Analysis on the MinRank Attack using Kipnis-Shamir Method Against Rainbow

Shuhei Nakamura*, Yacheng Wang†and Yasuhiko Ikematsu ‡

Abstract

Minrank problem is investigated as a problem related to a rank attack in multivariate cryptography and decoding of a rank code in coding theory. Recently, the Kipnis-Shamir method for solving this problem has been made significant progress due to Verbel et al. As this method reduces the problem to the MQ problem that asks for a solution of a system of quadratic equations, its complexity depends on the solving degree of a quadratic system deduced from the method. A theoretical value introduced by Verbel et al. approximates the minimal solving degree of the quadratic systems in the method although their value is defined under a certain limit for a considering system. A quadratic system outside their limitation often has the larger solving degree, but its solving complexity is not necessary larger since it has a smaller number of variables and equations. Thus, in order to discuss the best complexity of the Kipnis-Shamir method, we need a theoretical value approximating the solving degree of each deduced quadratic system. A quadratic system deduced from the Kipnis-Shamir method has a multi-degree always, and its solving complexity is influenced by this property. In this paper, we introduce a theoretical value defined by such a multi-degree and show it approximates the solving degree of each quadratic system. Thus we are able to compare the systems in the method and to discuss the best complexity. As its application, in the Minrank problem from the rank attack using the Kipnis-Shamir method against Rainbow, we show a case that a quadratic system outside Verbel et al.'s limitation is the best. Consequently, by using our estimation, the complexities of the attack against Rainbow parameter sets Ia, IIIc and Vc are improved as $2^{160.6}$, $2^{327.9}$ and $2^{437.0}$, respectively.

*Department of Liberal Arts and Basic Sciences, Nihon University, Japan (E-mail: nakamura.shuhei@nihon-u.ac.jp)

†Department of Mathematical Informatics, University of Tokyo, Japan (E-mail: yacheng_wang@mist.i.u-tokyo.ac.jp)

‡Institute of Mathematics for Industry, Kyushu University, Japan (E-mail: ikematsu@imi.kyushu-u.ac.jp)

1 Introduction

Minrank problem that asks for a linear combination of given matrices such that has a target rank at most, is firstly introduced by Shallit et al. [1] and is an NP complete problem. A rank attack [17, 14, 4] in multivariate cryptography and decoding of a rank code [14, 8] in coding theory are related to this problem. In NIST post-quantum cryptography (PQC) standardization project [19] toward building cryptosystem resistant to attacks using quantum computers, not only multivariate cryptography but also code-based cryptography is investigated and an analysis for this problem is important.

The minors method [4], the Kipnis-Shamir (KS) method [17] and the linear algebra search [16] are well-known as non-trivial methods solving a Minrank problem. In this paper, we investigate the KS method for the Minrank problem arisen from a rank attack in multivariate cryptography, i.e. the MinRank attack using the KS method. The KS method reduces a Minrank problem to the MQ problem that asks for a solution of a system of quadratic polynomial equations, and a certain parameter in the method decides the number of the variables and the equations of a deduced quadratic system called a *KS system*. Since the complexity of solving a KS system dominates the overall complexity of the method, this parameter is important to the complexity estimation of the KS method.

The complexity of a Gröbner basis algorithm [6] for solving a polynomial system depends on the solving degree that is the maximal degree required to compute its Gröbner basis. For example, the complexity of the Gröbner basis algorithm F4 [12] is estimated by

$$\binom{n + d_{slv}}{d_{slv}}^{\omega}$$

where $2 < \omega \leq 3$ is a linear algebra constant, n is the number of the variables of the given polynomial system and d_{slv} is the solving degree. Since the solving degree is an experimental value, we need to consider a theoretical value approximating the solving degree. When a given polynomial system is semi-regular [2, 3], the degree of regularity [2] is well-known as a proxy for the solving degree and is given by the degree of the first term whose coefficient is non-positive in a certain power series. On the other hand, for a non-semi-regular system, the first fall degree [11] as such a proxy is defined by using its syzygies and captures the first degree at which occurs a non-trivial degree fall during a Gröbner basis algorithm.

Since a KS system is often non-semi-regular, Verbel et al. [20] discuss its concrete syzygies and introduce a theoretical value for approximating the solving degree of a KS system through its first fall degree. Their theoretical value has a limit for the range of the parameter in the method, but it approximates the minimal solving degree of the KS systems. Consequently, they give a complexity

estimation using the theoretical value for the KS method. However, since a KS system outside their limitation has a smaller number of variables and equations, the complexity does not necessary larger and not enough to discuss which KS system to solve. Thus we have to consider a theoretical value approximating the solving degree of each KS system.

1.1 Our contribution

Each KS system has a multi-degree always [14] although its bi-degree has been investigated, and its solving complexity is influenced by this property. In this paper, in order to approximate the solving degree of each KS system, we introduce a theoretical value by employing a multi-degree. This theoretical value is also available for the hybrid approach that, after fixing some variables, solves a given system, e.g. an underdetemined system. Thus it is widely applied to a polynomial system having a multi-degree.

Our theoretical value approximates the solving degree of each KS system and that deduced through the hybrid approach. Hence we are able to compare the systems in the method and to discuss the best complexity. As its application, in the MinRank attack using the KS method against Rainbow [9], we show a case that a certain KS system outside the limit of Verbel et al.'s estimation is the best. Then, by using our estimation, the complexities of the attack against Rainbow parameter sets Ia, IIIc and Vc are improved as $2^{160.6}, 2^{327.9}$ and $2^{437.0}$, respectively, and are better than the previous estimation [10] in the 2nd round of NIST PQC standardization project.

1.2 Organization

This paper is organized as follows. In Section 2, we recall the KS method solving Minrank problem and the MinRank attack using the KS method against Rainbow. In Section 3, we explain Verbel et al.'s estimation for the KS method and consider a certain parameter in the method. In Section 4, we introduce a theoretical value which is available for each KS system and show that this approximates the solving degree. In Section 5, by using the observation in Section 4, we gives a complexity estimation for the MinRank attack using the KS method against Rainbow parameter sets Ia, IIIc and Vc proposed in NIST PQC standardization project. In Section 6, we conclude our results.

2 Preliminaries

In this section, we explain the MinRank attack using Kipnis-Shamir (KS) method against Rainbow. We recall the Rainbow scheme in Subsection 2.1 and the KS method for Minrank problem in Subsection 2.2, and then explain the MinRank

attack using the KS method against Rainbow. In Subsection 2.3, we explain the complexity estimation for a Gröbner basis algorithm.

2.1 Rainbow

Let n and m be positive integers. We denote by $\mathbb{F}$ the finite field of order q. An element $(f_1, \ldots, f_m)$ of $\mathbb{F}[x_1, \ldots, x_n]^m$ is called a *polynomial system* and gives a map $\mathbb{F}^n \to \mathbb{F}^m$ by $\mathbf{a} \mapsto (f_1(\mathbf{a}), \ldots, f_m(\mathbf{a}))$ which is called a *polynomial map*.

A multivariate public key signature scheme consists of the following three algorithms:

> Key generation: We construct two invertible linear maps $S : \mathbb{F}^n \to \mathbb{F}^n$ and $T : \mathbb{F}^m \to \mathbb{F}^m$ randomly and an easily invertible quadratic map $F : \mathbb{F}^n \to \mathbb{F}^m$ which is called a *central map*, and then compute the composition $P := T \circ F \circ S$. The *public key* is given as P. The tuple (T, F, S) is a *secret key*.
>
> Signature generation: For a message $\mathbf{b} \in \mathbb{F}^m$, we compute $\mathbf{b}' = T^{-1}(\mathbf{b})$. Next, we can compute an element $\mathbf{a}'$ of $F^{-1}(\{\mathbf{b}'\})$ since F is easily invertible. Consequently, we obtain a signature $\mathbf{a} = S^{-1}(\mathbf{a}') \in \mathbb{F}^n$.
>
> Verification: We verify whether $P(\mathbf{a}) = \mathbf{b}$ holds.

Since an attacker can forge a signature $\mathbf{a}$ by solving the system $P(\mathbf{x}) = \mathbf{b}$ of quadratic polynomial equations, the security of this scheme depends on the so-called *MQ problem* that asks for a solution of a quadratic system.

Rainbow is a multivariable signature scheme proposed by J. Ding and D. Schmidt in 2005 [9]. For positive integers v, o_1 and o_2, let $\mathbf{x} = \{x_1, \ldots, x_v\}, \mathbf{y} = \{y_1, \ldots, y_{o_1}\}$ and $\mathbf{z} = \{z_1, \ldots, z_{o_2}\}$ be three variable sets and put $n = v + o_1 + o_2$ and $m = o_1 + o_2$. The central map $F = (f_1, \ldots, f_m) \in \mathbb{F}[\mathbf{x}, \mathbf{y}, \mathbf{z}]^m$ of Rainbow is defined by

$$\begin{cases} f_1 = & g^{(1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(1)}(\mathbf{x}) y_i, \\ & \vdots \\ f_{o_1} = & g^{(o_1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(o_1)}(\mathbf{x}) y_i, \\ f_{o_1+1} = & g^{(o_1+1)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+1)}(\mathbf{x}, \mathbf{y}) z_i, \\ & \vdots \\ f_{o_1+o_2} = & g^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+o_2)}(\mathbf{x}, \mathbf{y}) z_i, \end{cases} \tag{1}$$

where $g^{(j)}$ and $l_i^{(j)}$ are randomly chosen quadratic polynomials and linear polynomials, respectively. Rainbow parameter Ia, IIIc and Vc proposed in NIST PQC 2nd round are $(q, v, o_1, o_2) = (16, 32, 32, 32), (256, 68, 36, 36)$ and $(256, 92, 48, 48)$, respectively. In particular, we see that $o_1 = o_2$ and $v = o_i$ or $2o_i - 4$.

2.2 The KS method for the Minrank problem

Let q, n, m and r be positive integers. For given $m+1$ square matrices $A_0, A_1, \ldots, A_m$ of size n, the *Minrank problem* asks $x_1, \ldots, x_m \in \mathbb{F}_q$ giving a linear combination such that

$$\mathrm{Rank}\left(A_0 + \sum_{i=1}^{m} x_i A_i\right) \leq r.$$

We denote by $MR(q, n, m, r)$ this problem. For correct $x_1, \ldots, x_m$, the dimension of the kernel space $\mathrm{Ker}\,(A_0 + \sum_i x_i A_i)$ is at least $n-r$. Hence, when there are $n-r$ bases of the form $\widehat{\mathbf{y}}_i = (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0, y_{1i}, \ldots, y_{ri}), 1 \leq i \leq n-r$ for correct $x_1, \ldots, x_m$, the KS method [17] reduces the Minrank problem to the MQ problem as follows. Regarding $\{x_i\}_{1 \leq i \leq m}$ and $\{y_{ij}\}_{1 \leq i \leq r, 1 \leq j \leq n-r}$ as variables, obtain a quadratic polynomial system called a *KS system* from a relation

$$\left(A_0 + \sum_{i=1}^{m} x_i A_i\right) {}^t\widehat{\mathbf{y}}_j = \mathbf{0}, \quad 1 \leq j \leq c, \tag{2}$$

where $c \leq n - r$. Then the part $x_1, \ldots, x_m$ of its solution gives an answer of the Minrank problem. Here the KS system consists of cn equations in $m + cr$ variables.

For Rainbow parameters v, o_1 and o_2, the matrices $A_{f_1}, \ldots, A_{f_{o_1+o_2}}$ corresponding the central quadratic polynomials (1) are of the form

$$A_{f_i} = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & \text{if } 1 \leq i \leq o_1, \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & \text{if } o_1 + 1 \leq i \leq o_1 + o_2, \end{cases} \tag{3}$$

where $*_{i\times j}$ are i-by-j matrices over $\mathbb{F}$. Since $A_{f_1}, \ldots, A_{f_{o_1}}$ has at most rank $v + o_1$, the matrices $A_{p_1}, \ldots, A_{p_{o_1+o_2}}$ corresponding the public key has a linear combination such that

$$\mathrm{Rank}\left(A_{p_1} + \sum_{i=2}^{o_1+o_2} x_i A_{p_i}\right) \leq v + o_1,$$

where $x_2, \ldots, x_{o_1+o_2} \in \mathbb{F}$, i.e. an instance of $MR(q, v+o_1+o_2, o_1+o_2-1, v+o_1)$. Since ${}^t(1, x_2, \ldots, x_{o_1+o_2})$ correspond to a column of a secret key T, the *MinRank attack* recovers a secret key by repeating this. In the Rainbow case, for $o_2 + 1$ matrices from the public key, we also can obtain these linear combination having rank $v+o_1$. Namely, it suffices to solve an instance of $MR(q, v+o_1+o_2, o_2, v+o_1)$.

2.3 Gröbner basis algorithm

A Gröbner basis algorithm that computes a Gröbner basis for the ideal generated by a given polynomial system was discovered by B. Buchberger [6], and improved as faster algorithms, for example, XL [21], F_4 [12] and F_5 [13]. It is also used as an algorithm for solving a polynomial system and its complexity depends on the solving degree that is the maximal degree in steps which add a new non-zero polynomial during the Gröbner basis algorithm. For example, the complexity of the F_4 algorithm solving a polynomial system in n variables is given by

$$\binom{n + d_{slv}}{d_{slv}}^{\omega},$$

where $2 < \omega \leq 3$ is a linear algebra constant and d_{slv} is the solving degree. Moreover, by using the *hybrid approach* [3] of brute-force search and Gröbner basis algorithm which solves a polynomial system in $n - k$ variables after fixing k variables, the complexity is improved as

$$\min_k \; q^k \cdot \binom{n - k + d_{slv}}{d_{slv}}^{\omega}. \tag{4}$$

The solving degree is important for obtaining the complexity, but is an experimental value. In order to estimate the complexity of solving a large scale polynomial system, we need to find a theoretical value approximating the solving degree. For a semi-regular quadratic system [2, 3], the degree of regularity [2] is well-known as a proxy for the solving degree and is given by the degree D_{reg} of the first term whose coefficient is non-positive in

$$\frac{(1 - t^2)^m}{(1 - t)^n}, \tag{5}$$

where m and n are the number of the equations and the variables of the system, respectively. On the other hand, for a non-semi-regular quadratic system, the first fall degree d_{ff} [11] as a proxy for the solving degree has been investigated. For a given polynomial system, the first fall degree is defined by using its syzygies and captures the first degree at which occurs a non-trivial degree fall during a Gröbner basis algorithm. Since a KS system is non-semi-regular, Verbel et al. [20] discuss its concrete syzygies and give a certain theoretical value as an upper bound for its d_{ff}. In the next section, we explain their complexity estimation for the KS method using this theoretical value.

3 Previous Estimation on the MinRank attack using the KS method

In this section, we explain Verbel et al.'s estimation for the KS method solving Minrank problem and consider a certain parameter in the method. We recall

their complexity estimation in Subsection 3.1 and compare the complexities of F4 and their **y**-XL in Subsection 3.2. Then we investigate the hybrid approach on a KS system in Subsection 3.3.

3.1 Previous estimation for the KS method

In [20], Verbel et al. show that there is a certain non-trivial syzygy of a KS system under their assumption and give an upper bound for the first fall degree d_{ff}. Moreover, they show that the KS system is solved by an XL algorithm called **y**-*XL algorithm* which multiplies only variables $\{y_{ij}\}_{i,j}$ to the equation (2).

For $MR(q, n, m, r)$ such that $m < nr$, i.e. *superdetermined case*, the paper [20] concludes that the complexity of the KS method using **y**-XL algorithm is given by

$$\mathrm{C}_{\mathbf{y}\text{-XL}}(D_{KS}) = \left(m\binom{cr + D_{KS}}{D_{KS}}\right)^{\omega} \tag{6}$$

where $D_{KS} = d_{KS} + 2$, $\max\{\lceil m/(n-r)\rceil, d_{KS}+1\} \leq c \leq n - r$ and

$$d_{KS} = \min_{1\leq d\leq r}\left\{d : \binom{r}{d}n > \binom{r}{d+1}m\right\}. \tag{7}$$

Here $\binom{a}{b} = 0$ for $a < b$. In their limitation on the parameter c of (6), the condition $\lceil m/(n-r)\rceil \leq c$ implies that a KS system is overdetermined, and the condition $d_{KS} + 1 \leq c$ guarantees that a non-trivial degree fall at D_{KS} occurs in a KS system, i.e. $d_{ff} \leq D_{KS}$.

For $MR(q, n, m, r)$, the best complexity from the formula (6) must take the minimum c in their limitation since the definition D_{KS} is independent of c. Namely, $c = \max\{\lceil m/(n-r)\rceil, d_{KS}+1\}$. However, by experiments, the paper [20] mentions that the minimum c is not always the best. Moreover, when $d_{KS} + 1 > c$, the solving degree may increase, but the complexity with such a small c not necessary. Furthermore, when $\lceil m/(n-r)\rceil > c$, i.e. a KS system is underdetermined, we can solve the system after fixing some variables by the hybrid approach (see Subsection 2.3).

3.2 F4 vs y-XL

In this subsection, we explain that our research uses the F4 algorithm rather than the **y**-XL algorithm to investigate a KS system with a widely chosen c.

The complexity of the KS method for $MR(q, n, m, r)$ is given either as the **y**-XL algorithm case from (6), i.e.

$$\mathrm{C}_{\mathbf{y}\text{-XL}}(d_{slv}) = \left(m\binom{cr + d_{slv}}{d_{slv}}\right)^{\omega}, \text{or} \tag{8}$$

the F4 algorithm case

$$\mathrm{C}_{F4}(d_{slv}) = \binom{cr + m + d_{slv}}{d_{slv}}^{\omega}. \tag{9}$$

where $2 < \omega \leq 3$ is a linear algebra constant. Solving degrees d_{slv} of these algorithms are the same in [20], but the complexity of the F4 algorithm is asymptotically better than one of the **y**-XL algorithm for $cr \gg m$. Indeed, for $cr \gg m$, we have

$$\mathrm{C}_{F4}(d_{slv}) \approx (cr+m)^{d_{slv}\omega} \approx (cr)^{d_{slv}\omega} < m^{\omega}(cr)^{d_{slv}\omega} \approx \mathrm{C}_{\mathbf{y}\text{-XL}}(d_{slv}).$$

In an instance from Rainbow, for small c outside Verbel's limitation, there exists a case that the complexity of the **y**-XL algorithm is better than that of the F4 algorithm. Moreover, the termination of the **y**-XL algorithm on an inhomogeneous system is not clear, and its complexity depends on the existence of a non-trivial syzygy on each system and its discussion is delicate except for their superdetermined case. For these reasons, our research uses the F4 algorithm that can be uniformly applied to a KS system with widely chosen c. Thus the purpose of this paper is to find a theoretical value approximating the solving degree of the F4 algorithm and d_{slv} denotes it from here.

3.3 Rainbow parameter set Ia and a certain parameter in the KS method

The assertions in this paper were verified by using the Gröbner basis algorithm F_4 with respect to the graded reverse lexicographic monomial order in Magma V2.24-4 [5] on CPU: 3.2 GHz Intel Core i7.

In this subsection, in order to discuss the parameter c, we take the concrete parameter set $(q, v, o_1, o_2) = (16, 5, 5, 5)$ as a scaled-down Rainbow Ia, and then MinRank attack against it derives $MR(16, 15, 5, 10)$. For the solving degree d_{slv} of the F4 algorithm, Table 1 shows running time and complexities using the formulas (8) and (9). In this case, the KS system satisfies $m = 5 < 15 \cdot 10 = nr$, i.e. superdetermined case which is a target of Verbel et al.'s research. The formula (8) suggests $c = \max\{\lceil m/(n-r) \rceil, d_{KS} + 1\} = 3$ as the best case since $\lceil m/(n-r) \rceil = 1$ and $d_{KS} = 2$. Indeed, Table 1 shows the case $c = 3$ is actually the best. Note that $c = 1$ and 2 derive ovedetermined KS systems since $\lceil m/(n-r) \rceil = 1$ (see Subsection 3.1).

According to Table 2, we see that the case $c = 1$ in Table 1 is different from that for a random instance in $MR(16, 15, 5, 10)$. Then a KS system with $c = 1$ for a random instance is solved faster than for Rainbow, and its complexity is $\mathrm{C}_{F4}(d_{slv}) = 2^{38}$ and $\mathrm{C}_{\mathbf{y}\text{-XL}}(d_{slv}) = 2^{37}$ with $d_{slv} = 6$ which becomes the best in Table 1. Note that, for $c \neq 1$ or the odd characteristic case, such a phenomenon

Table 1: Experiments on a KS system for an instance from Rainbow in $MR(16, 15, 5, 10)$. The complexities $\mathrm{C}_{F4}(d_{slv})$ and $\mathrm{C}_{\mathbf{y}\text{-XL}}(d_{slv})$ are from the equations (8) and (9), respectively, for the solving degree d_{slv} of the F4 algorithm.

c	$\mathrm{C}_{F4}(d_{slv})$ (bits)	$\mathrm{C}_{\mathbf{y}\text{-XL}}(d_{slv})$ (bits)	F4	
			Time (s)	d_{slv}
5	46	50	386.7	4
4	43	47	78.4	4
3	40	43	29.7	4
2	42	44	506.5	5
1	58	52	136.0	12

Table 2: Comparison between KS systems with $c = 1$ for an instance from Rainbow and a random instance in $MR(16, 15, 5, 10)$. Two positive integers k_0 and k_1 are the number of variables fixed in $\mathbf{x}$ and $\mathbf{y}_1$, respectively. The positive integers d_{slv} and d_{ff} are the solving degree and the first fall degree in the F4 algorithm.

# fixed variables		Rainbow		Random	
$\sum_i k_i$	(k_0, k_1)	d_{slv}	d_{ff}	d_{slv}	d_{ff}
0	(0,0)	12	6	6	6
1	(0,1)	6	6	6	6
	(1,0)	5	5	5	5
2	(0,2)	5	5	5	5
	(1,1)	5	4	5	4
	(2,0)	4	4	4	4
3	(0,3)	5	5	5	5
	(1,2)	4	4	4	4
	(2,1)	4	4	4	4
	(3,0)	3	3	3	3

does not occur in our experiments. Table 2 further shows that a KS system with some variables fixed has the same solving degree in both of an instance from Rainbow and a random instance. Hence we expect that the complexity of the KS method is improved by the hybrid approach. In the next section, we introduce a theoretical value for approximating the solving degree and it is available for widely chosen c and the hybrid approach.

4 Theoretical value using a multivariate power series

In this section, we introduce a theoretical value which is available for each KS system and that deduced through the hybrid approach, and show that this value approximates the solving degree. We introduce the theoretical value in Subsection 4.1 and compare with the solving degree of a random instance in Minrank problem with $n = m$ in Subsection 4.2. Moreover, in Subsection 4.3, we show that the theoretical value tightly approximates the solving degree of the best MinRank attack using the KS method against Rainbow.

4.1 Multivariate power series

In this subsection, we show that the top homogeneous component of the KS system has multi-degrees and introduce a theoretical value using its multi-degrees.

Definition 4.1. A commutative ring R is $\mathbb{Z}^s_{\geq 0}$-graded if it satisfies the following two conditions:

1. $R = \bigoplus_{\mathbf{d} \in \mathbb{Z}^s_{\geq 0}} R_{\mathbf{d}}$
2. $R_{\mathbf{d}_1} R_{\mathbf{d}_2} \subseteq R_{\mathbf{d}_1 + \mathbf{d}_2}$

An element $h \in R_{\mathbf{d}}$ is called $\mathbb{Z}^s_{\geq 0}$-homogeneous, and denote $\mathbf{d}$ by $\deg_{\mathbb{Z}^s_{\geq 0}} h$ which is called the $\mathbb{Z}^s_{\geq 0}$-*degree of* h.

The variables of a KS system consists of variable sets $\mathbf{x} = \{x_1, \ldots, x_m\}$ and $\mathbf{y}_i = \{y_{i1}, \ldots, y_{ir}\}$ for $i = 1, \ldots, c$. Then the polynomial ring $\mathbb{F}[\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_c]$ is $\mathbb{Z}^{c+1}_{\geq 0}$-graded by

$$\deg_{\mathbb{Z}^{c+1}_{\geq 0}} x_i = \mathbf{e}_1 \text{ and } \deg_{\mathbb{Z}^{c+1}_{\geq 0}} y_{ij} = \mathbf{e}_{i+1},$$

where $\mathbf{e}_i = (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0)$. A KS system consists of each quadratic polynomials $(h_{i1}, \ldots, h_{in})$ given as a multiplication of $(A_0 + \sum_i x_i A_i)$ by i-th kernel vector $\widehat{\mathbf{y}}_i = (0, \ldots, 0, 1, 0, \ldots, 0, y_{i1}, \ldots, y_{ir})$. Then $h_{i1}, \ldots, h_{in}$ are bilinear polynomials in two variable sets $\mathbf{x}$ and $\mathbf{y}_i$, and we have

$$\deg_{\mathbb{Z}^{c+1}_{\geq 0}} h^{top}_{i1} = \cdots = \deg_{\mathbb{Z}^{c+1}_{\geq 0}} h^{top}_{in} = \mathbf{e}_1 + \mathbf{e}_{i+1},$$

where h^{top}_{ij} are the top homogeneous component of h_{ij} with respect to the total degree. Thus, the top homogeneous component of the KS system is included in $\bigoplus_{j=1}^{c} \mathbb{F}[\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_c]^n_{\mathbf{e}_1 + \mathbf{e}_{j+1}}$ and is $\mathbb{Z}^{c+1}_{\geq 0}$-homogeneous. This fact is also mentioned in [14], but [15] defines a theoretical value using two variable sets $\mathbf{x}$ and $\mathbf{y} := \cup_i \mathbf{y}_i$, as of a $\mathbb{Z}^2_{\geq 0}$-graded system (see Table 3 and Remark 4.3).

For $\mathbb{Z}^s_{\geq 0}$-homogeneous system, we give the following definition:

Definition 4.2. Let $h_1, \ldots, h_m \in \mathbb{F}[\mathbf{x}_1, \ldots, \mathbf{x}_s]$ with $\deg_{\mathbb{Z}^s_{\geq 0}} \mathbf{x}_i = \mathbf{e}_i$ be $\mathbb{Z}^s_{\geq 0}$-homogeneous. Then, putting

$$\sum_{\mathbf{d} \in \mathbb{Z}^s_{\geq 0}} a_{\mathbf{d}} \mathbf{t}^{\mathbf{d}} = \frac{\prod_{i=1}^{m} (1 - \mathbf{t}^{\deg_{\mathbb{Z}^s_{\geq 0}} h_i})}{(1-t_1)^{n_1} \cdots (1-t_s)^{n_s}} \in \mathbb{Z}[[t_1, \ldots, t_s]], \tag{10}$$

we define $D_{mdg} = \inf\{|\mathbf{d}| \mid a_{\mathbf{d}} < 0\} \cup \{\infty\}$ where $\mathbf{d} = (d_1, \ldots, d_s)$ and $\mathbf{t}^{\mathbf{d}} = t_1^{d_1} \cdots t_s^{d_s}$. Moreover, when the top homogeneous component of $f_1, \ldots, f_m$ are $\mathbb{Z}^s_{\geq 0}$-homogeneous, we define $D_{mdg}(f_1, \ldots, f_m) = D_{mdg}(f_1^{top}, \ldots, f_m^{top})$.

Let n, m and r be parameters in Minrank problem. A KS system consists of nr quadratic equations in $rc+m$ variables and its top homogeneous component is included in $\bigoplus_{j=1}^{c} \mathbb{F}[\mathbf{x}, \mathbf{y}_1, \ldots, \mathbf{y}_c]^n_{\mathbf{e}_1 + \mathbf{e}_{j+1}}$ where $\mathbf{x} = \{x_1, \ldots, x_m\}$ and $\mathbf{y}_i = \{y_{i1}, \ldots, y_{ir}\}$. Then, the multivariable series (10) in Definition 4.2 is

$$\frac{\prod_{i=1}^{c} (1 - t_0 t_i)^n}{(1-t_0)^m (1-t_1)^r \cdots (1-t_c)^r}. \tag{11}$$

When the KS system is underdetermined, i.e. $nr < rc + m$, we fix $rc + m - nr$ variables and solve the resulting system. Furthermore, the hybrid approach fixes more variables in the system and solves it. When denote by k_0 and k_i the number of fixed variables in $\mathbf{x}$ and $\mathbf{y}_i$ by the hybrid approach, respectively, we modify the multivariable series (11) to

$$\frac{\prod_{i=1}^{c} (1 - t_0 t_i)^n}{(1-t_0)^{m-k_0} (1-t_1)^{r-k_1} \cdots (1-t_c)^{r-k_c}}, \tag{12}$$

where $k_0 < m$ and $k_i < r$.

4.2 Experiments on random instances

For $i \geq 1$, let k_0 and k_i be the number of fixed variables in $\mathbf{x}$ and $\mathbf{y}_i$ by the hybrid approach on a KS system, respectively, and denote this case by $(k_0, k_1, \ldots, k_c)$.

Table 3 shows that the state of D_{mgd} introduced in Subsection 4.1 for overdetermined KS systems of random instances of Minrank problem with $n = m$ as a case mentioned in [20]. In this case, D_{mgd} is an upper bound for the solving degree d_{slv}. The value D_{bi} (see Remark 4.3) and D_{reg} (see Subsection 2.3) are available for each c, but Table 3 shows that they more overestimate the solving degree. Note that $d_{ff} \leq D_{KS} (= d_{KS} + 2)$ is actually guaranteed on $\max\{\lceil 8/(8-r) \rceil, d_{KS} + 1\} \leq c \leq 8 - r$ (see Subsection 3.1). Moreover, Table 4 is for underdetermined KS systems from $MR(31, 8, 8, 5)$ in Table 3, i.e. $c = 1, 2$. Then note that Verbel et al.'s D_{KS} does not depend on c and is five always. By growing the number of fixed variables, our D_{mgd} tightly approximates the solving degree d_{slv}.

Table 3: Experiments on overdetermined KS systems not fixing variables from random instances of $MR(13, 8, 8, r)$. The experimental values d_{slv} and d_{ff} are the solving degree and the first fall degree in the F4 algorithm. The theoretical values D_{mgd} and D_{DK} are decided by the power series (11) and the formula (7), respectively. The value D_{bi} is $\min\{8, rc\} + 1$ in [15] (see Remark 4.3). The value D_{reg} is decided by the power series (5) if a KS system is semi-regular.

r	c	D_{mgd}	d_{slv}	d_{ff}	D_{KS}	D_{bi}	D_{reg}
5	3	7	6	5	5	9	13
4	4	6	4	4	4	9	8
	3	6	4	4	4	9	8
	2	6	6	4	4	9	17
3	5	5	4	4	4	9	6
	4	5	4	4	4	9	6
	3	5	4	4	4	9	6
	2	5	4	4	4	7	7

r	c	D_{mgd}	d_{slv}	d_{ff}	D_{KS}	D_{bi}	D_{reg}
2	6	4	3	3	3	9	4
	5	4	3	3	3	9	4
	4	4	3	3	3	9	5
	3	4	3	3	3	7	5
	2	4	3	3	3	5	5

Table 4: The hybrid approach on underdetermined KS systems with $c = 1, 2$ from random instances of $MR(13, 8, 8, 5)$. Two positive integers k_0 and k_i are the number of variables fixed in $\mathbf{x}$ and $\mathbf{y}_i$, respectively. The experimental values d_{slv} and d_{ff} are the solving degree and the first fall degree in the F4 algorithm. The theoretical value D_{mgd} is deduced by the power series (12). The value D_{reg} is decided by the power series (5) at $n = 21 - \sum_i k_i$ if a KS system is semi-regular after fixing $\sum_i k_i$ variables.

c	(k_0, k_1, k_2)	D_{mgd}	d_{slv}	d_{ff}	D_{reg}
2	(0,2,0)	6	6	5	17
	(0,1,1)	6	6	4	17
	(1,1,0)	6	6	5	17
	(2,0,0)	6	5	5	17
	(0,3,0)	4	5	4	9
	(0,2,1)	5	5	4	9
	(1,2,0)	5	5	5	9
	(1,1,1)	6	5	4	9
	(2,1,0)	5	5	5	9
	(3,0,0)	5	5	4	9

c	(k_0, k_1)	D_{mgd}	d_{slv}	d_{ff}	D_{reg}
1	(1,4)	2	3	2	9
	(2,3)	3	4	3	9
	(3,2)	4	4	4	9
	(4,1)	5	5	5	9
	(5,0)	4	4	4	9
	(2,4)	2	2	2	5
	(3,3)	3	3	3	5
	(4,2)	3	3	3	5
	(5,1)	3	3	3	5
	(6,0)	3	3	3	5

Remark 4.3. The paper [14] mentions that a KS system has a multi-degree, but this property uses as a bi-degree in [15]. Then the solving degree is bounded by the minimum number of each variable set plus one, i.e. $\min\{m, rc\} + 1$ for parameters n, m and r of Minrank problem. Although this bound is far from the solving degree in Table 4, not for an instance from the MinRank attack against Rainbow. In fact, in Table 6 for a scaled-down Rainbow parameter set III/V, we have $\min\{m, rc\} + 1 = \min\{o, (3o - 4)c\} + 1 = o + 1 > o = d_{slv}$ at the best $c = 2$.

4.3 Experiments on instances from Rainbow

By using D_{mgd} introduced in Subsection 4.1, the complexity of the MinRank attack using the KS method against Rainbow with parameter set (q, v, o_1, o_2) is given by

$$\mathrm{C}_{HybF4}(D_{mgd}) = \min_{(k_0,k_1,\ldots,k_c)} q^k \cdot o_1 \cdot \binom{c(v+o_1)+o_2-k+D_{mdg}}{D_{mdg}}^{\omega}, \quad (13)$$

where $k = \sum_{i=0}^{c} k_i$, $2 < \omega \leq 3$ is a linear algebra constant and D_{mdg} is the minimum total degree of the terms whose coefficient is negative in the multivariable series (12) at $n = v + o_1 + o_2$ and $r = v + o_1$. Then, since $\lceil m/(n-r) \rceil = \lceil o_i/(v + 2o_i - (v + o_i)) \rceil = 1$, a KS system is always overdetermined (see Subsection 3.1).

For scaled-down Rainbow Ia instances, our experiments show that the case $(k_0, k_1) = (o_i - 1, 0)$ gives the best complexity and $\mathrm{C}_{HybF4}(d_{slv}) = \mathrm{C}_{HybF4}(D_{mdg})$. In particular, the case avoids the complicated case $(k_0, k_1) = (0, 0)$ at $c = 1$ mentioned in Subsection 3.3 (see Table 2). For any $(k_0, 0)$ with $k_0 \gg 0$, Table 5 shows that $d_{slv} = D_{mgd}$ holds always.

Table 5: The hybrid approach with $(k_0, 0)$ on a KS system for an instance from Rainbow in $MR(16, 3o, o, 2o)$ where $\lfloor o/2 \rfloor \leq k_0 \leq o - 1$. The theoretical value D_{mgd} is deduced by the power series (12). The experimental value d_{slv} is the solving degree in the F4 algorithm. The positive integer k_0 is the number of variables fixed in $\mathbf{x}$.

o	7				8				9					10				
k_0	3	4	5	6	4	5	6	7	4	5	6	7	8	5	6	7	8	9
D_{mgd}	5	4	3	2	5	4	3	2	5	4	4	3	2	5	4	4	3	2
d_{slv}	5	4	3	2	5	4	3	2	5	4	4	3	2	5	4	4	3	2

For scaled-down Rainbow IIIc/Vc instances, our experiments show that the best complexity $C_{HybF4}(d_{slv})$ is given by $(k_0, k_1, k_2) = (0, 0, 0)$ at $c = 2$, and namely does not fix a variable in the KS system. In this case, our experiments always show that $d_{slv} = D_{mgd}$ holds (see Table 6). However, by the same reason as Subsection 3.3, note that $\mathrm{C}_{HybF4}(d_{slv}) > \mathrm{C}_{HybF4}(D_{mdg})$ if we consider the complicated case $(k_0, k_1) = (0, 0)$. Thus, in this case, we need to use the formula (13) with $(k_1, \ldots, k_c) \neq (0, 0)$ and then have $\mathrm{C}_{HybF4}(d_{slv}) = \mathrm{C}_{HybF4}(D_{mdg})$.

Since $\lceil m/(n-r) \rceil = 1$, Verbel et al.'s limitation on c is $c \geq d_{KS} + 1$ (see Subsection 3.1). The cases $o = 4$ and 5 in Table 6 show that the complexity at $c = 2$ is better than that at $c = d_{KS} + 1 = 3$ as the minimum in their limitation. Since the best complexity for Rainbow takes $c = 1, 2$, it is worth introducing our D_{mgd} being available for a smaller c than $d_{KS} + 1$.

Table 6: Experiments on a KS system with $(k_0, k_1, \ldots, k_c) = (0, 0, \ldots, 0)$ for an instance from Rainbow in $MR(256, 4o-4, o, 3o-4)$. The theoretical values D_{mgd} and D_{KS} are deduced by the power series (12) and the formula (7). The experimental value d_{slv} is the solving degree in the F4 algorithm, and the value $\mathrm{C}_{F4} = \mathrm{C}_{HybF4}(d_{slv})$ is deduced by the formula (13). The case $c = 1$, i.e. $(k_0, k_1) = (0, 0)$, is a complicated mentioned in Subsection 3.3.

$o = 3$				C_{F4}
c	D_{mgd}	D_{KS}	d_{slv}	(bits)
1	4	3	6	28
2	3	3	3	**22**
3	3	3	3	25

$o = 4$				C_{F4}
c	D_{mgd}	D_{KS}	d_{slv}	(bits)
1	5	4	9	44
2	4	4	4	**33**
3	4	4	4	37
4	4	4	4	40

$o = 5$				C_{F4}
c	D_{mgd}	D_{KS}	d_{slv}	(bits)
1	6	4	13	63
2	5	4	5	**43**
3	5	4	5	48
4	5	4	4	44
5	5	4	4	47

5 Complexity estimation

In this section, by using the observation in Subsection 4.3, we gives the complexity estimation for the MinRank attack using the KS method against Rainbow parameter set Ia, IIIc and Vc proposed in NIST PQC standardization project.

Table 7 shows the known security analysis of the proposed Rainbow parameter set where, due to the NIST specification, the number of gates satisfies

$$\gamma := \sharp \text{ gates}/\sharp \text{ field multiplications} = (2 \cdot \log_2(q)^2 + \log_2(q)).$$

Table 7: Complexities ($\log_2(\sharp$classical gates)) of known attacks against Rainbow (from tables of Section 7.2 in [10])

parameter set	(q, v, o_1, o_2)	direct	Minrank	HighRank	UOV	RBS
Ia	$(16, 32, 32, 32)$	164.5	161.3	150.3	149.2	**145.0**
IIIc	$(256, 68, 36, 36)$	**215.2**	585.1	313.9	563.8	217.4
Vc	$(256, 92, 48, 48)$	**275.4**	778.8	411.2	747.4	278.6

Assume that D_{mgd} introduced in Section 4 bounds the solving degree d_{slv} except for the complicated case $(k_0, k_1) = (0, 0)$ (see Subsection 3.1). Then the complexity of the KS modeling of MinRank attack against Rainbow with parameters q, v, o_1 and o_2 is given by

$$\min_{(k_0,k_1,\ldots,k_c)\neq(0,0)} q^k \cdot o_1 \cdot \binom{c(v+o_1) + o_2 - k + D_{mdg}}{D_{mdg}}^{\omega},$$

where $k = \sum_{i=1}^{c} k_i$, $2 < \omega \leq 3$ is a linear algebra constant and D_{mdg} is the minimum total degree of the terms whose coefficient is negative in the multivariable series (12), i.e.

$$\frac{\prod_{i=1}^{c}(1-t_0t_i)^{v+o_1}}{(1-t_0)^{o_2-k_0}(1-t_1)^{v+o_1-k_1}\cdots(1-t_c)^{v+o_1-k_c}}.$$

The complexity at $(k_0, k_1) = (31, 0)$ for Rainbow parameter set Ia has $D_{mdg} = 2$ and $\gamma = 36$ and is

$$16^{31} \cdot 32 \cdot \binom{64+32-31+2}{2}^{2.376} \cdot 36 \lesssim 2^{160.6}.$$

Here we took $\omega = 2.376$ as a linear algebra constant. Moreover, the complexity at $(k_0, k_1, k_2) = (0, 0, 0)$ for Rainbow parameter set IIIc has $D_{mdg} = 30$ and $\gamma = 136$ and is

$$36 \cdot \binom{2 \cdot 72 + 36 + 30}{30}^{2.376} \cdot 136 \lesssim 2^{327.9}.$$

The complexity for Rainbow parameter set Vc has $D_{mgd} = 40$ and is

$$48 \cdot \binom{2 \cdot 96 + 48 + 40}{40}^{2.376} \cdot 136 \lesssim 2^{437.0}.$$

Hence our D_{mgd} shows that the MinRank attack using the KS method is the best among MinRank attacks investigated in Table 7. Furthermore, we confirm that, for $(k_0, k_1) = (o_i - 1, 0)$ at $c = 1$ and $(k_0, k_1, k_2) = (0, 0, 0)$ at $c = 2$, the **y**-XL algorithm terminates within the solving degree d_{slv} of the F4 algorithm. Then, due to the smallness of the parameter c, the complexities of the attack using the **y**-XL algorithm for Rainbow parameter sets Ia, IIIc and Vc above are slightly improved as $2^{160.5}$, $2^{324.8}$ and $2^{430.0}$, respectively, where

$$\min_{(k_0,k_1,\ldots,k_c)\neq(0,0)} q^k \cdot o_1 \cdot \left((o_2 - k) \cdot \binom{c(v+o_1) + D_{mdg}}{D_{mdg}}\right)^{\omega}.$$

By Verbel et al.'s estimation using D_{KS}, the complexities of the attack at $c = \max\{\lceil m/(n-r)\rceil, d_{KS}+1\}$ and $(k_0, \ldots, k_c) = (0, \ldots, 0)$ for the parameter sets Ia, IIIc and Vc are $2^{329.2}$, $2^{457.9}$ and $2^{624.9}$, respectively.

In the third round for NIST PQC standardization project, the Rainbow parameter sets I, III and V are planed as $(q, v, o_1, o_2) = (16, 36, 32, 32)$, $(256, 68, 32, 48)$ and $(256, 96, 36, 64)$. For scaled-down models for I, the best case is given by $(k_0, k_1) = (o_i - 1, 0)$. For scaled-down models for III/V, the best case is given by $(k_0, k_1, k_2) = (0, 0, 0)$ or $(k_0, k_1) = (1, 0)$. Our experiments show $D_{mgd} = d_{slv}$ in each cases and, for larger instances of parameter sets III/V, the value D_{mgd} at $(k_0, k_1, k_2) = (0, 0, 0)$ is better than at $(k_0, k_1) = (1, 0)$. Then these complexities of the MinRank attack using the KS method against the parameter sets I, III and V are $2^{161.0}$, $2^{373.1}$ and $2^{469.7}$, respectively. Namely, we can confirm that Rainbow in this case is also secure from the attack.

6 Conclusion

In this paper, we investigated a KS systems that is a quadratic system solved in the Kipnis-Shamir (KS) method for Minrank problem and, in particular, it from the MinRank attack using the KS method against Rainbow. The previous estimation by Verbel et al. gave a precise analysis for non-trivial syzygies on some KS systems, but is not an analysis for each KS system. Actually, our experiments on a Minrank instance from Rainbow showed a case that a certain KS system which has not been not estimated by them is better.

In order to estimate the complexity of solving each KS system, we introduced theoretical value D_{mgd} using such a multi-degree as a KS system has, and saw that this is available for each KS system and that deduced through the hybrid approach. We showed that D_{mgd} approximates the solving degree of a KS system and, in particular, coincides with the solving degree deducing the best complexity of the MinRank attack using the KS method against Rainbow. Consequently, by using our estimation, the complexities of the MinRank attack using the KS method against Rainbow parameter sets Ia, IIIc and Vc are improved as $2^{160.6}$, $2^{327.9}$ and $2^{437.0}$, respectively which are the best among MinRank attacks investigated in NIST PQC 1st round. Moreover, for the planed parameter sets I, III and V in NIST PQC 3rd round, the complexities of the attack are $2^{161.0}$, $2^{373.1}$ and $2^{469.7}$, respectively, and we was able to confirm that Rainbow is secure from the attack.

In this paper, in order to estimate the complexity of several KS systems, we used the F4 algorithm and showed that solving very small KS systems are better for Rainbow. Then, we can expect that the $\mathbf{y}$-XL algorithm is better than the F4 algorithm and that using the known complexity estimation of the Wiedemann XL algorithm improves the complexity of the method. However, since a Macaulay matrix from a KS system has a large kernel space, we need to decide the complexity of the Wiedemann algorithm up to obtaining a solution of a KS system as future work.

References

[1] Shallit, J.O., Frandsen, G.S. and Buss., J.F.: The Computational Complexity of some Problems of Linear Algebra. BRICS series report, Aarhus, Denmark, RS-96-33.

[2] Bardet, M., Faugère, J.C. and Salvy, B.: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations, In: Proc. International Conference on Polynomial System Solving (ICPSS), pp. 71–75 (2004).

[3] Bettale, L., Faugère, J. C. and Perret, L.: hybrid approach for solving multivariate systems over finite fields. J. Math. Crypt., vol. 3, pp. 177–197 (2009).

[4] Bettale, L., Faugère, J. and Perret, L.: Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Des. Codes Cryptogr. vol. 69, pp. 1–52 (2013).

[5] Bosma, W., Cannon, J. and Playoust, C.: The Magma algebra system. I. The user language, J. Symbolic Comput. **24**, 235–265 (1997)

[6] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. PhD thesis, Universität Innsbruck (1965)

[7] Casanova, A., Faugere, J.-C., Macario-Rat, G., Patarin, J., Perret, L., Ryckeghem, J.: G*e*MSS: A Gr*e*at Multivariate Short Signature. Specification document of NIST PQC 2nd round submission package (2019) `https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification_round2.pdf`

[8] Courtois, N.: Decoding Linear and Rank-Distance Codes, Minrank problem and Multivariate Cryptanalysis. In: CLC 2006, Darmstadt, September (2006).

[9] Ding, J. and Schmidt, D. S.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A. D., Yung, M. (eds.) ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005).

[10] Ding, J., Chen, M.-S., Petzoldt, A., Schmidt, D., Yang, B.-Y.: Rainbow - Algorithm Specification and Documentation. Specification document of NIST PQC 2nd round submission package (2019)

[11] Dubois, V., Gama, N.: The degree of regularity of HFE systems. In: Abe, M. (ed.) ASIACRYPT 2010, LNCS, vol. 6477, pp. 557–576. Springer, Berlin (2010).

[12] Faugère, J. C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure App. Algebra, **139**(1), 61–88 (1999)

[13] Faugère, J. C.: A new efficient algorithm for computing Gröbner Bases without reduction to zero (F5). In: Bose, P., Morin, P. (eds.) ISSAC 2002, pp. 75–83. (2002).

[14] Faugère, J.C., Levy-dit-Vehel, F. and Perret, L.: Cryptanalysis of Minrank. CRYPTO 2008, pp. 280–296 (2008).

[15] Faugère, J.C., El Din, M.S., and Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. ISSAC 2010, pp. 257–264 (2010).

[16] Goubin, L. and Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In Advances in Cryptology ASIACRYPT 2000, LNCS, vol. 1976, pp. 44–57. Springer (2000).

[17] Kipnis, A., Shamir, A.: Cryptanalysis of the Oil and Vinegar signature scheme. In: Krawczyk H. (ed.) CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998).

[18] Nakamura, S., Ikematsu, Y., Wang, Y., Ding, J. and Takagi, T.: New Complexity Estimation on the Rainbow-Band-Separation Attack, IACR Cryptology ePrint Archive, Report 2020/703 (2020). `https://eprint.iacr.org/2020/703.pdf`

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

[20] Verbel, J., Baena, J., Cabarcas, D., Perlner, R. and Smith-Tone, D.: On the Complexity of "Superdetermined" Minrank Instances, IACR Cryptology ePrint Archive, Report 2019/731 (2019). `https://eprint.iacr.org/2019/731.pdf`

[21] Yang, B.-Y. and Chen, J.-M.: All in the XL family: Theory and practice. In: Park, C., Chee, S. (eds.) ICISC 2004, LNCS, vol. 3506, pp. 67–86. Springer, Heidelberg (2007)