Computer Security Symposium 2020
26 - 29 October 2020

# New Complexity Estimation on the Rainbow-Band-Separation Attack

Shuhei Nakamura[1,a)] Yasuhiko Ikematsu[2] Yacheng Wang[†1] Jintai Ding[†2]
Tsuyoshi Takagi[†1]

**Abstract:** Multivariate public key cryptography is a candidate for post-quantum cryptography, and it allows generating particularly short signatures and fast verification. The Rainbow signature scheme proposed by J. Ding and D. Schmidt is such a multivariate cryptosystem and is considered secure against all known attacks. The Rainbow-Band-Separation attack recovers a secret key of Rainbow by solving certain systems of quadratic equations, and its complexity is estimated by the well-known indicator called the degree of regularity. However, the degree of regularity generally is larger than the solving degree in experiments, and an accurate estimation cannot be obtained. In this paper, we propose a new indicator for the complexity of the Rainbow-Band-Separation attack using the $F_4$ algorithm, which gives a more precise estimation compared to one using the degree of regularity. This indicator is deduced by the two-variable power series

$$\frac{\prod_{i=1}^{m}(1-t_1^{d_{i1}}t_2^{d_{i2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}},$$

which coincides with the one-variable power series at $t_1 = t_2$ deriving the degree of regularity. By considering this relation and our indicator, we obtain a new complexity estimation for the Rainbow-Band-Separation attack. Consequently, we are able to understand the precise security of Rainbow against the Rainbow-Band-Separation attack using the $F_4$ algorithm.

**Keywords:** Multivariate public key cryptography, Rainbow-Band-Separation attack, degree of regularity

## 1. Introduction

Standard RSA and EC cryptosystems are designed based on difficult mathematical problems such as prime factorization and discrete logarithm problems. However, these mathematical problems are known to be solved in polynomial time by a large scale quantum computer. Therefore, it is required to construct cryptography that is based on new mathematical problems and is resistant to quantum computers. Such cryptography is referred to as post-quantum cryptography. In 2015, National Security Agency (NSA) announced a plan of a transition to post-quantum cryptography, and National Institute of Standards and Technology (NIST) started a public recruitment of such cryptography candidates in 2016 [23].

Multivariate public key cryptography [10] is based on an NP-hard problem of solving a system of quadratic equations, that is called the MQ problem [18]. It is especially expected to have potential in building post-quantum signature schemes. Rainbow is a multivariate signature scheme proposed by J. Ding and D. Schmidt in 2005 [9]. This signature scheme can be implemented simply and efficiently using linear algebra methods over a small finite field, and in particular produces shorter signatures than those of RSA and other post-quantum signature schemes [13]. In NIST Post-Quantum Cryptography (PQC) 2nd round, secure Rainbow parameter sets are proposed and several attacks against them are analyzed [13]. In particular, the Rainbow-Band-Separation (RBS) attack [11] is the best among known attacks against Rainbow with a certain parameter set and is important.

Previous estimation methods [13], [29] for the complexity of the RBS attack use the *degree of regularity* [1], [2] as its indicator under the assumption that the system of quadratic equations solved in the attack is *semi-regular* (see [1] for the definition). For a semi-regular system, the degree of regularity is given as the degree $D_{reg}$ of the first term whose coefficient is non-positive in the power series

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

where $m$ and $n$ are the numbers of equations and variables, respectively. Since a public quadratic system solved in the

[1] Department of Liberal Arts and Basic Sciences, Nihon University, Japan
[2] Institute of Mathematics for Industry, Kyushu University, Japan
[†1] Presently with Department of Mathematical Informatics, University of Tokyo, Japan
[†2] Presently with Department of Mathematical Sciences, University of Cincinnati, USA
[a)] nakamura.shuhei@nihon-u.ac.jp

direct attack is often semi-regular, the complexity estimation of the direct attack uses the degree of regularity [2], [13]. However, by our experiments, the quadratic system solved in the RBS attack is non-semi-regular. Therefore, it is important to find an optimal indicator for estimating the complexity of the RBS attack.

### 1.1 Our Contributions

The purpose of this paper is to give a more precise complexity estimation for the RBS attack. Since the attack solves a certain quadratic system whose solving complexity dominates the overall attack, that we call a *RBS dominant system*, we need to estimate the complexity of a *Gröbner basis* algorithm solving this system. In particular, for estimating the complexity, this paper considers (theoretical) indicators approximating its *solving degree*, that the maximal degree in steps which add a new non-zero polynomial during the Gröbner basis algorithm $F_4$ [15]. As mentioned above, previous estimation methods have used the degree of regularity as its indicator. However, an RBS dominant system is solved faster than a semi-regular system, and its solving degree is lower than the degree of regularity. These are probably caused by the fact that an RBS dominant system has a relation between its variables which is said to be *bi-graded*.

In this paper, we consider a polynomial $h$ in $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ graded by

$$(d_1, d_2) = (\deg_{x_1,\ldots,x_{n_1}} h, \deg_{y_1,\ldots,y_{n_2}} h) \in \mathbb{Z}^2_{\geq 0}$$

which is called a *bi-graded* polynomial, such as a bilinear polynomial graded by $(1, 1)$. Then, for a bi-graded polynomial system $(h_1, \ldots, h_m)$, we introduce a new indicator $D_{bgd}$ that is defined as the minimum total degree of the terms whose coefficient are negative in the two-variable power series

$$\frac{\prod_{i=1}^{m}(1 - t_1^{d_{i1}} t_2^{d_{i2}})}{(1 - t_1)^{n_1}(1 - t_2)^{n_2}}. \tag{2}$$

For a Rainbow parameter set $(v, o_1, o_2)$, the top homogeneous component of an RBS dominant system consists of $v + o_1 + o_2 - 1$ bilinear polynomials and $o_1 + o_2$ quadratic homogeneous polynomials in $v + o_1$ and $o_2$ variables. Namely, RBS dominant systems are bi-graded. By our experiments using $F_4$ on RBS dominant systems with $v = o_i$ and $v \lesssim 2o_i$ $(i = 1, 2)$, we show that our new indicator $D_{bgd}$ tightly approximates the solving degree of the system than the degree of regularity $D_{reg}$. Note that the one-variable power series (1) deriving the previous indicator $D_{reg}$ is the same as the two-variable power series (2) at $t = t_1 = t_2$. Hence, we can expect a relation $D_{bgd} \leq D_{reg}$ since $t^{D_{reg}}$ in the series (1) has a negative coefficient in our experiments, which deduces one of $t_1^{d_1} t_2^{d_2}$ in the series (2) where $d_1 + d_2 = D_{reg}$.

By using our indicator, we can obtain a new complexity estimation for the RBS attack using $F_4$. Consequently, we are able to understand the precise security of Rainbow against the RBS attack using $F_4$.

Our work is independent of the paper [25] which was submitted to the Cryptology ePrint Archive (`https://eprint.iacr.org`) one day before the preprint version [24] of this paper.

### 1.2 Organization

This paper is organized as follows. In Section 2, we explain Rainbow and the RBS attack. In Section 3, we explain the previous complexity estimation of the RBS attack using the degree of regularity and present experiments for scaled down Rainbow parameter sets in NIST PQC 2nd round. In Section 4, we introduce a new indicator for estimating the complexity of the RBS attack and demonstrate that this indicator more tightly approximates the solving degree of the quadratic system solved in the attack. In Section 5, by using our indicator, we give a new complexity estimation for the RBS attack. In Section 6, we conclude the results.

## 2. The Rainbow Signature Scheme

In this section, we briefly explain the Rainbow signature scheme and several attacks against it. We explain Rainbow in Subsection 2.1 and its parameter sets in Subsection 2.2. In Subsection 2.3, we describe the Rainbow-Band-Separation (RBS) attack in detail.

### 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.

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 the equations (3) where $g^{(j)}$ and $l_i^{(j)}$ are randomly chosen quadratic polynomials and linear polynomials, respectively.

$$\begin{cases} f_1 = & g^{(1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(1)}(\mathbf{x}) y_i, \\ & \vdots \\ f_{o_1} = & g^{(o_1)}(\mathbf{x}) + \sum_{i=1}^{o_1} l_i^{(o_1)}(\mathbf{x}) y_i, \\ f_{o_1+1} = & g^{(o_1+1)}(\mathbf{x},\mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+1)}(\mathbf{x},\mathbf{y}) z_i, \\ & \vdots \\ f_{o_1+o_2} = & g^{(o_1+o_2)}(\mathbf{x},\mathbf{y}) + \sum_{i=1}^{o_2} l_i^{(o_1+o_2)}(\mathbf{x},\mathbf{y}) z_i, \end{cases} \tag{3}$$

### 2.2 Parameters of Rainbow

In this subsection, we briefly explain several attacks against Rainbow.

The central map of Rainbow with a parameter set $(v, o_1, o_2)$ can be regard as a UOV [20] instance with the parameter set $(v + o_1, o_2)$. Hence the UOV attack [19] is available as an attack against Rainbow, and we have to take the Rainbow parameter set such that

$$v + o_1 \approx s o_2 \ (s = 2, 3, 4, \dots).$$

We can also consider attacks using the special structure of the Rainbow central map (3) above. The HighRank attack [7] and the MinRank attack [3] are such attacks. Due to influences of the UOV attack and the HighRank attack, we set

$$o_1 = o_2.$$

Moreover, for a public key $P$ and a given message $\mathbf{b}$, the direct attack [2] forges a signature by solving $P(\mathbf{x}) = \mathbf{b}$ directly. Complexity estimations for the direct attack and the RBS attack [11], which also solves a certain quadratic system to recovery a secret key (see Subsection 2.3 for detail), are important in deciding concrete parameters $v, o_1$ and $o_2$. In this paper, we assume $o_1 = o_2$ implicitly and consider a parameter set with $v = o_i$ or $v \lesssim 2o_i$ $(i = 1, 2)$.

NIST PQC standardization project [23] gives six security categories (see Table 1). Here, due to the NIST specification, the number of gates is given by

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

**Table 1** NIST security categories (Table 10 in [13])

| category | $\log_2$ classical gates | $\log_2$ quantum gates |
|---|---|---|
| I | 143 | 130/106/74 |
| II | 146 | |
| III | 207 | 193/169/137 |
| IV | 210 | |
| V | 272 | 258/234/202 |
| VI | 274 | |

Table 2 shows the Rainbow parameter sets Ia, IIIc and Vc [13] proposed in NIST PQC 2nd round and the complexities of the above attacks. Here, the bold numbers in Table 2 mean the best complexity of attacks in each parameter set. Table 2 shows that the direct attack is the best among attacks against the parameter sets IIIc and Vc in classical gates. The parameter sets Ia, IIIc and Vc are designed to satisfy the NIST security categories I, III/IV and V/VI in Table 1, respectively [13].

**Table 2** Complexities ($\log_2(\sharp$classical gates)) of known attacks against Rainbow parameter sets $(q, v, o_1, o_2) =$ Ia: $(16, 32, 32, 32)$, IIIc: $(256, 68, 36, 36)$ and Vc: $(256, 92, 48, 48)$ (from tables of Section 7.2 in [13])

| Type | direct | MinRank | HighRank | UOV | RBS |
|---|---|---|---|---|---|
| Ia | 164.5 | 161.3 | 150.3 | 149.2 | **145.0** |
| IIIc | **215.2** | 585.1 | 313.9 | 563.8 | 217.4 |
| Vc | **275.4** | 778.8 | 411.2 | 747.4 | 278.6 |

### 2.3 Rainbow-Band-Separation Attack

In this subsection, we describe the Rainbow-Band-Separation (RBS) attack [11] and a certain quadratic system solved in the attack which are subjects of our research in this paper. For simplicity, we assume that the characteristic of $\mathbb{F}$ is odd in this subsection. We then use the symmetric matrix representation of a quadratic homogeneous polynomial.

Let $(v, o_1, o_2)$ be a Rainbow parameter set and put $n = v + o_1 + o_2$ and $m = o_1 + o_2$. For a Rainbow public key $P = (p_1, \dots, p_m)$, the RBS attack recovers its secret key $(T, F, S)$ as follows. By the definition (3) of the central map $F = (f_1, \dots, f_m)$, each matrix corresponding to $f_i$ has the following form:

$$M_{f_i} = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & \text{if } 1 \le i \le o_1, \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & \text{if } o_1 + 1 \le i \le o_1 + o_2. \end{cases} \tag{4}$$

Here, $*_{k\times l}$ mean $k$-by-$l$ matrices over $\mathbb{F}$. Similarly, the matrices corresponding to $S$ and $T$ can be written as follows:

$$M_S = \begin{pmatrix} I_v & 0_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & I_{o_1} & 0_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & I_{o_2} \end{pmatrix}, \quad M_T = \begin{pmatrix} I_{o_1} & 0_{o_1\times o_2} \\ *_{o_2\times o_1} & I_{o_2} \end{pmatrix}. \tag{5}$$

If $S$ and $T$ are taken as random invertible linear maps, then $M_S$ and $M_T$ cannot be written as in the form (5). However, it is known that the security of Rainbow does not decrease, even if $S$ and $T$ are took as in the form (5). Therefore, $S$ and $T$ in [11] are set to be in the form (5), which induces a reduction in the secret key size. The matrices $M_{p_1}, \dots, M_{p_m}$ corresponding to the public polynomials $p_1, \dots, p_m$ are given as

$$(M_{p_1}, \dots, M_{p_m}) = (M_S {M_{f_1}}^t M_S, \dots, M_S {M_{f_m}}^t M_S) M_T. \tag{6}$$

By the form (5), there exists an $n$-by-1 vector $\mathbf{s} = (\lambda_1, \dots, \lambda_{v+o_1}, 0, \dots, 0, 1)$ such that $\mathbf{s} \cdot M_S = (0, \dots, 0, 1)$. Then, for $i = 1, \dots, m$, we have

$$\mathbf{s} \cdot M_S {M_{f_i}}^t M_S \cdot {}^t\mathbf{s} = (0, \dots, 0, 1) \cdot M_{f_i} \cdot {}^t(0, \dots, 0, 1) = 0.$$

Since each $M_{p_k}$ is a linear combination of $M_S {M_{f_1}}^t M_S$, $\dots$, $M_S {M_{f_m}}^t M_S$, we obtain

$$\mathbf{s} \cdot M_{p_k} \cdot {}^t\mathbf{s} = 0, \quad k = 1, \ldots, m. \tag{7}$$

By the form (5), there exists an $m$-by-1 vector $\mathbf{t} = (1, 0 \ldots, 0, \lambda_{v+o_1+1}, \ldots, \lambda_{v+o_1+o_2})$ such that $M_T \cdot {}^t\mathbf{t} = {}^t(1, 0, \ldots, 0)$. Then, multiplying the equation (6) by ${}^t\mathbf{t}$, we get

$$M_{p_1} + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} M_{p_{o_1+i}} = M_S {M_{f_1}}^t M_S.$$

Moreover, multiplying this equation by $\mathbf{s}$, we have

$$\mathbf{s}\cdot M_{p_1} + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} \mathbf{s}\cdot M_{p_{o_1+i}} = \mathbf{s}\cdot M_S {M_{f_1}}^t M_S = (0, \ldots, 0).$$

Thus, we have the following equations

$$\mathbf{s}\cdot M_{p_1}\cdot {}^t\mathbf{e}_k + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} \mathbf{s}\cdot M_{p_{o_1+i}} \cdot {}^t\mathbf{e}_k = 0, \quad k = 1, \ldots, n-1, \tag{8}$$

where $\mathbf{e}_k$ is the $n$-by-1 vector $(0, \ldots, 0, \overset{k}{1}, 0, \ldots, 0)$. Here, we remove the case $k = n$, since the equation (8) for $k = n$ follows from the equation (7).

Since $\mathbf{s} = (\lambda_1, \ldots, \lambda_{v+o_1}, 0, \ldots, 0, 1)$, it is clear that the equations (7) and (8) are $n + m - 1$ quadratic equations in $n$ variables $\lambda_1, \ldots, \lambda_n$, and are constructed from the public key $p_1, \ldots, p_m$. Solving these quadratic system, an attacker can recover a part of the secret key $S$ and $T$, namely, $\mathbf{s}$ and $\mathbf{t}$. The RBS attack can recovery $S$ and $T$ by repeating similar discussions as above (see [11] for detail). Since the complexity of solving the quadratic system dominates one of the RBS attack, it suffices to treat only the system. We refer to the quadratic system consisting of the equations (7) and (8) as the *RBS dominant system*.

# 3. Revisiting Previous Complexity Estimation for the RBS Attack

In this section, we explain the previous complexity estimation for the RBS attack. In Subsection 3.1, by using a certain experimental degree called the *solving degree*, we explain the complexity of a Gröbner basis algorithm for solving a quadratic system. In Subsection 3.2, we recall the *degree of regularity* to approximate the solving degree for such a quadratic system. In Subsection 3.3, we show that RBS dominant systems have a gap between the solving degree and the degree of regularity.

## 3.1 Complexity of Attacks using a Gröbner Basis Algorithm

In the RBS attack, Gröbner basis algorithms are used for solving the RBS dominant system.

A Gröbner basis algorithm that computes a Gröbner basis for the ideal generated by a given polynomial system was discovered by B. Buchberger [5], and improved as faster algorithms, for example, XL [30], $F_4$ [15] and $F_5$ [16]. In this paper, we use the following complexity of the $F_4$ algorithm solving a polynomial system in $n$ variables:

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

where $2 < \omega \leq 3$ is a linear algebra constant and $d_{slv}$ is the maximal degree in steps which add a new non-zero polynomial during the Gröbner basis algorithm and is called the *solving degree*.

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 its (theoretical) *indicator* approximating the solving degree (see Subsection 3.2).

Using the solving degree $d_{slv}$, we describe the complexity of the RBS attack against Rainbow with a parameter set $(v, o_1, o_2)$ as follows. Put $n = v + o_1 + o_2$ and $m = o_1 + o_2$. Since the RBS dominant system then has $n+m-1$ quadratic equations in $n$ variables (see the equations (7) and (8)), the complexity of the attack is given by

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

Furthermore, by using the *hybrid approach* [2] of brute-force search and Gröbner basis algorithm which solves the RBS dominant system in $n - k$ variables after fixing $k$ variables, the complexity is improved as

$$\min_k q^k \cdot \binom{n - k + d_{slv}}{d_{slv}}^{\omega}. \tag{9}$$

## 3.2 Degree of Regularity

In this subsection, we explain the degree of regularity as an indicator approximating the solving degree.

Denoting by $\mathbb{F}[x_1, \ldots, x_n]_d$ the vector space generated by the monomials of the total degree $d$ over $\mathbb{F}$ in $\mathbb{F}[x_1, \ldots, x_n]$, we have the following decomposition:

$$\mathbb{F}[x_1, \ldots, x_n] = \oplus_{d \geq} \mathbb{F}[x_1, \ldots, x_n]_d.$$

We denote by $\langle f_1, \ldots, f_m \rangle$ the ideal generated by $f_1, \ldots, f_m$, and by $\langle f_1, \ldots, f_m \rangle_d$ its component of degree $d$ in the decomposition if $f_1, \ldots, f_m$ are homogeneous.

For a polynomial system $(f_1, \ldots, f_m)$, M. Bardet et al. [1] considered the *degree of regularity* as the minimal value of the following set if it exists:

$$\left\{ d \mid \langle f_1^{top}, \ldots, f_m^{top} \rangle_d = \mathbb{F}[x_1, \ldots, x_n]_d \right\}.$$

For a polynomial system whose top homogeneous component is *semi-regular* [1], the degree of regularity is equal to the degree $D_{reg}$ of the first term whose coefficient is nonpositive in the following power series (see [1] for detail):

$$\frac{\prod_{i=1}^{m} (1 - t^{\deg f_i})}{(1 - t)^n}. \tag{10}$$

Note that a quadratic system whose coefficients are randomly chosen is often semi-regular. For this reason, in using the degree of regularity for a quadratic system, we assume

that the system is semi-regular, and also call $D_{reg}$ the degree of regularity.

By using the degree of regularity under the assumption that an RBS dominant system is semi-regular, the previous estimation method gives complexities of the RBS attack as follows. For a Rainbow parameter set $(v, o_1, o_2)$, the RBS dominant system has $m + n - 1$ quadratic polynomials in $n$ variables where $n = v + o_1 + o_2$ and $m = o_1 + o_2$ (see the equations (7) and (8)). Then, by the formula (9), the complexity in classical gates of the RBS attack is given by

$$\min_k \; q^k \cdot \binom{n-k+D_{reg}}{D_{reg}}^{\omega} \tag{11}$$

where $2 < \omega \leq 3$ is a linear algebra constant, $k$ is the number of variables fixed by the hybrid approach and $D_{reg}$ is given by the degree of the first term whose coefficient is non-positive in the power series

$$\frac{(1-t^2)^{m+n-1}}{(1-t)^{n-k}}. \tag{12}$$

In the next subsection, by our experiments, we show that an RBS dominant system is non-semi-regular.

### 3.3 Experiments on the Degree of Regularity

In this subsection, by our experiments on Rainbow parameter sets with $v \lesssim 2o_i$, we show that RBS dominant systems have a gap between the solving degree and the degree of regularity. 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 [4] on CPU: 3.2 GHz Intel Core i7. We denote by $d_{mem}$ the degree of the most memory-consuming step and by $d_{tim}$ the degree of the most time-consuming step during the Gröbner basis algorithm.

For small Rainbow parameter sets $(v, o_1, o_2)$ with $v \lesssim 2o_i$, Table 3 demonstrates the fundamental assertion that the degree of regularity $D_{reg}$ tightly approximates the solving degree $d_{slv}$ for a semi-regular system of $v + 2o_1 + 2o_2 - 1$ quadratic equations in $v+o_1+o_2$ variables which of the same size as the RBS dominant system (see the equations (7) and (8)). Under the assumption that an RBS dominant system is semi-regular, the previous estimation method [13], [29] for the RBS attack uses the degree of regularity $D_{reg}$ (see Subsection 3.2) as the solving degree $d_{slv}$. Table 3 also shows that this assumption does not hold for small Rainbow parameter sets $(v, o_1, o_2)$ with $v \lesssim 2o_i$.

In Table 3, we see that each RBS dominant system is solved faster than a semi-regular system of the same size and has a gap between the degree of regularity and the solving degree. Since the degree of regularity does not tightly approximate the solving degree of an RBS dominant system, it is important to find an optimal indicator for estimating the complexity of the RBS attack. Note that an experiment on the RBS attack is also carried out in the paper [29], and Table 2 in the paper shows that an RBS dominant system is solved faster than a semi-regular system of the same size. However, the paper [29] does not mention a relation between the degree of regularity and the solving degree.

**Table 3 (Gap Between $D_{reg}$ and $d_{slv}$ for an RBS Dominant System)** For the parameter relation $v \lesssim 2o_i$ $(i = 1, 2)$, the degree of regularity $D_{reg}$ (see the series (12)) and experimental values $d_{slv}$ (see Subsection 3.1) and $d_{tim}$ (see the first paragraph in Subsection 3.3) in the Gröbner basis algorithm $F_4$ for RBS dominant systems and semi-regular systems of the same size. Each RBS dominant system is solved faster than a semi-regular system of the same size, and has a gap between the degree of regularity $D_{reg}$ and the solving degree $d_{slv}$.

| $q = 256$ | $D_{reg}$ | Semi-regular system | | | RBS dominant system | | |
|---|---|---|---|---|---|---|---|
| $(v, o_i)$ | | Time (s) | $d_{slv}$ | $d_{tim}$ | Time (s) | $d_{slv}$ | $d_{tim}$ |
| $(4, 3)$ | 4 | 0.03 | 4 | 4 | 0.01 | 4 | 4 |
| $(5, 3)$ | 5 | 0.09 | 5 | 5 | 0.01 | 4 | 4 |
| $(6, 3)$ | 5 | 0.24 | 5 | 5 | 0.03 | 4 | 4 |
| $(6, 4)$ | 5 | 1.57 | 5 | 5 | 0.12 | 4 | 4 |
| $(7, 4)$ | 6 | 9.86 | 6 | 6 | 0.25 | 4 | 4 |
| $(8, 4)$ | 6 | 31.56 | 6 | 6 | 0.58 | 4 | 4 |
| $(8, 5)$ | 6 | 213.57 | 6 | 6 | 7.50 | 5 | 5 |
| $(9, 5)$ | 6 | 796.80 | 6 | 6 | 35.08 | 5 | 5 |
| $(10, 5)$ | 7 | 7818.25 | 7 | 7 | 71.54 | 5 | 5 |
| $(10, 6)$ | 7 | 47311.77 | 7 | 7 | 954.82 | 6 | 6 |
| $(11, 6)$ | 7 | $\geq 2$ days | - | - | 3265.14 | 6 | 6 |
| $(12, 6)$ | 7 | $\geq 2$ days | - | - | 6609.50 | 6 | 6 |

## 4. New Indicator for the Complexity of the RBS Attack

In this section, we propose an indicator for estimating the complexity of the RBS attack. We first explain the bi-graded polynomial. We then introduce a new indicator for bi-graded polynomial systems and show that this indicator tightly approximates the solving degree of an RBS dominant system than the degree of regularity by experiments using the $F_4$ algorithm.

### 4.1 Bi-graded Polynomial Systems

In this subsection, we explain the bi-graded polynomial and show that an RBS dominant system is bi-graded.

**Definition. 4.1.** A commutative ring $R$ is said to be bi-graded if the two following conditions holds:

(1) $R = \oplus_{\mathbf{d} \in \mathbb{Z}^2_{\geq 0}} R_{\mathbf{d}}$
(2) $R_{\mathbf{d}_1} R_{\mathbf{d}_2} \subseteq R_{\mathbf{d}_1 + \mathbf{d}_2}$ for all $\mathbf{d}_i \in \mathbb{Z}^2_{\geq 0}$

Moreover, an element in a bi-graded commutative ring $R$ is said to be bi-graded if it is contained in $R_{\mathbf{d}}$ for some $\mathbf{d} \in \mathbb{Z}^2_{\geq 0}$. Then, for a bi-graded element $h \in R_{\mathbf{d}}$, we define $\deg_{\mathbb{Z}^2_{\geq 0}} h$ as $\mathbf{d} \in \mathbb{Z}^2_{\geq 0}$.

**Remark. 4.2.** In this paper, an element of $R$ whose top homogeneous component is bi-graded is also said to be bi-graded.

For a Rainbow parameter set $(v, o_1, o_2)$, the RBS dominant system consists of $m$ quadratic polynomials (7) in a variable set $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $n - 1$ bilinear polynomials (8) in two variable sets $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $\{\lambda_{v+o_1+1}, \ldots, \lambda_n\}$ where $n = v + o_1 + o_2$ and $m = o_1 + o_2$ (see Subsection 2.3). The polynomial ring $\mathbb{F}[\lambda_1, \ldots, \lambda_n]$ can be graded by

$$\deg_{\mathbb{Z}^2_{\geq 0}} \lambda_1 = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} \lambda_{v+o_1} = (1,0) \text{ and,}$$

$$\deg_{\mathbb{Z}^2_{\geq 0}} \lambda_{v+o_1+1} = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} \lambda_n = (0,1).$$

Top homogeneous components $h_1, \ldots, h_m$ of quadratic polynomials (7) are contained in $\mathbb{F}[\lambda_1, \ldots, \lambda_n]_{(2,0)}$, and those $h_{m+1}, \ldots, h_{m+n-1}$ of quadratic polynomials (8) are in $\mathbb{F}[\lambda_1, \ldots, \lambda_n]_{(1,1)}$. Namely,

$$\begin{aligned} \deg_{\mathbb{Z}^2_{\geq 0}} h_1 = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} h_m = (2,0), \\ \deg_{\mathbb{Z}^2_{\geq 0}} h_{m+1} = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} h_{m+n-1} = (1,1). \end{aligned} \quad (13)$$

Hence, the RBS dominant system is a bi-graded polynomial system.

In the next section, based on the fact that an RBS dominant system is bi-graded, we introduce an indicator for estimating the complexity of the RBS attack.

### 4.2 New Indicator for the Complexity of Solving a Bi-graded Polynomial System

In this subsection, we introduce a new indicator for bi-graded polynomial systems and show that this indicator tightly approximates the solving degree of an RBS dominant system than the degree of regularity.

We introduce the following indicator for the complexity of a Gröbner basis algorithm with a bi-graded polynomial system:

**Definition. 4.3.** For a bi-graded polynomial system $(h_1, \ldots, h_m)$ in $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]^m$ where $\deg_{\mathbb{Z}^2_{\geq 0}} h_i = (d_{i1}, d_{i2})$, let

$$\sum_{(d_1,d_2)\in\mathbb{Z}^2_{\geq 0}} a_{(d_1,d_2)} t_1^{d_1} t_2^{d_2} = \frac{\prod_{i=1}^m (1 - t_1^{d_{i,1}} t_2^{d_{i,2}})}{(1-t_1)^{n_1}(1-t_2)^{n_2}}, \quad (14)$$

and we define $D_{bgd} = D_{bgd}(h_1, \ldots, h_m)$ as the minimal value of $\{d_1 + d_2 \mid a_{(d_1,d_2)} < 0\}$ if it exists.

The two-variable series in (14) is regarded as a bi-graded version of the Hilbert series (see [21] for example).

**Remark. 4.4.** For a bi-graded polynomial system, we note that the one-variable power series (10) deducing $D_{reg}$ coincides with the two-variable power series (14) when $t = t_1 = t_2$. Hence, if we define $D'_{bgd}$ as the minimum value of the set

$$\{d_1 + d_2 \mid a_{(d_1,d_2)} \leq 0\}$$

where $a_{(d_1,d_2)}$ is the coefficient of $t_1^{d_1} t_2^{d_2}$ in the series (14) and it exists, then $D'_{bgd} \leq D_{reg}$. $D'_{bgd}$ is often smaller than the solving degree for some Rainbow parameter sets. Thus we do not use $D'_{bgd}$ as a suitable indicator. On the other hand, the term $t^{D_{reg}}$ in the series (10) often has a negative coefficient which deduces one of $t_1^{d_1} t_2^{d_2}$ in the series (14) where $d_1 + d_2 = D_{reg}$. Namely, the relation $D_{bgd} \leq D_{reg}$ often holds (see Table 4 and Table 5 below).

In the reminder of this subsection, by our experiments, we show that the introduced indicator $D_{bgd}$ tightly approximates the solving degree on an RBS dominant system than the degree of regularity. By Definition 4.3 and the equation (13), the indicator $D_{bgd}$ for an RBS dominant system with a parameter set $(v, o_1, o_2)$ is given by the minimal total degree of the terms whose coefficient are negative in the two-variable power series

$$\frac{(1-t_1t_2)^{v+o_1+o_2-1}(1-t_1^2)^{o_1+o_2}}{(1-t_1)^{v+o_1}(1-t_2)^{o_2}}. \quad (15)$$

Table 4 compares the indicator $D_{bgd}$ and the degree of regularity $D_{reg}$ for RBS dominant systems with $v = o_i$ and $v \lesssim 2o_i$.

**Table 4** **($D_{bgd}$ vs $D_{reg}$ for an RBS Dominant System)** Experimental degrees $d_{slv}$ (see Subsection 3.1), $d_{mem}$ and $d_{tim}$ (see the first paragraph in Subsection 3.3) in the $F_4$ algorithm and theoretical degrees $D_{bgd}$ (from the series (15)) and $D_{reg}$ (from the series (12) at $k = 0$) for an RBS dominant system with $v \lesssim 2o_i$ or $v = o_i$ $(i = 1, 2)$. The proposed indicator $D_{bgd}$ coincides with $d_{slv}$ in the cases except for $(q, v, o_i) = (256, 8, 4), (16, 8, 8)$. The degree of regularity $D_{reg}$ is always larger than $d_{slv}$ except for $(q, v, o_i) = (256, 4, 4)$.

| $q = 256$ | Exper. | | | Theor. | |
|---|---|---|---|---|---|
| $(v, o_i)$ | $d_{slv}$ | $d_{tim}$ | $d_{mem}$ | $D_{bgd}$ | $D_{reg}$ |
| $(4, 3)$ | 4 | 4 | 4 | 4 | 4 |
| $(5, 3)$ | 4 | 4 | 4 | 4 | 5 |
| $(6, 3)$ | 4 | 4 | 4 | 4 | 5 |
| $(6, 4)$ | 4 | 4 | 4 | 4 | 5 |
| $(7, 4)$ | 4 | 4 | 4 | 4 | 6 |
| $(8, 4)$ | 4 | 4 | 4 | 5 | 6 |
| $(8, 5)$ | 5 | 5 | 5 | 5 | 6 |
| $(9, 5)$ | 5 | 5 | 5 | 5 | 6 |
| $(10, 5)$ | 5 | 5 | 5 | 5 | 7 |
| $(10, 6)$ | 6 | 6 | 6 | 6 | 7 |
| $(11, 6)$ | 6 | 6 | 6 | 6 | 7 |
| $(12, 6)$ | 6 | 6 | 6 | 6 | 7 |

| $q = 16$ | Exper. | | | Theor. | |
|---|---|---|---|---|---|
| $(v, o_i)$ | $d_{slv}$ | $d_{tim}$ | $d_{mem}$ | $D_{bgd}$ | $D_{reg}$ |
| $(3, 3)$ | 3 | 3 | 3 | 3 | 4 |
| $(4, 4)$ | 4 | 4 | 4 | 4 | 5 |
| $(5, 5)$ | 4 | 4 | 4 | 4 | 5 |
| $(6, 6)$ | 5 | 5 | 5 | 5 | 6 |
| $(7, 7)$ | 5 | 5 | 5 | 5 | 6 |
| $(8, 8)$ | 5 | 6 | 6 | 6 | 7 |
| $(9, 9)$ | 6 | 6 | 6 | 6 | 7 |

Furthermore, Table 5 compares the indicator $D_{bgd}$ and the degree of regularity $D_{reg}$ for the hybrid approach on the RBS attack against Rainbow parameter sets $(q, v, o_1, o_2) = (256, 10, 5, 5)$ and $(16, 8, 8, 8)$. Here, $k_1$ and $k_2$ are the numbers of variables fixed by the hybrid approach in $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $\{\lambda_{v+o_1+1}, \ldots, \lambda_{v+o_1+o_2}\}$, respectively, where $\lambda_1, \ldots, \lambda_{v+o_1+o_2}$ are the variables of an RBS dominant system (see the equations (7) and (8)). Then the indicator $D_{bgd}$ is given by the minimal total degree of the terms whose coefficient are negative in the two-variable power series

$$\frac{(1-t_1t_2)^{v+o_1+o_2-1}(1-t_1^2)^{o_1+o_2}}{(1-t_1)^{v+o_1-k_1}(1-t_2)^{o_2-k_2}}. \quad (16)$$

**Remark. 4.5.** By our experiments using the $F_4$ algorithm [15] in Section 4, we see that the Gröbner basis of the ideal generated by an RBS dominant system is computed within the introduced indicator $D_{bgd}$ and its solution can be obtained. Although our experiments were performed by using

**Table 5** **($D_{bgd}$ vs $D_{reg}$ for the Hybrid Approach on an RBS Dominant System)** Experimental degrees $d_{slv}$ (see Subsection 3.1), $d_{mem}$ and $d_{tim}$ (see the first paragraph in Subsection 3.3) in the $F_4$ algorithm and theoretical degrees $D_{bgd}$ (from the series (16)) and $D_{reg}$ (from the series (12)) of the hybrid approach on RBS dominant systems in variables $\{\lambda_1, \ldots, \lambda_{v+o_1+o_2}\}$ for $(q, v, o_1, o_2) = (256, 10, 5, 5)$ and $(16, 8, 8, 8)$. The integers $k_1$ and $k_2$ are the number of variables fixed by the hybrid approach in $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $\{\lambda_{v+o_1+1}, \ldots, \lambda_{v+o_1+o_2}\}$, respectively. The degree of regularity $D_{reg}$ is always larger than the solving degree $d_{slv}$. The proposed indicator $D_{bgd}$ tightly approximates $d_{slv}$ than $D_{reg}$ and is an upper bound of $d_{slv}$.

| $(256, 10, 5, 5)$ | | Exper. | | | Theor. | |
|---|---|---|---|---|---|---|
| $k_1 + k_2$ | $(k_1, k_2)$ | $d_{slv}$ | $d_{tim}$ | $d_{mem}$ | $D_{bgd}$ | $D_{reg}$ |
| 0 | $(0, 0)$ | 5 | 5 | 5 | 5 | 7 |
| 1 | $(1, 0)$ | 5 | 5 | 5 | 5 | 6 |
| | $(0, 1)$ | 4 | 4 | 4 | 5 | 6 |
| 2 | $(2, 0)$ | 4 | 5 | 5 | 5 | 6 |
| | $(1, 1)$ | 4 | 4 | 4 | 4 | 6 |
| | $(0, 2)$ | 4 | 4 | 4 | 4 | 6 |
| 3 | $(3, 0)$ | 4 | 4 | 4 | 4 | 6 |
| | $(2, 1)$ | 4 | 4 | 4 | 4 | 6 |
| | $(1, 2)$ | 3 | 4 | 4 | 4 | 6 |
| | $(0, 3)$ | 3 | 3 | 3 | 3 | 6 |
| 4 | $(4, 0)$ | 4 | 4 | 4 | 4 | 5 |
| | $(3, 1)$ | 3 | 4 | 4 | 4 | 5 |
| | $(2, 2)$ | 3 | 3 | 3 | 3 | 5 |
| | $(1, 3)$ | 3 | 3 | 3 | 3 | 5 |
| | $(0, 4)$ | 2 | 2 | 2 | 2 | 5 |

| $(16, 8, 8, 8)$ | | Exper. | | | Theor. | |
|---|---|---|---|---|---|---|
| $k_1 + k_2$ | $(k_1, k_2)$ | $d_{slv}$ | $d_{tim}$ | $d_{mem}$ | $D_{bgd}$ | $D_{reg}$ |
| 0 | $(0, 0)$ | 5 | 6 | 6 | 6 | 7 |
| 1 | $(1, 0)$ | 5 | 5 | 5 | 5 | 6 |
| | $(0, 1)$ | 5 | 5 | 5 | 5 | 6 |
| 2 | $(2, 0)$ | 5 | 5 | 5 | 5 | 6 |
| | $(1, 1)$ | 5 | 5 | 5 | 5 | 6 |
| | $(0, 2)$ | 5 | 5 | 5 | 5 | 6 |
| 3 | $(3, 0)$ | 4 | 5 | 5 | 5 | 6 |
| | $(2, 1)$ | 4 | 5 | 5 | 5 | 6 |
| | $(1, 2)$ | 4 | 5 | 5 | 5 | 6 |
| | $(0, 3)$ | 4 | 4 | 4 | 5 | 6 |
| 4 | $(4, 0)$ | 4 | 4 | 4 | 4 | 6 |
| | $(3, 1)$ | 4 | 4 | 4 | 5 | 6 |
| | $(2, 2)$ | 4 | 4 | 4 | 4 | 6 |
| | $(1, 3)$ | 4 | 4 | 4 | 4 | 6 |
| | $(0, 4)$ | 4 | 4 | 4 | 4 | 6 |

the $F_4$ algorithm, this fact is independent of such Gröbner basis algorithms. In fact, we can confirm the same fact for an XL algorithm that generates a Gröbner basis.

## 5. Our Complexity Estimation for the RBS Attack

In this section, we give a new complexity estimation of the RBS attack using the $F_4$ algorithm under the assumption that the indicator $D_{bgd}$ is an upper bound of the solving degree $d_{slv}$ (see Remark 4.5 in Subsection 4.2). Furthermore, we explain a complexity estimation for the Wiedemann XL algorithm without a Gröbner basis.

For simplicity, we explain only a complexity estimation in classical gates for the RBS attack against a Rainbow parameter set $(q, v, o_1, o_2)$. Put $n = v + o_1 + o_2$ and $m = o_1 + o_2$. Let $k_1$ and $k_2$ be the numbers of variables fixed by the hybrid approach in $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $\{\lambda_{v+o_1+1}, \ldots, \lambda_n\}$, respectively, where $\lambda_1, \ldots, \lambda_n$ are the variables of the RBS dominant system (see the equations (7) and (8)). When $k_1 < v + o_1$ and $k_2 < o_2$, the complexity is given by

$$q^{k_1+k_2} \cdot \binom{n - k_1 - k_2 + D_{bgd}}{D_{bgd}}^{\omega}$$

where $2 < \omega \leq 3$ is a linear algebra constant and $D_{bgd}$ is given by the minimal total degree in terms whose coefficient is negative in the two-variable power series (16) in Subsection 4.2, i.e.

$$\frac{(1 - t_1 t_2)^{v+o_1+o_2-1}(1 - t_1^2)^{o_1+o_2}}{(1 - t_1)^{v+o_1-k_1}(1 - t_2)^{o_2-k_2}}.$$

When $k_1 = v + o_1$ and $k_2 < o_2$, we obtain a system of $v + o_1 + o_2 - 1$ linear equations in $o_2 - k_2$ variables from the RBS dominant system fixed $k_1$ variables. Then, the complexity is given by $q^{k_1+k_2} \cdot (2(o_2 + 1)(v + o_1)(o_2 - k_2) + (o_2 - k_2)^{\omega})$. Similarly, when $k_1 < v + o_1$ and $k_2 = o_2$, we obtain a system consisting of $o_1 + o_2$ quadratic equations and $v + o_1 + o_2 - 1$ linear equations in $v + o_1 - k_1$ variables. Then, since it suffices to solve a system of linear equations in $v + o_1 - k_1$ variables, the complexity is given by $q^{k_1+k_2} \cdot (2(v + o_1 + 1)(v + o_1 - k_1)o_2 + (v + o_1 - k_1)^{\omega})$. When $k_1 = v + o_1$ and $k_2 = o_2$, the complexity of a brute-force search is given by $q^{k_1+k_2}$.

In NIST PQC 2nd round, the designer of Rainbow uses the Wiedemann XL algorithm for solving an RBS dominant system and estimates the complexity of the RBS attack [13]. Then the used complexity estimation [31] is better than the formula (9) of $F_4$ and is probably the best for solving a polynomial system. By applying our indicator $D_{bgd}$ to this complexity estimation, we can show that the complexities for the parameter sets Ia, IIIc and Vc are improved as $2^{142.9}, 2^{206.4}$ and $2^{267.4}$, respectively, and do not satisfy the security levels I, III/IV and V/VI, respectively. In fact, the paper [25] also proposes a similar indicator to our work and suggests the small parameter changes, and the designer of Rainbow plans to change the parameters in NIST PQC 3rd round [27]. However, the following paragraph shows that the actual complexity of the Wiedemann XL algorithm may be worse than the estimation [31] for the RBS attack.

The eXtended Linearization (XL) method extends a given polynomial system by multiplying all monomials up to a target degree and generates its corresponding *extended Macaulay matrix*. By using this matrix, an XL algorithm solves the given system through a technique such as generating a Gröbner basis. The Wiedemann XL algorithm solves a given system through finding a specific kernel vector of an extended Macaulay matrix and, if the matrix is full-rank, its unique kernel vector derives a solution of this system. Thus, if an extended Macaulay matrix up to our indicator $D_{bgd}$ from an RBS dominant system is full-rank, by applying the value $D_{bgd}$ to the complexity estimation [31], we can show that the complexities of the RBS attack against the parameter sets Ia, IIIc and Vc do not satisfy the security levels I, III/IV and V/VI, respectively. However, in our experiment on scaled-down parameters, the extended Macaulay matrix actually has a big kernel space and the XL algorithm requires iterations of the Wiedemann algorithm. Hence, although the

complexity estimation [31] ignoring such iterations is available for estimating the minimum required complexity of the RBS attack, we further need to estimate the number of iterations to a more precise estimation for the Wiedemann XL algorithm with an RBS dominant system.

## 6. Conclusion

In this paper, we introduced the indicator $D_{bgd}$ for estimating the complexity of Gröbner basis algorithms with bi-graded polynomial systems. Since the Rainbow-Band-Separation (RBS) attack recovers a secret key of Rainbow by solving a certain bi-graded polynomial system, we are able to utilize $D_{bgd}$ to estimate the complexity of this attack.

According to our experiments using $F_4$ on scaled down Rainbow parameter sets in NIST PQC 2nd round, the indicator $D_{bgd}$ tightly approximates its solving degree than the degree of regularity $D_{reg}$, which has been used previously. Then the relation $D_{bgd} \leq D_{reg}$ holds always. Furthermore, the RBS attack can reduce the bi-graded polynomial system to a linear system by using the hybrid approach with a special setting. Consequently, we can obtain a new complexity estimation of the RBS attack. Although the RBS attack is not enough to threaten the security of Rainbow, we were able to understand the security of Rainbow against the RBS attack using $F_4$. However, it is not clear whether an algorithm for finding a solution of the RBS dominant system, such as the Wiedemann XL algorithm, can terminate within our indicator $D_{bgd}$, future investigation is needed.

The two-variable power series used for deducing the indicator $D_{bgd}$ is available widely and can be extended more generally. Therefore, as future works, we need to investigate its influence on the security of several other schemes.

## Acknowledgement

This work was supported by JST CREST Grant Number JPMJCR14D6, JSPS KAKENHI Grant Number 20K19802, 19K20266 and 18J20866.

### References

[1] Bardet, M., Faugère, J. C., Salvy, B. and Yang, B. Y.: Asymptotic behavior of the index of regularity of quadratic semi-regular polynomial systems. In 8th International Symposium on Effective Methods in Algebraic Geometry (MEGA), pp. 1–14 (2005)

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

[3] Billet, O., Gilbert, H.: Cryptanalysis of Rainbow. In: De Prisco R., Yung M. (eds.) SCN 2006, LNCS, vol. 4116, pp. 336–347. Springer (2006).

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

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

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

[7] Coppersmith, D., Stern, J., Vaudenay, S.: Attacks on the birational signature scheme. In: Stinson D.R. (ed.) CRYPTO 1994, LNCS vol. 773, pp. 435–443. Springer (1994).

[8] Diem, C.: Bounded regularity. J. Algebra **423**, 1143–1160 (2015)

[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., Gower, J. E., Schmidt, D. S.: Multivariate Public Key Cryptosystems, Springer (2006)

[11] Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S. and Cheng, C.-M.: New differential-algebraic attacks and reparametrization of Rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008, LNCS, vol. 5037, pp. 242–257. Springer (2008).

[12] Ding, J. and Hodges, T. J.: Inverting hfe systems is quasi-polynomial for all fields. In: Rogaway, P. (Ed.) CRYPTO 2011, LNCS, vol. 6841, pp. 724–742. Springer (2011).

[13] 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)

[14] 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).

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

[16] 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).

[17] Gall, F. L.: Algebraic complexity theory and matrix multiplication. In: Nabeshima, K. (ed.) ISSAC 2014, Kobe, Japan, July 23-25, 2014.

[18] Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W. H. Freeman & Co., New York (1979)

[19] 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).

[20] Kipnis, A., Patarin, J., Goubin, L.: Unbalanced Oil and Vinegar schemes. In: Stern, J. (ed.) EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999).

[21] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 2. Springer, Heidelberg (2005)

[22] Lang, S.: Algebra, Graduate Texts in Mathematics. vol. 211 (Revised third ed.), Springer-Verlag, New York (2002)

[23] 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

[24] Nakamura, Shuhei, 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

[25] Perlner, R. and Smith-Tone, D.: Rainbow Band Separation is Better than we Thought, Cryptology ePrint Archive, Report 2020/702 (2020) https://eprint.iacr.org/2020/702

[26] Petzoldt, A., Bulygin, S. and Buchmann, J.: Selecting Parameters for the Rainbow Signature Scheme. In: Sendrier, N. (ed.) PQCrypto 2010, LNSC, vol. 6061, pp. 218–240. Springer (2010).

[27] Rainbow Team, Modified Parameters of Rainbow in Response to a Refined Analysis of the Rainbow Band Separation Attack by the NIST Team and the Recent New MinRank attacks, June 22, 2020. http://precision.moscito.org/by-publ/recent/rainbow-pars.pdf

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

[29] Thomae, E.: A Generalization of the Rainbow Band Separation Attack and its Applications to Multivariate Schemes, IACR Cryptology ePrint Archive (2012). https://eprint.iacr.org/2012/223

[30] 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).

[31] Yang B.-Y., Chen O.C.-H., Bernstein D.J., Chen J.-M.: Analysis of QUAD. In: Biryukov A. (eds) Fast Software Encryption. FSE 2007. LNCS, vol 4593. Springer (2007)