Recent progress in the security evaluation of multivariate public-key cryptography

Ikematsu, Yasuhiko
Institute of Mathematics for Industry, Kyushu University

Nakamura, Shuhei
Department of Liberal Arts and Basic Sciences, Nihon University

Takagi, Tsuyoshi
Department of Mathematical Informatics, The University of Tokyo

出版情報：IET Information Security. 17 (2), pp.210-226, 2022-09-03. Institution of Engineering and Technology (IET)
バージョン：

Received: 11 November 2021 | Revised: 16 March 2022 | Accepted: 17 August 2022

IET Information Security

DOI: 10.1049/ise2.12092

The Institution of Engineering and Technology WILEY

REVIEW

Recent progress in the security evaluation of multivariate public-key cryptography

Yasuhiko Ikematsu[1] | Shuhei Nakamura[2] | Tsuyoshi Takagi[3]

[1]Institute of Mathematics for Industry, Kyushu University, Nishi-ku, Fukuoka, Japan

[2]Department of Liberal Arts and Basic Sciences, Nihon University, Narashino, Chiba, Japan

[3]Department of Mathematical Informatics, The University of Tokyo, Bunkyo-ku, Tokyo, Japan

Correspondence

Yasuhiko Ikematsu, Institute of Mathematics for Industry, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, Japan.
Email: ikematsu@imi.kyushu-u.ac.jp

Funding information

Core Research for Evolutional Science and Technology, Grant/Award Number: JPMJCR2113; Japan Society for the Promotion of Science, Grant/Award Numbers: JP19K20266, JP20K19802

Abstract

Multivariate public-key cryptography (MPKC) is considered a leading candidate for post-quantum cryptography (PQC). It is based on the hardness of the multivariate quadratic polynomial (MQ) problem, which is a problem of finding a solution to a system of quadratic equations over a finite field. In this paper, we survey some recent progress in the security analysis of MPKC. Among various existing multivariate schemes, the most important one is the Rainbow signature scheme proposed by Ding et al. in 2005, which was later selected as a finalist in the third round of the PQC standardization project by the National Institute of Standards and Technology. Under the circumstances, some recent research studies in MPKC have focussed on the security analysis of the Rainbow scheme. In this paper, the authors first explain efficient algorithms for solving the MQ problem and the research methodology for estimating their complexity in MPKC. Then, the authors survey some recent results related to the security analysis of the Rainbow scheme. In particular, the authors provide a detailed description of the complexity analysis for solving the bi-graded polynomial systems studied independently by Nakamura et al. and Smith-Tone et al., and then expound the rectangular MinRank attack against Rainbow proposed by Beullens.

1 | INTRODUCTION

By Shor's quantum algorithms [1] in 1994, it is known that widely used public-key cryptosystems, such as RSA and ECC, can be broken if a large-scale quantum computer is built. Thus, it is important to study public-key cryptography that can potentially resist such quantum computer attacks, which is called post-quantum cryptography (PQC) [2]. In 2016, the National Institute of Standards and Technology (NIST) announced a PQC standardization project [3]. This project has now advanced to the third round, and PQC has been more actively researched.

Multivariate public-key cryptography (MPKC) (cf., Ref. [4]) is a leading candidate for PQC and is constructed using multivariate quadratic polynomial (MQ) maps $\mathcal{P}$ over a finite field $\mathbb{F}_q$ with a trap-door structure. The security of MPKC is dependent on the hardness of the multivariate quadratic polynomial (MQ) problem, which is to find a solution to a system of quadratic equations over a finite field. The MQ problem is known to be NP-hard [5].

MPKC has a relatively old history in PQC, and the first multivariate scheme was proposed by Matsumoto and Imai in 1988, called the MI scheme [6]. Subsequently, as a generalisation of the MI scheme, the Hidden Field Equation (HFE) scheme was proposed in 1996 by Patarin [7]. There are several signature schemes based on the HFE scheme such as GeMMS [8] and Gui [9]. Apart from that, the unbalanced oil and vinegar (UOV) signature scheme [10] is a well-established signature scheme proposed by Kipnis et al. in 1999. As its efficient multilayer variant, the Rainbow scheme was proposed by Ding et al. [11] in 2005. Because of its good performance and security, the Rainbow scheme was selected as a finalist in the third round of NIST PQC standardisation [12], and its security analysis has become an important research topic of MPKC. In addition, as a multivariate scheme without using any trap-door of special algebraic structure, in 2011 Sakumoto et al. [13] proposed an identification scheme that is proven to be secure purely under the hardness of the MQ problem. In this way, further more multivariate schemes have

been proposed so far, and MPKC has become a major topic in the research of PQC.

On the other hand, the security analysis of MPKC has also been intensively developed along with the afore-mentioned progress in the explicit constructions of MPKC. In some initial studies in the 90s, the MI scheme [6] was broken by Patarin [14] using the linearisation equation attack. Furthermore, the Oil Vinegar (OV) scheme was broken in polynomial time by Kipnis–Shamir (KS) attack [15] and then improved to its unbalanced variant, called the UOV scheme [15]. We stress that the linearisation attack and KS attack strongly depend on the special algebraic structures of MI and OV schemes, respectively. After those studies, two types of more general attacks applicable to various multivariate schemes have been proposed.

The first one is the direct attack wherein the system of quadratic equations associated with a public key (quadratic map) $\mathcal{P}$ and a ciphertext $\mathbf{w}$ (or signature) of $\mathcal{P}(\mathbf{x}) = \mathbf{w}$ is directly solved. In MPKC research, two major methods are often considered to solve such a system, namely Gröbner basis approaches and Wiedemann extended linearisation (XL) approach. For the F5 Gröbner basis algorithm [16] proposed by Faugère, the first HFE challenge [17] was solved in 2003 by Faugère et al. [18]. However, it is a non-trivial problem to evaluate the complexity of the direct attack. To study its accurate estimation, the degree of regularity d_{reg} and the first fall degree d_{ff} are extensively researched in Ref. [19–21] and so on. The complexity of solving semi-regular systems of quadratic equations is accurately estimated by the degree of regularity. However, many quadratic systems appearing in MPKC are not semi-regular, and thus the analysis of the first fall degree is an important research topic in MPKC. It has been shown that the first fall degree for the HFE scheme and its variants can be precisely estimated [20, 22, 23].

The second one is the MinRank attack, which exploits the special algebraic structure of MPKC, which was initially applied to the HFE scheme in Ref. [24]. A public key $\mathcal{P}$ of quadratic polynomials in n variables corresponds to some symmetric matrices of size n. The symmetric matrices corresponding to the public key $\mathcal{P}$ often generate a low-rank matrix because of its trapdoor structure. The MinRank attack tries to recover a secret key by finding such a low-rank matrix. Moreover, the related problem to find a low-rank matrix by computing a linear combination of given matrices over a finite field, called the MinRank problem, is another important research in the security analysis of MPKC. The MinRank problem is proven to be NP-hard [25]. In general, the MinRank problem can be solved by searching a hidden kernel space using linear algebra or by reducing it to polynomial systems. The latter method includes the minor modelling methods [26, 27] and the KS method [24], which require the polynomial system to be solved by algorithms used in the direct attack.

1.1 | Contribution

In this paper, we survey some recent progress in the security analysis of MPKC. The direct attack, which was initially developed via the security analysis on the HFE scheme, has become an important and fundamental tool to estimate the complexity of various attacks in MPKC. Moreover, the Rainbow scheme [11] is one of the most influential multivariate schemes owing to its selection as a finalist in the third round of the NIST PQC standardisation project. Some recent progress in MPKC has been made via the security analysis of the Rainbow scheme. Considering this situation, we mainly provide a survey on the following topics: the state-of-the-art approaches for solving polynomial systems used in MPKC and two recently improved attacks on the Rainbow scheme, namely the Rainbow-Band-Separation (RBS) attack [28] using the bi-graded polynomial system and the rectangular MinRank attack [29].

First, we explain the current knowledge on the direct attack. As stated above, there are two main approaches for solving a system of equations in MPKC research, namely, the Gröbner basis approach and Wiedeman XL approach. The Gröbner basis approach is to compute a Gröbner basis of the ideal associated with the solved system $\mathcal{P}(\mathbf{x}) = \mathbf{w}$. The algorithms F4 [30] and F5 [16] are often used in MPKC research. The XL approach tries to solve the linear system obtained from multiplying terms with a certain degree d by the solved system. The Wiedeman XL approach efficiently obtains a solution using the Wiedemann algorithm [31] if the linear system mentioned above is sparse with a few solutions. Note that Ars et al. [32] shows that the XL algorithm is also a Gröbner basis algorithm that can be represented as a redundant variant of the Gröbner basis algorithm F4 [30]. The crucial point for complexity estimation is to determine the appropriate degree d of the Macaulay matrix $\mathcal{M}_d$, inducing a correct solution of the solved system practically. We will explain how to estimate d in MPKC research.

Second, we discuss recent studies on the bi-graded polynomial systems. Though such systems do not appear in the direct attack against general multivariate schemes, they appear in the analysis of a MinRank attack against Rainbow, called the RBS attack [28]. The bi-graded system that appears in the RBS attack was initially analysed under the assumption that the system is semi-regular. However, it is already known in Ref. [33] in 2012 that such a bi-graded system does not behave like semi-regular in some experiments. In 2020, Nakamura et al. [34] and Smith-Tone et al. [35] independently studied the bi-graded systems that appear in the RBS attack. Their studies can show more accurate estimation focussing on the bi-graded structure, and thus it affects the proposed parameters of the Rainbow scheme. In our paper, following the work of Nakamura [36], we will explain the bi-graded version of semi-regularity and degree of regularity, which can be seen as a generalisation of the work by Diem [37] and Bardet et al. [19]. Moreover, following the way of Smith-Tone et al. [35], we will explain how to estimate the computational complexity of the bi-graded systems. Furthermore, we will describe the RBS attack [28], which is the motivation for the study of the bi-graded systems, and explain its complexity estimation using the above discussion.

Finally, we explain the rectangular MinRank attack [29] against the Rainbow scheme proposed by Beullens. This attack is carried out by deforming the MinRank problem associated with the Rainbow scheme to another MinRank problem and

solving it using the support minor modelling method proposed by Bardet et al. [26]. This attack affects the proposed parameters of the Rainbow scheme. We will describe how to deform the MinRank problem for the Rainbow scheme in terms of matrix representation, which was originally done in terms of polynomial representation in Ref. [29]. By using matrix representation, we can provide another description of the rectangular MinRank attack. The system that appears in the rectangular MinRank problem becomes a bi-graded homogeneous system. In Ref. [29], Beullens estimates the complexity of solving the bi-graded system based on the complexity analysis of the support minor modelling method [26], under a generic assumption. We will explicitly describe the generic assumption and explain the complexity estimation of the rectangular MinRank attack in Ref. [29]. We also state the support minor modelling method [26] to solve the MinRank problem.

Our paper is organised as follows. In Section 2, we briefly recall a general construction of multivariate schemes and the Rainbow signature scheme as an example. In addition, we explain how the security of multivariate schemes relates to the hardness of the MQ problem and the MinRank problem. In Section 3, we review some approaches to solve the MQ problem. In Section 4, we discuss the complexity estimations of the MQ problem using the approaches in Section 3. In Section 5, we explain the definition of the bi-graded systems and their complexity analysis to solve them. In addition, we recall the RBS attack against the Rainbow scheme and explain how its complexity is estimated. In Section 6, we explain the rectangular MinRank attack against the Rainbow scheme. Finally, we conclude our paper in Section 7.

2 | MPKC CONSTRUCTION AND ITS SECURITY

In this section, we recall a general construction of multivariate schemes and describe the construction of the Rainbow signature scheme [11] as an example. Subsequently, we review the MQ and MinRank problems, which essentially determine the security of MPKC.

2.1 | General construction

Let n, m be positive integers and $\mathbb{F}_q$ be a finite field with q elements. For m quadratic polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[\mathbf{x}]$ in n variables $\mathbf{x} = (x_1, \ldots, x_n)$ over $\mathbb{F}_q$, we define the following map

$$\mathcal{P} : \mathbb{F}_q^n \ni \mathbf{v} \mapsto (p_1(\mathbf{v}), \ldots, p_m(\mathbf{v})) \in \mathbb{F}_q^m.$$

Such a map is called a quadratic (polynomial) map.

To construct a multivariate scheme, we recall the following definition. Let $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a quadratic map. If for any element $\mathbf{w} \in \mathbb{F}_q^m$ the system of quadratic equations $\mathcal{F}(\mathbf{x}) = \mathbf{w}$ can be solved with less complexity, then $\mathcal{F}$ is said to be *easy-to-invert*. This map is the core object because it determines properties (e.g. security and efficiency) of the multivariate scheme constructed from the map.

In general, a multivariate scheme is constructed as follows. First, choose an easy-to-invert map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$. Next, randomly choose two invertible linear maps $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$. Then a public key is given by the composite

$$\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^m$$

and the secret key is given by $(\mathcal{F}, \mathcal{T}, \mathcal{S})$. Here, it is clear that $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is also a quadratic map.

The property of the easy-to-invert map $\mathcal{F}$ determines whether the constructed scheme becomes an encryption scheme or a signature scheme. In fact, if $\mathcal{F}$ is injective, then the constructed scheme becomes an encryption scheme. Then the encryption process is performed by substituting $\mathbf{c} := \mathcal{P}(\mathbf{m}) \in \mathbb{F}_q^m$ for a message $\mathbf{m} \in \mathbb{F}_q^n$. The decryption process of $\mathbf{c}$ is performed by computing three inverses: $\mathbf{w}_1 := \mathcal{T}^{-1}(\mathbf{c}), \mathbf{w}_2 := \mathcal{F}^{-1}(\mathbf{w}_1)$, and $\mathbf{m} = \mathcal{S}^{-1}(\mathbf{w}_2)$. Here, since $\mathcal{F}$ is easy-to-invert, the decryptor can easily and efficiently compute the inverse $\mathcal{F}^{-1}(\mathbf{w}_1)$. Namely, the decryption process is performed efficiently (See Figure 1).

On the other hand, if $\mathcal{F}$ is surjective, then the constructed scheme becomes a signature scheme. For a message $\mathbf{m} \in \mathbb{F}_q^m$ to be signed, a signature $\mathbf{s} \in \mathbb{F}_q^n$ is generated by three inverses: $\mathbf{w}_1 := \mathcal{T}^{-1}(\mathbf{m}), \mathbf{w}_2 := \mathcal{F}^{-1}(\mathbf{w}_1)$, and $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{w}_2)$. Here, $\mathcal{F}^{-1}(\mathbf{w}_1)$ means an element of the pre-image of the set $\{\mathbf{w}_1\}$ under the surjective map $\mathcal{F}$. The verification process is done by checking whether $\mathcal{P}(\mathbf{s}) = \mathbf{m}$ or not (See Figure 2).

The MI scheme, which was the first multivariate scheme, was proposed in 1988 by Matsumoto and Imai [6]. The corresponding easy-to-invert map $\mathcal{F}$ is constructed by using a monomial map $X \mapsto X^{q^{\theta_1}+q^{\theta_2}}$ on a large finite extension field of $\mathbb{F}_q$. As a generalisation, by extending such a monomial map to a

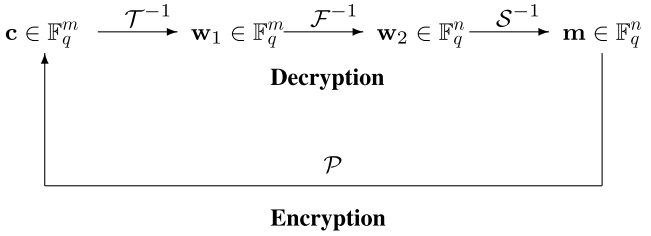

FIGURE 1 General workflow of multivariate encryption schemes

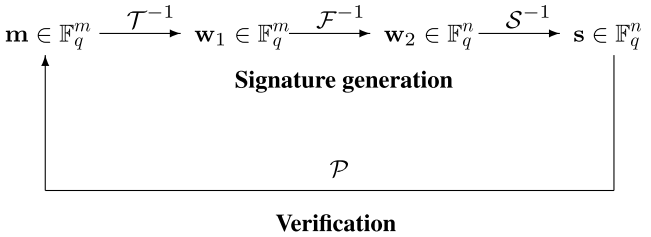

FIGURE 2 General workflow of multivariate signature schemes

polynomial map $X \mapsto \sum_{i,j} a_{ij} X^{q^i + q^j}$ with low degree, the HFE scheme was proposed by Patarin [7] in 1996. Thereafter, several multivariate schemes have been proposed, such as UOV [10], ABC [38], ZHFE [39], EFC [40], Gui [9], GeMMS [8], and HFERP [41]. In the next subsection, we explain the Rainbow [11] signature scheme, which is a variant of UOV [10].

2.2 | Rainbow

In this subsection, we describe Rainbow, a multivariate signature scheme that was proposed by Ding and Schmidt in 2005 [11] as an efficient variant of the UOV scheme [10].

Fix positive integers $v, o_1, o_2 \in \mathbb{N}$, and set $n := v + o_1 + o_2$ and $m := o_1 + o_2$. Let $\mathbf{x}_1 = (x_1, \ldots, x_v)$, $\mathbf{x}_2 = (x_{v+1}, \ldots, x_{v+o_1})$, and $\mathbf{x}_3 = (x_{v+o_1+1}, \ldots, x_n)$ be three sets of variables, and $\mathbf{x} = (x_1, \ldots, x_n)$. An easy-to-invert map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ of Rainbow is defined by

$$\begin{cases} f_1 = \sum_{1 \le i \le j \le v} a_{ij}^{(1)} x_i x_j + \sum_{\substack{1 \le i \le v \\ v+1 \le j \le v+o_1}} a_{ij}^{(1)} x_i x_j, \\ \vdots \\ f_{o_1} = \sum_{1 \le i \le j \le v} a_{ij}^{(o_1)} x_i x_j + \sum_{\substack{1 \le i \le v \\ v+1 \le j \le v+o_1}} a_{ij}^{(o_1)} x_i x_j, \\ f_{o_1+1} = \sum_{1 \le i \le j \le v+o_1} a_{ij}^{(o_1+1)} x_i x_j + \sum_{\substack{1 \le i \le v+o_1 \\ v+1 \le j \le n}} a_{ij}^{(o_1+1)} x_i x_j, \\ \vdots \\ f_m = \sum_{1 \le i \le j \le v+o_1} a_{ij}^{(m)} x_i x_j + \sum_{\substack{1 \le i \le v+o_1 \\ v+1 \le j \le n}} a_{ij}^{(m)} x_i x_j, \end{cases}$$

where each coefficient $a_{ij}^{(k)}$ is randomly chosen from $\mathbb{F}_q$. For an element $\mathbf{w} = (w_1, \ldots, w_m) \in \mathbb{F}_q^m$, the process of finding a solution to the equations $\mathcal{F}(\mathbf{x}) = \mathbf{w}$ (namely, the computation of $\mathcal{F}^{-1}(\mathbf{w})$) is as follows:

1. Randomly choose an element $\mathbf{z}' = (z_1', \ldots, z_v') \in \mathbb{F}_q^v$.
2. Find a solution $\mathbf{x}_2 = \mathbf{z}'' \in \mathbb{F}_q^{o_1}$ to the system of linear equations:

$$f_1(\mathbf{z}', \mathbf{x}_2) = w_1, \ldots, f_{o_1}(\mathbf{z}', \mathbf{x}_2) = w_{o_1}.$$

3. Find a solution $\mathbf{x}_3 = \mathbf{z}''' \in \mathbb{F}^{o_2}$ to the system of linear equations:

$$f_{o_1+1}(\mathbf{z}', \mathbf{z}'', \mathbf{x}_3) = w_{o_1+1}, \ldots, f_{o_1+o_2}(\mathbf{z}', \mathbf{z}'', \mathbf{x}_3) = w_m.$$

4. Let $\mathbf{z} := (\mathbf{z}', \mathbf{z}'', \mathbf{z}''') \in \mathbb{F}_q^n$, which is a solution to $\mathcal{F}(\mathbf{x}) = \mathbf{w}$.

In this algorithm, if there is no solution of the system to linear equations in Step 2 or 3, then go back to Step 1 or 2, respectively. It is clear that this algorithm is efficient; in fact, the complexity is given by $O(n^3)$ at most.

The Rainbow signature scheme [11] was proposed as an improved version of the OV and UOV schemes. If we remove the parameter o_2 (i.e. $o_2 = 0$) and set $v = o_1$ in the Rainbow signature scheme, then the obtained scheme becomes the OV signature scheme [42], which was proposed by Patarin in 1997. However, it is broken by the OV attack [15] in polynomial time. In 1999, Kipnis et al. proposed the Unbalanced OV (UOV) scheme [10] by modifying the parameter (v, o_1) as $v > o_1$ (and $o_2 = 0$), which can resist the OV attack. Finally, in 2005, the Rainbow scheme improved the efficiency of the UOV scheme by adding a new parameter o_2.

The Rainbow scheme was selected as a finalist in the third round of the NIST PQC standardisation [12]. Table 1 presents the proposed parameters. In this paper, we primarily focussed on the RBS and Rectangular MinRank attacks against the Rainbow scheme in order to understand some recent progress in the security analysis of MPKC. Recently, Beullens proposed a new attack, known as simple attack [43], in IACR ePrint. The parameters (Table 1) of the Rainbow scheme in the third round should be rescaled such that it is secure against the simple attack [43].

2.3 | MQ problem

In this subsection, we describe the MQ problem, which is strongly related to the security of multivariate schemes.

Clearly, by solving the equations $\mathcal{P}(\mathbf{x}) - \mathbf{w} = 0$ for a public key $\mathcal{P}$ and a ciphertext (or message) $\mathbf{w} \in \mathbb{F}_q^m$, we obtain the message $\mathbf{m}$ (or a signature $\mathbf{s}$). Thus, the following problem is important for understanding the security of multivariate schemes:

2.3.1 | Multivariate quadratic polynomial (MQ) problem

Given a system of m quadratic polynomial $g_1(\mathbf{x}), \ldots, g_m(\mathbf{x})$ in n variables, find a solution $\mathbf{x} \in \mathbb{F}_q^n$ to

$$g_1(\mathbf{x}) = \cdots = g_m(\mathbf{x}) = 0.$$

TABLE 1 The parameters of the rainbow scheme in the third round of National Institute of Standards and Technology post-quantum cryptography standardisation [12]

Security level	Parameter (q, v, o_1, o_2)	Public key size (KB)	Secret key size (KB)	Signature size (B)
I	(2^4, 36, 32, 32)	157.8	101.2	66
III	(2^8, 68, 32, 48)	861.4	611.3	164
V	(2^8, 96, 36, 64)	1885.4	1375.7	204

This problem is proven to be NP-hard for the binary field $\mathbb{F}_2$ [5]. Thus, it is considered to be difficult to solve a system of randomly chosen quadratic equations $g_1(\mathbf{x}) = \cdots = g_m(\mathbf{x}) = 0$.

In MPKC research, since a public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is constructed using an easy-to-invert map $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$, which has a special structure to realise an efficient inverting process, it is considered that the associated MQ problem $\mathcal{P}(\mathbf{x}) - \mathbf{w} = 0$ might be easier than the random MQ problem.

It is important to study the precise computational cost of solving a given system of equations $g_1(\mathbf{x}) = \cdots = g_m(\mathbf{x}) = 0$, since it directly affects the secure parameters of multivariate schemes. In Sections 3 and 4, we will discuss how the MQ problem is solved and how its complexity is estimated in MPKC research.

Remark 1 In general, it is difficult to prove a reduction of the security of multivariate schemes to the hardness of the MQ problem. As an exception, MQDSS [44] is the only signature scheme that uses multivariate polynomials such that it has provably security to the MQ problem. MQDSS was a candidate for the second round of NIST PQC standardisation [45] and is constructed based on the 5-pass identification scheme proposed by Sakumoto et al. [13]. Note that the construction of MQDSS does not follow the method in Section 2.1.

2.4 | MinRank problem

In this subsection, we describe the MinRank problem, which is also strongly related to the security of multivariate schemes. Before we state the MinRank problem, we recall a relation between quadratic polynomials and matrices.

For a homogeneous quadratic polynomial

$$g(\mathbf{x}) = \sum_{1 \le i \le j \le n} g_{ij} x_i x_j \in \mathbb{F}_q[\mathbf{x}],$$

we define the upper triangular matrix G^{up} by

$$G^{\mathrm{up}} := \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ 0 & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{nn} \end{pmatrix} \in \mathbb{F}_q^{n \times n}.$$

Then, we obtain the following equality

$$g(\mathbf{x}) = \mathbf{x} \cdot G^{\mathrm{up}} \cdot {}^t\mathbf{x},$$

where ${}^t\mathbf{x}$ denotes the transpose of $\mathbf{x}$. It is clear that the map $g \mapsto G^{\mathrm{up}}$ is a bijective map between the set of homogeneous quadratic polynomials in $\mathbb{F}_q[\mathbf{x}]$ and the set of upper triangular (square) matrices of size n. Let $\mathcal{S}$ be a linear map on $\mathbb{F}_q^n$, and let S be its corresponding matrix of size n. Then, we have

$$g \circ \mathcal{S}(\mathbf{x}) = \mathbf{x} \cdot S \cdot G^{\mathrm{up}} \cdot {}^tS \cdot {}^t\mathbf{x}.$$

However, since $S \cdot G^{\mathrm{up}} \cdot {}^tS$ is not an upper triangular matrix in general, the corresponding upper triangular matrix of $g \circ \mathcal{S}(\mathbf{x})$ is not equal to $S \cdot G^{\mathrm{up}} \cdot {}^tS$.

To avoid this inequality, it is necessary to consider symmetric matrices. For the above quadratic polynomial $g(\mathbf{x})$, we define the following symmetric matrix:

$$G := G^{\mathrm{up}} + {}^tG^{\mathrm{up}}.$$

Then, the corresponding symmetric matrix of $g \circ \mathcal{S}(\mathbf{x})$ is equal to

$$S \cdot G \cdot {}^tS.$$

Thus, if $(F_1, \ldots, F_m)$ and $(P_1, \ldots, P_m)$ are the corresponding symmetric matrices of the easy-to-invert map $\mathcal{F} = (f_1, \ldots, f_m)$ and the public key $\mathcal{P} = (p_1, \ldots, p_m)$, then we have

$$(P_1, \ldots, P_m) = (SF_1{}^tS, \ldots, SF_m{}^tS) \cdot T,$$

where S, T are the corresponding matrices of size n, m to the secret key $\mathcal{S}, \mathcal{T}$. As a result, it is considered that the symmetric matrices of the public key $\mathcal{P}$ inherit some properties of the symmetric matrices of the easy-to-invert map $\mathcal{F}$.

Remark 2 Since $g(\mathbf{x}) = \mathbf{x} \cdot {}^tG^{\mathrm{up}} \cdot {}^t\mathbf{x}$, we have

$$\mathbf{x} \cdot G \cdot {}^t\mathbf{x} = 2g(\mathbf{x}).$$

From this equality, it can be easily seen that if the characteristic of $\mathbb{F}_q$ is not 2, then the map $g \mapsto \frac{1}{2}G$ is a bijective map between the set of homogeneous quadratic polynomials and the set of symmetric matrices.

For example, the form of symmetric matrices $(F_1, \ldots, F_m)$ of the Rainbow easy-to-invert map $\mathcal{F} = (f_1, \ldots, f_m)$ in Section 2.2 is given as follows:

$$F_i = \begin{cases} \begin{pmatrix} *_{v \times v} & *_{v \times o_1} & 0_{v \times o_2} \\ *_{o_1 \times v} & 0_{o_1 \times o_1} & 0_{o_1 \times o_2} \\ 0_{o_2 \times v} & 0_{o_2 \times o_1} & 0_{o_2 \times o_2} \end{pmatrix} & (1 \le i \le o_1), \\ \begin{pmatrix} *_{v \times v} & *_{v \times o_1} & *_{v \times o_2} \\ *_{o_1 \times v} & *_{o_1 \times o_1} & *_{o_1 \times o_2} \\ *_{o_2 \times v} & *_{o_2 \times o_1} & 0_{o_2 \times o_2} \end{pmatrix} & (o_1 + 1 \le i \le m). \end{cases}$$

Here, $*_{k \times l}$ means a k-by-l matrix over $\mathbb{F}_q$. Since the rank of F_i $(1 \le i \le o_1)$ is less than or equal to $v + o_1$, we can generate a linear combination of the matrices $P_1, \ldots, P_m$ with rank $\le v + o_1$. Once an attacker finds such a low-rank matrix from the public key, the attacker can recover the secret key using the kernel of the low-rank matrix.

As stated in the Rainbow example, the problem of finding a low-rank matrix from linear combinations of the symmetric matrices $(P_1, \ldots, P_m)$ of the public key $\mathcal{P}$ is strongly related to the security of multivariate schemes. As a result, the following MinRank problem, which is a generalisation of this problem, is important for understanding the security of MPKC.

2.4.1 | MinRank problem

Given s matrices $M_1, \ldots, M_s \in \mathbb{F}_q^{t \times u}$ and integer $r > 0$, find a non-trivial $\mathbb{F}_q$-linear combination $M = \sum_{i=1}^{s} a_i M_i$ with Rank $(M) \leq r$, if it exists.

This is proven to be NP-hard [25]. Thus, it is considered to be difficult to solve a randomly chosen instance of the MinRank problem. In Section 6.1, we will explain the support minor modelling [26] as a method to solve the MinRank problem proposed by Bardet et al. in 2020.

Remark 3 Originally, the first key recovery attack using the MinRank problem was proposed in Ref. [24] in a security analysis against the HFE scheme [7].

Remark 4 Since the MinRank problem is NP-hard, it might be possible to construct a scheme based on the MinRank problem. For example, a zero-knowledge identification scheme based on the MinRank problem was proposed by Courtois [46].

3 | SOLVING MULTIVARIATE POLYNOMIAL SYSTEMS

In this section, we describe approaches of solving a system of polynomial equations. To solve such equations, the Gröbner basis approach or Wiedemann XL approach is mainly used in MPKC research. Moreover, solving equations is also important in the MinRank problem, since the MinRank problem can be reduced to a problem of solving polynomial equations.

In Section 3.1, we explain the Gröbner basis approach. In Section 3.2, we describe the Wiedemann XL approach.

3.1 | Gröbner basis approach

First, we briefly recall Gröbner basis. Gröbner basis is a good finite set of generators of an ideal in a polynomial ring, and it was introduced by Buchberger [47] in 1965. To state it more precisely, let $\succeq$ be a term order on the polynomial ring $\mathbb{F}_q[\mathbf{x}]$ and I be an ideal of $\mathbb{F}_q[\mathbf{x}]$, where $\mathbf{x} = (x_1, \ldots, x_n)$. Then a finite set $G_{\succeq} := \{h_1, \ldots, h_\ell\}$ of generators of I is called a Gröbner basis of I, and if it satisfies that for any $h \in I$ there exists $1 \leq i \leq \ell$ such that the leading term of h is divided by that of h_i. The algorithms F4 [30] and F5 [16] are known as efficient algorithms for computing Gröbner basis.

For $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$, a solution to $g_1 = \cdots = g_m = 0$ is computed using a Gröbner basis algorithm as follows. Define the ideal I by

$$I := \langle g_1, \ldots, g_m \rangle \subset \mathbb{F}_q[\mathbf{x}].$$

Using the Gröbner basis algorithm, compute a Gröbner basis G_{grev} of I with respect to the graded reverse lexicographic term order $\succeq_{\text{grev}}$. If the ideal I is zero-dimensional, one can convert G_{grev} into a lexicographic Gröbner basis G_{lex} of I using FGLM [48] or other algorithms. Then, the Gröbner basis $G_{\text{lex}} = \{h_1, \ldots, h_\ell\}$ has the following form:

$$\begin{aligned} h_1(x_n) &= 0, \\ h_2(x_{n-1}, x_n) &= 0, \\ &\vdots \\ h_\ell(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Thus, by solving these equations in the order from top to bottom, we can obtain a solution to $g_1 = \cdots = g_m = 0$.

Remark 5 If the system of equations $g_1 = \cdots = g_m = 0$ has finite solutions over an algebraic closure $\overline{\mathbb{F}_q}$, then the ideal I is said to be zero-dimensional. The complexity of the FGLM algorithm [48] is $O(nD^3)$, where D is the number of solutions to the system with multiplicities. When the Gröbner basis approach is used in MPKC research, the case where the ideal of system $g_1 = \cdots = g_m = 0$ is zero-dimensional and D is low is typically considered. Hence, in MPKC research, the complexity of the FGLM algorithm is typically disregarded.

It is known that the dominant complexity in the above procedure of solving equations $g_1 = \cdots = g_m = 0$ is that of computing G_{grev} when I is of zero dimension. Therefore, it is important to estimate the complexity of computing G_{grev}.

To compute a Gröbner basis using F4 or F5, a Macaulay matrix or a similar matrix is constructed from the equations $g_1 = \cdots = g_m = 0$ and then it is reduced by a reduction algorithm such as Gaussian elimination. Here, the Macaulay matrix $\mathcal{M}_d$ of degree d with respect to $g_1, \ldots, g_m$ is defined as follows. For any polynomial $g(\mathbf{x}) \in \mathbb{F}_q[\mathbf{x}]$ of degree $\leq d$, we denote by $\mathbf{v}_g$ the row vector of coefficients of $g(\mathbf{x})$, where the sorting order of coefficients is determined by the term order $\succeq$. Then, the matrix $\mathcal{M}_d$ is defined by concatenating the row vectors $\mathbf{v}_{ug_i}$, where $1 \leq i \leq m$ and u runs in the set of terms of degree $\leq d - \deg g_i$. Since the number of terms of degree $\leq d$ is $\binom{n+d}{d}$, the number of column vectors in the Macaulay matrix $\mathcal{M}_d$ is $\binom{n+d}{d}$.

The complexity of computing a Gröbner basis is dominated by that of reduction of the Macaulay matrix $\mathcal{M}_d$ with the largest degree d appeared in the Gröbner basis algorithm. As a result, if we denote the largest degree by $d_{\max}$, the complexity of solving the system of equations $g_1 = \cdots = g_m = 0$ is bounded by

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

where $2 < \omega \leq 3$ is a linear algebra constant. Therefore, it is important to determine the degree $d_{\max}$ to estimate the complexity of solving the system of equations $g_1 = \cdots = g_m = 0$. However, finding the degree $d_{\max}$ for a given system of equations $g_1 = \cdots = g_m = 0$ is generally difficult. In Section 4, we will discuss how $d_{\max}$ is currently estimated in MPKC research.

3.2 | Wiedemann XL approach

The Wiedemann XL approach is an accelerated version of the extended linearisation (XL) algorithm using the Wiedemann algorithm.

A variant of the XL algorithm [49] is a method of finding a solution of $g_1 = \cdots = g_m = 0$ by solving a linear system associated with the Macaulay matrix $\mathcal{M}_d$. More precisely, let X_d be a column vector of terms in the variables $\mathbf{x}$ of degree $\leq d$, where the sorting order of terms is determined by the term order $\succeq$. Then $\mathcal{M}_d \cdot X_d$ is the column vector consisting of polynomials ug_i, where $1 \leq i \leq m$ and u runs in the set of terms of degree $\leq d - \deg\ g_i$. A variant of XL algorithm solves the linear system $\mathcal{M}_d \cdot X_d = \mathbf{0}$ where each term in X_d is treated as a new variable, or the (inhomogeneous) linear system transposed the last column vector of $\mathcal{M}_d$ corresponding to 1 in X_d on the right hand side.

The Wiedemann XL approach finds a solution to $g_1 = \cdots = g_m = 0$ by solving such a linear system using Wiedemann algorithms such as in Ref. [31] or Ref. [50]. Such algorithms can solve a linear system faster than Gaussian elimination when the Macaulay matrix is sparse. Note that the algorithms [31, 50] aim to find a single solution of a linear system and not all possible solutions. Thus, if a linear system has many solutions, then it is not possible to find all the solutions in one trial in general. Therefore, when finding a solution to $g_1 = \cdots = g_m = 0$, the following conditions are required: (i) $g_1 = \cdots = g_m = 0$ has a few solutions. (ii) The rank of the Macaulay matrix $\mathcal{M}_d$ is approximately $\binom{n+d}{d} - 1$.

Condition (i) almost holds since the solved system of equations $g_1 = \cdots = g_m = 0$ is often of zero dimension in MPKC research. Therefore, condition (ii) is important. We define d_{full} as the degree d such that the rank of the Macaulay matrix $\mathcal{M}_d$ is approximately $\binom{n+d}{d} - 1$. Note that the Weidemann XL algorithm finds only one element from the right kernel of the Macaulay matrix $\mathcal{M}_d$. Thus, the Weidemann algorithm is applied for $\mathcal{M}_d$ at most $q^{\binom{n+d}{d} - \text{Rank}\mathcal{M}_d}$ times to find a solution of the system of equations $g_1 = \cdots = g_m = 0$. To reduce this time, the rank of the Macaulay matrix $\mathcal{M}_d$ needs to be low. In MPKC research, the rank of $\mathcal{M}_d$ to determine d_{full} is typically set to $\binom{n+d}{d} - 1$. Once d_{full} is determined, the complexity of solving a system of 'quadratic' equations $g_1 = \cdots = g_m = 0$ is obtained from Ref. [51] as

$$3\binom{n+d_{\text{full}}}{d_{\text{full}}}^2\binom{n}{2}.$$

In general, for any system of equations $g_1 = \cdots = g_m = 0$, it is difficult to estimate the degree d_{full}. In Section 4, we will discuss how d_{full} is currently estimated in MPKC research.

4 | COMPLEXITY OF SOLVING MQ PROBLEM

In this section, we discuss the complexity of solving the MQ problem. In Sections 4.1 and 4.2, we describe the degree of regularity d_{reg} and the first fall degree d_{ff} used in MPKC research as indicators of $d_{\max}$ and d_{full}. In Section 4.3, we explain how the complexity of solving the MQ problem that appears in MPKC is estimated using d_{reg} or d_{ff}. In Section 4.4, we explain the hybrid approach as an improvement on approaches addressed in Sections 3.1 and 3.2.

4.1 | Degree of regularity

First, we prepare some notations. Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$ be a polynomial system with degree $d_i := \deg\ g_i$. We denote by $\tilde{g}_1, \ldots, \tilde{g}_m$ their homogeneous parts of the highest degree. Set the ideals

$$\tilde{I} = \tilde{I}^{(m)} := \langle \tilde{g}_1, \ldots, \tilde{g}_m \rangle \text{ and } \tilde{I}^{(i)} := \langle \tilde{g}_1, \ldots, \tilde{g}_i \rangle,$$

where $i = 1, \ldots, m-1$. Moreover, for $d \in \mathbb{N}$, we define the following:

$$\mathbb{F}_q[\mathbf{x}]_d := \bigoplus_{j_1+\cdots+j_n=d} \mathbb{F}_q \cdot x_1^{j_1} \cdots x_n^{j_n},$$
$$\tilde{I}_d^{(i)} := \tilde{I}^{(i)} \cap \mathbb{F}_q[\mathbf{x}]_d.$$

Then, for $D \in \mathbb{N}$, the polynomial system $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$ is said to be *regular up to D* [37] if it satisfies for any $1 \leq i \leq m-1$ and any $d \leq D$, and the following map is injective:

$$\mathbb{F}_q[\mathbf{x}]_{d-d_{i+1}}/\tilde{I}^{(i)}_{d-d_{i+1}} \ni h \mapsto h \cdot \tilde{g}_{i+1} \in \mathbb{F}_q[\mathbf{x}]_d/\tilde{I}^{(i)}_d.$$

Note that this definition does not depend on the sorting order of the polynomials $g_1, \ldots, g_m$.

4.1.1 | Degree of regularity d_{reg}

For polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$, we define the degree of regularity d_{reg} [19] as follows:

$$d_{\text{reg}} := \min\{d \in \mathbb{N} \mid \mathbb{F}_q[\mathbf{x}]_d = \tilde{I}_d\}.$$

If there is no integer d such that $\mathbb{F}_q[\mathbf{x}]_d = \tilde{I}_d$, we define $d_{\text{reg}} = \infty$. Since we mainly treat the zero-dimensional case, the degree d_{reg} will not be ∞.

A polynomial system $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$ is said to be *semi-regular* [19] if it is regular up to $d_{\text{reg}} - 1$. Note that the definition we state here is given by Diem [37] and is equivalent to that of Ref. [19]. Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$ be a semi-regular system. Then the following lemma holds:

Lemma 1 ([19]). *For a semi-regular system $g_1, \ldots, g_m$ and $d < d_{\mathrm{reg}}$, the dimension* $\dim \mathbb{F}_q[\mathbf{x}]_d/\tilde{I}_d$ *is equal to the coefficient of degree d of the following power series*

$$H(t) := \frac{\Pi_{i=1}^{m}\left(1-t^{d_i}\right)}{(1-t)^n}. \tag{1}$$

The degree of regularity d_{reg} for a semi-regular system can be easily computed as the minimal degree with a non-positive coefficient in the power series $H(t)$.

The degree of regularity d_{reg} is defined by Bardet et al. [19]. As shown from the definition, any element of the reduced Gröbner basis of I is of degree d_{reg} at the most. With this fact, it is expected that $d_{\max}$ and d_{full} might be estimated by the degree of regularity d_{reg}. In Section 4.3, we will discuss how d_{reg} is utilised to estimate $d_{\max}$ and d_{full} in MPKC research.

4.2 | First fall degree

Define $B := \mathbb{F}_q[\mathbf{x}]/\langle x_1^q, \ldots, x_n^q\rangle$ and $B_d := \mathbb{F}_q[\mathbf{x}]_d/\langle x_1^q, \ldots, x_n^q\rangle_d$ for $d \in \mathbb{N}$. Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}]$ be a polynomial system such that $\tilde{g}_1, \ldots, \tilde{g}_m$ are of degree $d_0 \in \mathbb{N}$. We denote by $\overline{\tilde{g}}_i$ the image of $\tilde{g}_i \in \mathbb{F}_q[\mathbf{x}]_{d_0}$ in B_{d_0}. For a positive integer d, we consider the homomorphism

$$\Phi_d : B_{d-d_0}^m \to B_d, (b_1, \ldots, b_m) \mapsto b_1\overline{\tilde{g}}_1 + \cdots + b_m\overline{\tilde{g}}_m.$$

Then, we set

$$\overline{\pi}_{ij} := \left(0, \ldots, 0, \overset{i}{-\overline{\tilde{g}}_j}, 0, \ldots, 0, \overset{j}{\overline{\tilde{g}}_i}, 0, \ldots, 0\right) \in B^m,$$

$$\overline{\tau}_i := \left(0, \ldots, 0, \overset{i}{\overline{\tilde{g}}_i^{q-1}}, 0, \ldots, 0\right) \in B^m,$$

and define TSyz as the submodule of B^m generated by such elements and set $\mathrm{TSyz}_d := \mathrm{TSyz} \cap B_d^m$. In addition, we call an element in $\mathrm{Ker}\ \Phi_d \setminus \mathrm{TSzy}_d$ a *non-trivial syzygy*.

4.2.1 | First fall degree d_{ff}

Then, the first fall degree d_{ff} [20] is defined by

$$d_{\mathrm{ff}} := \min\left\{d \in \mathbb{N} \mid \mathrm{Ker}\ \Phi_d \neq \mathrm{TSzy}_d\right\}.$$

namely, d_{ff} is the smallest number d where a non-trivial syzygy appears.

The first fall degree d_{ff} and degree of regularity d_{reg} have the following relation:

Lemma 2 ([36]). *For a non-semi-regular system, if $d_{\mathrm{ff}} < q$, then we have $d_{\mathrm{ff}} \leq d_{\mathrm{reg}}$.*

The first fall degree d_{ff} was introduced by Dubois and Gama [20] in 2010 from a security analysis of the HFE scheme [7] and d_{ff} can represent the minimum of degrees of 'degree fall' for a given system $g_1 = \cdots = g_m = 0$. Note that initially, the first fall degree was called the degree of regularity, for example, in Ref. [20, 22]. In general, it is difficult to compute the first fall degree d_{ff} for a given polynomial system. Ding and Hodges [22] give an upper bound for the first fall degree d_{ff} by constructing a non-trivial syzygy for the HFE scheme [7]. In addition, Verbel et al. [52] construct non-trivial syzygies of a quadratic system in the Kipnis–Shamir method [15] for the MinRank problem and give an upper bound of the first fall degree d_{ff}.

4.3 | Complexity estimation of solving MQ problem

In this subsection, we explain how to estimate the complexity of solving a system of quadratic equations $g_1 = \cdots = g_m = 0$ using the Gröbner basis approach or Wiedemann XL approach. As stated in Section 3, we need to estimate $d_{\max}$ and d_{full}. This task is done using the degree of regularity or the first fall degree. We will divide the system $g_1, \ldots, g_m$ into two cases: (i) a semi-regular quadratic system and (ii) a quadratic system associated with a public key $\mathcal{P}$ of a multivariate scheme.

Let d_{reg} and d_{ff} be the degree of regularity and the first fall degree for $g_1, \ldots, g_m$, respectively. Moreover, let $d_{\mathrm{reg}}^{(n,m)}$ be the degree of regularity for a semi-regular system of m quadratic equations in n variables, which is efficiently computed by the power series $H(t)$ in Equation (1).

(i) Semi-regular case

As stated above, the degree of any element in the reduced Gröbner basis of the ideal $I = \langle g_1, \ldots, g_m\rangle$ is $\leq d_{\mathrm{reg}}^{(n,m)}$. From this, it is considered that the Gröbner basis is obtained by the reduction process of the Macaulay matrix $\mathcal{M}_d$ with some $d \leq d_{\mathrm{reg}}^{(n,m)}$. We define the homogeneous Macaulay matrix $\widetilde{\mathcal{M}}_d$ by concatenating the row vectors $\mathbf{v}_{u\tilde{g}_i}$ as in Section 3.1, where $1 \leq i \leq n$ and u runs in the set of terms of degree $d - \deg g_i$. From the definition of the degree of regularity [19], it is seen that if the system is semi-regular, then the rank of $\widetilde{\mathcal{M}}_d$ becomes full when $d = d_{\mathrm{reg}}^{(n,m)}$. From such observations, both $d_{\max}$ and d_{full} are estimated by $d_{\mathrm{reg}}^{(n,m)}$ in MPKC research. Thus, the complexity of solving a semi-regular system of m quadratic equations $g_1 = \cdots = g_m = 0$ in n variables using Gröbner basis or Wiedemann XL approaches is estimated by

$$\binom{n + d_{\mathrm{reg}}^{(n,m)}}{d_{\mathrm{reg}}^{(n,m)}}^{\omega} \quad \text{or} \quad 3\binom{n + d_{\mathrm{reg}}^{(n,m)}}{d_{\mathrm{reg}}^{(n,m)}}^{2}\binom{n}{2},$$

respectively. For instance, these estimations are used in Refs. [8, 12].

Note that a random instance of the MQ problem, which is a problem of solving a system of randomly chosen quadratic equations, is experimentally known to behave as a semi-regular system. Thus, its complexity is usually estimated to be the same as that of a semi-regular system.

(ii) **Multivariate scheme case**

We explain how to estimate the complexity of solving a system of quadratic equations $\mathcal{P}(\mathbf{x}) - \mathbf{w} = 0$ using the Gröbner basis approach or Wiedemann XL approach. Here, $\mathcal{P} = (p_1, \ldots, p_m)$ is a public key for a multivariate scheme and $\mathbf{w} = (w_1, \ldots, w_m) \in \mathbb{F}_q^m$ is a ciphertext or message to be signed. Solving the system using such approaches is known as *direct attack* in MPKC. Put the system

$$g_1 := p_1 - w_1, \ldots, g_m := p_m - w_m.$$

We assume that $n \leq m$; otherwise, we fix $n - m$ variables in the system. Since the fixed system has m equations in m variables, it has a solution with a high probability. Therefore, we can always assume $n \leq m$.

First, we experimentally investigate whether the system g_1, …, g_m is semi-regular or not. However, since it is not feasible for $\mathcal{P}$ with a larger (i.e. practical) parameter, we need to conduct some experiments for small parameters. If the systems g_1, …, g_m for $\mathcal{P}$ with small parameters behave as a semi-regular system of the same size, then we consider that the systems g_1, …, g_m for $\mathcal{P}$ with large parameters are also semi-regular. Then its complexity is given as in the case (i).

Next, we consider that systems g_1, …, g_m for $\mathcal{P}$ with small parameters do not behave as semi-regular systems. For this case, we often have $d_{\mathrm{reg}} > d_{\mathrm{reg}}^{(n,m)}$. However, it is known that a non-semi-regular system that appears in case (ii) can be solved faster than a semi-regular system with the same size. Thus, we cannot use d_{reg} to estimate the complexity of solving a non-semi-regular system. Instead, we try to use the first fall degree d_{ff}. This estimation method was initially applied to the security analysis of the HFE scheme [7]. In the HFE scheme, by constructing a non-trivial syzygy of g_1, …, g_m, Ding et al. [22] give an upper bound of the first fall degree d_{ff} and estimate $d_{\max}$ by using the upper bound of d_{ff}. They also experimentally confirmed that the upper bound of d_{ff} approximates $d_{\max}$ for small parameters. As a result, $d_{\max}$ for a large parameter of the HFE scheme is estimated by the upper bound of d_{ff}. However, for schemes other than the HFE scheme and its variants, it is necessary to theoretically and experimentally analyse case-by-case whether d_{ff} can approximate $d_{\max}$. Moreover, there is little research on whether d_{ff} correctly estimates d_{full}, and thus further research is required.

4.4 | Hybrid approach and its complexity

In Sections 3.1 and 3.2, we described two approaches for solving a given quadratic equations $g_1 = \cdots = g_m = 0$. As an improvement, a hybrid approach [53] with the brute-force search is often used, namely after fixing some variables in $\mathbf{x}$ (i.e. substituting elements of $\mathbb{F}_q$ into some variables), we solve the obtained equations by an approach discussed in Sections 3.1 or 3.2. Here, we assume that $n \leq m$ as in Section 4.3.

Let $0 \leq k \leq n$ be the number of fixed variables. We consider the case in which $g_1 = \cdots = g_m = 0$ is a semi-regular quadratic system. Then, the new system given by fixing k variables is also considered to be semi-regular. Therefore, the degree of regularity $d_{\mathrm{reg}}^{(n-k,m)}$ is given by the smallest integer d for which the coefficient of t^d in the power series $\frac{(1-t^2)^m}{(1-t)^{n-k}}$ is non-positive.

As stated in (i) of Section 4.3, we have the following complexity of the hybrid approach using the Gröbner basis approach:

$$\min_{0 \leq k \leq n} q^k \cdot \binom{n-k+d_{\mathrm{reg}}^{(n-k,m)}}{d_{\mathrm{reg}}^{(n-k,m)}}^{\omega}.$$

Moreover, we have the following complexity of the hybrid approach using the Wiedemann XL approach:

$$\min_{0 \leq k \leq n} q^k \cdot 3 \binom{n-k+d_{\mathrm{reg}}^{(n-k,m)}}{d_{\mathrm{reg}}^{(n-k,m)}}^{2} \binom{n-k}{2}.$$

Remark 6 The complexity of the direct attack against the Rainbow scheme [11] in Section 2.2 is considered as follows. First, since $n > m$, we fix $n - m$ variables in $\mathbf{x}$ and obtain a system of m quadratic equations in m variables. Through experiments, it is known that such systems behave as semi-regular. In Ref. [12], the complexity of the direct attack against the Rainbow scheme is estimated using the hybrid version of the Wiedemann XL approach as follows:

$$\min_{0 \leq k \leq m} q^k \cdot 3 \binom{m-k+d_{\mathrm{reg}}^{(m-k,m)}}{d_{\mathrm{reg}}^{(m-k,m)}}^{2} \binom{m-k}{2}.$$

5 | BI-GRADED POLYNOMIAL SYSTEMS AND RBS ATTACK

In this section, we consider to solve bi-graded polynomial systems. Such systems were mainly studied by Nakamura [36], Nakamura et al. [34] and Smith-Tone et al. [35] via the analysis of the RBS attack [28] against the Rainbow scheme [11].

In Section 5.1, following the work of Nakamura [36], we describe the bi-degree of regularity, which is a generalisation of the degree of regularity d_{reg}. In Section 5.2, following the idea of Smith-Tone et al. [35], we explain a complexity estimation of bi-graded instances of the MQ problem. Based on these, in Section 5.3, we explain a new analysis of the RBS attack given by the studies of Nakamura et al. [34] and Smith-Tone et al. [35].

5.1 | Regularity for bi-graded polynomial systems

In this subsection, we recall the definition of the bi-graded polynomials and describe a generalisation of the degree of regularity for them, following the work of Nakamura [36].

Let $\preceq$ be a relation on $\mathbb{N}^2$ defined by

$$(a,b) \preceq (c,d) \overset{\text{def}}{\iff} a \le c,\ b \le d.$$

We recall the definition of bi-graded polynomials. We consider two variable sets $\mathbf{x} = (x_1, \ldots, x_{n_1})$ and $\mathbf{y} = (y_1, \ldots, y_{n_2})$. Put the polynomial ring

$$\mathbb{F}_q[\mathbf{x}, \mathbf{y}] := \mathbb{F}_q[x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}].$$

For polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$, we denote their homogeneous parts of the highest degree by $\tilde{g}_1, \ldots, \tilde{g}_m$. Set the ideals

$$\tilde{I} = \tilde{I}^{(m)} := \langle \tilde{g}_1, \ldots, \tilde{g}_m \rangle \text{ and } \tilde{I}^{(i)} = \langle \tilde{g}_1, \ldots, \tilde{g}_i \rangle,$$

where $i = 1, \ldots, m-1$. For $\mathbf{d} = (d_1, d_2) \in \mathbb{N}^2$, we define the following:

$$\mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}} := \bigoplus_{\substack{i_1 + \cdots + i_{n_1} = d_1 \\ j_1 + \cdots + j_{n_2} = d_2}} \mathbb{F}_q \cdot x_1^{i_1} \cdots x_{n_1}^{i_{n_1}} \cdot y_1^{j_1} \cdots y_{n_2}^{j_{n_2}},$$

$$\tilde{I}_{\mathbf{d}}^{(i)} := \tilde{I}^{(i)} \cap \mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}}.$$

If $\tilde{g}_i$ is in $\mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}}$ and $g_i \in \bigoplus_{\mathbf{d}' \preceq \mathbf{d}} \mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}'}$, then g_i is called a *bi-graded* polynomial and we define bi-deg $g_i := \mathbf{d}$.

Assume that each g_i is bi-graded and $\mathbf{d}_i = (d_{i1}, d_{i2}) :=$ bi - deg $g_i \in \mathbb{N}^2$. Then, for $\mathbf{D} \in \mathbb{N}^2$, the polynomial system $g_1, \ldots, g_m$ is said to be *regular up to* $\mathbf{D}$ [36] if it satisfies that for any $1 \le i \le m-1$ and any $\mathbf{d} \preceq \mathbf{D}$ the following map is injective

$$\mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}-\mathbf{d}_i} / \tilde{I}_{\mathbf{d}-\mathbf{d}_i}^{(i)} \ni h \mapsto h \cdot \tilde{g}_{i+1} \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}} / \tilde{I}_{\mathbf{d}}^{(i)}.$$

5.1.1 | Bi-degree of regularity

For bi-graded quadratic polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$, we define the following sets:

$$\mathcal{D}_0 := \left\{ \mathbf{d} \in \mathbb{N}^2 \mid \mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}} = \tilde{I}_{\mathbf{d}} \right\},$$
$$\mathcal{D} := \{ \mathbf{d} \in \mathcal{D}_0 \mid \mathbf{d} : \text{minimum in } \mathcal{D}_0 \text{ w.r.t} \preceq \}.$$

We call an element of $\mathcal{D}$ a *bi-degree of regularity* for $g_1, \ldots, g_m$. Note that there is a case where the cardinality of $\mathcal{D}$ is ≥ 2, that is, a bi-degree of regularity is not unique in general.

Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ be a bi-graded system. Then the bi-graded system $g_1, \ldots, g_m$ is said to be *bi-graded semi-regular* if it is regular up to $\mathbf{d}$ for any $\mathbf{d} \prec \mathbf{D} \in \mathcal{D}$. Then the following lemma holds:

Lemma 3 ([36]). *Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ be a bi-graded semi-regular system. For any $\mathbf{d} \prec \mathbf{D} \in \mathcal{D}$, the dimension* $\dim \mathbb{F}_q[\mathbf{x}, \mathbf{y}]_{\mathbf{d}} / \tilde{I}_{\mathbf{d}}$ *is equal to the* $\mathbf{d}$ *degree coefficient of the following two-variable power series*

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

As a result, for a bi-graded semi-regular system, any bi-degree of regularity (i.e. $\mathcal{D}$) can be easily computed from bi-degrees of the coefficients in the two-variable power series Equation (2).

5.2 | Complexity estimation

In this subsection, using the idea of Smith-Tone et al. [35], we estimate the complexity of solving bi-graded instances of the MQ problem. This task is done using the bi-degrees of regularity in Section 5.1.

Let $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ be a quadratic bi-graded polynomial system. We consider how to solve such a quadratic bi-graded system using the Wiedemann XL approach. This is done as in Section 3.2, namely by solving the linear system associated with the bi-graded Macaulay matrix. Here, the bi-graded Macaulay matrix $\mathcal{M}_{\mathbf{d}}$ of bi-degree $\mathbf{d} \in \mathbb{N}^2$ with respect to $g_1, \ldots, g_m$ is defined as follows: For any bi-graded polynomial $g(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ of bi-degree $\preceq \mathbf{d}$, we denote by $\mathbf{v}_g$ the row vector of coefficients of $g(\mathbf{x}, \mathbf{y})$. Then the matrix $\mathcal{M}_{\mathbf{d}}$ is defined by concatenating the row vectors $\mathbf{v}_{ug_i}$, where $1 \le i \le m$ and u runs in the set of terms with bi-degree $\preceq \mathbf{d} - \mathbf{d}_i$. The number of terms of degree $\preceq \mathbf{d}$ is given as follows:

Lemma 4 ([35]). *The number of terms of degree $\preceq \mathbf{d}$ is equal to the coefficient $M_{\mathbf{d}} \in \mathbb{Z}$ of bi-degree $\mathbf{d}$ of the following two-variable power series:*

$$\frac{1}{(1-t_1)^{n_1+1}(1-t_2)^{n_2+1}}.$$

Moreover, the number of terms of degree $\mathbf{d}$ is equal to the coefficient $\tilde{M}_{\mathbf{d}} \in \mathbb{Z}$ of bi-degree $\mathbf{d}$ of the following two-variable power series:

$$\frac{1}{(1-t_1)^{n_1}(1-t_2)^{n_2}}.$$

Thus, from Lemma 4, the size of the bi-graded Macaulay matrix $\mathcal{M}_{\mathbf{d}}$ is considered to be approximately $M_{\mathbf{d}}$.

We explain the complexity estimation for solving a quadratic bi-graded semi-regular system. Then the rank of the homogeneous bi-graded Macaulay matrix $\widetilde{\mathcal{M}_{\mathbf{d}}}$ becomes full when $\mathbf{d}$ is a bi-degree of regularity $\mathbf{D} \in \mathcal{D}$ from Lemma 3. From such an observation, we can consider that a solution to the bi-graded semi-regular system can be found by solving a linear system with respect to $\mathcal{M}_{\mathbf{D}}$. Assume that $g_1, \ldots, g_m$ consist of m_1 polynomials with bi-degree (2, 0), m_2 polynomials with bi-degree (1, 1), and m_3 polynomials with bi-degree (0, 2). Set

$$N_1 := \begin{cases} \binom{n_1+1}{2} + n_1 + 1, & (m_1 > 0), \\ 0, & (otherwise), \end{cases}$$

$$N_2 := \begin{cases} (n_1+1)(n_2+1), & (m_2 > 0), \\ 0, & (otherwise), \end{cases}$$

$$N_3 := \begin{cases} \binom{n_2+1}{2} + n_2 + 1, & (m_3 > 0), \\ 0, & (otherwise). \end{cases}$$

Then, the complexity of solving the system $g_1 = \cdots = g_m = 0$ is estimated by

$$\min_{\mathbf{D}\in\mathcal{D}} \left\{ 3 \cdot M_{\mathbf{D}}^2 \cdot \max\{N_1, N_2, N_3\} \right\}.$$

Note that since a bi-degree of regularity $\mathbf{D}$ is not unique for $g_1,\ldots g_m$ in general, we need to take the minimum in the complexity estimation.

Remark 7 The idea of the estimation described in this subsection was given by Smith-Tone et al. [35]. In fact, they gave a complexity estimation of the bi-graded systems that appears in the RBS attack based on this idea. However, the complexity estimation we explained herein has not been sufficiently investigated for general bi-graded systems. It is noteworthy that a few studies regarding general bilinear systems (namely, bi-degree (1, 1)) have been reported in Ref. [54, 55]. Faugére et al. studied bilinear systems for under-determined cases in Ref. [55] using the F5 algorithm [16]. Meanwhile, Baena et al. studied them for over-determined cases in Ref. [54]. Baena et al. considered the behaviour of bilinear polynomials $g_1, \ldots, g_m \in \mathbb{F}_q[\mathbf{x}, \mathbf{y}]$ when only the terms in $\mathbf{y}$ are multiplied into $g_1, \ldots, g_m$, and then they defined the $\mathbf{y}$-semi-regularity and $\mathbf{y}$-degree of regularity. The exact complexity between our study and those of the abovementioned studies should be compared in the future.

5.3 | RBS attack and its new analysis

In this subsection, we describe the RBS attack [28] against the Rainbow scheme [11]. As stated above, the complexity estimation of solving bi-graded polynomial systems is developed via the analysis of the RBS attack. First, we explain the RBS attack. Then, based on Section 5.2, we explain a new complexity estimation of the RBS attack following Smith-Tone et al. [35].

5.3.1 | RBS attack

Let (v, o_1, o_2) be the Rainbow parameter set described in Section 2.2, and let $n = v + o_1 + o_2$ and $m = o_1 + o_2$. For a Rainbow public key $\mathcal{P} = (p_1, \ldots, p_m)$, the RBS attack recovers its secret key $(\mathcal{F}, \mathcal{T}, \mathcal{S})$ as follows: According to the definition of the easy-to-invert map $\mathcal{F} = (f_1, \ldots, f_m) : \mathbb{F}_q^n \to \mathbb{F}_q^m$, each symmetric matrix corresponding to f_i has the following form:

$$F_i = \begin{cases} \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & 0_{o_1\times o_1} & 0_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & (1 \le i \le o_1), \\ \begin{pmatrix} *_{v\times v} & *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times v} & *_{o_1\times o_1} & *_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & 0_{o_2\times o_2} \end{pmatrix} & (o_1 + 1 \le i \le m). \end{cases}$$

Similarly, the matrices corresponding to $\mathcal{S}$ and $\mathcal{T}$ can be written as follows:

$$S = \begin{pmatrix} I_v & 0_{v\times o_1} & 0_{v\times o_2} \\ *_{o_1\times v} & I_{o_1} & 0_{o_1\times o_2} \\ *_{o_2\times v} & *_{o_2\times o_1} & I_{o_2} \end{pmatrix}, \quad T = \begin{pmatrix} I_{o_1} & 0_{o_1\times o_2} \\ *_{o_2\times o_1} & I_{o_2} \end{pmatrix}. \tag{3}$$

Remark 8 It is known that the security of Rainbow does not decrease, even if $\mathcal{S}$ and $\mathcal{T}$ are taken in the form in Equation (3). Therefore, S and T are set to be in the form in Equation (3), which reduces the secret key size.

The symmetric matrices P_1, ..., P_m corresponding to the public polynomials p_1, ..., p_m are given as

$$(P_1, \ldots, P_m) = (SF_1{}^tS, \ldots, SF_m{}^tS) \cdot T. \tag{4}$$

According to the form in Equation (3), there exists an n-by-1 vector

$$\mathbf{s} = (\lambda_1, \ldots, \lambda_{v+o_1}, 0, \ldots, 0, 1)$$

such that

$$\mathbf{s} \cdot S = (0, \ldots, 0, 1).$$

Then, for $i = 1, \ldots, m$, we have

$$\mathbf{s} \cdot SF_i^tS \cdot {}^t\mathbf{s} = (0, \ldots, 0, 1) \cdot F_i \cdot {}^t(0, \ldots, 0, 1) = 0.$$

Since each P_k is a linear combination of

$$SF_1{}^tS, \ldots, SF_m{}^tS,$$

we obtain the equations in $\lambda_1, \ldots, \lambda_{v+o_1}$:

$$\mathbf{s} \cdot P_k \cdot {}^t\mathbf{s} = 0, \quad k = 1, \ldots, m. \tag{5}$$

By the form in Equation (3), 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

$$T\cdot {}^t\mathbf{t} = {}^t(1,0,\ldots,0).$$

Then, by multiplying Equation (4) by ${}^t\mathbf{t}$, we obtain

$$P_1 + \sum_{i=1}^{o_2} \lambda_{v+o_1+i} P_{o_1+i} = SF_1{}^tS.$$

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

$$\mathbf{s}\cdot P_1 + \sum_{i=1}^{o_2} \lambda_{v+o_1+i}\mathbf{s}\cdot P_{o_1+i} = \mathbf{s}\cdot SF_1{}^tS = (0,\ldots,0).$$

Consequently, for $k = 1, \ldots, n-1$, we obtain the following equations in $\lambda_1, \ldots, \lambda_n$:

$$\mathbf{s}\cdot P_1\cdot {}^t\mathbf{e}_k + \sum_{i=1}^{o_2} \lambda_{v+o_1+i}\mathbf{s}\cdot P_{o_1+i}\cdot {}^t\mathbf{e}_k = 0, \tag{6}$$

where $\mathbf{e}_k$ is the n-by-1 vector $\left(0,\ldots,0,1^k,0,\ldots,0\right)$. Here, we remove the case $k = n$ because Equation (6) for $k = n$ follows Equation (5).

Clearly, Equation (5) is a bi-graded system with bi-degree (2, 0) and Equation (6) is a bi-graded system with bi-degree (1, 1) with respect to $\{\lambda_1,\ldots,\lambda_{v+o_1}\}$, $\{\lambda_{v+o_1+1},\ldots,\lambda_n\}$. System Equations (5) and (6) consist of $n+m-1$ quadratic bi-graded equations in n variables. By solving the quadratic system, an attacker can recover a part of the secret key S and T, namely $\mathbf{s}$ and $\mathbf{t}$, respectively. The RBS attack can recover S and T by repeating a similar process (see Ref. [28] for details). Because the complexity of the RBS attack is dominated by that of solving the bi-graded quadratic system, it is sufficient to treat only the system. We refer to the quadratic system consisting of Equations (5) and (6) as the *RBS dominant system*.

5.3.2 | Complexity estimation

We first recall the complexity analysis of the RBS attack in the second round submission [56] of the NIST PQC standardisation project regarding the Rainbow scheme. As seen above, the RBS dominant system consists of n variables and $n+m-1$ quadratic equations. In Ref. [56], the complexity of solving the RBS dominant system was estimated using the hybrid version of the Wiedemann XL approach in Section 4.4 as follows:

$$\min_{0\le k\le n}\left\{q^k\cdot 3\binom{n+d_{\mathrm{reg}}^{(n-k,n+m-1)}}{d_{\mathrm{reg}}^{(n-k,n+m-1)}}^2\binom{n-k}{2}\right\}.$$

Namely, in Ref. [56] the complexity of the RBS dominant system was estimated without using the bi-graded structure and based on the assumption that the RBS dominant system is semi-regular. However, it is known in Ref. [33] in 2012 that the RBS dominant system does not behave as a semi-regular system in some experiments.

In 2020, Nakamura et al. [34] and Smith-Tone et al. [35] independently analysed the RBS dominant system by focussing on the bi-graded structure. The following estimation is given by Smith-Tone et al. [35]. The RBS dominant system consists of m polynomials with bi-degree (2, 0) and $n-1$ polynomials with bi-degree (1, 1). Then the complexity of solving the RBS dominant system can be estimated by

$$\min_{\mathbf{D}\in\mathcal{D}}\left\{3\cdot M_{\mathbf{D}}^2\cdot\max\left\{\binom{m+1}{2}+m+1,(m+1)n\right\}\right\}.$$

Here $\mathcal{D}$ is computed using

$$\frac{\prod_{i=1}^{m}(1-t_1^2)\prod_{i=1}^{n-1}(1-t_1t_2)}{(1-t_1)^{v+o_1}(1-t_2)^{o_2}}$$

as in Lemma 3, and $M_{\mathbf{D}}$ is given by Lemma 4 as $n_1 = v+o_1$ and $n_2 = o_2$.

Remark 9 The two-variable power series Equation (2) was introduced by Nakamura et al. [34] and Smith-Tone et al. [35] independently. Nakamura et al. [34] introduced Equation (2) as an analogy of the power series of Equation (1) in Lemma 1 and confirmed that $d_{\max}$ of the RBS dominant system can be approximated using the power series in Equation (2). Subsequently, Nakamura [36] arranged the theoretical background of the power series in Equation (2) by extending the studies of Diem [37] and Bardet et al. [19], for example, by using the idea of bi-graded semi-regularity and so on. On the other hand, Smith-Tone et al. [35] introduced the power series in Equation (2) based on two assumptions regarding maximal rank conjectures. It will be necessary to study the relationship between bi-graded semi-regularity and the two assumptions for further analysis. The complexity estimation of the bi-graded semi-regular system in this section follows the idea of Smith-Tone et al. [35]. Since the study of the bi-graded systems and their complexities have just begun, further research will be needed.

6 | RECTANGULAR MINRANK ATTACK

In this section, we explain the rectangular MinRank attack [29] against the Rainbow scheme proposed by Beullens. This attack is carried out by deforming the MinRank problem associated with the Rainbow scheme to another MinRank problem and by solving it using the support minor modelling method proposed by Bardet et al. [26].

In Section 6.1, we briefly explain the support minor modelling method [26] that solves the MinRank problem. In Section 6.2, we prepare some notations to explain the rectangular MinRank attack in terms of matrix representations. In Section 6.3, we describe the rectangular MinRank attack using matrix representation. In Section 6.4, we explain the

complexity estimation of the rectangular MinRank attack in Ref. [29].

6.1 | Support minor modelling method

In this subsection, we briefly explain the support minor modelling method [26] to solve the MinRank problem, which is an improvement of the minor modelling method [27].

Recall the MinRank problem: Given s matrices $M_1, \ldots, M_s \in \mathbb{F}_q^{t\times u}$ and an integer $r > 0$, find a non-trivial $\mathbb{F}_q$-linear combination $M = \sum_{i=1}^{s} a_i M_i$ with $\mathrm{Rank}(M) \le r$.

Let $M \in \mathbb{F}_q^{t\times u}$ be a correct solution for the MinRank problem and $\mathbf{w}_1, \ldots, \mathbf{w}_r$ be a set of row vectors of M such that the following r-by-u matrix W has the same rank as M:

$$W := \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_r \end{pmatrix} = \begin{pmatrix} w_{11} & w_{12} & \ldots & w_{1u} \\ \vdots & \vdots & \ddots & \vdots \\ w_{r1} & w_{r2} & \ldots & w_{ru} \end{pmatrix} \in \mathbb{F}^{r\times u}.$$

Then, any row vector $\mathbf{m}_i = (m_{i1}, \ldots, m_{iu})$ of M is a linear combination of $\mathbf{w}_1, \ldots, \mathbf{w}_r$, and the following $(r + 1)$-by-u matrix $W^{(i)}$ is of rank $\le r$:

$$W^{(i)} := \begin{pmatrix} \mathbf{m}_i \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_r \end{pmatrix}.$$

Thus, each minor of order $(r + 1)$ of $W^{(i)}$ is zero. The support minor modelling method constructs quadratic equations from this fact.

Let $\Delta = (\delta_1, \ldots, \delta_{r+1})$ be a subset of the index of column $\{1, \ldots, u\}$ with cardinality $r + 1$, where $\delta_1 < \ldots < \delta_{r+1}$. For any $1 \le i \le t$, the minor $c_{\Delta,i}$ of $W^{(i)}$ corresponding to Δ is written as follows:

$$c_{\Delta,i} := \det \begin{pmatrix} m_{i,\delta_1} & m_{i,\delta_2} & \ldots & m_{i,\delta_{r+1}} \\ w_{1,\delta_1} & w_{1,\delta_2} & \ldots & w_{1,\delta_{r+1}} \\ \vdots & \vdots & \ddots & \vdots \\ w_{r,\delta_1} & w_{r,\delta_2} & \ldots & w_{r,\delta_{r+1}} \end{pmatrix}$$

$$= \sum_{j=1}^{r+1} (-1)^{j+1} m_{i,\delta_j} \cdot \det \begin{pmatrix} & \overset{j}{\check{}} & & \\ w_{1,\delta_1} & w_{1,\delta_2} & \ldots & w_{1,\delta_{r+1}} \\ \vdots & \vdots & \ddots & \vdots \\ w_{r,\delta_1} & w_{r,\delta_2} & \ldots & w_{r,\delta_{r+1}} \end{pmatrix}.$$

Here, $\overset{j}{\check{}}$ shows that the j-th column vector is removed.

For $\Delta' \subset \{1, \ldots, u\}$ with cardinality r, we denote by $b_{\Delta'}$ the minor of W corresponding to Δ'. For instance, the determinant of the matrix in the second line in the definition of $c_{\Delta,i}$ is written as $b_{\Delta\setminus\{\delta_j\}}$. Thus, we have the equality:

$$c_{\Delta,i} = \sum_{j=1}^{r+1} (-1)^{j+1} m_{i,\delta_j} \cdot b_{\Delta\setminus\{\delta_j\}}.$$

Here, the (i, δ_j)-component m_{i,δ_j} of M is a linear combination of $a_1, \ldots, a_s$ since $M = \sum_{i=1}^{s} a_i M_i$. As a result, putting two sets of variables $\mathbf{a} = \{a_1, \ldots, a_s\}$ and $\mathbf{b} = \{b_{\Delta'}\}_{\Delta'}$, we have that $c_{\Delta,i}$ is a quadratic bi-graded homogeneous polynomial in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ with bi-degree (1, 1).

The support minor modelling method finds a low-rank matrix M by solving the system of bi-graded homogeneous equations in variables $\mathbf{a}$, $\mathbf{b}$:

$$c_{\Delta,i}(\mathbf{a}, \mathbf{b}) = 0 \quad (\Delta \subset \{1, \ldots, u\}, 1 \le i \le t).$$

This system consists of $t\binom{u}{r+1}$ equations in $s + \binom{u}{r}$ variables.

Next, we recall the complexity estimation for solving such a bi-graded system in Ref. [26]. We assume that the system has only one non-trivial solution up to a scalar multiple. Let J be the homogeneous ideal in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ generated by the system $c_{\Delta,i}(\mathbf{a}, \mathbf{b})$. For $d \in \mathbb{N}$, we define $J_{(d,1)} := \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)} \cap J$ as in Section 5.1. By an easy computation, we have

$$\dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)} = \binom{u}{r}\binom{s+d-1}{d}.$$

Let $d_{\min}$ be the smallest integer d such that

$$\dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J_{(d,1)} = 1.$$

When $d_{\min} < \min\{r + 2, q\}$, Bardet et al. [26] estimate the dimension of $\dim_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J_{(d,1)}$ for $d \le d_{\min}$ by constructing syzygies of the system as follows:

$$\dim \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J_{(d,1)}$$
$$= \binom{u}{r}\binom{s+d-1}{d} - \sum_{i=1}^{d} (-1)^{i+1} \binom{u}{r+i}\binom{t+i-1}{i}\binom{s+d-i-1}{d-i},$$

when the right-hand side is ≥ 2. Otherwise, the coefficient is 1. Then, by identifying each term in $J_{(d_{\min},1)}$ as a new variable, we obtain a linear system with one-dimensional solution space. By applying the Wiedemann XL approach to the linear system, we can solve the bi-graded system $c_{\Delta,i} = 0$. Therefore, the complexity of the support minor modelling method [26] is given by

$$3s(r+1)\left(\binom{u}{r}\binom{s+d_{\min}-1}{d_{\min}}\right)^2.$$

6.2 | Matrix deformation

As stated in Section 2.4, the security of the Rainbow scheme is reduced to an instance of the MinRank problem. The basic idea behind the rectangular MinRank attack [29] is to reveal

another instance of the MinRank problem lurking in the Rainbow scheme, which is different from the instance stated in Section 2.4. Beullens [29] explained this idea using the polynomial maps $\mathcal{P}$ and its polar forms. However, this idea can be explained in terms of the symmetric matrices of $\mathcal{P}$. For this purpose, we prepare some notations and a lemma in this subsection.

Let $(Q_1, \ldots, Q_m)$ be a set of n-by-n matrices over $\mathbb{F}_q$, and $\mathbf{q}_i^{(j)}$ denotes the j-th column vector of Q_i, namely,

$$Q_i = \begin{pmatrix} \mathbf{q}_i^{(1)} & \mathbf{q}_i^{(2)} & \cdots & \mathbf{q}_i^{(n)} \end{pmatrix} \in \mathbb{F}_q^{n\times n}.$$

Then, we define the new set $\left(\tilde{Q}_1, \ldots, \tilde{Q}_n\right)$ of n-by-m matrices as follows:

$$\begin{aligned} \tilde{Q}_1 &:= \begin{pmatrix} \mathbf{q}_1^{(1)} & \mathbf{q}_2^{(1)} & \cdots & \mathbf{q}_m^{(1)} \end{pmatrix}, \\ \tilde{Q}_2 &:= \begin{pmatrix} \mathbf{q}_1^{(2)} & \mathbf{q}_2^{(2)} & \cdots & \mathbf{q}_m^{(2)} \end{pmatrix}, \\ &\vdots \\ \tilde{Q}_n &:= \begin{pmatrix} \mathbf{q}_1^{(n)} & \mathbf{q}_2^{(n)} & \cdots & \mathbf{q}_m^{(n)} \end{pmatrix}. \end{aligned}$$

We call $\left(\tilde{Q}_1, \ldots, \tilde{Q}_n\right)$ the *matrix deformation* of $(Q_1, \ldots, Q_m)$. Then the following lemma can be easily proven:

Lemma 5 *Let* S be an n-by-n matrix and T be an m-by-m matrix. Then the matrix deformation of $(SQ_1{}^tS, \ldots, SQ_m{}^tS) \cdot T$ is given by

$$\left(S\tilde{Q}_1T, \ldots, S\tilde{Q}_nT\right)\cdot {}^tS.$$

The rectangular MinRank attack can be explained based on this lemma.

6.3 | Rectangular MinRank attack

Let $(P_1, \ldots, P_m)$ be the set of n-by-n symmetric matrices of the public key of the Rainbow scheme in Section 2.2. Then, by Lemma 5, we obtain

$$\left(\tilde{P}_1, \ldots, \tilde{P}_n\right) = \left(S\tilde{F}_1T, \ldots, S\tilde{F}_nT\right)\cdot {}^tS.$$

Here, $\tilde{F}_i$ has the following form:

$$\tilde{F}_i = \begin{cases} \begin{pmatrix} *_{v\times o_1} & *_{v\times o_2} \\ *_{o_1\times o_1} & *_{o_1\times o_2} \\ 0_{o_2\times o_1} & *_{o_2\times o_2} \end{pmatrix} & (1 \le i \le v), \\ \begin{pmatrix} *_{v\times o_1} & *_{v\times o_2} \\ 0_{o_1\times o_1} & *_{o_1\times o_2} \\ 0_{o_2\times o_1} & *_{o_2\times o_2} \end{pmatrix} & (v+1 \le i \le v+o_1), \\ \begin{pmatrix} 0_{v\times v} & *_{v\times o_2} \\ 0_{o_1\times v} & *_{o_1\times o_2} \\ 0_{o_2\times v} & 0_{o_2\times o_2} \end{pmatrix} & (v+o_1+1 \le i \le n). \end{cases}$$

Since $\tilde{F}_{v+o_1+1}, \ldots, \tilde{F}_n$ are of rank $\le o_2$, we have another instance of the MinRank problem. Beullens [29] proposed a key recovery attack based on this MinRank problem against the Rainbow scheme. This is called the rectangular MinRank attack.

More precisely, this attack is slightly modified in Ref. [29] as follows. With a high probability, there exists an n-by-1 vector

$$\mathbf{a} = (a_1, \ldots, a_{v+o_1+1}, 0, \ldots, 0) \in \mathbb{F}_q^n$$

such that $\mathbf{a}\cdot S = \left(\overbrace{0, \ldots, 0}^{v+o_1}, \overbrace{*, \ldots, *}^{o_2}\right)$. Then, we show that

$$\sum_{i=1}^{v+o_1+1} a_i\tilde{P}_i = \left(\tilde{P}_1, \ldots, \tilde{P}_n\right)\cdot {}^t\mathbf{a} = \left(S\tilde{F}_1T, \ldots, S\tilde{F}_nT\right)\cdot {}^t(\mathbf{a}\cdot S)$$

is a linear combination of $S\tilde{F}_{v+o_1+1}T, \ldots, S\tilde{F}_nT$. Thus, since this matrix is of rank $\le o_2$, the vector $\mathbf{a}$ gives a solution to the MinRank problem for $\left(\tilde{P}_1, \ldots, \tilde{P}_{v+o_1+1}\right)$ with the target rank o_2. Moreover, for $i = 1, \ldots, m$, we have

$$p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0,$$

where $\mathcal{P} = (p_1, \ldots, p_m)$ is a public key of the Rainbow scheme.

As a result, the vector $\mathbf{a}$ is a common solution of the following problems:

(i) $p_1(\mathbf{a}) = \cdots = p_m(\mathbf{a}) = 0$ for public key $\mathcal{P} = (p_1, \ldots, p_m)$,
(ii) MinRank problem for $\left(\tilde{P}_1, \ldots, \tilde{P}_{v+o_1+1}\right)$ with rank $r = o_2$.

The rectangular MinRank attack finds a common solution $\mathbf{a}$ of the above problems (i) and (ii).

6.4 | Complexity estimation

In this subsection, we explain the complexity estimation of the rectangular MinRank attack, namely finding a solution $\mathbf{a}$ to problems (i) and (ii). We assume that a solution $\mathbf{a}$ is unique up to a scalar multiple. Let J be the homogeneous ideal in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ generated by the support minor modelling method for MinRank problem (ii). The dimension of $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J_{(d,1)}$ for $d \le d_{\min}$ is given in Section 6.1 when $d_{\min} < \min\{o_2 + 2, q\}$. Let J' be the homogeneous ideal in $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]$ generated by J and $p_1(\mathbf{a}), \ldots, p_m(\mathbf{a})$. Beullens computes the dimension of $\mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J'_{(d,1)}$ under a generic assumption [29]. In the following, we explicitly describe the generic assumption. Let $H_J(t)$ be the partial Hilbert series of J with respect to (*, 1), namely

$$H_J(t) := \sum_d \left(\dim \mathbb{F}_q[\mathbf{a}, \mathbf{b}]_{(d,1)}/J_{(d,1)}\right)\cdot t^d.$$

Similarly, we define $H_{J'}(t)$ for J'. From Section 6.1, the coefficient of t^d in $H_J(t)$ is

$$\dim \mathbb{F}_q[\mathbf{a},\mathbf{b}]_{(d,1)}/J_{(d,1)} = \binom{m}{o_2}\binom{v+o_1+d}{d} - \sum_{i=1}^{d}(-1)^{i+1}\binom{m}{o_2+i}\binom{n+i-1}{i}\binom{v+o_1+d-i}{d-i}, \quad (7)$$

when the right-hand side is ≥ 2. Otherwise, the coefficient is 1.

Let $d'_{\min}$ be the smallest integer d such that the coefficient of degree d of $H_{J'}(t)$ is 1. Under the following generic assumption, we can compute $H_{J'}(t)$ and $d'_{\min}$ from $H_J(t)$.

Lemma 6 *For $1 \leq i \leq m$, let $J^{(i)}$ be the ideal generated by J and $p_1(\mathbf{a}), \ldots, p_i(\mathbf{a})$. Assume that for any $1 \leq i \leq m-1$ and any $d < d'_{\min}$, the following map is injective:*

$$\mathbb{F}_q[\mathbf{a},\mathbf{b}]_{(d-2,1)}/J^{(i)}_{(d-2,1)} \ni h \mapsto h \cdot p_{i+1}(\mathbf{a}) \in \mathbb{F}_q[\mathbf{a},\mathbf{b}]_{(d,1)}/J^{(i)}_{(d,1)}.$$

Then, we have

$$H_{J'}(t) = \left[(1-t^2)^m \cdot H_J(t)\right]^+, \quad (8)$$

where $[\ \cdot\ ]^+$ means $\left[\sum_i c_i t^i\right]^+ := \sum_{i<i_0} c_i t^i + \sum_{i \geq i_0} t^i$ and $i_0 := \min\{i \mid c_i \leq 1\}$.

Thus, if the assumption of Lemma 6 is satisfied, then $d'_{\min}$ is computed from the explicit Equation (8) of $H_{J'}(t)$ in Lemma 6. This lemma follows from similar discussions of the proofs for Lemmas 1 and 3 (see Refs. [19, 36]).

Then, by identifying each term in $J'_{(d'_{\min},1)}$ as a new variable, we obtain a linear system with one-dimensional solution space. By applying the Wiedemann XL approach to the linear system, we can find a common solution to problems (i) and (ii). Therefore, the complexity of the support minor modelling method is given by

$$3(o_2+1)(n+o_1+1)\left(\binom{m}{o_2}\binom{v+o_1+d'_{\min}}{d'_{\min}}\right)^2. \quad (9)$$

Remark 10 Beullens [29] mentioned that when the characteristic of $\mathbb{F}_q$ is 2, the above estimation of $\dim \mathbb{F}_q[\mathbf{a},\mathbf{b}]_{(d,1)}/J_{(d,1)}$ does not hold because of some syzygies of the system. To avoid this situation, Beullens [29] removes the first rows in matrices $\tilde{P}_1, \ldots, \tilde{P}_{v+o_1+1}$ in MinRank problem (ii) and experimentally confirms that the estimation holds. Then, the complexity estimation in this case is given by changing n to $n-1$ in Equations (7) and (9).

7 | CONCLUSION

In this paper, we surveyed some recent progress in the security analysis of MPKC, which is a leading candidate for PQC. The Rainbow scheme is one of the most influential multivariate schemes owing to its selection as a finalist in the third round of the NIST PQC standardisation project, and thus some recent progress in MPKC has been made via the security analysis of the Rainbow scheme.

Considering this situation, we mainly provided a survey on the following topics: the state-of-the-art approaches for solving a polynomial system used in MPKC and two recently improved attacks on the Rainbow scheme, namely the RBS attack using the bi-graded polynomial system in the studies of Nakamura et al. and Smith-Tone et al. and the rectangular MinRank attack proposed by Beullens.

In particular, we defined the semi-regularity of the bi-graded systems based on the work of Nakamura and explained the complexity estimation for solving a bi-graded system based on the idea of Smith-Tone et al. Moreover, we provided another description for the rectangular MinRank attack, which was originally proposed by Beullens, based on a matrix representation. By explicitly describing the generic assumption for the bi-graded system appearing in the rectangular MinRank attack, we reconfirmed the complexity estimation of solving the bi-graded system of the attack.

We believe this survey will be useful for future developments in MPKC research.

ACKNOWLEDGEMENTS

This work was supported by JST CREST Grant Number JPMJCR2113 and JSPS KAKENHI Grant Number JP19K20266, JP20K19802.

CONFLICT OF INTEREST

The authors declared that they have no conflicts of interest to this work.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Yasuhiko Ikematsu https://orcid.org/0000-0002-9714-2675

REFERENCES

1. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997). https://doi.org/10.1137/s0097539795293172
2. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-quantum Cryptography. Springer, Heidelberg (2009)
3. National Institute of Standards and Technology: Post-quantum cryptography standardization. https://csrc.nist.gov/projects/post-quantum-cryptography
4. Ding, J., Petzoldt, A., Schmidt, D.S.: Multivariate Public Key Cryptosystems, 2nd edn. Springer, New York (2020)
5. Garey, M.R., Johnson, D.S.: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (1979)
6. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: EUROCRYPT 1988, LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)

7. Patarin, J.: Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: EUROCRYPT 1996, LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
8. Casanova, A., et al.: GeMSS: A Great Multivariate Short Signature. Specification document of NIST PQC 2nd round submission package (2019)
9. Ding, J., et al.: Gui. Technical report. National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-submissions
10. Kipnis, A., Patarin, L., Goubin, L.: Unbalanced oil and vinegar schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer, Heidelberg (1999)
11. Ding, J., Schmidt, D.S.: Rainbow, a new multivariate polynomial signature scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005)
12. Ding, J., et al.: Rainbow. Technical report. National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-3-submissions
13. Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification schemes based on multivariate quadratic polynomials. In: CRYPTO 2011, LNCS, vol. 6841, pp. 706–723. Springer, Heidelberg (2011)
14. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. In: CRYPTO 1995, LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)
15. Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 98, LNCS, vol. 1462, pp. 257–266. Springer, Heidelberg (1998)
16. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: ISSAC 2002, pp. 75–83 (2002)
17. Patarin, J.: HFE first challenge. http://www.minrank.org/hfe/%23challenge (1996)
18. Faugére, J.C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: CRYPTO 2003, LNCS, vol. 2729, pp. 44–60 (2003)
19. Bardet, M., et al.: 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)
20. Dubois, V., Gamma, N.: The degree of regularity of HFE systems. In: Asiacrypt 2010, LNCS, vol. 6477, pp. 557–576. Springer, Heidelberg (2010)
21. Granboulan, L., Joux, A., Stern, J.: Inverting HFE is quasipolynomial. In: CRYPTO 2006, LNCS, vol. 4117, pp. 345–356. Springer, Heidelberg (2006)
22. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: CRYPTO 2011, LNCS, vol. 6841, pp. 724–742. Springer, Heidelberg (2011)
23. Ding, J., Yang, B.Y.: Degree of regularity for HFEv and HFEv-. In: PQCrypto 2013, LNCS, vol. 7932, pp. 52–66. Springer, Heidelberg (2013)
24. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: CRYPTO 99, LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
25. Buss, J., Frandsen, G., Shallit, J.: The computational complexity of some problems of linear algebra. J. Comput. Syst. Sci. 58(3), 572–596 (1999). https://doi.org/10.1006/jcss.1998.1608
26. Bardet, M., et al.: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In: International Conference on the Theory and Application of Cryptology and Information Security (2020)
27. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In: ISSAC 2010, pp. 257–264 (2010)
28. Ding, J., et al.: New differential-algebraic attacks and reparametrization of Rainbow. In: ACNS 2008, LNCS, vol. 5037, pp. 242–257. Springer, Heidelberg (2008)
29. Beullens, W.: Improved cryptanalysis of UOV and rainbow. In: EUROCRYPT 2021, LNCS, vol. 12696, pp. 348–373. Springer, Heidelberg (2021)
30. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F4). J. Pure Appl. Algebra. 139(1–3), 61–88 (1999). https://doi.org/10.1016/s0022-4049(99)00005-5
31. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE Trans. Inf. Theory. 32(1), 54–62 (1986). https://doi.org/10.1109/tit.1986.1057137
32. Ars, G., et al.: Comparison between XL and Gröbner basis algorithms. In: ASIACRYPT 2004. LNCS, vol. 3329, pp. 338–353. Springer, Heidelberg (2004)
33. 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. Accessed 22 September 2020
34. Nakamura, S., et al.: New complexity estimation on the rainbow-band-separation attack. Theor. Comput. Sci. 896, 1–8 (2021). https://doi.org/10.1016/j.tcs.2021.09.043
35. Smith-Tone, D., Perlner, R.A.: Rainbow Band Separation Is Better Than We Thought. IACR Cryptology ePrint Archive, 2020/702 (2020)
36. Nakamura, S.: Formal Power Series on Algebraic Cryptanalysis. arXiv.org e-Print archive (30 July 2020). arXiv. https://arxiv.org/abs/2007.14729
37. Diem, C.: Bound of regularity. J. Algebra. 423, 1143–1160 (2015). https://doi.org/10.1016/j.jalgebra.2014.09.029
38. Tao, C., et al.: Simple matrix scheme for encryption. In: PQCrypto 2013, LNCS, vol. 7932, pp. 231–242. Springer, Heidelberg (2013)
39. Porras, J., Baena, J., Ding, J.: ZHFE, a new multivariate public key encryption scheme. In: PQCrypto 2014, LNCS, vol. 8772, pp. 229–245. Springer, Heidelberg (2014)
40. Szepieniec, A., Ding, J., Preneel, B.: Extension field cancellation: a new central trapdoor for multivariate quadratic systems. In: PQCrypto 2016, LNCS, vol. 9606, pp. 182–196. Springer, Heidelberg (2016)
41. Ikematsu, Y., et al.: HFERP – a new multivariate encryption scheme. In: PQCrypto 2018, LNCS, vol. 10786, pp. 396–416. Springer, Heidelberg (2018)
42. Patarin, J.: The oil and vinegar algorithm for signatures. In: Dagstuhl Workshop on Cryptography (September 1997)
43. Beullens, W.: Breaking rainbow takes a weekend on a laptop. In: IACR Cryptology ePrint Archive (2022). https://eprint.iacr.org/2022/214.pdf
44. Chen, M.S., et al.: From 5-pass MQ-based identification to MQ-based signatures. In: ASIACRYPT 2016, LNCS, vol. 10032, pp. 135–165. Springer, Heidelberg (2016)
45. Chen, M.S., et al.: MQDSS. Technical report. National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-3-submissions
46. Courtois, N.T.: Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In: ASIACRYPT 2001, LNCS, vol. 2248, pp. 402–421. Springer, Heidelberg (2001)
47. Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. PhD thesis. Universität Innsbruck (1965)
48. Faugére, J.C., et al.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. 16(4), 329–344 (1993). https://doi.org/10.1006/jsco.1993.1051
49. Courtois, N., et al.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: EUROCRYPT 2000, LNCS, vol. 1807, pp. 392–407 (2000)
50. Coppersmith, D.: Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. Math. Comput. 62(205), 333–350 (1994). https://doi.org/10.2307/2153413
51. Yang, B.Y., et al.: Analysis of QUAD. In: FSE 2007, LNCS, vol. 4593, pp. 290–308. Springer, Heidelberg (2007)
52. Verbel, J.A., et al.: On the complexity of "superdetermined" MinRank instances. In: PQCrypto 2019, LNCS, vol. 11505, pp. 167–186. Springer, Heidelberg (2019)
53. Bettale, L., Faugère, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. J. Math. Cryptol. 3, 177–197 (2009). https://doi.org/10.1515/jmc.2009.009
54. Baena, J., Cabarcas, D., Verbel, J.: On the Complexity of Solving Generic Over-Determined Bilinear Systems. arXiv:2006.09442. https://arxiv.org/abs/2006.09442

55. Faugère, J.C., Safey El Din, M., Spaenlehauer, P.J.: Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): algorithms and complexity. J. Symb. Comput. 46(4), 406–437 (2011). https://doi.org/10.1016/j.jsc.2010.10.014
56. Ding, J., et al.: Rainbow. Technical report. National Institute of Standards and Technology. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-submissions

How to cite this article: Ikematsu, Y., Nakamura, S., Takagi, T.: Recent progress in the security evaluation of multivariate public-key cryptography. IET Inf. Secur. 17(2), 210–226 (2023). https://doi.org/10.1049/ise2.12092