A Simple Noncommutative UOV Scheme

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

Abstract

In this paper, we propose a simple noncommutative-ring based UOV signature scheme with key-randomness alignment: Simple NOVA, which can be viewed as a simplified version of NOVA[48]. We simplify the design of NOVA by skipping the perturbation trick used in NOVA, thus shortens the key generation process and accelerates the signing and verification. Together with a little modification accordingly, this alternative version of NOVA is also secure and may be more suitable for practical uses. We also use Magma to actually implement and give a detailed security analysis against known major attacks. [1]

1 Introduction

Before NOVA[48], 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 $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ 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 [22]. The

[*] Corresponding author: Lih-Chung Wang

[†] Lih-Chung Wang, Email: lcwang@gms.ndhu.edu.tw Address: Department of Applied Mathematics, National Dong Hwa 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 Dong Hwa 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 Dong Hwa 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 Dong Hwa 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

private key of a usual multivariate scheme consists of three maps: $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$, $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$, $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ 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, there are multivariate schemes presented such as C^* [29], HFE [36], MFE [25], UOV [26], Rainbow [16], TRMS [47], TRMC [46], ABC [41] . . . , etc.

Among the above multivariate schemes, by its simplicity, UOV is worth more explaining. The central map of UOV scheme $F : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is as below.

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

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 $x_j x_k$ terms. This kind of phenomenon is analogous to that oil and vinegar won't mix completely and this enables us to invert F easily.

The variables $x_1, \cdots, x_v$ are called the vinegar variables, and $x_{v+1}, \cdots, x_n$ oil variables. It is required that $v > o$ in order to resist the K-S attack[27] on the OV scheme[35]. This is the reason why the scheme is called Unbalanced Oil and Vinegar (UOV).

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.

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.

Although simple, UOV suffers extremely large public key sizes in order to be secure. Thus it is not practical if nothing new is done. It is quite a challenge to overcome it. NOVA takes on the challenge by choosing the coefficients of the polynomials used in the multivariate quadratic system of UOV in a noncommutative ring, and also employs the technique of key-randomness alignment[38] and some particular designs. One such particular design in NOVA is the use of "self-canceling" perturbation technique. As a result, NOVA successfully solves the problem of large public key size suffered by UOV.

Although the use of perturbation trick is creative in designing, the security analysis becomes more complicated, thus we try to find an alternative way to design NOVA by skipping the perturbation trick and cook up the Simple NOVA (may also be called SNOVA where S denotes "Simple"). By skipping the perturbation trick, not only the security analysis is now more clear, but also the key generation process is shortened and both the signing and verification are accelerated.

In Section 2, we first briefly introduce the notations and conventions used in this paper, some basic notions, and explain UOV in more details. We then give a clear review on NOVA in Section 3.

In Section 4, we give a full description of our Simple NOVA. A detailed security analysis of SNOVA is Section 5.

We use Magma to actually implement. Also a comparison table on public key size and signature size of NIST level 1 with the NISTPQC signature finalists and MAYO[8] is given in Section 6.

A conclusion is given in Section 7 followed by acknowledgement.

2 Preliminaries

2.1 Notations and Conventions

The following Tables 1, 2 are tables that list some symbols fixed with specific meaning and some conventions on notations, respectively.

Table 1: The table of notations used in this paper.

Symbol	**Description**
$\mathbb{F}_q$	finite field of order q
$\mathcal{R}$	$\text{Mat}_{l\times l}(\mathbb{F}_q)$, matrix ring consisting by $l \times l$ matrices over $\mathbb{F}_q$
v	number of vinegar variables
o	number of oil variables
S	symmetric matrix in $\mathcal{R}$ with irreducible characteristic polynomial
$n = v + o$	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
$[P_i]$	matrix corresponding to P_i in P
ε	perturbation in NOVA 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 a MQ system of M equations in N variables over $\mathbb{F}_q$

Table 2: The table of conventions in this paper.

Description	**The font denoted with**	**Example**
Integers	lower case letters	n, m and l
Elements in $\mathcal{R}$	upper case letters	A, S and Q
Variables over $\mathcal{R}$	upper case letters	$X_1, \cdots, X_n$
Elements in $\mathbb{F}_q$	lower case letters	$a_0, \cdots, a_{l-1}$
Variables over $\mathbb{F}_q$	lower case letters	$x_1, \cdots, x_n$
Vectors of any dimension	boldface letters with arrow on top	$\vec{\mathbf{X}}$ and $\vec{\mathbf{x}}$
Vector spaces and rings	calligraphic font	$\mathcal{O}$ and $\mathcal{R}$
The (j,k)-th entry of the matrix $[F_i]$, $[T]$ and $[P_i]$, respectively	subscript j, k	$F_{i,jk}$, T_{jk} and $P_{i,jk}$
Block form of matrices $[T]$	upper case letters	$[T] = \begin{bmatrix} T^{11} & T^{12} \\ T^{21} & T^{22} \end{bmatrix}$
Block form of matrices $[F_i]$	upper case letters	$[F_i] = \begin{bmatrix} F_i^{11} & F_i^{12} \\ F_i^{21} & 0 \end{bmatrix}$
Block form of matrices $[P_i]$	upper case letters	$[P_i] = \begin{bmatrix} P_i^{11} & P_i^{12} \\ P_i^{21} & P_i^{22} \end{bmatrix}$

2.2 Basic Notions

MQ problem. Let $\mathbb{F}_q$ be a finite field of order q. Given M quadratic polynomials $P(\vec{\mathbf{x}}) = [P_1(\vec{\mathbf{x}}), \cdots, P_M(\vec{\mathbf{x}})]$ in N variables $\vec{\mathbf{x}} = (x_1, \cdots, x_N)$ and a vector $\vec{\mathbf{y}} \in \mathbb{F}_q^M$, to find a vector $\vec{\mathbf{u}} \in \mathbb{F}_q^N$ such that $P(\vec{\mathbf{u}}) = [P_1(\vec{\mathbf{u}}), \cdots, P_M(\vec{\mathbf{u}})] = \vec{\mathbf{y}}$. This problem is known to be NP-hard [22]. Note that, it is generically expected to be exponentially hard in the case $N \sim M$ and it can be solved in polynomial time for $M \geq \frac{N(N+1)}{2}$ or $N \geq M(M+1)$ [7].

In this paper, we use $MQ(N, M, q)$ to denote the complexity of solving such an MQ problem. There are several algorithms to solve a multivariate quadratic system of M equations in N variables over finite fields such as F_4 [19], F_5 [20] and XL variants [14, 49].

Polar forms. The polar form of a homogeneous multivariate quadratic map $P(\vec{\mathbf{x}}) = [P_1(\vec{\mathbf{x}}), \cdots, P_M(\vec{\mathbf{x}})]$, consisting of M multivariate homogeneous quadratic polynomial in n variables, is defined to be the map

$$P'(\vec{\mathbf{x}}, \vec{\mathbf{y}}) = [P_1'(\vec{\mathbf{x}}, \vec{\mathbf{y}}), \cdots, P_M'(\vec{\mathbf{x}}, \vec{\mathbf{y}})]$$

where the polar form of $P_i(\vec{\mathbf{x}})$ is defined by

$$P_i'(\vec{\mathbf{x}}, \vec{\mathbf{y}}) = P_i(\vec{\mathbf{x}} + \vec{\mathbf{y}}) - P_i(\vec{\mathbf{x}}) - P_i(\vec{\mathbf{y}})$$

which is symmetric and bilinear. Note that if $[P_i]$ is the matrix related to P_i, i.e., $P_i(\vec{\mathbf{x}}) = \vec{\mathbf{x}}^t\,[P_i]\,\mathbf{x}$ then the matrix related to P_i' is $[P_i'] = [P_i] + [P_i]^t$

2.3 Unbalanced Oil and Vinegar Signature Scheme

The Unbalanced Oil and Vinegar (UOV) signature scheme [26] signature scheme is a slight modification of the Oil and Vinegar (OV) [35] signature scheme, proposed by Patarin in 1997. This scheme is based on a trapdoor map F which is easily inverted and it also can resist the K-S attack [27] on OV.

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

Central map. The central map of UOV scheme is $F = [F_1, \cdots, F_m] : \mathbb{F}_q^n \to \mathbb{F}_q^m$ where each F_i is of the form

$$F_i = \sum_{j=1}^{v} \sum_{k=j}^{n} f_{i,jk} x_j x_k.$$

The coefficients $f_{i,jk}$'s are chosen randomly from $\mathbb{F}_q$. Note that each F_i is a homogeneous quadratic polynomials in n variables which has no terms $x_j x_k$ for $j, k = v+1, \cdots, n$ over $\mathbb{F}_q$. The variables $x_1, \cdots, x_v$ are called the vinegar variables and $x_{v+1}, \cdots, x_n$ are called the oil variables.

Private key and Public key. The private key of UOV is the pair (F, T) where $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is an invertible linear map which is randomly chosen. The map $P = F \circ T :\ \mathbb{F}_q^n \to \mathbb{F}_q^m$ where $P_i = F_i \circ T$. The quadratic form of P_i is $P_i = \vec{\mathbf{u}}^t\,[P_i]\,\vec{\mathbf{u}}$ where $\vec{\mathbf{u}} = (u_1, \cdots, u_n)^t$ and $[P_i] = [T]^t\,[F_i]\,[T]$ where $[T]$ is the matrix related to T.

Oil space, $\mathcal{O}$. The special structure of F in UOV scheme indicates that F vanishes on the linear space $\mathcal{O} = \{\vec{\mathbf{x}} \in \mathbb{F}_q^n : x_1 = \cdots = x_v = 0\}$ called the oil space of central map F and hence the oil space of public key P will be the space $T^{-1}(\mathcal{O})$.

Public key generation and drawback. A. Petzoldt [37] and Rainbow [15] of the third-round of NIST proposal realized that the part of the randomness of the private key can be transferred to the public key and then a large part of public key can be generated by a PRNG. This reduces the public key size of UOV to the order $O(m^3 \cdot \log q)$. However, the size of the public key of UOV scheme is still too large to be a practical scheme, for example, to meet the security levels I, III, and V in the PQC project of NIST [31].

3 NOVA, a Noncommutative-ring Based Signature Scheme

In [48], we proposed NOVA, a noncommutative-ring based signature scheme, which is based on matrix ring $\mathcal{R} = \mathrm{Mat}_{l\times l}(\mathbb{F}_q)$. The central map of NOVA $F : \mathcal{R}^n \to \mathcal{R}^m$ is designed to be like a UOV map but over $\mathcal{R}$. However, a (v, o, q, l) NOVA scheme can also be regarded as a (l^2v, l^2o, q) UOV scheme when we regard F as a map over $\mathbb{F}_q$ with the explosion of numbers of variables and equations.

The subring $\mathbb{F}_\mathbf{q}[\mathbf{S}]$. Let S be a $l \times l$ symmetric matrix with irreducible characteristic polynomial. The subring $\mathbb{F}_q[S]$ of $\mathcal{R}$ is defined to be

$$\mathbb{F}_q[S] = \{a_0 + a_1S + \cdots + a_{l-1}S^{l-1} : a_0, a_1, \cdots, a_{l-1} \in \mathbb{F}_q\}$$

and note that the elements in $\mathbb{F}_q[S]$ are also symmetric and they all commutes.

Let v, o be positive integers with $v > o$, q be a power of a prime, $n = v + o$ and $m = o$. A (v, o, q, l) NOVA signature scheme is constructed as following.

Central map. Let the central map of NOVA scheme be $F = [F_1, \cdots, F_m] : \mathcal{R}^n \to \mathcal{R}^m$. Let $\Omega = \{(j, k) : 1 \le j, k \le n\} \setminus \{(j, k) : m+1 \le j, k \le n\}$. For $i = 1, \cdots, m$, we define

$$F_i = \sum_{\alpha=1}^{l^2} \sum_{(j,k)\in\Omega} A_{\alpha 1} \cdot X_j^t (Q_{\alpha 1} F_{i,jk} Q_{\alpha 1}^{-1} - Q_{\alpha 2} F_{i,jk} Q_{\alpha 2}^{-1}) X_k \cdot A_{\alpha 2}$$

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

In analogy to UOV, the first v ring variables $X_1, \cdots, X_v$ are called the vinegar variables, and the remaining $m = o$ variables $X_{v+1}, \cdots, X_n$ are called the oil variables. Since the index of inner summation is running over Ω, F_i is the map over $\mathcal{R}$ in the variables X_i's such that there are no terms which correspond to a product of any two oil variables. From this point of view, the central map of NOVA keeps the spirit of UOV at the ring level. Therefore, NOVA can be regard as a generalization of a UOV scheme over a noncommutative ring.

The matrix of F_i over $\mathcal{R}$ 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.

Invertible linear map. The invertible linear map in NOVA scheme is the map $T : \mathcal{R}^n \to \mathcal{R}^n$ 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 entries T_{ij} chosen randomly in $\mathbb{F}_q[S]$. Note that T_{ij} is symmetric and commutes with other elements in $\mathbb{F}_q[S]$. The matrices I^{11} and I^{22} are the diagonal matrices with all diagonal entries being the $l \times l$ identity matrix, i.e. the unity in $\mathcal{R}$. Therefore, $[T]$ is invertible and hence T.

The map $\tilde{F}$. Let $\tilde{F} = F \circ T$. For $i = 1, 2, \ldots, m$, each component map $\tilde{F}_i = F_i \circ T$. According to the relation $\overrightarrow{\mathbf{X}} = [T] \cdot \overrightarrow{\mathbf{U}}$ where $\overrightarrow{\mathbf{U}} = (U_1, \cdots, U_n) \in \mathcal{R}^n$, we get

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

where $\tilde{F}_{i,d_j d_k} = \sum_{\Omega} T_{j,d_j} \cdot F_{i,jk} \cdot T_{k,d_k}$ by the commutativity of $\mathbb{F}_q[S]$.

For $i = 1, 2, \ldots, m$, the matrix of $\tilde{F}_i$ is obtained by

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

"Self-canceling" perturbation on $\tilde{F}_i$. In [48], we introduce a technique called "self-canceling" perturbation and use it to disturb every entries of $[\tilde{F}_i]$, the matrix related to $\tilde{F}_i$. We randomly choose $\varepsilon_{i,d_j d_k} \in \mathbb{F}_q[S]$ and the matrix of perturbations $\varepsilon_{i,d_j d_k}$'s is denoted by $[\varepsilon_i]$. Let $P_{i,d_j d_k} = \tilde{F}_{i,d_j d_k} + \varepsilon_{i,d_j d_k}$ and then we have

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

The second equality shows that the perturbations $\varepsilon_{i,d_j d_k}$ will be "self-canceled". Thus, the verification of signature will not be affected by those perturbations.

For $i = 1, 2, \ldots, m$, the matrix of P_i is

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

where $[\tilde{F}_i]$ is the matrix of $\tilde{F}_i$ and $[\varepsilon_i] = \begin{bmatrix} \varepsilon_i^{11} & \varepsilon_i^{12} \\ \varepsilon_i^{21} & \varepsilon_i^{22} \end{bmatrix} \in \mathrm{Mat}_n(\mathbb{F}_q[S])$.

Private key and public key. The public key consists of 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 $\alpha = 1, 2, \ldots, l^2$ and $k = 1, 2$. The private key of NOVA is (F, T), i.e., the matrices $[T]$ and the matrices $[F_i]$ for $i = 1, 2, \ldots, m$.

Structure of NOVA. Note that an equation of n variables in $\mathcal{R}$ with coefficients over $\mathcal{R}$ gives l^2 equations of $l^2 n$ variables in $\mathbb{F}_q$ with coefficents over $\mathbb{F}_q$. Thus a NOVA scheme can be regarded as a UOV scheme in $\mathbb{F}_q$ variables over $\mathbb{F}_q$. Therefore, a (v, o, q, l) NOVA scheme over $\mathcal{R}$ can be regarded as an $(l^2 v, l^2 o, q)$ UOV scheme over $\mathbb{F}_q$. On the other hand, it is impossible to write the public key in quadratic form $P_i(\overrightarrow{\mathbf{U}}) = (\overrightarrow{\mathbf{U}})^t \, [P_i] \, \overrightarrow{\mathbf{U}}$ over $\mathcal{R}$, although it is possible to write the public key of NOVA in quadratic form when we regard it as a UOV scheme over $\mathbb{F}_q$.

4 Simple NOVA, a simplified variant of NOVA

In this section, we introduce SNOVA which is a simplified variant of NOVA signature scheme. Compare with NOVA, SNOVA does not use the "self-canceling" perturbation in the public key. This variant makes the structure of central map simpler and increases the usability and efficiency of the implementation. Moreover, from the perspective of degree of regularity, SNOVA behaves more like a semi-regular system, see Section 5.

4.1 Description

Let v, o be positive integers with $v > o$ and $\mathbb{F}_q$ be of characteristic 2. For example, we choose $\mathbb{F}_q = \mathrm{GF}(16)$ for our implementation. Let $n = v + o$ and $m = o$. Similar to NOVA, a (v, o, q, l) SNOVA signature scheme is defined as the following.

Subring $\mathbb{F}_q[S]$ and elements in $\mathbb{F}_q[S]$. Since S is a $l \times l$ symmetric matrix with irreducible characteristic polynomial. Then every element $Q \in \mathbb{F}_q[S]$ is also symmetric and commutes with each other.

Central map. The central map of SNOVA scheme is $F = [F_1, \cdots, F_m] : \mathcal{R}^n \to \mathcal{R}^m$ and for $i = 1, \cdots, m$, F_i is defined to be

$$F_i = \sum_{\alpha=1}^{l^2} A_\alpha \cdot \left(\sum_{(j,k)\in\Omega} X_j^t \left(Q_{\alpha 1} F_{i,jk} Q_{\alpha 2}\right) X_k \right) \cdot B_\alpha$$

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

Due to the noncommutativity of matrix ring $\mathcal{R}$, the matrix $[F_i]$ over $\mathcal{R}$ corresponding to F_i is of the form

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

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.

Structure of F. In [43], a MinRank attack against NC-Rainbow [52] is presented. Thomae indicates that the sparsity of the matrix of the central map can improve the MinRank attack when a ring-based scheme is considered to be a scheme over field. Moreover, Thomae shows that the rank of the matrix of the central map of NC-Rainbow is lower than the expected rank in [52]. In order to avoid such sparsity, l^2 copies with A_α and B_α are used in F_i of SNOVA.

Invertible linear map. The invertible linear map in SNOVA scheme is the map $T : \mathcal{R}^n \to \mathcal{R}^n$ related to the matrix

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

which is same as the one in NOVA scheme. Note that when $\mathbb{F}_q$ is of characteristic 2 then the matrix $[T^{-1}] = [T]$.

Private key. The private key of SNOVA is (F, T), i.e., the matrix $[T]$ and the matrices $[F_i]$ for $i = 1, 2, \ldots, m$.

Public key. Let $P = F \circ T$ be the public key of SNOVA scheme. For $i = 1, 2, \ldots, m$, $P_i = F_i \circ T$. The relation $\overrightarrow{\mathbf{X}} = [T] \cdot \overrightarrow{\mathbf{U}}$ where $\overrightarrow{\mathbf{U}} = (U_1, \cdots, U_n) \in \mathcal{R}^n$ implies that

$$P_i(\overrightarrow{\mathbf{U}}) = F_i(T(\overrightarrow{\mathbf{U}})) = \sum_{\alpha=1}^{l^2} \sum_{d_j=1}^{n} \sum_{d_k=1}^{n} A_\alpha \cdot U_{d_j}^t (Q_{\alpha 1} P_{i,d_j d_k} Q_{\alpha 2}) U_{d_k} \cdot B_\alpha$$

where $P_{i,d_j d_k} = \sum_{\Omega} T_{j,d_j} \cdot F_{i,jk} \cdot T_{k,d_k}$ by the commutativity of $\mathbb{F}_q[S]$. Therefore, the public key consists of the corresponding matrices

$$[P_i] = [T]^t \, [F_i] \, [T] \, , \; i = 1, \cdots, m$$

and the matrices $A_\alpha, \; B_\alpha$ and $Q_{\alpha k}$ for $\alpha = 1, 2, \ldots, l^2$ and $k = 1, 2$.

Signature. Let D be the document to be signed and $Hash(D) = \overrightarrow{\mathbf{Y}} = (Y_1, \cdots, Y_m) \in \mathcal{R}^m$ be its hash value. We compute the signature $\overrightarrow{\mathbf{U}}$ step by step. First, We assign values to vinegar variables $X_1, \cdots, X_v$ randomly and the resulting system can be seen as a linear system over the $\mathbb{F}_q$-entries of oil variables $X_{v+1}, \cdots, X_n$. The remaining is the same as in UOV scheme. Secondly, the signature is $\overrightarrow{\mathbf{U}} = T^{-1}(\overrightarrow{\mathbf{X}}) \in \mathcal{R}^n$.

Verification. Let $\overrightarrow{\mathbf{U}} = (U_1, \cdots, U_n) \in \mathcal{R}^n$ be the signature to be verified. If $Hash(D) = P(\overrightarrow{\mathbf{U}})$, then the signature is accepted, otherwise rejected.

Structure of SNOVA. Similar to NOVA, a (v, o, q, l) SNOVA over $\mathcal{R}$ can be regarded as an $(l^2 v, l^2 o, q)$ UOV scheme over $\mathbb{F}_q$. The noncommutativity of matrix ring $\mathcal{R}$ implies that we can not write the public key of SNOVA into a quadratic form $P_i(\overrightarrow{\mathbf{U}}) = (\overrightarrow{\mathbf{U}})^t \, [P_i] \, \overrightarrow{\mathbf{U}}$ over $\mathcal{R}$.

Degree of regularity of SNOVA. In Section 5.3, our experiments show that the public key of SNOVA behaves like a semi-regular system when we execute direct attack on SNOVA. Moreover, [43] indicates that the randomness of coefficients of NC-Rainbow is much less than the randomness of original Rainbow and it is not possible to be as secure as original Rainbow. In general, both X_j, X_k consist of l^2 variables in F_q, thus the maximal number of monomials induced by entry-wise product of the components of X_j, X_k should be l^4. However, in our case, for each $X_j^t \cdot H \cdot X_k$ where H is a ring coefficient, due to the structure of matrix multiplication, only l^2 monomials appear. By α running from 1 to l^2, we introduce l^2 different copies in the central map of SNOVA, therefore, the randomness of SNOVA is recovered to $l^2 \cdot l^2 = l^4$.

4.2 Key generation process of SNOVA

In this section, we give the standard key generation process of SNOVA and the key generation process with key-randomness alignment technique. Note that in SNOVA scheme, $\mathbb{F}_q$ is of the characteristic 2.

Standard key generation process. For $i = 1, 2, \ldots, m$, the matrix $[P_i]$ is obtained by relation

$$[P_i] = [T]^t \, [F_i] \, [T] \, .$$

Then, we have the following

$$\begin{aligned}
P_i^{11} &= F_i^{11} \\
P_i^{12} &= F_i^{11} T^{12} + F_i^{12} \\
P_i^{21} &= (T^{12})^t F_i^{11} + F_i^{21} \\
P_i^{22} &= (T^{12})^t \cdot \left(F_i^{11} T^{12} + F_i^{12} \right) + F_i^{21} T^{12}.
\end{aligned}$$

Therefore, to generate the public key we generate the matrices $[F_i]$, $[T]$ from a seed $\mathbf{s}_{\mathbf{private}}$ at first and then compute the public key $[P_i]$ for $i = 1, \cdots, m$ with the formulas above.

Key generation with randomness alignment. The following are steps of key generation process of SNOVA with key randomness alignment.

First Step: Generate S, P_i^{11}, P_i^{12} and P_i^{21} for $i = 1, \cdots, m$, and $[T]$ from two seeds $\mathbf{s}_{\mathbf{public}}$ and $\mathbf{s}_{\mathbf{private}}$ respectively. We also generate the matrices A_α, B_α and $Q_{\alpha k}$ for $\alpha = 1, 2, \ldots, l^2$ and $k = 1, 2$ from $\mathbf{s}_{\mathbf{public}}$.

Second Step: Compute the matrix $F_i^{11}, F_i^{12}, F_i^{21}, P_i^{22}$ for $i = 1, \cdots, m$ as below.

For $i = 1, 2, \ldots, m$, we have

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

Therefore, the following equations hold

$$\begin{aligned}
F_i^{11} &= P_i^{11} \\
F_i^{12} &= P_i^{11} T^{12} + P_i^{12} \\
F_i^{21} &= (T^{12})^t P_i^{11} + P_i^{21} \\
0 = F_i^{22} &= (T^{12})^t \cdot \left(P_i^{11} T^{12} + P_i^{12} \right) + P_i^{21} T^{12} + P_i^{22}.
\end{aligned}$$

In other words, we then have

$$P_i^{22} = \left(T^{12}\right)^t \cdot \left(P_i^{11} T^{12} + P_i^{12} \right) + P_i^{21} T^{12}.$$

Public key size. The reduced size of the public key of SNOVA using alignment is

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

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

5 Security Analysis

In this section, we give the security analysis of SNOVA scheme. Since SNOVA can not only be regarded as a signature scheme over the matrix ring $\mathcal{R}$, but also as a UOV over $\mathbb{F}_q$. The security analysis are given in two different aspects, i.e., over the ring $\mathcal{R}$ and over the field $\mathbb{F}_q$.

5.1 Solving MQ systems and Complexity Estimation

There are several algorithms to solve a quadratic system of M equations in N variables over finite fields such as F_4 [19], F_5 [20] and XL variants [14, 11, 49].

Solving MQ problem. The complexity of solving M homogeneous quadratic equations in N variables [6, 11] can be estimated by

$$MQ(N, M, q) = 3 \cdot \binom{N - 1 + d_{reg}}{d_{reg}}^2 \cdot \binom{N+1}{2}$$

field multiplications where d_{reg} is the degree of regularity of a semi-regular polynomial system and it is equal to the smallest positive integer such that the coefficient of t^d term in the series generated by

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

is non-positive.

Hybrid approach. The hybrid approach [5] randomly guesses k variables before solving the MQ system and the corresponding complexity is $q^k \cdot MQ(N-k, M, q)$ field multiplications for the classical case and $q^{k/2} \cdot MQ(N-k, M, q)$ field multiplications when applying Grover's algorithm [23] for the quantum case.

Methods solving underdetermined MQ. On the other hand, Thomae and Wolf [44], Furue, Nakamura and Takagi [21], Hashimoto [24] provide several methods to solve an underdetermined multivariate quadratic system P of M equations in N variables over a finite field, i.e., $N > M$. The main idea 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 reduces to an $MQ(M - k - \alpha_k,\ M - \alpha_k,\ q)$ problem and hence can by solved using the hybrid approach [5]. 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 [44, 21, 24] are the same but with different optimal values α_k. Hence, the main term of complexity of solving MQ system under this technique is given by

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

field multiplications in the classical case and

$$\min_k \; q^{k/2} \cdot MQ(M-k-\alpha_k,\ M-\alpha_k,\ q)$$

in the quantum case with different optimal values α_k corresponding to different methods.

The optimal values α_k of [44, 21] are $\alpha_{\mathrm{TW}} = \lfloor \frac{N}{M} \rfloor - 1$, $\alpha_{\mathrm{F}} = \lfloor \frac{N-k}{M-k} \rfloor - 1$, respectively, and $\alpha_{\mathrm{HMa}} = \lfloor \frac{N}{M-k} \rfloor - 1$, α_{HMb} is the maximal integer such that $N \geq M - (\alpha_k + k - M)\alpha_k$ holds, where α_{HMa} and α_{HMb} are corresponding to the two algorithms proposed in [24], respectively. Note that, the attack in [24] would be the sharpest among [44, 21, 24].

Algorithms for super-underdetermined MQ. Note that, [27, 13, 30, 12] indicate that when the number of variables N is sufficiently larger than the number of equations M in a MQ problem then we can solve this MQ in polynomial time. Please refer to the table in [24] for more information. Note that these four algorithms are not applicable to the parameter settings of SNOVA.

5.2 MinRank Problem and Support-Minors Modeling

MinRank problem. For $M_1, \cdots, M_k \in \mathbb{F}_q^{M\times N}$ and a target rank r, the MinRank problem asks to find a non-trivial linear combination of the matrices which has rank at most r. That is, to find a vector $\vec{\mathbf{x}} \in \mathbb{F}_q^k$ such that

$$\operatorname{rank}\left(\sum_{i=1}^{k} x_i M_i\right) \leq r.$$

Solving MinRank problem. Notice that the MinRank problem is NP-hard [10] and it plays a central role in the cryptanalysis of MPKC. Recently, Bardet *et al.* proposed the Support-Minors (SM) modeling algorithm [3] to solve MinRank problem. This powerful algorithm transform the rank condition into a large bilinear system which is sparse and then use the linearization method to solve it. The complexity of this algorithm is estimated by

$$MinRank(M,N,k,r) = 3 \cdot k(r+1) \cdot \left(\binom{N}{r}\binom{k+b-1}{b}\right)^2$$

where b is the smallest positive integer such that

$$\binom{N}{r}\binom{k+b-1}{b}-1 \leq \sum_{i=1}^{b}(-1)^{i+1}\binom{N}{r+i}\binom{M+i-1}{i}\binom{k+b-i-1}{b-i}$$

holds.

Moreover, Bardet *et al.* point out that one may choose to use the first $N' \leq N$ columns when applying their algorithm and for some optimal N' so that $r+1 \leq N' \leq N$ the cost of computation can be further reduced.

Superdetermined MinRank problem. Superdetermined MinRank problem is defined in [45] as the MinRank problem with $k < rM$. Moreover, in [1] Bardet and Bertin indicate that the modeling in [45] can be seen as a special case of SM modeling and the best complexity will be the one that solving the associated Macaulay matrix by linearization. If we consider the minors as new variables, the system can be solved whenever $M(N-r) \geq k(r+1)$, i.e., $b=1$. Moreover, with Plücker coordinates, the Macaulay matrix has a special form and this can help us to solve the problem more quickly. For $1 \leq d \leq r-1$, if

$$m\binom{n-r}{d+1}\binom{r}{d} \geq k\binom{n-r}{d+1}\binom{r}{d+1}+k\binom{n-r}{d}\binom{r}{d}-1,$$

then with overwhelming probability the solution can be obtained [1].

SM modeling with hybrid technique. In [2], Bardet *et al.* show that we can solve a $MinRank(M,N,k,r)$ problem by performing q^{ar} attacks on those much more smaller $MinRank(M,N-a,k-am,r)$ instances where a is a positive integer so that $k-am \geq 0$ and then only one of them has the solution. Therefore, the complexity of SM modeling with hybrid technique is

$$MinRank_{Hybrid}(M,N,k,r)=\min_{a\geq 0}\left(q^{ar}\cdot MinRank(M,N-a,k-am,r)\right).$$

5.3 Direct Attack

For a quadratic multivariate polynomial system $P=[P_1,\cdots,P_m]$ consisting of m equations in n variables over $\mathbb{F}_q$ and $\vec{\mathbf{y}} \in \mathbb{F}_q^m$, an attacker can directly try to solve the solution $\vec{\mathbf{u}}$ of the system $P(\vec{\mathbf{u}})=\vec{\mathbf{y}}$ algebraically with Gröbner basis approach such as [19, 20, 14, 11, 49]. In the case of UOV, the public key is underdetermined, that is, $n > m$. Therefore we can assign the values to $n-m$ variables in the system $P(\vec{\mathbf{u}})=\vec{\mathbf{y}}=Hash(D)$ randomly and then obtain a MQ system of m equations in m

variables which can be solved with high probability. Once the system can be solved, the solution $\vec{\mathbf{u}}$ will be a valid fake signature and hence $P(\vec{\mathbf{u}}) = \vec{\mathbf{y}}$.

The public key of UOV is considered to be a semi-regular system [4]. Therefore, the complexity of direct attack is

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

field multiplications and the complexity of the quantum direct attack is

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

field multiplications when applying Grover's algorithm [23].

In the case of SNOVA, if the attacker wants to solve a quadratic system over the ring $\mathcal{R}$ directly then he will suffer from the fact that there is no efficient algorithm like F_4, F_5 and XL to compute the solution $\vec{\mathbf{U}}$ of the system $P(\vec{\mathbf{U}}) = \vec{\mathbf{Y}}$ over the noncommutative ring $\mathcal{R}$.

However, since each equation over $\mathcal{R}$ gives us l^2 equations over $\mathbb{F}_q$ corresponding to the l^2 components of ring variables $\vec{\mathbf{U}} = (U_1, \cdots, U_n)$, it follows that the main idea of the direct attack still works and it can be done by solving the system over a finite field $\mathbb{F}_q$. Then we obtain a MQ system is 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 SNOVA behaves like a random systems of $l^2 \cdot m$ equations in $l^2 \cdot m$ variables over a $\mathbb{F}_q$.

The complexity of classical direct attack is

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

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

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

field multiplications.

The complexity of classical direct attack using technique in [44, 21, 24] is

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

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

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

field multiplications.

The following table gives comparison of the degree at the first step degree falls or goes flat using F_4 algorithm [19], which is strongly connected to the degree of regularity [17], in Magma algebra system [9] that starts to go either down or flat among all step degrees of the quadratic system obtained by SNOVA and a random quadratic system respectively.

Table 3: Table of comparison of the degree at the first step degree falls or goes flat between SNOVA and random systems.

(v, o, q, l, k)	SNOVA system	random system
$(6, 1, 16, 2, 1)$	3	3
$(6, 2, 16, 2, 1)$	5	5
$(6, 2, 16, 2, 2)$	4	4
$(6, 2, 16, 2, 3)$	3	3
$(6, 3, 16, 2, 1)$	7	7
$(6, 3, 16, 2, 2)$	6	6
$(6, 3, 16, 2, 3)$	5	5
$(6, 4, 16, 2, 2)$	7	7
$(6, 4, 16, 2, 3)$	6	6
$(6, 1, 16, 3, 2)$	4	4
$(6, 1, 16, 3, 3)$	4	4
$(6, 1, 16, 3, 4)$	3	3
$(6, 2, 16, 3, 3)$	7	7
$(6, 2, 16, 3, 4)$	6	6
$(6, 2, 16, 3, 5)$	5	5
$(6, 1, 16, 4, 1)$	9	9
$(6, 1, 16, 4, 2)$	7	7
$(6, 1, 16, 4, 3)$	6	6
$(6, 1, 16, 4, 4)$	5	5
$(6, 1, 16, 4, 5)$	5	5

5.4 MinRank Alike Key Recovery Attacks

Reconciliation Attack. The reconciliation attack proposed by [18] against UOV is trying to find a vector $\vec{\mathbf{o}} \in T^{-1}(\mathcal{O})$ by solving the system $P(\vec{\mathbf{o}}) = 0$ and hence the basis of $T^{-1}(\mathcal{O})$ can be recovered. This implies that $P(\vec{\mathbf{o}}) = 0$ 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 $\vec{\mathbf{o}}$. Hence the complexity of this attack is mainly given by that of solving the quadratic system of m equations in v variables.

A reconciliation attack on SNOVA, if considered over field, is as an attack on UOV, thus we are in the case of solving the quadratic system of l^2m equations in $v > o = l^2m$ variables. Hence the reconciliation attack usually will not outperform the direct attack in which the complexity comes from solving l^2m quadratic equations in l^2m variables. Furthermore, if the attack on SNOVA is considered over ring, it even suffers from the fact that there is no efficient algorithm to complete the attack over $\mathcal{R}$.

New MinRank attacks. Although, in [6, 7], Rectangular MinRank attack, Simple attack and Combine attack are new attacks against Rainbow, these attacks all rely on the multi-layer structure of Rainbow. Therefore, these attacks on Rainbow have no security implications on our scheme since SNOVA has no multi-layer structure as Rainbow.

MinRank attack against NC-Rainbow. The NC-Rainbow signature scheme [52] is a variant of Rainbow which is based on Quaternion ring over a finite field $\mathbb{F}_q$ of characteristic 2. However, [43] indicates 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 F of NC-Rainbow will be lower than original Rainbow. Moreover, the corresponding matrices will have a particular form and such a form is sparse. The MinRank attack of [43] is based on the multi-layer structure and the sparse form caused from the special structure of multiplication of Quaternion ring. Note that the public key of SNOVA has neither that sparsity nor a special form in its matrix representation. Furthermore, SNOVA has no multi-layer structure in the central map F.

5.5 K-S Attack (UOV Attack)

The K-S attack [27] is trying 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 equivalent $[F_i]$ by the relation $[F_i] = [T^{-1}]^t [P_i] [T^{-1}]$. Note that [27] shows that $T^{-1}(\mathcal{O})$, the oil subspace of the public key P of UOV, induces an equivalent key.

In [27], it shows that $T^{-1}(\mathcal{O})$ is an invariant subspace of $[P_i]^{-1} [P_j]$. The K-S attack is trying to find a vector in $T^{-1}(\mathcal{O})$. Once one such vector is found, then we expect that the whole 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

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

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 SNOVA 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 SNOVA over $\mathcal{R}$. Note that [35] 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, an attacker may treat a (v, o, q, l) SNOVA scheme over $\mathcal{R}$ as an (l^2v, l^2o, q) UOV system over $\mathbb{F}_q$ and carry out the K-S attack against SNOVA over $\mathbb{F}_q$.

Then we have

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

field multiplications for classical attack and

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

field multiplications for quantum attack.

5.6 Intersection Attack

In [7], Beullens proposed the intersection attack to attack UOV scheme. It uses the polar form of the public key P, that is, $P' = [P'_1, \cdots, P'_m]$ with $P'_i(\overrightarrow{\mathbf{u_1}}, \overrightarrow{\mathbf{u_2}}) = \overrightarrow{\mathbf{u_1}}^t \, [P'_i] \, \overrightarrow{\mathbf{u_2}}$ where $[P'_i] = [P_i] + [P_i]^t$.

The intersection attack is trying to first find a vector $\overrightarrow{\mathbf{y}}$ in the subspace, namely the intersection $\Big([P'_i] \, (T^{-1}\mathcal{O}) \Big) \cap \Big([P'_j] \, (T^{-1}\mathcal{O}) \Big)$ where $[P'_i], [P'_j]$ are invertible, and then to obtain an equivalent key by recovering the subspace $T^{-1}(\mathcal{O})$.

Since $([P_i']^{-1})\vec{\mathbf{y}}$, $(\left[P_j'\right]^{-1})\vec{\mathbf{y}} \in T^{-1}(\mathcal{O})$, we obtain the following system.

$$\begin{cases} P\Big(\left([P_i']^{-1}\right)\vec{\mathbf{y}}\Big) = 0 \\ P\Big((\left[P_j'\right]^{-1})\vec{\mathbf{y}}\Big) = 0 \\ P'\Big(([P_i']^{-1})\vec{\mathbf{y}}, (\left[P_j'\right]^{-1})\vec{\mathbf{y}}\Big) = 0 \end{cases}$$

Whenever $\mathbf{2.5m < n < 3m}$. If $2.5m < n < 3m$, there is a $3m - n$ dimensional subspace of solutions. 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. Then the complexity is

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

field multiplications.

Whenever $\mathbf{n < 2.5m}$. If $n < 2.5m$, the attack can become more powerful by seeking a vector $\vec{\mathbf{y}}$ in the intersection of k subspaces $[P_i']^{-1}\,(T^{-1}\mathcal{O})$ 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.

In case of intersection attack against SNOVA, due to our construction, we can not write the public polynomial P_i of SNOVA in quadratic form, namely $\overrightarrow{\mathbf{u_1}}^t\,[P_i']\,\overrightarrow{\mathbf{u_2}}$, 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 SNOVA, we need to regard SNOVA 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.

Whenever $\mathbf{n < 2.5m}$. 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

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

field multiplications

Whenever 2.5m < n < 3m. In the case $2.5m < n < 3m$, $N = 2(l^2n) - 3(l^2m),\ M = 3(l^2m)$, and

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

field multiplications.

Whenever n ≥ 3m. If $n \geq 3m$, then there is no guarantee that the subspace, namely the intersection $\Big([P'_i]\,(T^{-1}\mathcal{O})\Big) \cap \Big([P'_j]\,(T^{-1}\mathcal{O})\Big)$ will exist. Therefore, the intersection attack becomes a probabilistic attack against SNOVA. In this case, the complexity is

$$\text{Comp}_{\text{Intersection}}\text{SNOVA} = q^{(l^2n)-3(l^2m)+1} \cdot MQ(N+1,\ M,\ q)$$

field multiplications where $N = l^2n, M = 3(l^2m)$.

5.7 Equivalent Key Attack

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 $P(T^{-1}(\vec{\mathbf{x}})) = F(\vec{\mathbf{x}})$ and solve for $[T^{-1}]$ by comparing both sides of equation at ring level. Then it induces a system of $m \cdot m^2 \cdot l^2$ quadratic equations in lvo variables over $\mathbb{F}_q$ and hence can be solved by F_4, F_5 and XL.

Therefore, the complexity is

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

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

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

field multiplications with applying Grover's algorithm.

Note that the multivariate quadratic system constructed by $[T^{-1}]$ attack is overdetermined, hence [26, 13, 30, 12, 44, 21, 24] are not applicable.

On the other hand, one may consider that executing $[T^{-1}]$ attack that regards a (v, o, q, l) NOVA as an (l^2v, l^2o, q) UOV then inducing a quadratic system of $M = (l^2m) \cdot (l^2m) \cdot \frac{l^2m+1}{2}$ equations in lvo variables over $\mathbb{F}_q$. However, this does not increase the number of independent equations compared to the above formulations.

5.8 Quadratic Forms Over Ring

In this section, we introduce a new way to attack SNOVA scheme (or more generally, an alternative way to attack a signature scheme which is constructed over ring) and discuss its possibility. The main insight is that when a signature scheme is constructed form a quadratic form over ring then it would share its private key with another signature scheme over ring whose structure is more simpler.

UOV over ring. Notice that the central map of SNOVA is of the form

$$F_i = \sum_{\alpha=1}^{l^2} A_\alpha \cdot \left(\sum_{(j,k)\in\Omega} X_j^t \left(Q_{\alpha 1} F_{i,jk} Q_{\alpha 2}\right) X_k \right) \cdot B_\alpha$$

and the public key is generated by the congruence relation $[P_i] = [T]^t [F_i] [T]$. Therefore, we can construct a UOV scheme over $\mathcal{R}$ that shares the same private key T with SNOVA scheme. Namely, this more simpler scheme is the UOV scheme over $\mathcal{R}$ whose central map has the form of

$$\tilde{F}_i = \sum_{(j,k)\in\Omega} X_j^t F_{i,jk} X_k$$

and the corresponding public key $\tilde{P} = \left[\tilde{P}_1, \cdots, \tilde{P}_m\right]$ where $\tilde{P}_i = \tilde{F}_i \circ T$ and T is private key of SNOVA. Once we recover the private key T by attacking this ring UOV over $\mathcal{R}$ then we also find an equivalent key of SNOVA scheme.

However, to our best knowledge, we do not find a complete key recovery attack against this ring UOV. On the other hand, this ring UOV also induces a UOV over field, thus we still give some complexity estimations of the related problems corresponding to this ring UOV when considered as over field. The details are as following.

Kernel of ring UOV. Note that for the central map F of UOV vanishes on the oil space $\mathcal{O}$. As we mentioned, we can regard this (v, o, q, l) ring UOV as a $(l^2 v, l^2 o, q)$ UOV scheme over $\mathbb{F}_q$ and the corresponding matrices, say $M_1, \cdots, M_{l^2 o}$, are sparse. One may worry about that this sparsity will make these matrices vanish on a linear space lager than the oil space $\mathcal{O}$. Although we can see that for each i, the matrix M_i vanishes on a linear space $\mathcal{W}_i$ so that $\mathcal{O} \subseteq \mathcal{W}_i$ and $\dim \mathcal{O} \leq \dim \mathcal{W}_i$, the intersection of $\mathcal{W}_i$ is still the oil space $\mathcal{O}$ (we can easily see this phenomenon in toy examples). Therefore, we conclude that this $(l^2 v, l^2 o, q)$ UOV will not vanish on a linear space which is larger than oil space $\mathcal{O}$ from this point of view.

No multi-layer structure. Note that the Rainbow scheme [16] is a MQ signature scheme with multi-layer UOV structure. Such multi-layer structure will result in nested structure of oil spaces [7]. SNOVA has no multi-layer structure, thus the linear spaces

$\mathcal{W}_i$ mentioned above have no nested structure. Hence the MinRank alike attacks in [6, 7] have no security impact on SNOVA scheme at all.

Intersection of the null spaces of public key differential. In [34], Park broke the Matrix-based UOV scheme [42] which is proposed by Tan and Tang. We can regard the matrices of the differential of the central map and the public key of Matrix-based UOV as linear operators. Then the sparsity of these matrices makes the intersections of the corresponding null spaces non-trivial, while general UOV do not have this phenomenon. And any basis of this non-trivial intersection can be used to build an equivalent private key.

Note that the null spaces of the differential of the central map and the public key of the ring UOV corresponding to SNOVA have no structure same as that in Matrix-based UOV. Therefore, the attack in [34] is not applicable to this ring UOV and hence the attack will not affect the security of SNOVA.

Matrices may have low rank. When we regard this (v, o, q, l) ring UOV as a (l^2v, l^2o, q) UOV scheme over $\mathbb{F}_q$, we discover that some corresponding matrices has rank at most lv. However, note that the MinRank attack in [43] is based on the multilayer structure of Rainbow and its nested kernel relation. In conclusion, we do not find a complete key recovery attack based on this MinRank problem.

On the other hand, this phenomenon still induces a $MinRank(l^2n, l^2n, l^2m, lv)$ MinRank problem. For the sake of security, we estimate the complexity of solving this MinRank problem using Support-Minors algorithm and take this into account when we choose our parameter settings of SNOVA scheme in Section 6. If there were a key recovery attack using this MinRank problem, then its complexity should be greater than this MinRank problem. Hence the security of our parameter setting will not be affected.

Superdetermined and hybrid approach. The $MinRank(l^2n, l^2n, l^2m, lv)$ instance above is superdetermined and then the technique in [1] can be applied to this instance. Note that [1] also shows that executing the computation at the smallest degree and with the smallest number of variables will not always be the best estimation. In conclusion, our complexity estimations take both strategies, the technique in [1] and solving system in higher degree $b > 1$, into consideration. As a result, the approach in [1] will not affect the security of our parameters. On the other hand, note that the hybrid approach in [2] is not applicable to the instance above. Therefore, these two approaches are not crucial for our parameters.

Forgery attack. An alternative possibility trying to use ring UOV to attack SNOVA is to forge a fake signature of ring UOV. However, the construction of SNOVA, namely the matrices A_α, B_α act like a disturbance on the public key P and hence this approach is impossible. Because of this, the fake signature of ring UOV is not a valid fake signature for the public key of SNOVA.

6 Implementation and Parameters

In [31], NIST suggested several security levels for post-quantum cryptosystem design. In the new call for additional digital signature scheme project, NIST slightly modified their security level request. In this section, we propose our parameters aiming at three security levels in the new call of NIST PQC project [32] levels I, III and V, respectively.

6.1 NIST Security Level

Herein, We focus on level I, III, and V. The NIST security level I, III and V requiring that a classical attacker needs 2^{143}, 2^{207} and 2^{272} classical gates to break the scheme, and 2^{61}, 2^{125} and 2^{189} quantum gates for a quantum attacker, respectively.

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 and for each field multiplication in the computation, it also needs an addition of field elements, each takes $\log_2 q$ bit additions.

6.2 To Attain EUF-CMA Security

For practical considerations, we use a random binary vector, called salt in order to achieve Existential Unforgeability under Chosen Message Attack (EUF-CMA) Security [33].

Signature. Let D be the document to be sign, we randomly choose **salt** and then generate a signature for the hash value $\overrightarrow{\mathbf{Y}} = Hash(Hash(D)||\mathbf{salt})$. Therefore, the corresponding signature is of the form $\vec{\sigma} = (\overrightarrow{\mathbf{U}}||\mathbf{salt})$ where $\overrightarrow{\mathbf{U}}$ is the signature of $\overrightarrow{\mathbf{Y}}$ generated by the SNOVA signer. Note that we want almost no **salt** is used for more than one signature. Therefore, the length of **salt** is chosen to be 16 Bytes under the assumption of up to 2^{64} signatures being generated with the system.

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

6.3 Proposed Parameter Settings

In this section, we give our proposed parameters and the corresponding sizes of public key and signature respectively. Finally, the comparison table of SNOVA with NIST finalists [39, 28] and MAYO [8] is given.

The following table shows the complexity of respective attacks against our parameters. "Dir.", "TWFH.", "K-S.", "Int.", "$[T^{-1}]$." and "MinRank." denote direct attack, direct attack using technique in [44, 21, 24], K-S attack [27], intersection attack [7] and $[T^{-1}]$ attack and the complexity for the MinRank problem 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 4: Table of complexity in $\log_2(\sharp\text{gates})$.

SL	(v,o,q,l)	Dir.	TWFH.	K-S.	Int.	$[T^{-1}]$.	MinRank.
I	$(31,15,16,2)$	154/116	153/109	280/154	433	217/217	**150**
	$(34,7,16,3)$	161/120	**149**/93	997/513	1154	379/379	153
	$(25,8,16,3)$	180/135	175/126	637/333	819	231/231	**148**
	$(24,5,16,4)$	197/149	188/134	1242/636	1439	286/286	**150**
	$(19,6,16,4)$	232/177	227/171	859/445	1101	188/188	**152**
III	$(47,23,16,2)$	223/166	223/160	411/221	632	321/321	**214**
	$(49,11,16,3)$	238/177	230/162	1395/713	1631	530/530	**215**
	$(40,12,16,3)$	257/191	253/183	1036/534	1294	372/372	**212**
	$(37,8,16,4)$	299/224	291/214	1885/959	2192	424/424	**217**
	$(29,9,16,4)$	334/252	329/246	1309/671	1662	282/282	**212**
V	$(64,31,16,2)$	291/215	291/210	556/294	846	430/430	**278**
	$(66,15,16,3)$	314/232	307/220	1865/949	2178	707/707	**280**
	$(57,16,16,3)$	334/245	329/237	1505/769	1842	550/550	**277**
	$(60,10,16,4)$	367/271	355/255	3230/1632	3602	812/812	**278**
	$(50,11,16,4)$	401/298	393/288	2527/1281	2939	575/575	**279**

The key-size and the length of the signature are shown as below. Herein, the notation

Size_{pk} denotes the public key size and Size_{sig} denotes the signature size.

Table 5: Table of key-sizes and lengths of the signature of NOVA parameter settings.

Security Level	(v, o, q, l)	Size_{pk} (Bytes)	Size_{sig} (Bytes)
I	$(31, 15, 16, 2)$	6750	92(+16)
	$(34, 7, 16, 3)$	1543.5	184.5(+16)
	$(25, 8, 16, 3)$	2304	148.5(+16)
	$(24, 5, 16, 4)$	1000	232(+16)
	$(19, 6, 16, 4)$	1728	200(+16)
III	$(47, 23, 16, 2)$	24334	140(+16)
	$(49, 11, 16, 3)$	5989.5	270(+16)
	$(40, 12, 16, 3)$	7776	234(+16)
	$(37, 8, 16, 4)$	4096	360(+16)
	$(29, 9, 16, 4)$	5832	304(+16)
V	$(64, 31, 16, 2)$	59582	190(+16)
	$(66, 15, 16, 3)$	15187.5	364.5(+16)
	$(57, 16, 16, 3)$	18432	328.5(+16)
	$(60, 10, 16, 4)$	8000	560(+16)
	$(50, 11, 16, 4)$	10648	488(+16)

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

Table 6: A comparison table of SNOVA with the NISTPQC signature finalists and MAYO aims at NIST security level I.

Signature Scheme	Size of public key (Bytes)	Size of signature (Bytes)
Dilithium-2	1312	2420
Falcon-512	897	666
SPHINCS$^+$-128s	32	7856
SPHINCS$^+$-128f	32	17088
MAYO-I, leaky	518	494
MAYO-I, tight	730	501
SNOVA$(24, 5, 16, 4)$	1000	232(+16)
SNOVA$(19, 6, 16, 4)$	1728	200(+16)
SNOVA$(34, 7, 16, 3)$	1543.5	184.5(+16)
SNOVA$(25, 8, 16, 3)$	2304	148.5(+16)
SNOVA$(31, 15, 16, 2)$	6750	92(+16)

In [50, 51], they both pointed out that the protocol 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 well compatible with the existing framework. Note that [51] gives the corresponding condition: six times signature size and two times of public key size fit in 9KB. According to the specification of SNOVA, SNOVA could be a more practical general-purpose signature scheme.

7 Conclusion

The Simple NOVA (SNOVA) scheme simplifies the design of NOVA scheme by skipping the perturbation trick, thus shortens the key generation process and accelerates the signing and verification. Both SNOVA and NOVA have shown that multivariate signature schemes over noncommutative rings could be beneficial to security and key size reduction. We put most of our efforts on security analysis. To our best knowledge, SNOVA scheme is capable of resisting all known attacks for multivariate cryptosystems. By comparison with other post-quantum signature schemes, SNOVA is a practical secure signature scheme which is relatively efficient on both public key size and signature size.

Acknowledgement

The first author would like to express thanks to Prof. Jintai Ding for his encouragement. The first author and the second author are partially supported by MOST110-2122-M-259-001. The third author is partially supported by MOST111-2115-M-259-001-MY2.

References

[1] Bardet, M., Bertin, M.: **Improvement of Algebraic Attacks for Solving Superdetermined MinRank Instances.** In: Cheon, J.H., Johansson, T. (eds) Post-Quantum Cryptography. PQCrypto 2022. Lecture Notes in Computer Science, vol 13512. Springer, Cham. https://doi.org/10.1007/978-3-031-17234-2_6

[2] Bardet, M., Briaud, P., Bros, M., Gaborit, P., Tillich, J.P.: **Revisiting Algebraic Attacks on MinRank and on the Rank Decoding Problem.** Available at https://eprint.iacr.org/2022/1031.pdf.

[3] Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D, Tillich, J.P., Verbel, J.A.: **Improvements of algebraic attacks for solving the rank decoding and MinRank problems.** In Shiho Moriai and Huaxiong Wang, editors, ASIACRYPT 2020, Part I, volume 12491 of LNCS, pages 507–536. Springer, Heidelberg, December 2020.

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

[5] 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).

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

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

[8] 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`.

[9] 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)

[10] Buss, J.F., Frandsen, G.S., Shallit, J.O.: **The computational complexity of some problems of linear algebra.** Journal of Computer and System Sciences 58(3), 572– 596 (1999).

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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`

[16] 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.

[17] 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`.

[18] 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).

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

[20] 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.

[21] 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.

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

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

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

[25] 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.

[26] 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.

[27] 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.

[28] 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`.

[29] 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.

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

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

[32] NIST: **Post-Quantum Cryptography: Digital Signature Schemes.** Available at `https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals`

[33] 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`

[34] Park, C.M.: **Cryptanalysis of Matrix-based UOV.** In Finite Fields and Their Applications, Volume 50, 2018, Pages 209-221, ISSN 1071-5797, `https://doi.org/10.1016/j.ffa.2017.11.012`.

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

[36] 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.

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

[38] 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.

[39] 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`.

[40] 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).

[41] 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).

[42] Tan, Y., Tang, S.: **Two Approaches to Build UOV Variants with Shorter Private Key and Faster Signature Generation.** In: Lin, D., Wang, X., Yung, M. (eds) Information Security and Cryptology. Inscrypt 2015. Lecture Notes in Computer Science(), vol 9589. Springer, Cham. `https://doi.org/10.1007/978-3-319-38898-4_4`.

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

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

[45] Verbel, J., Baena, J., Cabarcas, D., Perlner, R., Smith-Tone, D.: **On the complexity of "Superdetermined" minrank instances.** In: Ding, J., Steinwandt, R. (eds.) PQCrypto 2019. LNCS, vol. 11505, pp. 167–186. Springer, Cham (2019). `https://doi.org/10.1007/978-3-030-25510-7_10`

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

[47] 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.

[48] Wang, L.C., Tseng, P.E., Kuan, Y.L., Chou, C.Y.: **NOVA, a Noncommutative-ring Based Unbalanced Oil and Vinegar Signature Scheme with Key-randomness Alignment**, 2022. Available at `https://eprint.iacr.org/2022/665`.

[49] 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

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

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

[52] 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.