient algorithm like F_4, F_5 and XL to compute the solution u of the system $P(u) = y$ over the noncommutative ring $\mathcal{R}$.

However, the main idea of the direct attack still works and it can be done by solving the system over a finite field $\mathbb{F}_q$ instead of over the ring $\mathcal{R}$. For the sake of brevity, as mentioned before, we set $\mathcal{R}$ to be the ring of $l \times l$ matrix over $\mathbb{F}_q$, thus each equation over $\mathcal{R}$ gives us l^2 equations over $\mathbb{F}_q$ corresponding to the l^2 components of ring variables. Therefore, the resulting system can be viewed as a quadratic system of l^2m equations in l^2m field variables. Our experiment shows that, see table below, in the case of small size parameter sets such a quadratic system constructed from NOVA that consisting of $l^2 \cdot m$ equations induced by l^2 components of m equations in m variables over $\mathcal{R}$ behaves like a random systems of $l^2 \cdot m$ equations in $l^2 \cdot m$ variables over a $\mathbb{F}_q$ but with the reduction of degree of regularity at most one with high probability.

For security purposes, we will use $d_{\text{NOVA}} = d_{reg} - 1$ in our complexity estimations of NOVA and the corresponding complexity is denoted by $MQ_{\text{NOVA}}(N, M, q)$ when solving the multivariate quadratic system of M equations in N variables constructed by public polynomials of NOVA. Note that we can see this downward trend disappears as the parameters get larger enough.

Hence we can estimate the complexity of the direct attack against NOVA from the discussion above. The complexity of classical direct attack is then given by

$$\text{Comp}_{\text{Direct; classical}}\text{NOVA} = \min_k \; q^k \cdot MQ_{\text{NOVA}}(l^2m - k + 1, \; l^2m, \; q)$$

field multiplications, and the complexity of the quantum direct attack is given by

$$\text{Comp}_{\text{Direct; quantum}}\text{NOVA} = \min_k \; q^{k/2} \cdot MQ_{\text{NOVA}}(l^2m - k + 1, \; l^2m, \; q)$$

field multiplications.

The complexity of classical direct attack using technique in [39, 18, 21] is

$$\text{Comp}_{\text{TWFH; classical}}\text{NOVA} = \min_k \; q^k \cdot MQ_{\text{NOVA}}(l^2m - k - \alpha_k + 1, \; l^2m - \alpha_k, \; q)$$

field multiplications, and the complexity of the quantum direct attack is given by

$$\text{Comp}_{\text{TWFH; quantum}}\text{NOVA} = \min_k \; q^{k/2} \cdot MQ_{\text{NOVA}}(l^2m - k - \alpha_k + 1, \; l^2m - \alpha_k, \; q)$$

field multiplications.

The following table gives comparison of the degree at the first step degree falls or goes flat using F_4 algorithm [16], which is strongly connected to the degree of regularity [13], in Magma algebra system [6] that starts to go either down or flat among all step

degrees of the quadratic system obtained by NOVA and a random quadratic system respectively. The experimental results on NOVA sometimes gives two numbers. We show the less frequent one in parenthesis.

Table 1: Table of comparison of the degree at the first step degree falls or goes flat between NOVA and random systems.

(v, o, q, l, k)	NOVA system	random system
$(6, 1, 16, 2, 1)$	3 (2)	3
$(6, 2, 16, 2, 1)$	4	5
$(6, 2, 16, 2, 2)$	4	4
$(6, 2, 16, 2, 3)$	3	3
$(6, 3, 16, 2, 1)$	6 (5)	7
$(6, 3, 16, 2, 2)$	5	6
$(6, 3, 16, 2, 3)$	4	5
$(6, 4, 16, 2, 2)$	7	7
$(6, 4, 16, 2, 3)$	5	6

5.3 MinRank Alike Attacks

Reconciliation Attack. The reconciliation attack proposed by [14] against UOV tries to solve the system $P(\tilde{o}) = 0$ by finding a vector $\tilde{o} \in T^{-1}(\mathcal{O})$ and hence the basis of $T^{-1}(\mathcal{O})$ where $\mathcal{O} = \{(x_1, \cdots, x_n) : x_1 = \cdots = x_v = 0\}$. This implies that $P(\tilde{o}) = 0$ is a quadratic system that having a solution space of dimension m. To expect a unique solution, we can impose m linear constraints with respect to the components of $\tilde{o}$. Hence the complexity of this attack is mainly given by that of solving the quadratic system of m equations in v variables.

However, as an attack on UOV, where $v > o = m$, the complexity of reconciliation attack usually will be greater than the complexity of direct attack which tries to solve m quadratic equations in m variables. In other words, the performance of reconciliation attack usually is not better than that of direct attack. In the case of NOVA, the execution of Reconciliation Attack against NOVA as over ring even suffers from the fact that there is no efficient algorithm to complete the attack over $\mathcal{R}$.

Note that using the MinRank alike attacks for UOV systems to attack NOVA will also suffer very high computing complexity by the same reasoning.

New MinRank attacks. In [3, 4], Beullens proposed Rectangular MinRank attack, Simple attack and Combine attack that are new attacks against Rainbow signature scheme. These attacks are based on the multi-layer structure of Rainbow. Therefore, these attacks have no security implications on our scheme since NOVA has no multi-layer structure.

MinRank attack against NC-Rainbow. In 2012, [45] proposed a variant of Rainbow based on Quaternion ring over a finite field $\mathbb{F}_q$ of characteristic 2. However, [38] shows that if an attacker regards an NC-Rainbow scheme as a Rainbow scheme over $\mathbb{F}_q$, then the rank of the corresponding matrix to the central map of NC-Rainbow will be lower than original Rainbow. The key point is, by doing so, the corresponding matrices will be of a particular form and such a form is sparse. The MinRank attack of [38] is based on the multi-layer structure of NC-Rainbow and the particular structure of multiplication of Quaternion ring together with the sparsity mentioned above. Note that NOVA has neither that sparsity nor a special form in its matrix representation. On the other hand, NOVA has no multi-layer structure in the central map F. As a result, the MinRank in [38] is not applicable to NOVA.

5.4 K-S Attack (UOV Attack)

The goal of the K-S attack [24] is to find an equivalent private key by finding an equivalent invertible linear map T and hence the corresponding matrix $[T]$. Once we have an equivalent $[T]$, we can recover $[F_i]$ by the relation $[F_i] = [T^{-1}]^t [P_i] [T^{-1}]$. To do this, [24] shows that $T^{-1}(\mathcal{O})$, the oil subspace of the public key P of UOV, induces an equivalent key.

Note that $T^{-1}(\mathcal{O})$ is an invariant subspace of $[P_i]^{-1} [P_j]$, where $[P_i]$ and $[P_j]$ are any two public key matrices. The K-S attack tries to find a vector in $T^{-1}(\mathcal{O})$. Once one such vector is found, then we expect that the space $T^{-1}(\mathcal{O})$ can be recovered with q^{n-2m} attempts. Note that if there are $[P_i]$'s not invertible, then we can replace $[P_i]$ with invertible linear combinations of $[P_i]$'s randomly chosen and the cryptanalysis of K-S attack remains the same. Therefore the complexities of K-S attack and quantum K-S attack are estimated by

$$\mathrm{Comp}_{\text{K-S; classical}}\mathrm{UOV} = q^{n-2m-1} \cdot m^4$$

field multiplications and

$$\mathrm{Comp}_{\text{K-S; quantum}}\mathrm{UOV} = q^{(n-2m-1)/2} \cdot m^4$$

field multiplications, respectively.

From the design of central map F of NOVA and the noncommutativity of $\mathcal{R}$, there does not exist the notion of oil space of F over $\mathcal{R}$ analogous to the space $\mathcal{O}$ of UOV and hence the notion of $T^{-1}(\mathcal{O})$ in the sense that regarding $T^{-1}(\mathcal{O})$ as a left-module or a right-module over $\mathcal{R}$. Such a requirement is necessary for K-S attack, since to execute K-S attack over $\mathcal{R}$, the consistency of multiplication over $\mathcal{R}$ given by a left-module or a right-module over $\mathcal{R}$ is needed. Therefore, K-S attack is not applicable to NOVA over $\mathcal{R}$. [30] also proposes two methods to find an invariant subspace: the Linearization method and the Characteristic Polynomial method. These two methods become invalid over $\mathcal{R}$ since they still suffer from the noncommutativity of $\mathcal{R}$.

However, based on the same reason we mentioned before, an attacker may treat a (v, o, q, l) NOVA scheme over $\mathcal{R}$ as an (l^2v, l^2o, q) UOV system over $\mathbb{F}_q$ and follows the cryptanalysis of Direct attack to carry out K-S attack against NOVA over $\mathbb{F}_q$.

In such a case, we have

$$\text{Comp}_{\text{K-S; classical}}\text{NOVA} = q^{l^2n-2l^2m-1} \cdot (l^2m)^4$$

field multiplications for classical attack and

$$\text{Comp}_{\text{K-S; quantum}}\text{NOVA} = q^{(l^2n-2l^2m-1)/2} \cdot (l^2m)^4$$

field multiplications for quantum attack.

5.5 Intersection Attack

In [4], Beullens proposed a new attack against UOV scheme called the intersection attack. The main idea of the intersection attack is to use the polar form of the public key P, that is, $P' = [P'_1, \cdots, P'_m]$ with $P'_i(u_1, u_2) = (u_1)^t \hat{M}_i u_2$ where $\hat{M}_i = [P_i] + [P_i]^t$.

The goal of the intersection attack is to seek a vector y in the intersection $\hat{M}_i(T^{-1}(\mathcal{O})) \cap \hat{M}_j(T^{-1}(\mathcal{O}))$ where $\hat{M}_i, \hat{M}_j$ are invertible, and then to obtain an equivalent key by recovering the subspace $T^{-1}(\mathcal{O})$ as in K-S attack. Because $\hat{M}_i^{-1}y, \hat{M}_j^{-1}y \in T^{-1}(\mathcal{O})$, we obtain the following system.

$$\begin{cases} P(\hat{M}_i^{-1}y) = 0 \\ P(\hat{M}_j^{-1}y) = 0 \\ P'(\hat{M}_i^{-1}y, \hat{M}_j^{-1}y) = 0 \end{cases}$$

If $2.5m < n < 3m$, the dimension of the solution space corresponding to the system is $3m - n$. To obtain a unique solution with high probability, we can add $3m - n$ linear random equations. Hence the complexity of solving the system is equivalent to that of solving quadratic system with $M = 3m$ equations and $N = n - (3m - n) = 2n - 3m$ variables.

If $n < 2.5m$, the attack can become more powerful by seeking a vector y in the intersection of k subspaces $\hat{M}_i(T^{-1}(\mathcal{O}))$ with $k \geq 2$. The complexity of this case is equal to the complexity of that solving the quadratic system with $M = \binom{k+1}{2}m - 2\binom{k}{2}$ equations and $N = nk - (2k-1)m$ variables.

Therefore, when $n < 2.5m$, we have $N = nk - (2k-1)m,\ M = \binom{k+1}{2}m - 2\binom{k}{2}$, and

$$\text{Comp}_{\text{Intersection}}\text{UOV} = MQ(N+1,\ M,\ q)$$

field multiplications, and in the case $2.5m < n < 3m$, $N = 2n - 3m,\ M = 3m$, and

$$\text{Comp}_{\text{Intersection}}\text{UOV} = MQ(N+1,\ M,\ q)$$

field multiplications.

In case of intersection attack against NOVA, due to our construction, we can not write the public polynomial P_i of NOVA in quadratic form, namely $(u_1)^t\,[P_i]\,u_2$, when considered as over $\mathcal{R}$. Thus, the implementation of intersection attack still face the same problem as in direct attack, that is, there is no efficient algorithm like F_4, F_5 and XL to compute. Hence to implement intersection attack against NOVA, we need to regard NOVA as a UOV system over $\mathbb{F}_q$ and then solve a system over $\mathbb{F}_q$. Therefore, the complexity is estimated by the following.

If $n < 2.5m$, we have $N = (l^2n)k - (2k-1)(l^2m),\ M = \binom{k+1}{2}(l^2m) - 2\binom{k}{2}$, and

$$\mathrm{Comp}_{\mathrm{Intersection}}\mathrm{NOVA} = MQ(N+1,\ M,\ q)$$

field multiplications, and in the case $2.5m < n < 3m$, $N = 2(l^2n) - 3(l^2m),\ M = 3(l^2m)$, and

$$\mathrm{Comp}_{\mathrm{Intersection}}\mathrm{NOVA} = MQ(N+1,\ M,\ q)$$

field multiplications.

If $n \geq 3m$, then there is no guarantee that the space $\hat{M}_i(T^{-1}(\mathcal{O})) \cap \hat{M}_j(T^{-1}(\mathcal{O}))$ will exist. Therefore, the intersection attack becomes a probabilistic attack against NOVA. In this case, we estimate the complexity by obtain a lower bound of it as shown in the table of complexity.

5.6 Equivalent Key Attack

According to the core idea of our design, an attacker may try to find the submatrix $(T^{-1})^{12}$ of matrix $[T^{-1}]$ in the top right corner by algebraic attacks. Once the matrix $[T^{-1}]$ is found, the central map F can be recovered. This can be done by considering the system $P(T^{-1}(x)) = F(x)$ and solve for $[T^{-1}]$ by comparing both sides of equation at ring level. Therefore, this induces $m \cdot m^2 \cdot l^2$ quadratic equations in lvo variables and then can be solved by F_4, F_5 and XL. Therefore, the complexity is

$$\mathrm{Comp}_{[T^{-1}]\text{ attack; Classical}}\mathrm{NOVA} = \min_k q^k \cdot MQ(lvo + 1 - k,\ m^3l^2,\ q)$$

field multiplications and the complexity of the quantum direct attack is given by

$$\mathrm{Comp}_{[T^{-1}]\text{ attack; Quantum}}\mathrm{NOVA} = \min_k q^{k/2} \cdot MQ(lvo + 1 - k,\ m^3l^2,\ q)$$

field multiplications with applying Grover's algorithm.

Based on the above reason, we take this attack into account in our proposed parameter settings. We would like to mention that the multivariate quadratic system constructed by $[T^{-1}]$ attack is overdetermined hence [23, 9, 27, 8, 39, 18, 21] are not applicable.

On the other hand, one may consider that executes $[T^{-1}]$ attack that regards a (v, o, q, l) NOVA as an (l^2v, l^2o, q) UOV then induces a quadratic system of $M = (l^2m) \cdot (l^2m) \cdot$

$\frac{(l^2m+1)}{2}$ equations in $l \cdot vo$ variables over $\mathbb{F}_q$. However, this does not increase the number of independent equations compared to the above formulations.

6 Implementation and Parameter Settings

In this section, to begin with, we propose our parameter settings for three security levels in the NIST PQC project levels I, III and V, respectively. Secondly, we estimate the complexity of attacks against NOVA with parameter settings we proposed.

6.1 To attain EUF-CMA Security

For practical considerations, we use a random binary vector, called salt, in NOVA scheme in order to achieve Existential Unforgeability under Chosen Message Attack (EUF-CMA) Security [29]. The modifications are listed in the following.

Signature. To sign a signature for the document D, we randomly choose **salt** and then generate a signature for the hash value $y = Hash(Hash(D)||\textbf{salt})$. Therefore, the corresponding signature is of the form $\sigma = (u||\textbf{salt})$ where u is the signature of y generated by the NOVA signer. The length of **salt** is chosen to be 16 Bytes under the assumption of up to 2^{64} signatures being generated with the system and hence the consideration that we want almost no **salt** is used for more than one signature.

Verification. If $P(u) = Hash(Hash(D)||\textbf{salt})$, the signature is accepted, otherwise rejected.

6.2 Proposed Parameter Settings

In this section, we give our proposed parameter settings and therefore their size of public key and signature respectively. Finally, the comparison table of NOVA with NIST finalists [12, 34, 25] and MAYO [5] is given.

The following table shows that the complexity of attacks against our parameter settings. Here, "Dir.", "TWFH.", "K-S.", "Int." and "$[T^{-1}]$." denote the direct attack, direct attack using technique in [39, 18, 21], K-S attack [24], intersection attack [4] and $[T^{-1}]$ attack mentioned in Sec. 5, respectively. In any pair of complexity the left one denotes the complexity in classical gates and the right one denotes in quantum gates, respectively. The lowest complexity is marked in bold fonts.

Table 2: Table of complexity in $\log_2(\sharp\text{gates})$.

SL	(v, o, q, l)	Dir.	TWFH.	K-S.	Int.	$[T^{-1}]$.
I	$(23, 15, 16, 2)$	154/113	**150**/106	153/91	207	158/158
	$(17, 7, 16, 3)$	161/118	154/108	385/207	$\geq$378	**149**/149
	$(14, 4, 16, 4)$	163/119	154/102	665/347	$\geq$315	**152**/152
III	$(38, 23, 16, 2)$	223/163	**219**/157	267/149	362	242/242
	$(26, 10, 16, 3)$	219/160	**213**/151	603/317	$\geq$570	222/222
	$(21, 6, 16, 4)$	232/169	223/156	988/510	$\geq$524	**213**/213
V	$(54, 32, 16, 2)$	299/218	**295**/212	381/207	519	332/332
	$(35, 14, 16, 3)$	295/215	289/207	785/409	$\geq$831	**288**/288
	$(28, 8, 16, 4)$	299/218	291/208	1309/671	$\geq$745	**285**/285

The next table shows the key-sizes and lengths of the signature of NOVA, respectively. Here the notation Size_{rpk} denotes the reduced public key size and Size_{sig} is for the signature size.

Table 3: Table of key-sizes and lengths of the signature of NOVA parameter settings.

Security Level	(v, o, q, l)	Size_{rpk} (KBytes)	Size_{sig} (Bytes)
I	$(23, 15, 16, 2)$	6.6	76(+16)
	$(17, 7, 16, 3)$	1.5	108(+16)
	$(14, 4, 16, 4)$	0.5	144(+16)
III	$(38, 23, 16, 2)$	23.8	122(+16)
	$(26, 10, 16, 3)$	4.4	162(+16)
	$(21, 6, 16, 4)$	1.7	216(+16)
V	$(54, 32, 16, 2)$	64	172(+16)
	$(35, 14, 16, 3)$	12.1	220.5(+16)
	$(28, 8, 16, 4)$	4	288(+16)

The last table gives the comparison of NOVA with the parameter settings that aim at the security level I of the NISTPQC signature finalists and MAYO. Based on the public key sizes and signature sizes of NOVA, we consider NOVA to be a competitive signature system. Note that the 16 Bytes **salt** is included in the size of NOVA signature.

Table 4: A comparison table of NOVA with the NISTPQC signature finalists and MAYO aims at NIST security level I.

Signature Scheme	Size of public key (KBytes)	Size of signature (Bytes)
Dilithium-2	1.312	2420
Falcon-512	0.897	666
MAYO-I, leaky	0.614	392
MAYO-I, tight	0.835	459
NOVA$(14, 4, 16, 4)$	0.5	160
NOVA$(17, 7, 16, 3)$	1.5	124
NOVA$(23, 15, 16, 2)$	6.6	92
Rainbow-Ia	58.8	66

In [43, 44], they both pointed out that TLS, which we used to protect our web browsing, is no longer secure due to the impact of the quantum computer. Making TLS post-quantum is an important task, but such a fundamental change could take years and be quite costly if we do not have a quantum-resistant signature that is relatively compatible well with the existing framework. Note that [44] gives the corresponding condition: six times signature size and two times of public key size fit in 9KB. According to the specification of NOVA, NOVA could be a more practical general-purpose signature scheme.

7 Conclusion

The NOVA scheme was cooked up to the best of our knowledge. It assures that secure multivariate signature schemes over noncommutative rings are possible. And such technique could be beneficial to security and key size reduction. According to the result of our security analysis, the NOVA scheme is capable of resisting all known attacks for multivariate cryptosystems. By comparison with other post-quantum signature schemes, it seems that we have found a practical secure signature scheme which is relatively efficient in public key size and signature size both.

Acknowledgement

The first author would like to express thanks to Prof. Jintai Ding for discussions on security analysis of multivariate cryptosystems. We also would like to express thanks to Dongyu Wu who suggests that we should choose the symmetric matrix s with irreducible characteristic polynomial over $\mathbb{F}_q$. The first author and the second author are partially supported by MOST110-2122-M-259-001. The third author is partially supported by MOST109-2115-M-259-005-MY2.

References

[1] 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 Interna- tional Symposium on Effective Methods in Algebraic Geometry (MEGA), pp. 1–14 (2005).

[2] 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).

[3] Beullens, W.: **Breaking Rainbow Takes a Weekend on a Laptop.** Cryptology ePrint Archive, Report 2022/214, 2022. `https://eprint.iacr.org/2022/214.pdf`.

[4] Beullens, W.: **Improved cryptanalysis of UOV and Rainbow.** Cryptology ePrint Archive, Report 2020/1343, 2020. `https://eprint.iacr.org/2020/1343.pdf`.

[5] Beullens, W.: **MAYO: Practical Post-Quantum Signatures from Oil-and-Vinegar Maps.** Cryptology ePrint Archive, Report 2021/1144, 2021. `https://eprint.iacr.org/2021/1144.pdf`.

[6] Bosma, W., Cannon, J., Playoust, C.: **The Magma algebra system. I. The user language.** Journal of Symbolic Computation 24(3-4), pp. 235–265 (1997)

[7] Cheng, C.M., Chou, T., Niederhagen, R., Yang, B.Y.: **Solving quadratic equations with XL on parallel architectures.** In Emmanuel Prouff and Patrick Schaumont, editors, CHES 2012, volume 7428 of LNCS, pages 356–373. Springer, Heidelberg, September 2012.

[8] Cheng, C.M., Hashimoto, Y., Miura, H., Takagi, T.: **A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics**. In PQCrypto'14, LNCS 8772 (2014), pp.40–58.

[9] Courtois, N., Goubin, L., Meier, W., Tacier, J.-D.: **Solving underdefined systems of multivariate quadratic equations**. In PKC'02, LNCS 2274 (2002), pp.211–227.

[10] Courtois, N., Klimov, A., Patarin, J., Shamir, A.: **Efficient algorithms for solving overdefined systems of multivariate polynomial equations.** In Bart Preneel, editor, EUROCRYPT 2000, volume 1807 of LNCS, pages 392–407, Bruges, Belgium, May 14–18, 2000. Springer, Heidelberg, Germany.

[11] Ding, J., Chen, M.S., Kannwischer, M., Patarin, J., Petzoldt, A., Schmidt, D., Yang, B.Y.: **Rainbow. NIST Post-Quantum Cryptography Standardization Round 3 Submissions**, available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions`

[12] Ding, J., Schmidt, D.: **Rainbow, a new multivariable polynomial signature scheme.** In International Conference on Applied Cryptography and Network Security, pages 164–175. Springer, 2005.

[13] Ding, J., Schmidt, D.: **Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields.** In: Fischlin, M., Katzenbeisser, S. (eds) Number Theory and Cryptography. Lecture Notes in Computer Science, vol 8260. Springer, Berlin, Heidelberg, 2013. https://doi.org/10.1007/978-3-642-42001-6_4.

[14] Ding, J., Yang, B.Y., 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).

[15] Ding, J., Yang, B.Y.: **Multivariates Polynomials for Hashing.** In Pei, D., Yung, M., Lin, D., Wu, C. (eds) Information Security and Cryptology. Inscrypt 2007. Lecture Notes in Computer Science, vol 4990. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-79499-8_28

[16] Faugère, J.C.: **A new efficient algorithm for computing Gröbner bases (F4).** Journal of Pure and Applied Algebra, 139:61–88 (1999).

[17] Faugère, J.C.: **A new efficient algorithm for computing Gröbner bases without reduction to zero (F5).** In Proceedings of the 2002 international symposium on Symbolic and algebraic computation, pages 75–83, 2002.

[18] Furue, H., Nakamura, S., Takagi, T.: **Improving Thomae-Wolf algorithm for solving underdetermined multivariate quadratic polynomial problem**. In PQC'21, LNCS 12841 (2021), pp.65–78.

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

[20] Grover, L.-K.: **A fast quantum mechanical algorithm for database search.** In STOC 1996, pp. 212–219. ACM (1996).

[21] Hashimoto, Y.: **Minor improvements of algorithm to solve under-defined systems of multivariate quadratic equations.** Available at https://eprint.iacr.org/2021/1045.pdf.

[22] Hu, Y.H., Wang, L.C., Yang, B.Y.: **"A "Medium-Field" Multivariate Public-Key Encryption Scheme."** Proc. 7th Cryptographer's Track RSA Conference, volume 3860, Lecture Notes in Computer Science, pages 132-149, 2006.

[23] Kipnis, A., Patarin, J., Goubin, L.: **Unbalanced oil and vinegar signature schemes.** In Jacques Stern, editor, EUROCRYPT'99, volume 1592 of LNCS, pages 206–222. Springer, Heidelberg, May 1999.

[24] Kipnis, A., Shamir, A.: **Cryptanalysis of the oil and vinegar signature scheme.** In Hugo Krawczyk, editor, CRYPTO'98, volume 1462 of LNCS, pages 257–266. Springer, Heidelberg, August 1998.

[25] Lyubashevsky, V., Ducas, L., Kiltz, E., Lepoint, T., Schwabe, P., Seiler, G., Stehlè, D., Bai, S.: **CRYSTALS-DILITHIUM.** Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

[26] Matsumoto, T., Imai, H.: **Public quadratic polynomial-tuples for efficient signature verification and message-encryption.** In Advances in Cryptology — EUROCRYPT 1988, volume 330 of Lecture Notes in Computer Science, pages 419–545. Christoph G. Günther, ed., Springer, 1988.

[27] Miura, H., Hashimoto, Y., Takagi, T.: **Extended algorithm for solving underdefined multivariate quadratic equations.** In PQCryoto'13, LNCS 7932 (2013), pp.118–135.

[28] NIST: **Post-quantum cryptography CSRC.** Available at `https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization`

[29] NIST: **Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process.** Available at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf`

[30] Patarin, J.: **The oil and vinegar signature scheme.** In Dagstuhl Workshop on Cryptography September, 1997.

[31] Patarin, J.: **Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) Two New Families of Asymmetric Algorithms.** In EUROCRYPT'96, LNCS v. 1070, pp. 33-48.

[32] Petzoldt, A.: **Selecting and reducing key sizes for multivariate cryptography.**

[33] Petzoldt, A., Thomae, E., Bulygin, S., Wolf, C.: **Small public keys and fast verification for Multivariate Quadratic public key systems.** In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of LNCS, pages 475–490, Nara, Japan, September 28–October 1, 2011. Springer, Heidelberg, Germany.

[34] Prest, T., Fouque, P. A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: **FALCON.** Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

[35] Shor, P. W.: **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.** In SIAM Journal on Computing 26(5), pp. 1484-1509 (1997).

[36] Szepieniec, A., Ding, J., Preneel, B.: **Extension Field Cancellation: A New Central Trapdoor for Multivariate Quadratic Systems.** In: Takagi, T. (eds) Post-Quantum Cryptography. PQCrypto 2016. Lecture Notes in Computer Science(), vol 9606. Springer, Cham. https://doi.org/10.1007/978-3-319-29360-8_12

[37] Tao, C., Diene, A., Tang, S., Ding, J.: **Simple matrix scheme for encryption.** In Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp.231-242. Springer, Heidelberg (2013).

[38] Thomae, E.: **Quo Vadis Quaternion? Cryptanalysis of Rainbow over non-commutative rings.** In SCN'12, Lect. Notes Comput. Sci. 7485, pp.361–363, 2012.

[39] Thomae, E., Wolf, C.: **Solving underdetermined systems of multivariate quadratic equations**, revisited. In PKC'12, LNCS 7293 (2012), pp.156–171.

[40] Wang, L.C., Chang, F.H.: **Tractable Rational Map Cryptosystem** Available at http://eprint.iacr.org/2004/046.pdf.

[41] Wang, L.C., Hu, Y.H., Lai, F., Chou, C.Y., Yang, B.Y.: **Tractable rational map signature.** In PKC, Serge Vaudenay, ed., Public Key Cryptography — PKC 2005, (2005), pages 244–257. ISBN 3-540-24454-9.

[42] Wang, L.C., Wei, T.J., Shih, J.M., Hu, Y.H., Hsieh, C.C.:**An algorithm for solving over-determined multivariate quadratic systems over finite fields.** doi: 10.3934/amc.2022001

[43] Wiggers, T.: **Making protocols post-quantum.** In the Cloudflare blog. Available at https://blog.cloudflare.com/making-protocols-post-quantum/

[44] Westerbaan, B.: **Sizing Up Post-Quantum Signatures.** In the Cloudflare blog. Available at https://blog.cloudflare.com/sizing-up-post-quantum-signatures/

[45] Yasuda, T., Sakurai, K., Takagi, T.: **Reducing the Key Size of Rainbow Using Non-Commutative Rings.** In CT-RSA, volume 7178 of Lecture Notes in Computer Science, pages 68-83. Springer, 2012.

Appendix: A Variant of NOVA Scheme

Whipping NOVA: In [5], Beullens proposed a new technique called Whipping UOV map and used this technique to construct a new signature scheme, MAYO. A whipping

UOV map is a multivariate quadratic map $P^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ where $n = v + o$. To construct the map P^*, [5] uses a public key P constructed by a (v, o, q) UOV scheme but with $\dim(T^{-1}(\mathcal{O})) = o < m$ which is different from the usual UOV map ($m = o$). Namely, the whipping UOV map $P^* : \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ is constructed by

$$P^*(u_1, \cdots, u_k) = \sum_{1 \le i \le j \le k} E_{i,j}(P(u_i + u_j))$$

where $E_{i,j}$ are $m \times m$ invertible linear matrices over $\mathbb{F}_q$ and k is a positive integer such that $ko \ge m$.

Together with the technique in [11] and [32], a large part of public key can be pseudo-randomly generated. Therefore, the overall public key size can be reduced to $O(mo^2 \log q)$.

Note that a (v, o, q, l) NOVA scheme can be viewed as a $(l^2 v, l^2 o, q)$ UOV scheme. That is, in this sense, we see that whipping technique can be applied to NOVA. In conclusion, if the scheme with whipping technique is confirmed to be secure, then the public key size of NOVA can be further reduced.