Theoretical Computer Science 896 (2021) 1–18

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

New complexity estimation on the Rainbow-Band-Separation attack

Shuhei Nakamura [a,*], Yasuhiko Ikematsu [b], Yacheng Wang [c], Jintai Ding [d], Tsuyoshi Takagi [c]

[a] Department of Liberal Arts and Basic Sciences, Nihon University, Japan
[b] Institute of Mathematics for Industry, Kyushu University, Japan
[c] Department of Mathematical Informatics, University of Tokyo, Japan
[d] Department of Mathematical Sciences, University of Cincinnati, USA

ARTICLE INFO

Article history:
Received 10 November 2020
Received in revised form 5 July 2021
Accepted 29 September 2021
Available online 5 October 2021
Communicated by G. Yang

Keywords:
Multivariate public key cryptography
Rainbow
Rainbow-Band-Separation attack
Gröbner basis algorithm
Degree of regularity

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 Ding and Schmidt is such a multivariate cryptosystem, and it 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 theoretical value called the degree of regularity. However, the degree of regularity is generally larger than the solving degree in experiments, and an accurate estimation cannot be obtained. In this article, we propose a new theoretical value for the complexity of the Rainbow-Band-Separation attack using a Gröbner basis algorithm, which provides a more precise estimation compared to that using the degree of regularity. This theoretical value is deduced by the two-variable power series

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

Since the two-variable power series coincides with the one-variable power series at $t_1 = t_2$ deriving the degree of regularity, the theoretical value is less than or equal to the degree of regularity under a certain condition. Moreover, we show a relation between the Rainbow-Band-Separation attack using the hybrid approach and the HighRank attack. By considering this relation and our theoretical value, we obtain a new complexity estimation for the Rainbow-Band-Separation attack. Furthermore, applying our theoretical value to the complexity formula used in the NIST PQC 2nd round, we show that a slight modification of the proposed Rainbow parameter sets is required. Consequently, we provide a new theoretical value for generally estimating the solving degree of a bi-graded polynomial system, which can influence the parameter selection of Rainbow in the NIST PQC standardization project.

* Corresponding author.
E-mail address: nakamura.shuhei@nihon-u.ac.jp (S. Nakamura).

https://doi.org/10.1016/j.tcs.2021.09.043
0304-3975/

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 using a large-scale quantum computer [32]. It is therefore necessary to construct cryptography based on new mathematical problems resistant to quantum computers. Such cryptography is referred to as post-quantum cryptography. In 2015, the National Security Agency announced a plan for a transition to post-quantum cryptography, and the National Institute of Standards and Technology (NIST) started public recruitment of such cryptography candidates in 2016 [23].

Multivariate public key cryptography [11] is based on an NP-hard problem of solving a system of quadratic equations, called the MQ problem [20], which is expected to have a particularly high potential for building post-quantum signature schemes. Rainbow is a multivariate signature scheme proposed by J. Ding and D. Schmidt in 2005 [10]. This signature scheme can be simply and efficiently implemented using linear algebra methods over a small finite field, and in particular, it produces shorter signatures than those of RSA and other post-quantum signature schemes [14]. In the NIST post-quantum cryptography (PQC) 2nd round, secure Rainbow parameter sets are proposed, and several attacks against them have been analyzed [14]. The Rainbow-Band-Separation (RBS) attack [13], in particular, is important as the best among the known attacks against Rainbow with a certain parameter set.

Previous methods [14,33] for estimating the complexity of an RBS attack use the *degree of regularity* [1,2] as its theoretical value, 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 number of equations and variables, respectively. Because a public quadratic system solved in the direct attack is often semi-regular, the complexity estimation of the direct attack uses the degree of regularity [2,14]. However, in our experiments, the quadratic system solved in the RBS attack is non-semi-regular. Therefore, it is important to find an optimal theoretical value for estimating the complexity of an RBS attack.

1.1. Our contributions

The purpose of this article is to give a more precise complexity estimation for the RBS attack. Because the attack solves a certain quadratic system whose solving complexity dominates the overall attack, which we call an *RBS dominant system*, we need to estimate the complexity of a *Gröbner basis* algorithm to solve this system. In particular, for estimating the complexity, this article considers theoretical values approximating its *solving degree*, that is the maximal degree of steps that add a new non-zero polynomial during a Gröbner basis algorithm. As mentioned above, previous estimation methods have used the degree of regularity as its theoretical value. However, an RBS dominant system is solved faster than a semi-regular system, and its solving degree is lower than the degree of regularity. This is 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 article, we consider a polynomial h in $\mathbb{F}_q[x_1,\ldots,x_{n_1},y_1,\ldots,y_{n_2}]$ 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 theoretical value D_{bgd}, which is defined as the minimum total degree of the terms whose coefficients are negative in the two-variable power series

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

Since the one-variable power series (1) deriving the previous theoretical value D_{reg} is the same as the two-variable power series (2) at $t=t_1=t_2$, we have the relation $D_{bgd}\leq D_{reg}$ when the coefficient of $t^{D_{reg}}$ in (1) is negative. Moreover, for a bi-graded polynomial system satisfying the condition $D_{bgd}<q$, we can prove that the theoretical value D_{bgd} is an upper bound for its *first fall degree* [16], which was introduced to approximate the solving degree of a non-semi-regular system, such as HFE [26] or its variants.

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 polynomials in $v+o_1+o_2$ variables, which are partitioned into $v+o_1$ variables and o_2 variables. In other words, the RBS dominant systems are bi-graded. Through our experiments on RBS dominant systems with $v=o_i$ and $v\lesssim 2o_i$ $(i=1,2)$, we show that our theoretical value D_{bgd} tightly approximates the solving degree of the system than the degree of regularity D_{reg}.

We also show a relation between the RBS attack and the HighRank attack, which recovers a lower-rank quadratic polynomial by using a brute-force search. Since an RBS dominant system has many bilinear polynomials, the hybrid approach [2,34] on the RBS attack provides an overdetermined linear system by fixing one of the two sets of variables. In this case, the RBS attack becomes similar to the HighRank attack (see Subsection 5 for details). This fact has not been mentioned in previous research [14,28,29,33].

By using our theoretical value and reconsidering the hybrid approach on the RBS attack, we can obtain a new complexity estimation for the RBS attack. Moreover, by applying our theoretical value to the complexity formula used in the NIST PQC 2nd round, we show that a slight modification on the proposed Rainbow parameter sets is required. Consequently, we provide a new theoretical value for generally estimating the solving degree of a bi-graded polynomial system, which can influence the parameter selection of Rainbow in the NIST PQC standardization project.

Our work is independent of the study [27], which was submitted on the Cryptology ePrint Archive (https://eprint.iacr.org) one day prior to the preprint version [24] of this article (see also Remark 4.6). The estimation using the first fall degree in [27] requires a certain assumption, and they performed experiments on scaled-down Rainbow parameter sets in order to verify whether this assumption holds. On the other hand, we can obtain an estimation only by theoretical discussion. In particular, our estimation is applicable not only to an RBS system, but generically to a bi-graded polynomial system that satisfies $D_{bgd} < q$.

1.2. Organization

This article is organized as follows. In Section 2, we describe 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 the NIST PQC 2nd round. In Section 4, we introduce a new theoretical value for estimating the complexity of an RBS attack and demonstrate that this theoretical value more tightly approximates the solving degree of the quadratic system solved in the attack. In Section 5, by using our theoretical value and reconsidering the hybrid approach on the RBS attack, we give a new complexity estimation for the RBS attack and investigate the security of the parameter sets proposed in the NIST PQC 2nd round. In Section 6, we conclude the results.

2. The Rainbow signature scheme

In this section, we briefly describe the Rainbow signature scheme and several attacks against it. We detail Rainbow in Subsection 2.1 and its parameter set 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 Ding and Schmidt in 2005 [10]. 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 sets of variables, 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

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

where $g^{(j)}$ and $l_i^{(j)}$ are randomly chosen quadratic and linear polynomials, respectively. Then, in the signature generation algorithm above, we can easily compute an element $\mathbf{a}'$ in the pre-image of any element $\mathbf{b}' = (b'_1, \ldots, b'_{o_1+o_2})$ in $\mathbb{F}^m$ under F as follows:

1. Randomly choose $\mathbf{a}'_v = (a'_1, \ldots, a'_v)$ as $\mathbf{x}$.

Table 1
NIST security categories (Table 10 in [14]).

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
(Classical attacks) Complexities ($\log_2$(♯classical gates)) of known attacks against Rainbow (from Tables in Section 7.2 in [14]).

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

Table 3
(Quantum attacks) Complexities ($\log_2$(♯quantum gates)) of known attacks against Rainbow (from Tables in Section 7.2 in [14]).

Parameter set	(q, v, o_1, o_2)	Direct	MinRank	HighRank	UOV	RBS
Ia	(16, 32, 32, 32)	146.5	95.3	**86.3**	87.2	145.0
IIIc	(256, 68, 36, 36)	183.5	309.1	**169.9**	295.8	217.4
Vc	(256, 92, 48, 48)	235.5	406.8	**219.2**	393.4	278.6

2. Solve a system of linear equations

$$f_1(\mathbf{a}'_v, \mathbf{y}) = b'_1, \ldots, f_{o_1}(\mathbf{a}'_v, \mathbf{y}) = b'_{o_1}.$$

Let $\mathbf{a}'_{o_1} = (a'_{v+1}, \ldots, a'_{v+o_1})$ be one of its solutions if it exists. Otherwise, return to the step 1.

3. Solve a system of linear equations

$$f_{o_1+1}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+1}, \ldots, f_{o_1+o_2}(\mathbf{a}'_v, \mathbf{a}'_{o_1}, \mathbf{z}) = b'_{o_1+o_2}.$$

Let $\mathbf{a}'_{o_2} = (a'_{v+o_1+1}, \ldots, a'_{v+o_1+o_2})$ be one of its solutions if it exists. Otherwise, return to the step 1.

4. Obtain an element $\mathbf{a}' = (a'_1, \ldots, a'_{v+o_1+o_2})$ in the pre-image of $\mathbf{b}'$.

2.2. Parameters of Rainbow

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

The central map of Rainbow with a parameter set (v, o_1, o_2) can be regarded as a UOV [22] instance with the parameter set $(v + o_1, o_2)$. Hence the UOV attack [21] is available as an attack against Rainbow, and we have to take the Rainbow parameter set such that

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

We can also consider attacks using the special structure of the Rainbow central map (3). The HighRank attack [8] and the MinRank attack [4] are such attacks. Due to the influence 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 [13], which also solves a quadratic system to recover a secret key (see Subsection 2.3 for details), are important in deciding the concrete parameters v, o_1 and o_2. In this article, we implicitly assume $o_1 = o_2$ and consider a parameter set with $v = o_i$ or $v \lesssim 2o_i$ $(i = 1, 2)$.

The NIST PQC standardization project [23] provides six security categories (see Table 1). Here, due to the NIST specification, the number of gates is given by ♯ gates = ♯ field multiplications $\cdot (2 \cdot \log_2(q)^2 + \log_2(q))$.

Table 2 and Table 3 show the Rainbow parameter sets Ia, IIIc and Vc [14] proposed in the NIST PQC 2nd round and the complexities of the above attacks. Here, the bold numbers in Table 2 and Table 3 indicate the best complexity of attacks in each parameter set. Table 2 shows that the direct attack is the best among attacks against parameter sets IIIc and Vc in classical gates, and Table 3 shows that the HighRank attack is the best among attacks against all parameter sets in quantum 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 [14].

2.3. RBS attack

In this subsection, we describe the RBS attack [13] and a certain quadratic system solved in the attack, which are the subjects of our research. For simplicity, we assume in this subsection that the characteristic of $\mathbb{F}$ is odd. 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 $P = (p_1, \ldots, p_m)$, the RBS attack recovers its secret key (T, F, S) as follows. By the definition (3) of the central map $F = (f_1, \ldots, f_m)$, 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 in the form (5). However, it is known that the security of Rainbow does not decrease, even if S and T are taken in the form (5). Therefore, S and T in [13] are set to be in the form (5), which induces a reduction in the secret key size. The matrices $M_{p_1}, \ldots, M_{p_m}$ corresponding to the public polynomials $p_1, \ldots, p_m$ are given as

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

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

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

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

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

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 $k = n$, because 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 system of the equations (7) and (8) consists of $n+m-1$ quadratic equations in n variables $\lambda_1, \ldots, \lambda_n$, which is constructed from the public key $p_1, \ldots, p_m$. By solving the 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 recover S and T by repeating a similar approach as above (see [13] for details). Because the complexity of solving the quadratic system dominates that 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 the previous complexity estimation for the RBS attack

In this section, we describe the previous complexity estimation for the RBS attack. In Subsection 3.1, by using a certain experimental degree called the *solving degree*, we describe 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. In Subsection 3.4, we show the state of the step degrees in the Gröbner basis algorithm with the RBS dominant system for a concrete Rainbow parameter set.

3.1. Complexity of attacks using a Gröbner basis algorithm

In the RBS attack, Gröbner basis algorithms are used to solve the RBS dominant system.

A Gröbner basis algorithm, which computes a Gröbner basis for the ideal generated by a given polynomial system, was discovered by Buchberger [6], and improved as faster algorithms, such as XL [35], F_4 [17] and F_5 [18]. In this article, we use the following complexity of the F_4 algorithm to solve 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 that add a new non-zero polynomial during the Gröbner basis algorithm, called the *solving degree*.

Although the solving degree is important for obtaining the complexity, it is an experimental value. In order to estimate the complexity of solving a large-scale polynomial system, we need to find a theoretical value that approximates 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 (7) and (8) then has $n + m - 1$ quadratic equations in n variables, the complexity of the attack is given by

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

Furthermore, by using the *hybrid approach* [2,34] of the 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

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

In quantum gates, by using Grover's algorithm, the complexity is given by

$$\min_k q^{k/2} \cdot \binom{n-k+d_{slv}}{d_{slv}}^{\omega}. \tag{10}$$

3.2. Degree of regularity

In this subsection, we describe the degree of regularity as a theoretical value 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:

$$\mathbb{F}[x_1, \ldots, x_n] = \oplus_{d \geq 0} \mathbb{F}[x_1, \ldots, x_n]_d.$$

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 $f_1, \ldots, f_m$, the quotient $R := \mathbb{F}[x_1, \ldots, x_n]/\langle f_1^{top}, \ldots, f_m^{top} \rangle$ has a decomposition $R = \oplus_{d \in \mathbb{Z}_{\geq 0}} R_d$ such that

$$R_{d_1} R_{d_2} \subseteq R_{d_1+d_2}, \forall d_i \in \mathbb{Z}_{\geq 0},$$

where $R_d = \mathbb{F}[x_1, \ldots, x_n]_d / \langle f_1^{top}, \ldots, f_m^{top} \rangle_d$. Moreover, the Hilbert series $\mathrm{HS}_R(t)$ of such a ring R is defined as $\mathrm{HS}_R(t) = \sum_{d \geq 0} (\dim R_d) t^d$. For a polynomial system $f_1, \ldots, f_m$, Bardet et al. [1] considered the *degree of regularity* d_{reg} as the minimal value of the set $\{d \in \mathbb{Z}_{\geq 0} \mid \dim R_d = 0\}$ if it exists. When $f_1, \ldots, f_m$ is *semi-regular* [1], its Hilbert series coincides with the sum of terms whose coefficient is non-negative in

$$\frac{\prod_{i=1}^{m} (1 - t^{\deg f_i})}{(1-t)^n}. \tag{11}$$

Table 4
(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 (13)) and experimental values d_{slv} (see Subsection 3.1), d_{tim} and d_{mem} (see Subsection 3.4) 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 there is a gap between the degree of regularity D_{reg} and the solving degree d_{slv}.

$q = 256$	# eq.	# var.	D_{reg}	Semi-regular system				RBS dominant system			
(v, o_i)				Time (sec)	d_{slv}	d_{tim}	d_{mem}	Time (sec)	d_{slv}	d_{tim}	d_{mem}
$(4, 3)$	15	10	4	0.03	4	4	4	0.01	4	4	4
$(5, 3)$	16	11	5	0.09	5	5	5	0.01	4	4	4
$(6, 3)$	17	12	5	0.24	5	5	5	0.03	4	4	4
$(6, 4)$	21	14	5	1.57	5	5	5	0.12	4	4	4
$(7, 4)$	22	15	6	9.86	6	6	6	0.25	4	4	4
$(8, 4)$	23	16	6	31.56	6	6	6	0.58	4	4	4
$(8, 5)$	27	18	6	213.57	6	6	6	7.50	5	5	5
$(9, 5)$	28	19	6	796.80	6	6	6	35.08	5	5	5
$(10, 5)$	29	20	7	7818.25	7	7	7	71.54	5	5	5
$(10, 6)$	33	22	7	47311.77	7	7	7	954.82	6	6	6
$(11, 6)$	34	23	7	$\geq$ 2 days	-	-	-	3265.14	6	6	6
$(12, 6)$	35	24	7	$\geq$ 2 days	-	-	-	6609.50	6	6	6

Thus the degree of regularity d_{reg} is equal to the degree D_{reg} of the first term whose coefficient is non-positive in the power series (11). Because it is hard to compute the degree of regularity d_{reg} for any polynomial system, the cryptanalysis in multivariate public key cryptography often uses the degree D_{reg} as the degree of regularity d_{reg} by assuming that the polynomial system is semi-regular.

For the same reason, the RBS dominant system is also assumed to be semi-regular. Under the assumption, the previous estimation [14,33] for the complexity of the RBS attack is given as follows. For a Rainbow parameter set (v, o_1, o_2), the RBS dominant system (7) and (8) has $m + n - 1$ quadratic polynomials in n variables where $n = v + o_1 + o_2$ and $m = o_1 + o_2$. Then, by the formula (9), the complexity in classical gates of the RBS attack is given by

$$\min_k q^k \cdot \binom{n - k + D_{reg}}{D_{reg}}^{\omega} \tag{12}$$

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

$$\frac{(1 - t^2)^{m+n-1}}{(1 - t)^{n-k}}. \tag{13}$$

In quantum gates, by using Grover's algorithm, the complexity is given by

$$\min_k q^{k/2} \cdot \binom{n - k + D_{reg}}{D_{reg}}^{\omega}. \tag{14}$$

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, through our experiments on Rainbow parameter sets with $v \lesssim 2o_i$, we show that RBS dominant systems have a gap between the solving degree d_{slv} and the degree of regularity D_{reg}. The experiments in this article were performed by using the Gröbner basis algorithm F_4 with respect to the graded reverse lexicographic monomial order in Magma V2.24-4 [5] on a 3.2 GHz Intel Core i7 CPU.

For small Rainbow parameter sets (v, o_1, o_2) with $v \lesssim 2o_i$, Table 4 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 are of the same size as the RBS dominant system (7) and (8). Under the assumption that an RBS dominant system is semi-regular, the previous estimation method [14,33] for an RBS attack uses the degree of regularity D_{reg} (see Subsection 3.2) as the solving degree d_{slv}. Table 4 shows that this assumption does not hold for small Rainbow parameter sets (v, o_1, o_2) with $v \lesssim 2o_i$.

In Table 4, 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 closely approximate the solving degree of an RBS dominant system, it is important to find an optimal theoretical value for estimating the complexity of an RBS attack. Note that an experiment on the RBS attack was also carried out in [33], and Table 2 in [33] shows that an RBS dominant system is solved faster than a semi-regular system of the same size. However, [33] does not mention the relation between the degree of regularity and the solving degree.

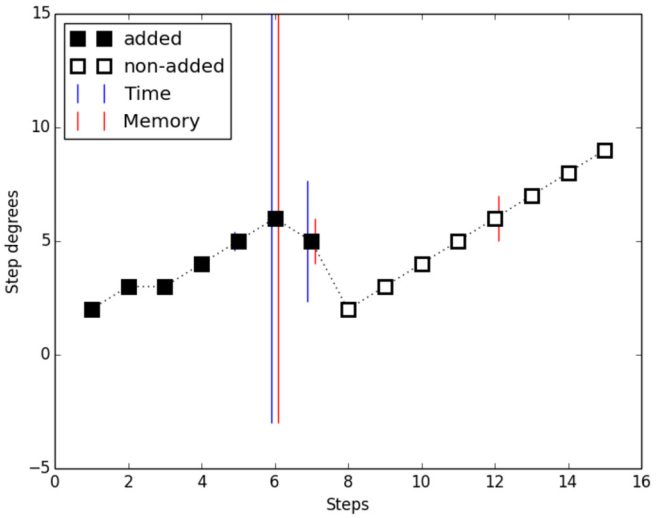

Fig. 1. The state of the step degrees in the Gröbner basis algorithm F_4 with the RBS dominant system for the parameter set $(q, v, o_1, o_2) = (256, 11, 6, 6)$. A step marked with the square black box adds a new polynomial. A step marked with the square white box does not add a new polynomial. The relation $d_{slv} \leq d_{tim} = d_{mem}$ holds. (d_{slv}: Subsection 3.1, d_{tim} and d_{mem}: Subsection 3.4). (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

3.4. State of the step degrees

In this subsection, we show the state of the step degrees in the Gröbner basis algorithm with the RBS dominant system for a concrete Rainbow parameter set.

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. A number of experiments in Subsection 3.3 show that the relation

$$d_{slv} \leq d_{tim} = d_{mem} \tag{15}$$

holds on an RBS dominant system for small parameter sets with $v \lesssim 2o_i$. Fig. 1 shows the state of the step degrees in the Gröbner basis algorithm with the RBS dominant system for the Rainbow parameter set $(q, v, o_1, o_2) = (256, 11, 6, 6)$ as input. Then, in the Gröbner basis algorithm, steps after the 8th step do not find new polynomials. Hence, $d_{slv} = 6$. We can verify the relation (15). Here, to obtain the Gröbner basis, it suffices to compute up to the 7th step for the RBS attack.

As shown in Subsection 3.3, the RBS dominant system has a gap between the solving degree d_{slv} and the degree of regularity D_{reg} since it is non-semi-regular. In order to approximate the solving degree d_{slv} of a non-semi-regular system, Dubois and Gama [16] investigate the step degree of the first step where a (step) degree fall occurs. The work [12] experimentally shows that such a step degree approximates the solving degree d_{slv} of a non-semi-regular system given as a public key of HFE [26].

In Fig. 1, a degree fall occurs at the 6th step, whose step degree is the solving degree d_{slv}. However, an insignificant degree fall occurs at the 2nd step. We can remove this degree fall at the 2nd step as follows. For simplicity, we assume the characteristic of $\mathbb{F}$ is odd. Let $q_1, \ldots, q_m$ be m quadratic polynomials (7) and $b_1, \ldots, b_{n-1}$ be $n-1$ bilinear polynomials (8) (see Subsection 2.3). Using the notations in the equations (7) and (8), we consider the matrix

$$M = \begin{pmatrix} \mathbf{s} \cdot M_{p_1} \\ \vdots \\ \mathbf{s} \cdot M_{p_m} \end{pmatrix}.$$

The top homogeneous components of $q_1, \ldots, q_m$ are given as the components of $M \cdot {}^t\mathbf{s}$, and those of $b_1, \ldots, b_{n-1}$ are given as the first $n-1$ components of $\mathbf{t} \cdot M$. Thus, there is a non-trivial syzygy obtained from the top homogeneous components of the relation $\mathbf{t} \cdot (M \cdot {}^t\mathbf{s}) = (\mathbf{t} \cdot M) \cdot {}^t\mathbf{s}$. By the reduction with this syzygy, we can construct the bilinear polynomial

$$\lambda_1 b_1 + \cdots + \lambda_{v+o_1} b_{v+o_1} - \lambda_{v+o_1+1} q_{m-o_2+1} - \cdots - \lambda_{v+o_1+o_2} q_m.$$

This is the reason that the degree fall at the 2nd step occurs. Hence, adding the constructed bilinear polynomial to the 2nd step, we can remove this degree fall.

We call the step degree of the first step where a degree fall can not be removed by the *first fall degree* d_{ff}. For a quadratic system given as the public key of HFE [26], the degree d_{ff} coincides with the solving degree d_{slv}. Similarly, for the RBS dominant system with the parameter set $(q, v, o_1, o_2) = (256, 11, 6, 6)$, Fig. 1 shows

$$d_{slv} = d_{ff}.$$

In Subsection 4.2, we show this equality holds for many Rainbow parameter sets with $v = o_i$ and $v \lesssim 2o_i$.

4. New theoretical value for the complexity of the RBS attack

In this section, we propose a theoretical value for estimating the complexity of the RBS attack. We first introduce the bi-graded polynomial and a new theoretical value for it. We then show that an RBS dominant system is bi-graded and that the introduced theoretical value tightly approximates its solving degree than the degree of regularity by experiments (see Remark 4.7).

4.1. New theoretical value for a bi-graded polynomial system

In this subsection, we describe the bi-graded polynomial and introduce a new theoretical value for it. Moreover, we show that, under the reasonable condition, this theoretical value is an upper bound for the first fall degree which has been used to approximate the solving degree of a non-semi-regular system.

When a polynomial system is semi-regular, the theoretical value D_{reg} deduced from (11) coincides with the degree of regularity d_{reg}. However, as shown in Subsection 3.3, an RBS dominant system which we investigate is not semi-regular. It is necessary to consider another theoretical value different from the degree of regularity. In order to approximate the solving degree of a non-semi-regular system, such as HFE [26] and its variant (e.g. GeMSS [7]), the *first fall degree* [16] was introduced as a theoretical formulation for the degree d_{ff} defined in Subsection 3.4, and it is defined as follows.

Definition 4.1. Let $B = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots, x_n^q \rangle$ with the standard graded decomposition $B = \oplus_{d \geq 0} B_d$. Let d_0 be a positive integer and $h_1, \ldots, h_m$ be homogeneous polynomials of degree d_0 in $\mathbb{F}_q[x_1, \ldots, x_n]$. Put $\varphi_d : B_{d-d_0}^m \to B_d, (\overline{b}_1, \ldots, \overline{b}_m) \mapsto \overline{b}_1\overline{h}_1 + \cdots + \overline{b}_m\overline{h}_m$ where $\overline{h}_i$ is an image in B of h_i. For $h_1, \ldots, h_m$, the *first fall degree* D_{ff} is the minimum value of the following set if it exists:

$$\{d \mid \mathrm{Ker}(\varphi_d) \neq \mathrm{TSyz}_B(\overline{h}_1, \ldots, \overline{h}_m)_d\},$$

where $\mathrm{TSyz}_B(\overline{h}_1, \ldots, \overline{h}_m)_d := \langle \overline{b}_{ij}\overline{\tau}_{ij}, \overline{b}_i\overline{\tau}_i \mid \overline{b}_{ij} \in B_{d-d_0}, \overline{b}_i \in B_{d-d_0(q-1)} \rangle_{\mathbb{F}_q}$, $\overline{\tau}_{ij} := (0, \ldots, 0, -\overline{h}_j, 0, \ldots, 0, \overline{h}_i, 0, \ldots, 0)$, and $\overline{\tau}_i := (0, \ldots, 0, \overline{h}_i^{q-1}, 0, \ldots, 0)$. Moreover, for any polynomial system $f_1, \ldots, f_m$, the *first fall degree* is defined as $D_{ff}(f_1^{top}, \ldots, f_m^{top})$.

In the remainder of this subsection, we consider the bi-graded polynomial system which is not necessary to be semi-regular, and show that the theoretical value deduced from the corresponding two-variable series is an upper bound for its first fall degree.

Definition 4.2. A commutative ring R is said to be *bi-graded* if it has a decomposition $R = \oplus_{\mathbf{d} \in \mathbb{Z}_{\geq 0}^2} R_{\mathbf{d}}$ such that

$$R_{\mathbf{d}_1} R_{\mathbf{d}_2} \subseteq R_{\mathbf{d}_1 + \mathbf{d}_2}, \forall \mathbf{d}_i \in \mathbb{Z}_{\geq 0}^2$$

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 $\mathbf{d} \in \mathbb{Z}_{\geq 0}^2$. Then, for a bi-graded element $h \in R_{\mathbf{d}}$, we define $\deg_{\mathbb{Z}_{\geq 0}^2} h$ as $\mathbf{d} \in \mathbb{Z}_{\geq 0}^2$. In this article, an element of R whose top homogeneous component is bi-graded is also said to be *bi-graded*.

For example, by setting $\deg x_1 = \cdots = \deg x_{n_1} = (1, 0)$ and $\deg y_1 = \cdots = \deg y_{n_2} = (0, 1)$, the polynomial ring $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ is bi-graded. In the following definition, we define a two-variable power series decided by the bi-degrees of a bi-graded polynomial system and the theoretical value D_{bgd}.

Definition 4.3. Let $f_1, \ldots, f_m$ be bi-graded polynomials in the bi-graded polynomial ring $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$ where $\deg_{\mathbb{Z}_{\geq 0}^2} f_i = (d_{i1}, d_{i2})$. Put integers $a_{(d_1,d_2)}$ as

$$\sum_{(d_1,d_2) \in \mathbb{Z}_{\geq 0}^2} a_{(d_1,d_2)} t_1^{d_1} t_2^{d_2} = \frac{\prod_{i=1}^m (1 - t_1^{d_{i,1}} t_2^{d_{i,2}})}{(1 - t_1)^{n_1} (1 - t_2)^{n_2}}. \tag{16}$$

We define $D_{bgd} = D_{bgd}(f_1, \ldots, f_m)$ as the minimal value of $\{d_1 + d_2 \mid a_{(d_1,d_2)} < 0\}$ if it exists.

For bi-graded polynomials $f_1, \ldots, f_m$, the quotient $R := \mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]/\langle f_1, \ldots, f_m \rangle$ is also bi-graded. Then we define *the bi-graded Hilbert series* $\mathrm{HS}_R(t_1, t_2) = \sum_{(d_1,d_2)\in\mathbb{Z}^2_{\geq 0}} (\dim R_{(d_1,d_2)}) t_1^{d_1} t_2^{d_2}$. Under the assumption of Lemma A in Appendix, the two-variable power series (16) in Definition 4.3 can compute the bi-graded Hilbert series (see Lemma A and Lemma B in Appendix).

By the definition, we have the following theorem:

Theorem 4.4. *Let $f_1, \ldots, f_m$ be bi-graded polynomials in the bi-graded polynomial ring $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$. If the coefficient of $t^{D_{reg}}$ in (11) decided by these bi-degrees is negative, then we have*

$$D_{bgd} \leq D_{reg}.$$

Proof. Put $\sum_{d\geq 0} a_d t^d = \prod_{i=1}^m (1 - t^{\deg f_i})/(1-t)^n$. If we set $t_1 = t_2 = t$, then the series (16) coincides with the one-variable power series (11). Hence, comparing the coefficients of both power series, we have

$$\sum_{d_1+d_2} a_{(d_1,d_2)} = a_d. \tag{17}$$

By the assumption, the coefficient of $t^{D_{reg}}$ in (11) is negative, i.e. $a_{D_{reg}} < 0$. Thus, in the left hand side of the equality (17), there exists a pair (d_1, d_2) such that $a_{(d_1,d_2)} < 0$ and $d_1 + d_2 = D_{reg}$, and it follows that $D_{bgd} \leq D_{reg}$. □

By the following theorem, under the condition $D_{bgd} < q$, we see that the theoretical value D_{bgd} in Definition 4.3 is an upper bound for the first fall degree of a bi-graded polynomial system.

Theorem 4.5. *Let $f_1, \ldots, f_m$ be bi-graded polynomials in the bi-graded polynomial ring $\mathbb{F}[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}]$. If $D_{bgd} < q$, then we have*

$$D_{ff} \leq D_{bgd},$$

where D_{ff} is the first fall degree in Definition 4.1.

Proof. See Appendix. □

In the next section, we show that an RBS dominant system is bi-graded. Moreover, for almost parameter sets performed on our experiments in the next section, the degree d_{ff} attains the bound D_{bgd} in Theorem 4.5. Note that, for the proposed Rainbow parameter sets Ia, IIIc and Vc, the RBS dominant system that gives the best complexity satisfies the assumptions in Theorem 4.4 and Theorem 4.5 (see Remark 5.2).

Remark 4.6. Note that Theorem 4.5 is not proved in [27]. Perlner and Smith-Tone's value approximating the solving degree is determined by the lowest term whose coefficient is non-positive in the power series (16). Due to this setting, their estimation using the first fall degree requires a certain assumption (see Corollary 2 in [27]). In order to verify whether this assumption holds, they performed experiments on scaled-down Rainbow parameter sets. On the other hand, our theoretical value D_{bgd} is determined by the lowest term whose coefficient is negative (see Definition 4.3). It is possible to show the existence non-trivial syzygies by the homology of the Koszul complex (see Appendix), and we can obtain an estimation only by theoretical discussion as Theorem 4.5. In particular, our estimation is applicable not only to an RBS system, but generically to a bi-graded polynomial system that satisfies $D_{bgd} < q$.

4.2. Experimental estimation for the solving degree of an RBS dominant system

In this section, we confirm that an RBS dominant system is bi-graded, and experimentally show that the introduced theoretical value tightly approximates the solving degree of an RBS dominant system than the degree of regularity.

For a Rainbow parameter set (v, o_1, o_2), the RBS dominant system consists of m quadratic polynomials (7) in a set $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ of variables and $n-1$ bilinear polynomials (8) in two sets $\{\lambda_1, \ldots, \lambda_{v+o_1}\}$ and $\{\lambda_{v+o_1+1}, \ldots, \lambda_n\}$ of variables 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

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

The 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 $h_{m+1}, \ldots, h_{m+n-1}$ of quadratic polynomials (8) are in $\mathbb{F}[\lambda_1, \ldots, \lambda_n]_{(1,1)}$. Namely,

Table 5
(D_{bgd} vs D_{reg} for an RBS dominant system) Experimental values d_{slv} (see Subsection 3.1), d_{ff} and d_{tim} (see Subsection 3.4) in the F_4 algorithm and theoretical values D_{bgd} (from the series (19)) and D_{reg} (from the series (13) at $k=0$) for an RBS dominant system with $v \lesssim 2o_i$ or $v = o_i$ $(i = 1, 2)$. The proposed theoretical value D_{bgd} coincides with d_{slv} in all cases except for $(q, v, o_i) = (256, 8, 4)$. 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_{ff}	d_{tim}	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_{ff}	d_{tim}	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
$(8, 8)$	6	6	6	6	7
$(9, 9)$	6	6	6	6	7

$$\begin{aligned} \deg_{\mathbb{Z}^2_{\geq 0}} h_1 = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} h_m = (2, 0), \\ \deg_{\mathbb{Z}^2_{\geq 0}} h_{m+1} = \cdots = \deg_{\mathbb{Z}^2_{\geq 0}} h_{m+n-1} = (1, 1). \end{aligned} \tag{18}$$

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

By Definition 4.3 and the equation (18), the theoretical value 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 coefficients are negative in the two-variable power series

$$\frac{(1 - t_1 t_2)^{v+o_1+o_2-1}(1 - t_1^2)^{o_1+o_2}}{(1 - t_1)^{v+o_1}(1 - t_2)^{o_2}}. \tag{19}$$

Table 5 compares the theoretical value D_{bgd} and the degree of regularity D_{reg} for RBS dominant systems with $v = o_i$ and $v \lesssim 2o_i$.

Furthermore, Table 6 compares the theoretical value 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 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, where $\lambda_1, \ldots, \lambda_{v+o_1+o_2}$ are the variables of an RBS dominant system (7) and (8). Then the theoretical value D_{bgd} is given by the minimal total degree of the terms whose coefficients are negative in the two-variable power series

$$\frac{(1 - t_1 t_2)^{v+o_1+o_2-1}(1 - t_1^2)^{o_1+o_2}}{(1 - t_1)^{v+o_1-k_1}(1 - t_2)^{o_2-k_2}}. \tag{20}$$

Remark 4.7. In our experiments using the F_4 algorithm [17] in Section 4, we see that the Gröbner basis of the ideal generated by an RBS dominant system is computed within the introduced theoretical value D_{bgd}, and its solution can be obtained. Although our experiments were performed using the F_4 algorithm, this fact is independent of such Gröbner basis algorithms. Indeed, 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 by using our theoretical value introduced in Subsection 4.2 and reconsidering the hybrid approach. In Subsection 5.2, applying our theoretical value to the complexity formula [14] used in the NIST PQC 2nd round, we show that a slight modification of the Rainbow parameter sets is required.

5.1. Complexity estimation based on the bi-graded polynomial system

In this section, we give a new complexity estimation of the RBS attack under the assumption that the theoretical value D_{bgd} is an upper bound of the solving degree d_{slv} (see Subsection 4.2). Moreover, we investigate the relation between the RBS attack using the hybrid approach and the HighRank attack.

For simplicity, we explain only the 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 number 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 (7) and (8). When $k_1 < v + o_1$ and $k_2 < o_2$, the complexity is given by

Table 6
(D_{bgd} vs D_{reg} for the hybrid approach on an RBS dominant system) Experimental values d_{slv} (see Subsection 3.1), d_{ff} and d_{tim} (see Subsection 3.4) in the F_4 algorithm and theoretical values D_{bgd} (from the series (20)) and D_{reg} (from the series (13)) 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 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. The degree of regularity D_{reg} is always larger than the solving degree d_{slv}. The proposed theoretical value 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_{ff}	d_{tim}	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)	5	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)	4	4	4	4	6
	(0, 3)	3	3	3	3	6
4	(4, 0)	4	4	4	4	5
	(3, 1)	4	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_{ff}	d_{tim}	D_{bgd}	D_{reg}
0	(0, 0)	6	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)	5	5	5	5	6
	(2, 1)	5	5	5	5	6
	(1, 2)	5	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

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

where $2 < \omega \leq 3$ is a linear algebra constant and D_{bgd} is given by the minimal total degree in terms whose coefficients are negative in the two-variable power series (20) in Subsection 4.2. 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 summary, the complexity in classical gates of the RBS attack against Rainbow with a parameter set (q, v, o_1, o_2) is given as the minimal value of

$$\begin{cases} q^{k_1+k_2} \cdot \binom{n-k_1-k_2+D_{bgd}}{D_{bgd}}^{\omega} & \text{if } k_1 < v+o_1 \text{ and } k_2 < o_2, \\ q^{k_1+k_2} \cdot (2(o_2+1)(v+o_1)(o_2-k_2) + (o_2-k_2)^{\omega}) & \text{if } k_1 = v+o_1 \text{ and } k_2 < o_2, \\ q^{k_1+k_2} \cdot (2(v+o_1+1)(v+o_1-k_1)o_2 + (v+o_1-k_1)^{\omega}) & \text{if } k_1 < v+o_1 \text{ and } k_2 = o_2, \\ q^{k_1+k_2} & \text{if } k_1 = v+o_1 \text{ and } k_2 = o_2, \end{cases} \tag{21}$$

where $2 < \omega \leq 3$ is a linear algebra constant and D_{bgd} is given by the minimal total degree in terms whose coefficients are negative in the two-variable power series (20), i.e.

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

Moreover, using Grover's algorithm, the complexity in quantum gates is given as the minimal value of

$$\begin{cases} q^{(k_1+k_2)/2} \cdot \binom{n-k_1-k_2+D_{bgd}}{D_{bgd}}^{\omega} & \text{if } k_1 < v+o_1 \text{ and } k_2 < o_2, \\ q^{(k_1+k_2)/2} \cdot (2(o_2+1)(v+o_1)(o_2-k_2) + (o_2-k_2)^{\omega}) & \text{if } k_1 = v+o_1 \text{ and } k_2 < o_2, \\ q^{(k_1+k_2)/2} \cdot (2(v+o_1+1)(v+o_1-k_1)o_2 + (v+o_1-k_1)^{\omega}) & \text{if } k_1 < v+o_1 \text{ and } k_2 = o_2, \\ q^{(k_1+k_2)/2} & \text{if } k_1 = v+o_1 \text{ and } k_2 = o_2. \end{cases} \tag{22}$$

Table 7
(Classical attacks) In the RBS attack, the old complexity $\log_2(\sharp\text{classical gates})$ using D_{reg} and the new complexity using D_{bgd}.

Parameter set	Direct	MinRank	HighRank	UOV	RBS	
					old	new
Ia	164.5	161.3	150.3	149.2	145.0	**142.9**
IIIc	215.2	585.1	313.9	563.8	217.4	**206.4**
Vc	275.4	778.8	411.2	747.4	278.6	**267.4**

Table 8
(Quantum attacks) The new complexity $\log_2(\sharp\text{quantum gates})$ of the RBS attack using D_{bgd} and the complexity of the HighRank attack in Table 3.

Parameter set	Direct	MinRank	HighRank	UOV	RBS
					new
Ia	146.5	95.3	**86.3**	87.2	87.3
IIIc	183.5	309.1	**169.9**	295.8	170.8
Vc	235.5	406.8	**219.2**	393.4	220.0

We explain that the RBS attack using the hybrid approach at $k_2 = o_2$ becomes similar to the HighRank attack [8]. Since a Rainbow central map has low rank matrices $M_{f_1}, \ldots, M_{f_{o_1}}$ (see the form (4)), we can obtain a lower-rank quadratic polynomial by finding a linear combination of $M_{p_1}, \ldots, M_{p_m}$. For $o_2 + 1$ matrices from $M_{p_1}, \ldots, M_{p_m}$, the HighRank attack recovers such a quadratic polynomial by finding a linear combination of matrices whose kernel subspace is of dimension one. On the other hand, the RBS attack using the hybrid approach at $k_2 = o_2$ fixes o_2 values $\lambda_{v+o_1+1}, \ldots, \lambda_{v+o_1+o_2}$ to obtain a linear combination

$$M_{p_1} + \sum_{j=1}^{o_2} \lambda_{v+o_1+j} M_{p_{o_1+j}}$$

of $o_2 + 1$ matrices $M_{p_1}, M_{p_{o_1+1}}, \ldots, M_{p_{o_1+o_2}}$ and solves a system of linear equations (8) in $v + o_1 - k_1$ variables. Then the attack has a lower-rank quadratic polynomial and becomes a HighRank attack. Although this attack with $k_1 > 0$ corresponds a HighRank attack with the hybrid approach, we set $k_1 = 0$ to compare the HighRank attack [8]. Note that, in the next subsection, we will show this case is the best in quantum gates for the proposed Rainbow parameter sets. Then, by the formula (21), the complexity in classical gates is given by

$$q^{o_2} \cdot (2(v + o_1 + 1)(v + o_1)o_2 + (v + o_1)^{\omega}), \tag{23}$$

where $2 < \omega \leq 3$ is a linear algebra constant. On the other hand, in [13], the complexity of the HighRank attack [8] is given by

$$q^{o_2} \cdot (o_2(v + o_1 + o_2)^2 + (v + o_1 + o_2)^{\omega}/6). \tag{24}$$

For parameter sets such that $o_1 = o_2$ and $v = \varepsilon o_i$ with a constant ε, the substituting part dominates this complexity when $\omega < 3$. Then the complexities (23) and (24) are $2(\varepsilon+1)^2 o_i^3 q^{o_2}$ and $(\varepsilon+2)^2 o_i^3 q^{o_2}$, respectively, and the HighRank attack [8] is better than that from the RBS attack when $\varepsilon > \sqrt{2}$. However, their difference is only a constant multiple. In quantum gates, the same can be seen from the above discussion replaced q^{o_2} by $q^{o_2/2}$. Note that, since the complexity $(v + o_1 + o_2)^{\omega}/6$ dropped the substituting part from (24) is used in Table 8, the complexity for the Rainbow parameter set Ia (i.e. $\varepsilon = 1$) is better than that for the RBS attack.

5.2. Updated complexity estimation for the NIST PQC 2nd round

In this subsection, applying our theoretical value to the complexity formula [14] used in the NIST PQC 2nd round, we obtain new complexities of the RBS attack against the proposed Rainbow parameter sets. Moreover, we investigate whether the used formula is suitable for the RBS attack.

In the NIST PQC standardization project, the Rainbow designer applies the degree of regularity D_{reg} to the following complexity formula [14,36] of the Wiedemann XL algorithm, which is better than the formula (9), and it estimates the complexity of the RBS attack.

$$\min_k q^k \cdot 3 \cdot \binom{n-k+d_{slv}}{d_{slv}}^2 \cdot \binom{n-k}{2}. \tag{25}$$

In Table 7 and Table 8, applying our theoretical value D_{bgd} to the complexity formula (25), we deduce the complexities of the RBS attack against the Rainbow parameter sets proposed in the NIST PQC 2nd round (see Remark 5.2 for details).

In classical gates, Table 7 shows that the RBS attack is the best among known attacks. Furthermore, although the Rainbow parameter sets Ia, IIIc and Vc are designed for NIST security categories I ($\geq 2^{143}$), III/IV ($\geq 2^{207}$) and V/VI ($\geq 2^{272}$) in Table 1, respectively, Table 7 also shows that they do not satisfy these conditions. In quantum gates, Table 8 shows that the complexities of the RBS attack against the parameter sets Ia, IIIc and Vc are almost similar to those of the HighRank attack [8] in Table 3 (see Section 5.1 and Remark 5.2). Here, we took a linear algebra constant as $\omega = 2.3728639$ [19]. Consequently, for the complexity estimation [14] using the formula (25), a slight modification of the proposed parameter sets is required [15]. In fact, Perlner and Smith-Tone (NIST team) [27] also propose a similar theoretical value to our work and suggest the small parameter changes (see Remark 5.1), and the Rainbow designer proposes the new parameters in the NIST PQC 3rd round [15,30]. The next paragraph shows that the actual complexity of the Wiedemann XL algorithm with an RBS dominant system may be worse than the complexity estimation using the formula (25) with D_{reg} or D_{bgd}.

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 by finding a specific kernel vector of an extended Macaulay matrix and uses the Wiedemann algorithm to find this vector. If the extended Macaulay matrix up to a degree is full rank,[1] its kernel vector derives a unique solution to this system (see Remark 5.1). Note that this unique solution provides the Gröbner basis of degree one. However, in our experiment on scaled-down Rainbow parameters in the NIST PQC 2nd round, an extended Macaulay matrix up to D_{reg} or D_{bgd} has a big kernel space, and the XL algorithm requires an iteration of the Wiedemann algorithm. Hence, although the complexity estimation using the formula (25) 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.

Remark 5.1. Perlner and Smith-Tone [27] introduce an XL algorithm that arranges polynomials extended from an RBS dominant system according to its bi-degree. They claim that this XL algorithm terminates within the bi-degree of the lowest term whose coefficient is non-positive in the two-variable power series (16). Since the XL algorithm generates a smaller Macaulay matrix up to the bi-degree, they improve the formula (25) and conclude that the parameter sets Ia, IIIc and Vc fall short of the claimed security levels in [14] by at least 3, 6 and 10 bits, respectively. In [3], Beullens proposes two new attacks, i.e. the Intersection attack and the Rectangular MinRank attack. The latter shows that the cost of key recovery against the parameter sets I, III and V proposed in the NIST PQC 3rd round is reduced by a factor of $2^{20}, 2^{40}$ and 2^{55}, respectively. Although quadratic systems solved in his attacks are different from the RBS dominant system, they are bi-graded. Hence we can apply our analysis to these systems and obtain an estimation for the attacks. However, for his attacks, our estimation is worse than the estimation in [3]. This is because our analysis uses only information of the bi-degree of a bi-graded system, and his analysis further utilizes a feature of bi-graded systems solved in his attacks.

Remark 5.2. We describe calculating the complexities of Table 7 and Table 8 for the RBS attack. In Table 7, for a fixed Rainbow parameter set (q, v, o_1, o_2), the best complexity of the RBS attack is given as the minimal value of (21) replaced (9) by (25) in the two parameters (k_1, k_2) of the hybrid approach. For the Rainbow parameter set Ia $(q, v, o_1, o_2) = (16, 32, 32, 32)$, the best complexity occurs at $(k_1, k_2) = (0, 1)$ and is given by

$$q^k \cdot 3 \cdot \binom{n-k+D_{bgd}}{D_{bgd}}^2 \binom{n-k}{2} = 16 \cdot 3 \cdot \binom{3\cdot 32-1+15}{15}^2 \binom{3\cdot 32-1}{2} \approx 2^{142.9},$$

where $k = k_1 + k_2 = 1$, $n = v + o_1 + o_2 = 3 \cdot 32$ and $D_{bgd} = 15$ deduced from (20). Similarly, for the Rainbow parameter set IIIc and Vc, the complexity (25) is the minimum at $(k_1, k_2) = (0, 0)$, and $D_{bgd} = 23$ and 30, respectively. Note that, since $D_{bgd} < q$ and the coefficient of $t^{D_{reg}}$ in (11) are negative, the assumptions of Theorem 4.4 and Theorem 4.5 hold. Moreover, in Table 8, we use the following formula as (25) using Grover's algorithm:

$$\min_k q^{k/2} \cdot 3 \cdot \binom{n-k+d_{slv}}{d_{slv}}^2 \cdot \binom{n-k}{2}. \tag{26}$$

Then the best complexity of the RBS attack in quantum gates is given as the minimal value of (22) replaced (10) by (26) in two parameters (k_1, k_2) of the hybrid approach. For the Rainbow parameter set Ia $(q, v, o_1, o_2) = (16, 32, 32, 32)$, the best complexity (22) occurs at $(k_1, k_2) = (0, o_2)$ and is given by

$$\begin{aligned} &q^{(k_1+k_2)/2} \cdot (2(v+o_1+1)(v+o_1-k_1)o_2 + (v+o_1-k_1)^\omega) \\ &= 16^{32/2} \cdot (2(64+1) \cdot 64 \cdot 32 + 64^{2.3728639}) \approx 2^{87.3}. \end{aligned}$$

Moreover, for the Rainbow parameter set IIIc and Vc, the complexity (22) is also the minimum at $(k_1, k_2) = (0, o_2)$. Then the RBS attack becomes similar to the HighRank attack (see the last paragraph of Subsection 5.1).

[1] The rank of a Macaulay matrix is equal to the number of monomials of its degree or less other than the constant term 1.

6. Conclusion

In this article, we introduced the theoretical value D_{bgd} for estimating the complexity of Gröbner basis algorithms with bi-graded polynomial systems. Since the RBS attack recovers a secret key of Rainbow by solving a certain bi-graded polynomial system, we can utilize D_{bgd} to estimate the complexity of this attack.

According to our experiments on scaled-down Rainbow parameter sets in the NIST PQC 2nd round, the theoretical value D_{bgd} tightly approximates its solving degree than the degree of regularity D_{reg}, which has been used previously. Moreover, we proved that the relation $D_{bgd} \leq D_{reg}$ holds when the coefficient of the term of degree D_{reg} in the one-variable power series deriving D_{reg} is negative. We also proved that the value D_{bgd} is an upper bound for the first fall degree of a bi-graded polynomial system satisfying the condition $D_{bgd} < q$ where q is the order of a field.

Furthermore, the RBS attack can reduce the bi-graded polynomial system to a linear system by using a hybrid approach with a special setting. Then this attack becomes similar to the HighRank attack. Thus, we can obtain a new complexity estimation of the RBS attack.

Applying our theoretical value to the complexity formula used in the NIST PQC 2nd round, the proposed parameter sets Ia, IIIc and Vc are solved in $2^{142.9}$, $2^{206.4}$ and $2^{267.4}$ in classical gates, respectively. Therefore, a slight modification of the parameter sets is required. However, it is not clear whether the used complexity formula is suitable for the Wiedemann XL algorithm with an RBS dominant system, and future investigations on the security of the parameter sets are needed.

The two-variable power series used for deducing the theoretical value D_{bgd} is widely available and can be extended more generally. In fact, Beullens's recent work [3] using an estimation with such a power series shows that the cost of key recovery against the new Rainbow parameter sets I, III and V in the NIST PQC 3rd round is reduced by a factor of $2^{20}, 2^{40}$ and 2^{55}, respectively. Therefore, as future work, we need to investigate such an influence on the security of several other schemes.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

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

Appendix

In this appendix, we provide the proofs of Theorem 4.4 and Theorem 4.5 (see [25] for details).

Let R be a commutative ring. For $(h_1, \ldots, h_m) \in R^m$, we define an R-module homomorphism

$$R^m \to R, (b_1, \ldots, b_m) \mapsto \sum_{i=1}^{m} b_i h_i.$$

Then we denote by $\mathrm{Syz}_R(h_1, \ldots, h_m)$, or simply $\mathrm{Syz}(h_1, \ldots, h_m)$, the kernel of this homomorphism and its element is called a *syzygy* of $(h_1, \ldots, h_m)$. For example,

$$\pi_{ij} := (0, \ldots, 0, \underset{i}{-h_j}, 0, \ldots, 0, \underset{j}{h_i}, 0, \ldots, 0),$$

where $1 \leq i < j \leq m$, is such an element. Here, we denote by $\mathrm{KSyz}(h_1, \ldots, h_m)$ the submodule generated by the elements π_{ij} and its element is called a *Koszul syzygy*.

We assume that R be a bi-graded commutative ring. For bi-graded elements $h_1, \ldots, h_m \in R$ with $\mathbf{d}_i = \deg_{\mathbb{Z}^2_{\geq 0}} h_i$ and the free module $E = R^m$ with the standard basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$, we denote by K_i the i-th exterior power $\bigwedge^i E$ and give the *Koszul complex*

$$K(h_1, \ldots, h_m)_\bullet : \cdots \xrightarrow{\delta_4} K_3 \xrightarrow{\delta_3} K_2 \xrightarrow{\delta_2} K_1 \xrightarrow{\delta_1} R \to 0$$

by $\delta_l(\mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_l}) = \sum_{k=1}^{l} (-1)^{k+1} h_{i_k} \mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_{k-1}} \wedge \mathbf{e}_{i_{k+1}} \wedge \cdots \wedge \mathbf{e}_{i_l}$. Then we denote by $H_i(K(h_1, \ldots, h_m)_\bullet)$ the i-th homology group of the complex. Moreover, since δ_l are homogeneous, we denote by $K(h_1, \ldots, h_m)_{\mathbf{d}}$ the complex consisting of degree $\mathbf{d}$ components in $K(h_1, \ldots, h_m)_\bullet$. Then we have $H_i(K(h_1, \ldots, h_m)_\bullet)_{\mathbf{d}} = H_i(K(h_1, \ldots, h_m)_{\mathbf{d}})$. Note that

$$H_1(K(h_1, \ldots, h_m)_\bullet)_{\mathbf{d}} = \mathrm{Syz}(h_1, \ldots, h_m)_{\mathbf{d}} / \mathrm{KSyz}(h_1, \ldots, h_m)_{\mathbf{d}}.$$

Define $K(h_1,\dots,h_m)_\bullet(-\mathbf{d})$ as $K(h_1,\dots,h_m)_{\mathbf{d}_0}(-\mathbf{d}) := K(h_1,\dots,h_m)_{\mathbf{d}_0-\mathbf{d}}$ for any $\mathbf{d}_0$. Since $K(h_1,\dots,h_m)_\bullet$ is the mapping cone of

$$K(h_1,\dots,h_{m-1})_\bullet(-\mathbf{d}_m) \overset{\times h_m}{\to} K(h_1,\dots,h_{m-1})_\bullet,$$

we can obtain the following long exact sequence (see [9,31]):

$$\begin{aligned}\cdots \to H_2(K(h_1,\dots,h_{m-1})_\bullet)(-\mathbf{d}_m) &\overset{\times h_m}{\to} H_2(K(h_1,\dots,h_{m-1})_\bullet) \to H_2(K(h_1,\dots,h_m)_\bullet)\\ \to H_1(K(h_1,\dots,h_{m-1})_\bullet)(-\mathbf{d}_m) &\overset{\times h_m}{\to} H_1(K(h_1,\dots,h_{m-1})_\bullet) \to H_1(K(h_1,\dots,h_m)_\bullet)\\ \to R/\langle h_1,\dots,h_{m-1}\rangle(-\mathbf{d}_m) &\overset{\times h_m}{\to} R/\langle h_1,\dots,h_{m-1}\rangle \to R/\langle h_1,\dots,h_m\rangle \to 0\end{aligned} \tag{27}$$

Definition A. Let $\preceq$ be a well-ordering on $\mathbb{Z}^2_{\geq 0}$.

1. For a bi-graded commutative ring $R=\oplus_{\mathbf{d}}R_{\mathbf{d}}$ and two variables t_1 and t_2, the Hilbert series $\mathrm{HS}_R(\mathbf{t})$ of R is defined as $\mathrm{HS}_R(\mathbf{t})=\sum_{\mathbf{d}\in\mathbb{Z}^2_{\geq 0}}(\dim R_{\mathbf{d}})\mathbf{t}^{\mathbf{d}}\in\mathbb{Z}[[t_1,t_2]]$ where $\mathbf{t}=(t_1,t_2)$ and $\mathbf{t}^{\mathbf{d}}=t_1^{d_1}t_2^{d_2}$.
2. For two elements a,b of the formal power series ring $\mathbb{Z}[[t_1,t_2]]$, we denote $a\equiv_{\preceq\mathbf{d}} b$ if the coefficients of these monomials of degree less than or equal to $\mathbf{d}$ with respect to $\preceq$ are the same.
3. For a $\mathbb{Z}^2_{\geq 0}$-graded module M over a $\mathbb{Z}^2_{\geq 0}$-graded commutative ring R, i.e. it has $M=\bigoplus_{\mathbf{d}\in\mathbb{Z}^2_{\geq 0}}M_{\mathbf{d}}$ such that $R_{\mathbf{d}_1}M_{\mathbf{d}_2}\subseteq M_{\mathbf{d}_1+\mathbf{d}_2}$ for any $\mathbf{d}_i$, we put $M_{\preceq\mathbf{d}}=\bigoplus_{\mathbf{d}_0\preceq\mathbf{d}}M_{\mathbf{d}_0}$.

Lemma A. *Let S be a graded polynomial ring and $\preceq$ be a well-ordering on $\mathbb{Z}^2_{\geq 0}$ compatible with $<$ on $\mathbb{Z}_{\geq 0}$ such that $\mathbf{a}\prec\mathbf{b}$ if $|\mathbf{a}|<|\mathbf{b}|$ for $\mathbf{a},\mathbf{b}\in\mathbb{Z}^2_{\geq 0}$. Let $h_1,\dots,h_m$ be bi-graded elements such that $\mathbf{d}_i=\deg_{\mathbb{Z}^2_{\geq 0}}h_i\neq 0$. If $H_1(K(h_1,\dots,h_m)_\bullet)_{\preceq\mathbf{d}}=\{0\}$, then we have* $\mathrm{HS}_{S/\langle h_1,\dots,h_m\rangle}(\mathbf{t})\equiv_{\preceq\mathbf{d}}\prod_{i=1}^n(1-\mathbf{t}^{\deg h_i})\mathrm{HS}_S(\mathbf{t})$.

Proof. It is sufficient to prove that if $H_1(K(h_1,\dots,h_m)_\bullet)_{\preceq\mathbf{d}}=\{0\}$, then

$$H_1(K(h_1,\dots,h_l)_\bullet)_{\preceq\mathbf{d}}=\{0\} \text{ for each } 1\leq l\leq m-1. \tag{28}$$

Indeed, if the assertion (28) holds, the long exact sequence (27) gives the injection

$$\times h_l : (S/\langle h_1,\dots,h_{l-1}\rangle)(-\mathbf{d}_l)_{\mathbf{d}_0}\overset{\times h_l}{\to}(S/\langle h_1,\dots,h_{l-1}\rangle)_{\mathbf{d}_0},\ \forall\mathbf{d}_0\preceq\mathbf{d}.$$

Then we have

$$\begin{aligned}&\mathrm{HS}_{S/\langle h_1,\dots,h_m\rangle}(\mathbf{t})=\mathrm{HS}_R(\mathbf{t})-\mathrm{HS}_{\langle h_m\rangle_R}(\mathbf{t})\\ &\equiv_{\preceq\mathbf{d}}\mathrm{HS}_R(\mathbf{t})-\mathrm{HS}_R(\mathbf{t})\cdot\mathbf{t}^{\deg h_m}=(1-\mathbf{t}^{\deg h_m})\mathrm{HS}_R(\mathbf{t}),\end{aligned}$$

where $R=S/\langle h_1,\dots,h_{m-1}\rangle$. Thus, it follows Lemma A.

In (28), we first prove the case $l=m-1$. Suppose that there exists the minimum $\mathbf{d}'$ such that $H_1(K(h_1,\dots,h_{m-1})_\bullet)_{\mathbf{d}'}\neq 0$. Then, by $|\mathbf{d}_m|>0$ and $\mathbf{d}'\succ\mathbf{d}'-\mathbf{d}_m$, we obtain

$$H_1(K(h_1,\dots,h_{m-1})_\bullet)(-\mathbf{d}_m)_{\mathbf{d}'}=H_1(K(h_1,\dots,h_{m-1})_\bullet)_{\mathbf{d}'-\mathbf{d}_m}=0.$$

Hence we have $H_1(K(h_1,\dots,h_m)_\bullet)_{\mathbf{d}'}\neq 0$ by the short exact sequence

$$H_1(K(h_1,\dots,h_{m-1})_\bullet)(-\mathbf{d}_m)_{\mathbf{d}'}\overset{\times h_m}{\to}H_1(K(h_1,\dots,h_{m-1})_\bullet)_{\mathbf{d}'}\to H_1(K(h_1,\dots,h_m)_\bullet)_{\mathbf{d}'},$$

in the long exact sequence (27). Since $H_1(K(h_1,\dots,h_m)_\bullet)_{\preceq\mathbf{d}}=0$, we have $\mathbf{d}\prec\mathbf{d}'$. Therefore $H_1(K(h_1,\dots,h_{m-1})_\bullet)_{\preceq\mathbf{d}}=0$. Similarly, we can prove the cases $l=m-2,m-3,\dots,1$. □

The polynomial ring $S=\mathbb{F}[x_1,\dots,x_{n_1},y_1,\dots,y_{n_2}]$ is a bi-graded commutative ring with $x_i=(1,0)$, $y_i=(0,1)\in\mathbb{Z}^2_{\geq 0}$. Then its Hilbert series is the following:

Lemma B. *For the bi-graded polynomial ring $S=\mathbb{F}[x_1,\dots,x_{n_1},y_1,\dots,y_{n_2}]$ with $x_i=(1,0)$, $y_i=(0,1)\in\mathbb{Z}^2_{\geq 0}$, we have* $\mathrm{HS}_S(\mathbf{t})=1/(1-t_1)^{n_1}(1-t_2)^{n_2}$.

Thus, for bi-graded polynomials $h_1,\dots,h_m$ in S, under the assumption of Lemma A, the Hilbert series $\mathrm{HS}_{S/\langle h_1,\dots,h_m\rangle}(\mathbf{t})$ is computed by

$$\frac{\prod_{i=1}^{n}(1-\mathbf{t}^{\deg h_i})}{(1-t_1)^{n_1}(1-t_2)^{n_2}} \tag{$*$}$$

that is (16) in Definition 4.3. Note that this power series deduces the theoretical value D_{bgd}.

Proposition A. *For bi-graded polynomials $h_1,\ldots,h_m$, we have* $\min\{d \geq 0 \mid H_1(K(h_1,\ldots,h_m)_\bullet)_d \neq \{0\}\} \leq D_{bgd}(h_1,\ldots,h_m)$.

Proof. Consider the two-variable power series $(*)$. Then, by Lemma B, there exists $\mathbf{d}=(d_1,d_2)$ such that $\mathrm{HS}_{S/\langle h_1,\ldots,h_m\rangle}(\mathbf{t}) \not\equiv_{\preceq \mathbf{d}} \prod_{i=1}^{n}(1-\mathbf{t}^{\deg h_i})\mathrm{HS}_S(\mathbf{t})$ and $d_1+d_2=D_{bgd}$. Thus, by Lemma A, it follows that $H_1(K(h_1,\ldots,h_m)_\bullet)_{D_{bgd}} \neq \{0\}$. □

Now, we can prove Theorem 4.5 as follows.

Proof of Theorem 4.5. Let $h_i = f_i^{top}$ and $B=\mathbb{F}_q[x_1,\ldots,x_n]/\langle x_1^q,\ldots,x_n^q\rangle$. We use the notation in Definition 4.1. Put

$$d=\min\{d\geq 0 \mid H_1(K(h_1,\ldots,h_m)_\bullet)_d \neq \{0\}\}.$$

Since $H_1(K(h_1,\ldots,h_m)_\bullet)_d \neq 0$, there exists

$$\rho \in \mathrm{Syz}_R(h_1,\ldots,h_m)_d \setminus \mathrm{KSyz}_R(h_1,\ldots,h_m)_d.$$

In particular, $\overline{\rho} \in \mathrm{Syz}_B(\overline{h_1},\ldots,\overline{h_m})_d$. Although an element $\overline{b_i}\overline{\tau_i}$ for $\overline{b_i} \in B_{d-d_0(q-1)}$ is contained in $\mathrm{TSyz}_B(\overline{h_1},\ldots,\overline{h_m})_d$ as generators, they do not appear since $B_{d-d_0(q-1)}=0$ by $d_0\geq 2$ and $q>d$. Thus, if there exists $\overline{\rho}\in\mathrm{TSyz}_B(\overline{h_1},\ldots,\overline{h_m})_d$, then $\overline{\rho}=\sum_{i,j}\overline{b}_{ij}\overline{\pi}_{ij}$ for some $\overline{b}_{ij}$ where $\deg b_{ij}=d-d_0$ as a representative. Namely,

$$\rho-\sum_{i,j} b_{ij}\pi_{ij} \in \langle x_1^q,\ldots,x_n^q\rangle^m.$$

Since $d\leq D_{bgd}(h_1,\ldots,h_m)<q$ by Proposition A, we have $\rho-\sum_{i,j}b_{ij}\pi_{ij}=(0,\ldots,0)$. Thus, we obtain a contradiction $\rho=\sum_{i,j}b_{ij}\pi_{ij}\in\mathrm{KSyz}(h_1,\ldots,h_m)_d$. Therefore, $D_{ff}(h_1,\ldots,h_m)\leq d$, and it follows that

$$D_{ff}(h_1,\ldots,h_m)\leq D_{bgd}(h_1,\ldots,h_m). \quad \square$$

References

[1] M. Bardet, J.C. Faugère, B. Salvy, B.Y. Yang, Asymptotic behavior of the index of regularity of quadratic semi-regular polynomial systems, in: 8th International Symposium on Effective Methods in Algebraic Geometry (MEGA), 2005, pp. 1–14.
[2] L. Bettale, J.C. Faugère, L. Perret, Hybrid approach for solving multivariate systems over finite fields, J. Math. Cryptol. 3 (2009) 177–197.
[3] W. Beullens, Improved Cryptanalysis of UOV and Rainbow, arXiv.org e-Print archive, https://eprint.iacr.org/2020/1343, 30 October 2020.
[4] O. Billet, H. Gilbert, Cryptanalysis of Rainbow, in: R. De Prisco, M. Yung (Eds.), SCN 2006, in: LNCS, vol. 4116, Springer, 2006, pp. 336–347.
[5] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symb. Comput. 24 (1997) 235–265.
[6] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, PhD thesis, Universität Innsbruck, 1965.
[7] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, 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. (Accessed 22 September 2020).
[8] D. Coppersmith, J. Stern, S. Vaudenay, Attacks on the birational signature scheme, in: D.R. Stinson (Ed.), CRYPTO 1994, in: LNCS, vol. 773, Springer, 1994, pp. 435–443.
[9] C. Diem, Bound of regularity, J. Algebra 423 (2015) 1143–1160.
[10] J. Ding, D.S. Schmidt, Rainbow, a new multivariable polynomial signature scheme, in: J. Ioannidis, A.D. Keromytis, M. Yung (Eds.), ACNS 2005, in: LNCS, vol. 3531, Springer, 2005, pp. 164–175.
[11] J. Ding, J.E. Gower, D.S. Schmidt, Multivariate Public Key Cryptosystems, Springer, 2006.
[12] J. Ding, D.S. Schmidt, Solving degree and degree of regularity for polynomial systems over a finite fields, in: Number Theory and Cryptography, in: LNCS, vol. 8260, Springer, 2013.
[13] J. Ding, B.-Y. Yang, C.-H.O. Chen, M.-S. Chen, C.-M. Cheng, New differential-algebraic attacks and reparametrization of Rainbow, in: S.M. Bellovin, R. Gennaro, A.D. Keromytis, M. Yung (Eds.), ACNS 2008, in: LNCS, vol. 5037, Springer, 2008, pp. 242–257.
[14] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, Rainbow - Algorithm Specification and Documentation, Specification document of NIST PQC 2nd round submission package, 2019.
[15] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, Rainbow - Algorithm Specification and Documentation, Specification document of NIST PQC 3rd round submission package, 2020.
[16] V. Dubois, N. Gama, The degree of regularity of HFE systems, in: M. Abe (Ed.), ASIACRYPT 2010, in: LNCS, vol. 6477, Springer, Berlin, 2010, pp. 557–576.
[17] J.C. Faugère, A new efficient algorithm for computing Gröbner bases (F4), J. Pure Appl. Algebra 139 (1) (1999) 61–88.
[18] J.C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), in: P. Bose, P. Morin (Eds.), ISSAC 2002, 2002, pp. 75–83.
[19] F.L. Gall, Algebraic complexity theory and matrix multiplication, in: K. Nabeshima (Ed.), ISSAC 2014, Kobe, Japan, July 23-25, 2014.
[20] M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman & Co., New York, 1979.
[21] A. Kipnis, A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in: H. Krawczyk (Ed.), CRYPTO 1998, in: LNCS, vol. 1462, Springer, 1998, pp. 257–266.
[22] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar schemes, in: J. Stern (Ed.), EUROCRYPT 1999, in: LNCS, vol. 1592, Springer, 1999, pp. 206–222.

[23] NIST, Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf, 2016. (Accessed 22 September 2020).
[24] Shuhei Nakamura, Y. Ikematsu, Y. Wang, J. Ding, T. Takagi, New Complexity Estimation on the Rainbow-Band-Separation Attack, IACR Cryptology ePrint Archive, Report 2020/703, 11 June 2020, https://eprint.iacr.org/2020/703.pdf.
[25] Shuhei Nakamura, Formal power series on algebraic cryptanalysis, arXiv.org e-Print archive, arXiv:2007.14729, 30 July 2020.
[26] J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, in: U. Maurer (Ed.), EUROCRYPT 1996, in: LNCS, vol. 1070, Springer, 1996, pp. 33–48.
[27] R. Perlner, D. Smith-Tone, Rainbow Band Separation is Better than we Thought, Cryptology ePrint Archive, Report 2020/702, 2020, https://eprint.iacr.org/2020/702. (Accessed 22 September 2020).
[28] A. Petzoldt, S. Bulygin, J. Buchmann, Selecting parameters for the Rainbow signature scheme, in: N. Sendrier (Ed.), PQCrypto 2010, in: LNSC, vol. 6061, Springer, 2010, pp. 218–240.
[29] A. Petzoldt, S. Bulygin, J. Buchmann, Selecting parameters for the Rainbow signature scheme - extended version, http://eprint.iacr.org/2010/437, 2010. (Accessed 22 September 2020).
[30] 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, http://precision.moscito.org/by-publ/recent/rainbow-pars.pdf, June 22, 2020. (Accessed 22 September 2020).
[31] H. Schenck, Computational Algebraic Geometry, London Mathematical Society Student Texts, vol. 58, Cambridge University Press, 2003.
[32] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (5) (1997) 1484–1509.
[33] E. Thomae, 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. (Accessed 22 September 2020).
[34] B.-Y. Yang, J.-M. Chen, N. Courtois, On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis, in: ICICS 2004, in: LNCS, vol. 3269, Springer, 2004, pp. 401–413.
[35] B.-Y. Yang, J.-M. Chent, All in the XL family: theory and practice, in: C. Park, S. Chee (Eds.), ICISC 2004, in: LNCS, vol. 3506, Springer, Heidelberg, 2007, pp. 67–86.
[36] B.-Y. Yang, O.C.-H. Chen, D.J. Bernstein, J.-M. Chen, Analysis of QUAD, in: A. Biryukov (Ed.), Fast Software Encryption, FSE 2007, in: LNCS, vol. 4593, Springer, 2007.