Refined OJ Attacks: Tight Complexity for Rank Decoding Problems and Their Cryptographic Implications

Yongcheng Song[1,2], Rongmao Chen[2], Xinyi Huang[1⋆], Jiang Zhang[3], and Chao Lin[1]

[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
[2] State Key Laboratory of Cyberspace Security Defense (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085)
yongchengsong@outlook.com, xyhuang81@gmail.com, chaolin@nuaa.edu.cn
[3] School of Computer, National University of Defense Technology, Changsha, China
chromao@nudt.edu.cn
[4] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China
jiangzhang09@gmail.com

Abstract. The Rank Decoding (RD) problem lies at the core of rank-based cryptography. To enable efficient constructions, several variants have been introduced, notably the Non-Homogeneous RD (NHRD) problem and the Blockwise RD (BRD) problem. The *quantum* security of these systems is currently considered to be determined by the complexity of combinatorial attacks such as AGHT, PRR, and Ourivski–Johansson (OJ) attacks. However, for the OJ attack, the modeling, soundness, and relative complexities remain poorly understood, particularly for the NHRD and BRD variants, thereby limiting confidence in security claims and hindering the design of compact schemes.

In this work, we refine the modelings for the OJ attack (PIT, 2002) and the Improved OJ (IOJ, IEEE TIT 2025) attack, and obtain general and tight complexities on the RD, NHRD, and BRD problems. We show that the IOJ attack rests on optimistic assumptions that do not hold in practical random decoding scenarios, and thus its advantage over OJ should be disregarded in security assessments. For the RD problem, the OJ attack remains a strong candidate for the most powerful combinatorial attack in certain parameter regions, particularly when the code dimension k is small and the extension degree m is large. For the NHRD problem, we show that the OJ attack is the most powerful combinatorial attack for the parameters of NH-Multi-UR-AG, yielding up to a 100-bit improvement over the adapted AGHT attack (IEEE TIT 2024), while still preserving the claimed security level. For the BRD problem, we derive complexity formulas for general block structures, resolving questions posed in prior works (Asiacrypt 2023, IEEE TIT 2025, PQC 2024). Our analysis also reveals that the OJ attack is previously underestimated by about γ^2 bits, where γ denotes the minimum block weight. We further

⋆ Corresponding Author

show that the OJ attack outperforms AGHT and PRR attacks in certain parameter regions, achieving up to a 136-bit advantage over PRR (IEEE TIT 2025). Our work advances the understanding of decoding problems in the rank metrics and reinforces the security of related cryptosystems.

Keywords: Post-Quantum Cryptography, Rank-Based Cryptography, Rank Decoding Problem, OJ Attack, NIST PQC

1 Introduction

Code-based cryptography is a promising candidate for post-quantum cryptography. HQC [20] using Hamming metric codes recently has been selected by NIST PQC for the final standardization [22]. As an alternative, rank-based cryptography, namely code-based cryptography using rank metric codes, offers competitive performance [21]. Recent works [8,2,28,1,26] further explored the potential of rank metric cryptosystems, showing that McEliece, NTRU, Alekhnovich, and MPCitHead approaches outperform the Hamming metric counterparts in bandwidth. The typical cryptosystems are LowMS [2], ROLLO [28,1,26], RQC [28,1,26], Multi-UR-AG [8,26], and RYDE [9,10,11], whose security relies on the hardness of the rank decoding problems for $\mathbb{F}_{q^m}$-linear codes with rank metric.

$\mathbb{F}_{q^m}$-Linear Codes with Rank Metric. An $\mathbb{F}_{q^m}$-linear code ($[n,k]_{q^m}$-code) with rank metric of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_{q^m}^n$, which can be represented by a generator matrix of size $k \times n$ and rank k over $\mathbb{F}_{q^m}$. For a fixed basis of $\mathbb{F}_{q^m}$, any vector in $\mathbb{F}_{q^m}^n$ has an associated matrix in $\mathbb{F}_q^{m\times n}$. The rank weight of the vector is defined as the rank of its associated matrix. The support is the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ spanned by its coordinates. We call an error whose entries sharing a support a *homogeneous* (or *standard*) error. Any error of weight r and length n is determined by two parts: the basis (a vector in $\mathbb{F}_{q^m}^r$) of its support and the representation (a matrix in $\mathbb{F}_q^{r\times n}$) under the basis. The associated matrix of the basis is called the support matrix and the representation is called the coefficient matrix.

The RD/NHRD/BRD Problems. The Rank Decoding (RD) problem is to recover $\boldsymbol{x}$ and an error $\boldsymbol{e}$ from the noisy codeword $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$, given a generator matrix $\boldsymbol{G}$ of a random $[n,k]_{q^m}$-code. Recently, for designing efficient cryptosystems, two variants are proposed: the Non-Homogeneous RD (NHRD) problem [19,8] and the Blockwise RD (BRD) problem [27,28]. The main difference consists in the definition of the error $\boldsymbol{e}$. In the NHRD problem, one solves a non-homogeneous error, where an error is divided into three blocks whose first and third blocks share a support included in the support of the second block. The typical cryptosystems based on the NHRD problem are NH-Multi-RQC-AG and NH-Multi-UR-AG [8], two efficient encryptions. In the BRD problem, one solves a blockwise error, where an error is divided into some blocks whose supports are in direct sum. The BRD problem underlies blockwise RQC and ROLLO (BRQC and BROLLO), obtaining more practical bandwidths.

Attacks and Limitations. All known attacks against the above decoding problems are exponential, thereby making them promising hard problems for secure cryptosystems. The known attacks can be categorized into combinatorial attacks and algebraic attacks. The algebraic attacks have been extensively studied in recent years, with the Maximal Minors (MM) attack [4,6,5] emerging as the most powerful approach for most cryptographic parameter sets. The algebraic attacks typically determine the classical security level, since no direct quantum speedup is known for such attacks [9,11]. The combinatorial attacks are various: the Chabaud–Stern (CS) attack [14], the Ourivski-Johansson (OJ) attack [24], the Gaborit-Ruat-Schrek (GRS) attack [16], and the Aragon-Gaborit-Hauteville-Tillich (AGHT) attack [3]. For the NHRD and BRD problems, the tailored attacks have been proposed, including AGHT-NHRD [8] for NHRD, as well as Puchinger-Renner-Rosenkilde (PRR) [25] and Improved OJ (IOJ) [28] for BRD. Before the introduction of the MM attack, combinatorial attacks were commonly used to estimate both classical and quantum security of cryptosystems. Following the advent of the MM attack, they are now primarily used to estimate quantum security, typically by applying a quadratic speedup and dividing the exponential complexity by a factor of 2. For various current cryptographic parameters, the best combinatorial attack is not yet clearly identified. While the OJ and AGHT attacks often outperform the CS and GRS attacks, their concrete advantages are not always significant or well understood.

The OJ-type attacks consist of two techniques: basis enumeration and coordinate enumeration. Basis enumeration mainly guesses the support matrix, while coordinate enumeration focuses on the coefficient matrix. Unlike basis enumeration, coordinate enumeration strongly depends on the structure of error and becomes increasingly difficult for structured errors. Overall, despite several recent refinements [28,1] on the OJ-type attacks, the modeling, soundness, and complexity analysis remain poorly understood, especially for structured decoding problems such as NHRD and BRD. In particular, the interaction between basis enumeration, coordinate enumeration, and structured errors has not been systematically characterized, preventing the derivation of general and tight complexity. This gap undermines confidence in quantum security and hinders the design of compact schemes. RYDE's [9,10,11] recent exclusion from the next round of NIST PQC signature candidates [23] — partly due to the immature complexity analysis of the underlying decoding variants — further motivates a rigorous study of rank decoding.

1.1 Our Contributions

In this work, we develop a unified understanding of OJ-type attacks and their applications to structured rank decoding problems, and reinforce the security of related cryptosystems. Our main contributions are summarized as follows.

– **Unified (I)OJ modeling and tight complexity analysis.** We refine the (I)OJ modeling techniques and derive general, and tight complexity estimates for the RD, NHRD, and BRD problems. We show that basis enumeration is independent of the error structure, whereas coordinate enumeration

fundamentally depends on the structure of error representations. Moreover, we demonstrate that the IOJ attack relies on overly optimistic assumptions, which limits its applicability in practical random decoding settings.

- **Improved understanding of OJ attacks on the RD problem.** We derive a general complexity expression for the OJ attack on the RD problem for arbitrary code parameters. By our analysis, the OJ attack still has chance to outperform the AGHT attack and become the most powerful combinatorial attack for certain parameter regions, particularly those with small k and large m.
- **OJ attacks on the NHRD problem.** We adapt the OJ attack to the NHRD problem and show that, for the parameter sets of NH-Multi-UR-AG [8], it becomes the most powerful known combinatorial attack. Compared with the AGHT-NHRD attack [8], the complexity improvement reaches up to 100 bits. Nevertheless, NH-Multi-UR-AG still remains within its claimed security level.
- **OJ attacks on the BRD problem and implications for sum-rank decoding.** We derive general and tight complexity estimates for the OJ attack on the BRD problem with general block structures. We show that the OJ attack actually has higher complexity than the IOJ attack, with a gap of about γ^2 bits, where γ denotes the minimum block weight. For parameter regions with large m and small k, the OJ attack outperforms the AGHT and PRR attacks [28], thereby becoming the most powerful known combinatorial attack. For 256-bit secure BRQC instances, the complexity improvement over the PRR attack reaches up to 136 bits. Moreover, since blockwise errors are closely related to sum-rank metric errors [13,25,18], our analysis also advances the understanding of the OJ attack for decoding sum-rank codes.

1.2 Related Work

The Attacks on the RD Problem. There currently exist combinatorial attacks [14,24,16,3] and algebraic attacks [16,4,6,5] on the RD problem. The algebraic attacks resort to solve an algebraic system and the complexity is determined by the cost solving the system, specifically the number of unknowns and linearly independent equations. The first algebraic attack is the AP attack [16] exploiting annihilator polynomials. For current cryptographic parameters, this attack is considered to be very inefficient. A breakthrough algebraic attack is proposed in [4], where the authors found that the $\mathbb{F}_{q^m}$-linearity is allowed to devise a dedicated system, i.e., the Maximal Minors (MM) modeling. Then the MM modeling is refined and improved in [6]. The resulting MM modeling subtly reduces the RD problem to solving a linear system. This does not mean that the RD problem can be efficiently solved because the obtained system leads easily to an underdetermined case or is very huge. The authors in [6] also found that one can devise another algebraic system, i.e., the Support-Minors (SM) modeling, by combining equations of the MM modeling. The SM modeling later is proven to be too optimistic and underestimates the complexity since there exist a linear

dependency between the SM modeling and the MM modeling [5]. By excluding linear dependent equations, the authors obtained the SM-$\mathbb{F}_{q^m}^+$ modeling [5]. The analysis in [5] shows that the cost of the SM-$\mathbb{F}_{q^m}^+$ modeling is slightly large to that of the MM modeling [6]. These two algebraic attacks are independent of the size of q, can well exploit the structure of errors, and perform very powerful for most parameter regions.

The basic idea of the combinatorial attacks is to guess some unknowns about the information of error, then solve a linear system such as a parity-check equation to check the correctness of guess with the unique-solution condition, generally the equations are more than the unknowns. The guess cost is the main complexity for the combinatorial attacks. The first combinatorial attack is the CS attack proposed in [14]. Later, the CS attack was significantly improved in [24] by Ourivski and Johansson, namely the OJ attack. After 14 years, a new combinatorial attack was found, the GRS attack [16]. In 2018, Aragon, Gaborit, Hauteville, and Tillich further refined the GRS attack and proposed a new improvement, namely the AGHT attack [3]. The CS, GRS, and AGHT attacks consist of subtly guessing the support of the error then solving the parity-check equation to check the correctness of guessing. The OJ attack [24] transforms the quadratic multivariate system about the entries of support/coefficient matrices into a linear system. For currently most cryptographic parameters, the OJ and AGHT attacks are powerful combinatorial attacks. The former benefits from the small k and the latter from a small m and rate k/n. However, the underlying modelings remain insufficiently understood. This lack of understanding may weaken confidence in the security of the corresponding cryptosystems and hinder the identification of more compact parameter sets for efficient cryptographic constructions. One can observe that, while the works [4,6] exploit the underlying idea of the OJ attack to build the MM attack, they do not provide a general modeling for the OJ attack, nor do they elaborate on the basis/coordinate enumeration techniques.

The Attacks on the NHRD Problem. In [8], the authors introduce the NHRD problem and construct two cryptosystems, namely NH-Multi-RQC-AG and NH-Multi-UR-AG. To estimate the security of cryptosystems, they adapt the MM attack and the AGHT attack. We denote the adapted AGHT attack by AGHT-NHRD. This attack is regarded as the most powerful combinatorial attack for the NHRD problem. However, the impact of AGHT-NHRD appears to vary across different parameter regions of the two cryptosystems. In particular, for NH-Multi-UR-AG, the dimension parameter of the underlying NHRD instance is relatively small, which suggests that the OJ attack may become applicable and potentially more powerful than AGHT-NHRD. This indicates that the security of NHRD should also be evaluated with respect to the OJ attack. Nevertheless, adapting the OJ attack to the NHRD problem is non-trivial.

The Attacks on the BRD Problem. In addition to the SM modeling, typical combinatorial and algebraic attacks on the RD problem have been adapted to the BRD problem in [27,1,28,26]. In [28], the authors further adapt the PRR attack [25] for decoding sum-rank codes to the BRD problem. More recently,

the MM attack has been refined to obtain a more precise and general complexity analysis by deriving tight upper bounds on the number of independent equations across general block structures [26]. Regarding the OJ attack [24], the works [27,1,28] in fact give a refinement of the original framework. To distinguish it from the original OJ attack, we refer to this variant as the IOJ attack. However, several issues remain unresolved for the IOJ attack. Its soundness has not been fully established, and its complexity has only been analyzed for special cases—typically two or three equal-length blocks—rather than for general block structures. In particular, for structured errors such as blockwise errors, their representations typically exhibit specific algebraic structures, which make coordinate enumeration highly non-trivial and hinder the derivation of a general complexity expression. These issues stem from a limited understanding of the underlying (I)OJ modeling and the associated basis/coordinate enumeration techniques. Addressing these challenges requires a refined (I)OJ modeling for the BRD problem, together with a tight complexity over general block structures.

1.3 Organization

Section 2 presents notations and preliminaries. To derive the tight complexity for the OJ attack, Section 3 reduces the standard/non-homogeneous/blockwise errors. Section 4 refines the (I)OJ modeling and shows that the IOJ attack can be avoided. Sections 5, 6, and 7 respectively derive the complexity of the OJ attack against the RD/NHRD/BRD problems and obtain general and compact complexity expressions. We conclude this paper in Section 8.

2 Preliminaries

This section presents the used notations, then recalls some preliminaries including $\mathbb{F}_{q^m}$-linear codes and the RD/NHRD/BRD problems.

Notations. We denote by $\mathbb{N}$ the set of non-negative integers, q prime or prime power, and $\mathbb{F}_{q^m}$ an extension of degree m of the finite field $\mathbb{F}_q$. We view $\mathbb{F}_{q^m}$ as an m-dimensional vector space over $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^m}$ be a primitive element such that $\boldsymbol{\alpha} = (1, \alpha, , \ldots, \alpha^{m-1}) \in \mathbb{F}_{q^m}^m$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Vectors (resp. matrices) are denoted by lower-case (resp. upper-case) bold letters. For two positive integers N_1 and N_2 ($N_1 \leq N_2$), the notation $\{N_1 ... N_2\}$ represents positive integers from N_1 to N_2. The submatrix of a matrix $\boldsymbol{M}$ formed from the rows in I and columns in J is denoted by $\boldsymbol{M}_{I,J}$. When I (resp. J) consists of all the rows (resp. columns), we use the notation $\boldsymbol{M}_{*,J}$ (resp. $\boldsymbol{M}_{I,*}$). $\mathrm{GL}_\eta(\mathbb{F}_q)$ is a general linear group and represents the set of all invertible matrices of size η over $\mathbb{F}_q$. The matrix $\boldsymbol{I}_r$ is the identity matrix of size r. Let ω be the matrix multiplication exponent (or linear algebra constant) with $2 \leq \omega \leq 3$.

Definition 1 (Rank Metric). *Under the fixed basis* $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ *of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$*, for any* $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$*, write each coordinate as* $x_j =$

$\sum_{i=1}^{m} \alpha_i M_{ij}$ *with* $M_{ij} \in \mathbb{F}_q$*, and let* $\mathbf{Mat}(\boldsymbol{x}) = (M_{ij}) \in \mathbb{F}_q^{m \times n}$ *be its associated matrix. The rank weight* $\|\boldsymbol{x}\|_{\mathrm{R}}$ *of* $\boldsymbol{x}$ *is defined as the rank of* $\mathbf{Mat}(\boldsymbol{x})$*. The rank distance* $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y})$ *between* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *in* $\mathbb{F}_{q^m}^n$ *is defined by* $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y}) := \|\boldsymbol{x} - \boldsymbol{y}\|_{\mathrm{R}}$*.*

The support $\mathrm{Supp}(\boldsymbol{x})$ of $\boldsymbol{x}$ is defined as the $\mathbb{F}_q$-linear subspace $\langle x_1, x_2, \ldots, x_n \rangle_{\mathbb{F}_q}$, i.e., $\mathrm{Supp}(\boldsymbol{x}) = \langle x_1, x_2, \ldots, x_n \rangle_{\mathbb{F}_q}$. It follows that $\|\boldsymbol{x}\|_{\mathrm{R}} = \dim(\mathrm{Supp}(\boldsymbol{x}))$. The set of such vectors of weight r and length n is denoted by $\mathcal{S}_r^n$. Such vectors are referred to as *standard* (or *homogeneous*) errors.

Standard Error Decomposition. Let $\boldsymbol{e} \in \mathcal{S}_r^n$, and let $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_r) \in \mathbb{F}_{q^m}^r$ be a basis of $\mathrm{Supp}(\boldsymbol{e})$. Then there exists a matrix $\boldsymbol{C} \in \mathbb{F}_q^{r \times n}$ of rank r such that $\boldsymbol{e} = \boldsymbol{\varepsilon C}$. Fixing the basis $\boldsymbol{\alpha}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, there exists a matrix $\boldsymbol{S} \in \mathbb{F}_q^{m \times r}$ of rank r such that $\boldsymbol{\varepsilon} = \boldsymbol{\alpha S}$. Hence, $\boldsymbol{e} = \boldsymbol{\alpha SC}$. We refer to $\boldsymbol{\varepsilon}$ as a *(support) basis* of $\boldsymbol{e}$, $\boldsymbol{S}$ as the *support matrix*, and $\boldsymbol{C}$ as the *coefficient matrix*. Under the basis $\boldsymbol{\alpha}$, we write $\boldsymbol{e} = \boldsymbol{\varepsilon C} = \boldsymbol{\alpha SC} = \boldsymbol{\alpha}\,\mathbf{Mat}(\boldsymbol{e})$.

Definition 2 ($\mathbb{F}_{q^m}$-Linear Codes with Rank Metric). *An $\mathbb{F}_{q^m}$-linear code embedded with rank metric of length n and dimension k is a subspace of dimension k of $\mathbb{F}_{q^m}^n$. Such $\mathbb{F}_{q^m}$-linear codes are denoted by $[n, k]_{q^m}$.*

Given an $[n, k]_{q^m}$-linear code $\mathcal{C}$, a matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ is called *generator matrix* iff $\mathcal{C} = \left\{\boldsymbol{mG} \;:\; \boldsymbol{m} \in \mathbb{F}_{q^m}^k\right\}$ and a matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ is called *parity-check matrix* iff $\mathcal{C} = \left\{\boldsymbol{c} \in \mathbb{F}_{q^m}^n \;:\; \boldsymbol{Hc}^\top = \boldsymbol{0}\right\}$. The systematic form of $\boldsymbol{G}$ is defined as $[\boldsymbol{I}_k \;\; \boldsymbol{R}]$ where $\boldsymbol{R} \in \mathbb{F}_{q^m}^{k \times (n-k)}$.

2.1 The RD, BRD, and NHRD Problems

The Rank Decoding (RD) problem and its dual form, Rank Syndrome Decoding (RSD) problem, are as follows.

The RD Problem: Let $\boldsymbol{G}$ be a generator matrix of a random $[n, k]_{q^m}$-linear code $\mathcal{C}$, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, and $r \in \mathbb{N}$. The problem is to find a $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a standard error $\boldsymbol{e} \in \mathcal{S}_r^n$ such that $\boldsymbol{y} = \boldsymbol{xG} + \boldsymbol{e}$.

The RSD Problem: Let $\boldsymbol{H}$ be a generator matrix of a random $[n, k]_{q^m}$-linear code $\mathcal{C}$, $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$, and $r \in \mathbb{N}$. The problem is to find a standard error $\boldsymbol{e} \in \mathcal{S}_r^n$ such that $\boldsymbol{He}^\top = \boldsymbol{s}$.

We denote the RD/RSD problem by $\mathsf{RD}_{q,m,n,k,r}/\mathsf{RSD}_{q,m,n,k,r}$. They have equivalent hardness. For their hardness, it is not known to be NP-complete, but there is a randomized reduction from RSD to an NP-complete problem [17], namely decoding in the Hamming metric [7]. This reduction holds for sufficiently large m ($m \geq 4qn$), which is beyond the currently cryptographic parameters regions. Another evidence is that the RD problem can be *generally* reduced to the MinRank problem [15] which is proven NP-complete in [12].

The NHRD problem [28] is the first variant of the RD problem. In the NHRD problem, one finds a non-homogeneous error. Let $\boldsymbol{n} = (n_1, n_2, n_3) \in \mathbb{N}^3$, $\boldsymbol{r} = (r_1, r_2) \in \mathbb{N}^2$, $n = \sum_{i=1}^{3} n_i$, and $r = \sum_{i=1}^{2} r_i$.

Definition 3 (Non-Homogeneous Error [8]). *Let $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^{n_i}$ be a vector for $i \in \{1..3\}$. An error $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3) \in \mathbb{F}_{q^m}^{n}$ is called a non-homogeneous error if 1) $\|(\boldsymbol{e}_1, \boldsymbol{e}_3)\|_{\mathrm{R}} = r_1$; 2) $\|\boldsymbol{e}_2\|_{\mathrm{R}} = r_1 + r_2$; and 3) $\mathrm{Supp}((\boldsymbol{e}_1, \boldsymbol{e}_3)) \subset \mathrm{Supp}(\boldsymbol{e}_2)$. We denote the set of such non-homogeneous errors by $\widehat{\mathcal{S}}_{\boldsymbol{r}}^{\boldsymbol{n}}$.*

Non-Homogeneous Error Decomposition. From [19] (Section 6.2.2) and [8] (Section 5.2), for random $\boldsymbol{e} \in \widehat{\mathcal{S}}_{\boldsymbol{r}}^{\boldsymbol{n}}$, , there are a basis $\boldsymbol{\varepsilon}$, a support matrix $\boldsymbol{S}$, and a coefficient matrix $\boldsymbol{C}$ satisfying $\boldsymbol{e} = \boldsymbol{\varepsilon}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C}$ and

$$\boldsymbol{\varepsilon} = (\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2) \in \mathbb{F}_{q^m}^{r}, \quad \boldsymbol{\varepsilon} = \boldsymbol{\alpha}\boldsymbol{S}, \quad \boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_1 & \boldsymbol{C}_2 & \boldsymbol{C}_3 \\ \boldsymbol{0} & \boldsymbol{C}_4 & \boldsymbol{0} \end{bmatrix} \in \mathbb{F}_{q}^{r \times n}, \tag{1}$$

where $\boldsymbol{\varepsilon}_1 \in \mathbb{F}_{q^m}^{r_1}$, $\boldsymbol{\varepsilon}_2 \in \mathbb{F}_{q^m}^{r_2}$, $\boldsymbol{S} \in \mathbb{F}_{q}^{m \times r}$, $\boldsymbol{C}_1 \in \mathbb{F}_{q}^{r_1 \times n_1}$ (rank r_1), $\begin{bmatrix} \boldsymbol{C}_2 \\ \boldsymbol{C}_4 \end{bmatrix} \in \mathbb{F}_{q}^{r \times n_2}$ (rank r), and $\boldsymbol{C}_3 \in \mathbb{F}_{q}^{r_1 \times n_3}$ (rank r_1).

Definition 4 (Non-Homogeneous RD (NHRD) Problem [19,8]). *Let $\boldsymbol{G}$ be a generator matrix of a random $[n,k]_{q^m}$-linear code $\mathcal{C}$ and $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$. The problem is to find a $\boldsymbol{x} \in \mathbb{F}_{q^m}^{k}$ and a non-homogeneous error $\boldsymbol{e} \in \widehat{\mathcal{S}}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$.*

We denote the NHRD problem by $\mathsf{NHRD}_{q,m,n,k,r}^{\boldsymbol{n},\boldsymbol{r}}$. Its dual form is called the Non-Homogeneous RSD (NHRSD) problem, $\mathsf{NHRSD}_{q,m,n,k,r}^{\boldsymbol{n},\boldsymbol{r}}$.

The BRD problem [28] is another variant of the RD problem. In the BRD problem, one finds a blockwise error. Let $\ell \in \mathbb{N}$, $\boldsymbol{n} = (n_1, n_2, \ldots, n_\ell) \in \mathbb{N}^\ell$, $\boldsymbol{r} = (r_1, r_2, \ldots, r_\ell) \in \mathbb{N}^\ell$, $n = \sum_{i=1}^{\ell} n_i$, and $r = \sum_{i=1}^{\ell} r_i$.

Definition 5 (Blockwise Error [28]). *Let $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^{n_i}$ be a vector of weight r_i for $i \in [\ell]$. An error $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_\ell) \in \mathbb{F}_{q^m}^{n}$ is called a blockwise error if the supports of sub-vectors $\boldsymbol{e}_i$'s are in direct sum. We denote the set of such blockwise errors by $\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$.*

Since $\boldsymbol{e}_i$'s supports are in direct sum if and only if $\mathsf{dim}\left(\sum_{i=1}^{\ell} \mathrm{Supp}(\boldsymbol{e}_i)\right) = \sum_{i=1}^{\ell} \mathsf{dim}\left(\mathrm{Supp}(\boldsymbol{e}_i)\right)$, we have

$$\|\boldsymbol{e}\|_{\mathrm{R}} = \mathsf{dim}\left(\mathrm{Supp}(\boldsymbol{e})\right) = \mathsf{dim}\left(\sum_{i=1}^{\ell} \mathrm{Supp}(\boldsymbol{e}_i)\right) = \sum_{i=1}^{\ell} \mathsf{dim}\left(\mathrm{Supp}(\boldsymbol{e}_i)\right) = \sum_{i=1}^{\ell} r_i = r.$$

Blockwise Error Decomposition. From [28] (Section 4), for random $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$, there are a basis $\boldsymbol{\varepsilon}$, a support matrix $\boldsymbol{S}$, and a coefficient matrix $\boldsymbol{C}$ satisfying $\boldsymbol{e} = \boldsymbol{\varepsilon}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C}$ and

$$\boldsymbol{\varepsilon} = (\boldsymbol{\varepsilon}_1, \boldsymbol{\varepsilon}_2, \ldots, \boldsymbol{\varepsilon}_\ell) \in \mathbb{F}_{q^m}^{r}, \quad \boldsymbol{\varepsilon} = \boldsymbol{\alpha}\boldsymbol{S}, \quad \boldsymbol{C} = \mathbf{Diag}(\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_\ell) \in \mathbb{F}_{q}^{r \times n} \tag{2}$$

where $\boldsymbol{\varepsilon}_i \in \mathbb{F}_{q^m}^{r_i}$ and $\boldsymbol{C}_i \in \mathbb{F}_{q}^{r_i \times n_i}$ (rank r_i) for $i \in \{1..\ell\}$, and $\boldsymbol{S} \in \mathbb{F}_{q}^{m \times r}$.

Definition 6 (Blockwise RD (BRD) Problem [28]). *Let $\boldsymbol{G}$ be a generator matrix of a random $[n,k]_{q^m}$-linear code $\mathcal{C}$ and $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$. The problem is to find a $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a blockwise error $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$.*

When $\ell = 1$, the BRD problem is exactly the RD problem. Different from the works [27,28], we here slightly change the notations. We denote it by $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$. Its dual form is called the Blockwise RSD (BRSD) problem, $\mathsf{BRSD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$.

The building of the OJ attack exploits Equations (3) and (4) in Theorem 1. We refer to Section 4 for the OJ attack.

Theorem 1. *Solving the RD/NHR/BRD problems defined by an $[n,k]_{q^m}$ linear code $\mathcal{C}$ and instantiated by $(\boldsymbol{G},\boldsymbol{y},\boldsymbol{e})$ is equivalent to finding a codeword belonging to $\mathcal{S}_r^n/\widehat{\mathcal{S}}_{\boldsymbol{r}}^{\boldsymbol{n}}/\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ in the $[n,k+1]_{q^m}$ extended code $\mathcal{C}_{\boldsymbol{y}}$ of $\mathcal{C}$.*

Proof. Once obtaining word $\boldsymbol{y}$, one adds $\boldsymbol{y}$ to $\mathcal{C}$ and obtains an $[n,k+1]_{q^m}$ extended code $\mathcal{C}_{\boldsymbol{y}} = \mathcal{C} + \langle \boldsymbol{y} \rangle$ with a generator matrix $\begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{G} \end{bmatrix}$. In this way, $\boldsymbol{e} = \begin{pmatrix} 1 & -\boldsymbol{m} \end{pmatrix} \begin{bmatrix} \boldsymbol{y} \\ \boldsymbol{G} \end{bmatrix}$ is exactly a codeword of $\mathcal{C}_{\boldsymbol{y}}$. Let $\boldsymbol{G}_{\boldsymbol{y}} \in \mathbb{F}_{q^m}^{(k+1)\times n}$ be a generator matrix of $\mathcal{C}_{\boldsymbol{y}}$ and $\boldsymbol{H}_{\boldsymbol{y}} \in \mathbb{F}_{q^m}^{(n-k-1)\times n}$ be a parity-check matrix of $\mathcal{C}_{\boldsymbol{y}}$. Then solving the RD/NHRD/BRD problems is equivalent to finding an $\boldsymbol{u} \in \mathbb{F}_{q^m}^{k+1}$ such that

$$\boldsymbol{u}\boldsymbol{G}_{\boldsymbol{y}} = \boldsymbol{e}, \tag{3}$$

or finding an error $\boldsymbol{e} \in \mathcal{S}_r^n/\widehat{\mathcal{S}}_{\boldsymbol{r}}^{\boldsymbol{n}}/\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that

$$\boldsymbol{e}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \boldsymbol{0}_{n-k-1}. \tag{4}$$

□

3 Reduced Decomposition for Three Types of Errors

The OJ attack consists in exhaustively searching the unknown entries of the support matrix or the coefficient matrix, then solving another one from the parity-check equation Equation (4). The number of unknown entries determines the complexity. A smaller number of unknown entries leads to a more powerful attack. In this section, we present the reduction of decomposition for the standard/non-homogeneous/blockwise errors, and give reduced support/coefficient matrices. For the standard errors, the reduction is analyzed in [24] which has been used in [4,6]. The reduction of the blockwise errors is analyzed in [27,28]. We further reduce the decomposition of non-homogeneous errors.

3.1 Reduced Decomposition for Standard Errors

We use two well-known assumptions for random standard errors:

- The first coordinate of $\boldsymbol{e}$ is 1. One can observe that Equation (4) has a large number of solutions. All multiples $\beta\boldsymbol{e}$ for any non-zero $\beta \in \mathbb{F}_{q^m}^*$ are its solutions because $\beta\boldsymbol{e}$ keeps the weight of $\boldsymbol{e}$. This shows that Equation (4) includes a solution whose first coordinate is 1 because β can be specified to the inverse of the first coordinate of $\boldsymbol{e}$. Let the first coordinate of the solution be 1, then such a solution is unique to Equation (4). We find such a solution. Under the basis $\boldsymbol{\alpha}$, one can set the first column of $\boldsymbol{C}$ to $(1\ 0\ \cdots\ 0)^\top$ and the first column of $\boldsymbol{S}$ to $(1\ 0\ \cdots\ 0)^\top$.
- The first r coordinates of $\boldsymbol{e}$ are linearly independent over $\mathbb{F}_q$. This probability is equal to the probability that the random $r \times r$ matrix over $\mathbb{F}_q$ is invertible, ≥ 0.289 for increased q. If it does not hold, we can perform an invertible matrix $\boldsymbol{P} \in \mathbb{F}_q^{n\times n}$ on the instance $(\boldsymbol{G}, \boldsymbol{y}, \boldsymbol{e})$ of the RD problem until the first r coordinates of $\boldsymbol{eP}$ are independent over $\mathbb{F}_q$. By the probability, such $\boldsymbol{P}$ is easy to be found. Then one solves a new instance $(\boldsymbol{GP}, \boldsymbol{yP}, \boldsymbol{eP})$. Solving these two instances is equivalent because $\boldsymbol{eP}$ keeps the support of $\boldsymbol{e}$.

Combining two assumptions, $\boldsymbol{S}$ and $\boldsymbol{C}$ can be further reduced to the following two forms with fewer entries.

- $\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$. By Gaussian elimination on columns of $\boldsymbol{S}$, there exists a matrix $\boldsymbol{P} = \left[\begin{array}{c|c} 1 & \boldsymbol{p} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{P'} \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{p} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{P'} \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{SP} = \left[\begin{array}{c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} \end{array}\middle|\, \boldsymbol{S'}\right]$ and $\boldsymbol{P}^{-1}\boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \end{array}\middle|\, \boldsymbol{C'}\right]$ where $\boldsymbol{S'} \in \mathbb{F}_q^{(m-r)\times(r-1)}$ and $\boldsymbol{C'} \in \mathbb{F}_q^{r\times(n-1)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{P}\boldsymbol{P}^{-1}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} \end{array}\middle|\, \boldsymbol{S'}\right]\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \end{array}\middle|\, \boldsymbol{C'}\right]. \tag{5}$$

  The reduced support matrix is $\boldsymbol{S} := \boldsymbol{SP}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{P}^{-1}\boldsymbol{C}$.
- $\boldsymbol{C}_{*,\{1..r\}} = \boldsymbol{I}_r$. By Gaussian elimination on rows of $\boldsymbol{C}$, there exists a matrix $\boldsymbol{Q} = \left[\begin{array}{c|c} 1 & \boldsymbol{q} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{Q'} \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{q} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{Q'} \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{SQ}^{-1} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \end{array}\middle|\, \boldsymbol{S'}\right]$ and $\boldsymbol{QC} = [\boldsymbol{I}_r\ \boldsymbol{C'}]$ where $\boldsymbol{S'} \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C'} \in \mathbb{F}_q^{r\times(n-r)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{Q}^{-1}\boldsymbol{Q}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \end{array}\middle|\, \boldsymbol{S'}\right][\boldsymbol{I}_r\ \boldsymbol{C'}]. \tag{6}$$

  The reduced support matrix is $\boldsymbol{S} := \boldsymbol{SQ}^{-1}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{QC}$.

3.2 Reduced Decomposition for Non-Homogeneous Errors

For random non-homogeneous errors, we extend two assumptions of the standard errors to the non-homogeneous errors:

- The first coordinate of $\boldsymbol{e}$ be 1. Then one can set the first column of $\boldsymbol{C}$ to $(1\ 0\ \cdots\ 0)^\top$ and the first column of $\boldsymbol{S}$ to $(1\ 0\ \cdots\ 0)^\top$.
- The error is $(\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$. The first r_1 coordinates of $\boldsymbol{e}_1$ are independent over $\mathbb{F}_q$ and $\boldsymbol{C}_4$ is of systematic form.

With these two assumptions, $\boldsymbol{S}$ and $\boldsymbol{C}$ can be further reduced to two forms with fewer entries.

- $\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$. By Gaussian elimination on columns of $\boldsymbol{S}$, there exists a matrix $\boldsymbol{P} = \left[\begin{array}{c|c} 1 & \boldsymbol{p} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{P}' \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{p} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{P}' \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{SP} = \left[\begin{array}{c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} \end{array}\middle|\, \boldsymbol{S}'\right]$ and $\boldsymbol{P}^{-1}\boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \end{array}\middle|\, \boldsymbol{C}'\right]$ where $\boldsymbol{S}' \in \mathbb{F}_q^{(m-r)\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-1)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{P}\boldsymbol{P}^{-1}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} \end{array}\middle|\, \boldsymbol{S}'\right]\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \end{array}\middle|\, \boldsymbol{C}'\right]. \tag{7}$$

  The reduced support matrix is $\boldsymbol{S} := \boldsymbol{SP}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{P}^{-1}\boldsymbol{C}$.
- The error is $(\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$. $\boldsymbol{C}_1$ and $\boldsymbol{C}_4$ are of systematic form. By Gaussian elimination on row of $\boldsymbol{C}$, there exists a matrix $\boldsymbol{Q} = \left[\begin{array}{c|c} 1 & \boldsymbol{q} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{Q}' \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{q} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{Q}' \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{S}\boldsymbol{Q}^{-1} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \end{array}\middle|\, \boldsymbol{S}'\right]$ and $\boldsymbol{Q}\boldsymbol{C} = \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}'_1] & \boldsymbol{C}'_2 & \boldsymbol{C}'_3 \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}'_4] & \boldsymbol{0} \end{bmatrix}$ where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$, $\boldsymbol{C}'_1 \in \mathbb{F}_q^{r_1\times(n_1-r_1)}$, $\boldsymbol{C}'_2 \in \mathbb{F}_q^{r_1\times n_2}$, $\boldsymbol{C}'_3 \in \mathbb{F}_q^{r_1\times n_3}$, and $\boldsymbol{C}'_4 \in \mathbb{F}_q^{r_2\times(n_2-r_2)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{Q}^{-1}\boldsymbol{Q}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \end{array}\middle|\, \boldsymbol{S}'\right]\begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}'_1] & \boldsymbol{C}'_2 & \boldsymbol{C}'_3 \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}'_4] & \boldsymbol{0} \end{bmatrix}. \tag{8}$$

  The reduced support matrix is $\boldsymbol{S} := \boldsymbol{S}\boldsymbol{Q}^{-1}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{Q}\boldsymbol{C}$.

Since solving the permuted NHRD instance is equivalent to solving the original NHRD instance. We here consider permuting $\boldsymbol{e}_1$ and $\boldsymbol{e}_2$, the error $\boldsymbol{e} = (\boldsymbol{e}_2, \boldsymbol{e}_1, \boldsymbol{e}_3)$, and solving the corresponding NHRD instance. In this way, the coefficients matrix $\boldsymbol{C}$ of Equation (1) is

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{C}_2 & \boldsymbol{C}_1 & \boldsymbol{C}_3 \\ \boldsymbol{C}_4 & \boldsymbol{0} & \boldsymbol{0} \end{bmatrix} \in \mathbb{F}_q^{r\times n},$$

where $\boldsymbol{C}_1 \in \mathbb{F}_q^{r_1 \times n_1}$ (rank r_1), $\begin{bmatrix}\boldsymbol{C}_2\\ \boldsymbol{C}_4\end{bmatrix} \in \mathbb{F}_q^{r \times n_2}$ (rank r), and $\boldsymbol{C}_3 \in \mathbb{F}_q^{r_1 \times n_3}$ (rank r_1).

We extend two assumptions of the standard errors to such non-homogeneous errors:

- The first coordinate of $\boldsymbol{e}$ be 1. Then one can set the first column of $\boldsymbol{C}$ to $(1\ 0\ \cdots\ 0)^\top$ and the first column of $\boldsymbol{S}$ to $(1\ 0\ \cdots\ 0)^\top$.
- The first r coordinates of each $\boldsymbol{e}_2$ are independent over $\mathbb{F}_q$.

With these two assumptions, $\boldsymbol{S}$ and $\boldsymbol{C}$ can be further reduced to two forms with fewer entries. The first r coordinates of each $\boldsymbol{e}_2$ are independent over $\mathbb{F}_q$.

- $\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$. The reduced support/coefficient matrices are the same as Equation (7).
- $\begin{bmatrix}\boldsymbol{C}_2\\ \boldsymbol{C}_4\end{bmatrix}$ is of systematic form. By Gaussian elimination on row of $\boldsymbol{C}$, there exists a matrix $\boldsymbol{Q} = \left[\begin{array}{c|c} 1 & \boldsymbol{q} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{Q}' \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{q} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{Q}' \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{S}\boldsymbol{Q}^{-1} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right]$ and $\boldsymbol{Q}\boldsymbol{C} = \left[\begin{array}{c|cc} \boldsymbol{I}_r\ \boldsymbol{C}_2' & \boldsymbol{C}_1' & \boldsymbol{C}_3' \\ \hline & \boldsymbol{0} & \boldsymbol{0} \end{array}\right]$ where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$, $\boldsymbol{C}_2' \in \mathbb{F}_q^{r\times(n_2-r)}$, $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1\times n_1}$, and $\boldsymbol{C}_3' \in \mathbb{F}_q^{r_1\times n_3}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{Q}^{-1}\boldsymbol{Q}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right]\left[\begin{array}{c|cc} \boldsymbol{I}_r\ \boldsymbol{C}_2' & \boldsymbol{C}_1' & \boldsymbol{C}_3' \\ \hline & \boldsymbol{0} & \boldsymbol{0} \end{array}\right]. \tag{9}$$

The reduced support matrix is $\boldsymbol{S} := \boldsymbol{S}\boldsymbol{Q}^{-1}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{Q}\boldsymbol{C}$.

3.3 Reduced Decomposition for Blockwise Errors

For random blockwise errors, we extend two assumptions of the standard errors to the blockwise errors:

- The first coordinate of $\boldsymbol{e}$ be 1. Then one can set the first column of $\boldsymbol{C}$ to $(1\ 0\ \cdots\ 0)^\top$ and the first column of $\boldsymbol{S}$ to $(1\ 0\ \cdots\ 0)^\top$.
- The first r_i coordinates of $\boldsymbol{e}_i$ are independent over $\mathbb{F}_q$.

With these two assumptions, $\boldsymbol{S}$ and $\boldsymbol{C}$ can be further reduced to two forms with fewer entries.

- $\boldsymbol{S}_{\{1..r\},*} = \boldsymbol{I}_r$. By Gaussian elimination on columns of $\boldsymbol{S}$, there exists a matrix $\boldsymbol{P} = \left[\begin{array}{c|c} 1 & \boldsymbol{p} \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{P}' \end{array}\right] \in \mathrm{GL}_r(\mathbb{F}_q)$ where $\boldsymbol{p} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{P}' \in \mathrm{GL}_{r-1}(\mathbb{F}_q)$ such that $\boldsymbol{S}\boldsymbol{P} = \left[\begin{array}{c|c} \boldsymbol{I}_r & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right]$ and $\boldsymbol{P}^{-1}\boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{C}' \end{array}\right]$ where $\boldsymbol{S}' \in \mathbb{F}_q^{(m-r)\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-1)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{P}\boldsymbol{P}^{-1}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c|c} \boldsymbol{I}_r & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right]\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{C}' \end{array}\right]. \tag{10}$$

The reduced support matrix is $\boldsymbol{S} := \boldsymbol{S}\boldsymbol{P}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{P}^{-1}\boldsymbol{C}$.

– $\boldsymbol{C}_i$ is of systematic form. By Gaussian elimination on row of $\boldsymbol{C}$, there are matrices $\boldsymbol{Q}_i = \left[\begin{array}{c|c} 1 & \boldsymbol{q}_i \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{Q}'_i \end{array}\right] \in \mathrm{GL}_{r_i}(\mathbb{F}_q)$ where $\boldsymbol{q}_i \in \mathbb{F}_q^{1\times(r_i-1)}$ and $\boldsymbol{Q}'_i \in \mathrm{GL}_{r_i-1}(\mathbb{F}_q)$ for $i \in \{1..\ell\}$. Let $\boldsymbol{Q} = \mathbf{Diag}(\boldsymbol{Q}_1, \boldsymbol{Q}_2, \ldots, \boldsymbol{Q}_\ell)$. With such matrix $\boldsymbol{Q}$, we have $\boldsymbol{S}\boldsymbol{Q}^{-1} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right]$ and $\boldsymbol{Q}_i\boldsymbol{C}_i = [\boldsymbol{I}_{r_i}\ \boldsymbol{C}'_i]$ where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}'_i \in \mathbb{F}_q^{r_i\times(n_i-r_i)}$. Then

$$\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{Q}^{-1}\boldsymbol{Q}\boldsymbol{C} = \boldsymbol{\alpha}\left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right] \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}'_1] & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}'_2] & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & \cdots & [\boldsymbol{I}_{r_\ell}\ \boldsymbol{C}'_\ell] \end{bmatrix}. \tag{11}$$

The reduced support matrix is $\boldsymbol{S} := \boldsymbol{S}\boldsymbol{Q}^{-1}$ and the reduced coefficient matrix is $\boldsymbol{C} := \boldsymbol{Q}\boldsymbol{C}$.

4 (Improved) OJ Modeling

This section refines the (I)OJ modelings and shows that the IOJ attack rests on optimistic assumptions that do not hold in practical random decoding scenarios. We first derive the OJ modeling from the reduction of decomposition, then refine the IOJ modeling, and finally analyze the assumptions of the IOJ modeling.

4.1 Derivation of (I)OJ Modeling

We start with Theorem 1. Let $\boldsymbol{G}_{\boldsymbol{y}} = [\boldsymbol{I}_{k+1}\ \ \boldsymbol{R}] \in \mathbb{F}_{q^m}^{(k+1)\times n}$ be a systematic generator matrix of $\mathcal{C}_{\boldsymbol{y}}$ where $\boldsymbol{R} \in \mathbb{F}_{q^m}^{(k+1)\times(n-k-1)}$. Let $\overline{\boldsymbol{e}}_1$ and $\overline{\boldsymbol{e}}_2$ be $\boldsymbol{e}$'s first $k+1$ coordinates and last $n-k-1$ coordinates, respectively. Let $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ be $\boldsymbol{C}$'s first $k+1$ columns and last $n-k-1$ columns, respectively. Then

$$\begin{gathered} \boldsymbol{e} = (\overline{\boldsymbol{e}}_1, \overline{\boldsymbol{e}}_2) = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{\alpha}\boldsymbol{S}[\boldsymbol{A}_1, \boldsymbol{A}_2] = (\boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_1, \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_2) \\ \Longrightarrow \\ \overline{\boldsymbol{e}}_1 = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_1, \quad \overline{\boldsymbol{e}}_2 = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_2. \end{gathered} \tag{12}$$

From Equation (3), we have

$$\boldsymbol{u}\boldsymbol{G}_{\boldsymbol{y}} = \boldsymbol{e} \iff (\boldsymbol{u}\ \boldsymbol{u}\boldsymbol{R}) = (\overline{\boldsymbol{e}}_1, \overline{\boldsymbol{e}}_2) \iff \overline{\boldsymbol{e}}_1\boldsymbol{R} = \overline{\boldsymbol{e}}_2. \tag{13}$$

Combining Equations (12) and (13), we have

$$\boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_1\boldsymbol{R} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{A}_2. \tag{14}$$

By Equation (14), for $j \in \{1..n-k-1\}$, let $\boldsymbol{r}_j$ and $\boldsymbol{a}_j$ be the j-th column of $\boldsymbol{R}$ and $\boldsymbol{A}_2$, respectively, then

$$\boldsymbol{\alpha S A}_1 \boldsymbol{r}_j = \boldsymbol{\alpha S a}_j \iff \boldsymbol{\alpha S} \begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{a}_j \end{bmatrix} \begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = 0. \tag{15}$$

Let $\begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = \boldsymbol{T}_j \boldsymbol{\alpha}^\top$ where $\boldsymbol{T}_j \in \mathbb{F}_q^{(k+2)\times m}$ is the matrix expression of $\begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix}$ under the basis $\boldsymbol{\alpha}$. Equation (15) can be written as

$$\boldsymbol{\alpha S} \begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{a}_j \end{bmatrix} \boldsymbol{T}_j \boldsymbol{\alpha}^\top = 0. \tag{16}$$

From Equation (16), we have

$$\boldsymbol{S}[\boldsymbol{A}_1 \ \boldsymbol{a}_j]\boldsymbol{T}_j = \boldsymbol{0}_{m\times m}. \tag{17}$$

4.2 The OJ Modeling

We here refine the OJ modeling. The OJ modeling is built from Equation (15). Let J be a fixed and random subset of $\{1..n-k-1\}$ and $\#J = N$. The OJ modeling is:

$$\left\{ P_j = \boldsymbol{\alpha S} \begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{a}_j \end{bmatrix} \begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} \ : \ j \in J \right\} \tag{18}$$

Unknowns: $mr + (k+1+N)r$ entries of $\boldsymbol{S}$, $\boldsymbol{A}_1$, and $\boldsymbol{a}_j$ over $\mathbb{F}_q$,
Equations: N quadratic multivariate equations $P_j = 0$ over $\mathbb{F}_{q^m}$.

These equations hold over $\mathbb{F}_{q^m}$, but the unknowns are in the basis field $\mathbb{F}_q$. Since $mr + (k+1+N)r \gg N$, the modeling is underdetermined and has many solutions. However, one wants more equations such that the modeling is overdetermined for a unique solution. To obtain more equations, one unfolds the coefficients of P_j over $\mathbb{F}_q$. The resulting modeling includes:
Unknowns: $mr + (k+1+N)r$ entries of $\boldsymbol{S}$, $\boldsymbol{A}_1$, and $\boldsymbol{a}_j$ over $\mathbb{F}_q$,
Equations: mN quadratic multivariate equations over $\mathbb{F}_q$.

Once the OJ modeling is solved, one can obtain the entries of $\boldsymbol{S}$. Then from Equation (4): $\boldsymbol{e}\boldsymbol{H}_{\boldsymbol{y}}^\top = \boldsymbol{\alpha S C}\boldsymbol{H}_{\boldsymbol{y}}^\top = \boldsymbol{0}_{n-k-1}$, one can obtain $\boldsymbol{C}$. Finally, one determines $\boldsymbol{e}$ by computing $\boldsymbol{\alpha S C}$.

The idea of solving the OJ modeling is to transform the quadratic multivariate system into a linear system (with mN equations) by the basis enumeration or the coordinate enumeration. The former guesses the entries of $\boldsymbol{S}$ to solve a linear system in the entries of $[\boldsymbol{A}_1 \ \boldsymbol{a}_j]$ to determine $\boldsymbol{S}$. The latter guesses the entries of $[\boldsymbol{A}_1 \ \boldsymbol{a}_j]$ to solve a linear system in the entries of $\boldsymbol{S}$ to determine $\boldsymbol{S}$. For the coordinate enumeration, to obtain the whole $\boldsymbol{S}$, we must carefully choose $\boldsymbol{a}_j$ to construct a linear system whose unknowns include *all* entries of $\boldsymbol{S}$. The guess

cost dominates the complexity of the OJ attack. A smaller number of entries in $\boldsymbol{S}$ (resp. $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$) leads to a more powerful basis enumeration (resp. coordinate enumeration).

In the next Section 4.3 and Section 4.4, we analyze the structure of P_j for the best basis/coordinate enumeration with three types of errors.

4.3 Basis Enumeration

When $\boldsymbol{S}$ is reduced as the form of Equations (5), (7), and (10), the basis enumeration has the lowest complexity. At this point,

$$\boldsymbol{S} = \left[\begin{array}{c|c} \boldsymbol{I}_r & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{C}' \end{array}\right],$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{(m-r)\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-1)}$. **Note that the forms of $\boldsymbol{S}$ and $\boldsymbol{C}$ are independent of the structure of errors**.

Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By the OJ modeling in Equation (18), for all $j \in J$, we have

$$P_j = \boldsymbol{\alpha}\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\begin{bmatrix}\boldsymbol{r}_j \\ -1\end{bmatrix} = \boldsymbol{\alpha}\left[\begin{array}{c|c} \boldsymbol{I}_r & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right][\boldsymbol{A}_1\ \boldsymbol{a}_j]\begin{bmatrix}\boldsymbol{r}_j \\ -1\end{bmatrix} = 0.$$

For all $j \in J$, we can observe that $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$ includes $(k+N)r$ entries. The modeling gives a quadratic multivariate system with Nm equations and $(m-r)(r-1)+kr+Nr$ variables in entries of $\boldsymbol{S}$, $\boldsymbol{A}_1$, and $\boldsymbol{a}_j$.

By first guessing the entries of $\boldsymbol{S}'$, we can obtain a linear system with Nm equations and $(k+N)r$ unknowns in the entries of $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$ for all $j \in J$. If $(m-r)(r-1)$ entries of $\boldsymbol{S}'$ are correctly guessed and $(k+N)r \leq Nm$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$, and further determine $\boldsymbol{e}$ from Equation (4). Let $N = \left\lceil \frac{kr}{m-r} \right\rceil$. The complexity over $\mathbb{F}_q$ is bounded by $\mathcal{O}\left((mN)^\omega q^{(m-r)(r-1)}\right)$.

Since the derivation is independent of the structure of errors, we can conclude the complexity of the basis enumeration for three types of errors in Theorem 2.

Theorem 2. *For the standard/non-homogeneous/blockwise errors, by the basis enumeration, the OJ attack solves the RD/NHRD/BRD problems with complexity $\mathcal{O}\left((mN)^\omega\, q^{(m-r)(r-1)}\right)$ over $\mathbb{F}_q$ where $N = \left\lceil \frac{kr}{m-r} \right\rceil$ and $N \leq n-k-1$.*

4.4 Coordinate Enumeration

When $\boldsymbol{C}$ is reduced as the form of Equations (6), (8), (9), and (11), the coordinate enumeration has the lowest complexity. At this point,

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{C}' \end{array}\right],$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-1)}$. **Note that the form of $\boldsymbol{C}$ depends on the structure of errors.**

Let $\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \boldsymbol{s}' \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}'' \end{array}\right] \in \mathbb{F}_q^{m\times r}$ where $\boldsymbol{s}' = \boldsymbol{S}_{\{1\},\{2..r\}} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{S}'' = \boldsymbol{S}_{\{2..m\},\{2..r\}} \in \mathbb{F}_q^{(m-1)\times(r-1)}$. Recall that $\boldsymbol{C} = [\boldsymbol{A}_1\ \boldsymbol{A}_2]$ where $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ are $\boldsymbol{C}$'s first $k+1$ columns and last $n-k-1$ columns. Let

$$\boldsymbol{A}_1 = \left[\begin{array}{c|c} 1 & \boldsymbol{a}_1^* \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{A}_1^* \end{array}\right] \in \mathbb{F}_q^{r\times(k+1)}, \qquad \boldsymbol{A}_2 = \left[\begin{array}{c} \boldsymbol{a}_2^* \\ \hline \boldsymbol{A}_2^* \end{array}\right] \in \mathbb{F}_q^{r\times(n-k-1)}$$

where $\boldsymbol{a}_1^* = \boldsymbol{C}_{\{1\},\{2..k+1\}} \in \mathbb{F}_q^{1\times k}$, $\boldsymbol{A}_1^* = \boldsymbol{C}_{\{2..r\},\{2..k+1\}} \in \mathbb{F}_q^{(r-1)\times k}$, $\boldsymbol{a}_2^* = \boldsymbol{C}_{\{1\},\{k+2..n\}} \in \mathbb{F}_q^{1\times(n-k-1)}$, and $\boldsymbol{A}_2^* = \boldsymbol{C}_{\{2..r\},\{k+2..n\}} \in \mathbb{F}_q^{(r-1)\times(n-k-1)}$.

Let $J \subset \{1..n-k-1\}$ and $\#J = N$. We consider all $j \in J$. Recall that $\boldsymbol{r}_j$ and $\boldsymbol{a}_j$ are the j-th column of $\boldsymbol{R}$ and $\boldsymbol{A}_2$, respectively. Let $\boldsymbol{a}_j = \left[\begin{array}{c} \boldsymbol{a}_2^*(j) \\ \hline \boldsymbol{A}_2^*(j) \end{array}\right]$ where $\boldsymbol{a}_2^*(j) \in \mathbb{F}_q$ is the j-th column of $\boldsymbol{a}_2^*$, and $\boldsymbol{A}_2^*(j) \in \mathbb{F}_q^{r-1}$ is the j-th column of $\boldsymbol{A}_2^*$. By the OJ modeling in Equation (18), we have

$$\begin{aligned} P_j &= \boldsymbol{\alpha}\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\begin{bmatrix}\boldsymbol{r}_j \\ -1\end{bmatrix} = \boldsymbol{\alpha}\left[\begin{array}{c|c} 1 & \boldsymbol{s}' \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}'' \end{array}\right]\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* & \boldsymbol{a}_2^*(j) \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{A}_1^* & \boldsymbol{A}_2^*(j) \end{array}\right]\begin{bmatrix}\boldsymbol{r}_j \\ -1\end{bmatrix} \\ &= \boldsymbol{\alpha}\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right]\begin{bmatrix}\boldsymbol{r}_j \\ -1\end{bmatrix} = 0. \end{aligned} \tag{19}$$

The OJ modeling gives a quadratic multivariate system with mN quadratic polynomials whose variables are the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations whose unknowns are the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and unknowns $\leq mN$, the system can be solved uniquely to obtain the entries of $\boldsymbol{S}$. The complexity is determined by the cost of solving the linear system and guessing $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$.

Here we do not conclude the complexity of the coordinate enumeration for three types of errors since the complexity depends on the structure of errors. We independently analyze them in subsequent Sections 5, 6, and 7 for the standard/non-homogeneous/blockwise errors, respectively.

4.5 The IOJ Modeling

The IOJ modeling is built from Equation (17):

$$\Big\{\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j = \boldsymbol{0}_{m\times m}\ :\ \forall\ j \in \{1..n-k-1\}\Big\}. \tag{20}$$

Unknowns: $mr + (k+2)r$ entries of $\boldsymbol{S}$, $\boldsymbol{A}_1$, and $\boldsymbol{a}_j$ over $\mathbb{F}_q$,
Equations: m^2 quadratic multivariate equations over $\mathbb{F}_q$, i.e., m^2 entries of $\boldsymbol{S}(\boldsymbol{A}_1\ \boldsymbol{a}_j)\boldsymbol{T}_j$.

As the OJ modeling, the IOJ modeling is to transform the quadratic multivariate system into a linear system (with m^2 equations) by the basis or coordinate enumeration. The former guesses the entries of $\boldsymbol{S}$ to solve the linear system in the entries of $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$. The latter guesses the entries of $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$ to solve the linear system in the entries of $\boldsymbol{S}$. A smaller number of entries in $\boldsymbol{S}$ (resp. $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$) leads to a more powerful basis enumeration (resp. coordinate enumeration).

4.6 Soundness of the IOJ Attack

The IOJ attack relies on Equation (17). We show, however, that the event that this equation holds is negligible in practice, and when it does hold it forces the error $\boldsymbol{e}$ to be zero.

Theoretical negligibility. By the derivations in Section 4.1, we observe that $\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j \in \mathbb{F}_q^{m\times m}$ and $\boldsymbol{\alpha}\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j\boldsymbol{\alpha}^\top \in \mathbb{F}_{q^m}$. Although the coordinates of $\boldsymbol{\alpha}$ are linearly independent over $\mathbb{F}_q$, they are linearly dependent over $\mathbb{F}_{q^m}$. Hence, for random $\boldsymbol{S}$, $\boldsymbol{A}_1$, $\boldsymbol{a}_j$, and $\boldsymbol{T}_j$, the implication

$$\boldsymbol{\alpha}\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j\boldsymbol{\alpha}^\top = 0 \implies \boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j = \boldsymbol{0}_{m\times m}$$

is extremely unlikely.

More precisely, consider the linear system $\boldsymbol{\alpha}\boldsymbol{x}^\top = 0$ over $\mathbb{F}_{q^m}$ with unknown $\boldsymbol{x}$. The solution space has size roughly $q^{m(m-1)}$, and the number of non-zero solutions is $q^{m(m-1)} - 1$. Let $\boldsymbol{x}^\top = \boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j\boldsymbol{\alpha}^\top$. Then, the probability that $\boldsymbol{\alpha}\boldsymbol{x}^\top = 0$ leads to $\boldsymbol{x}^\top = \boldsymbol{0}$ is about $1/q^{m(m-1)}$, which is negligible. Our experiments confirm this negligibility; the scripts are available at https://github.com/RBC-PQC/OJ-Attack.

Zero-error implication. Even if Equation (17) holds, it forces the error to be zero. Since $\boldsymbol{R}$ is random, the matrix $\begin{bmatrix}\boldsymbol{r}_j\\ -1\end{bmatrix}$ is close to random, and hence $\boldsymbol{T}_j \in \mathbb{F}_q^{(k+2)\times m}$ is also close to random one. Because most current parameters satisfy $k+2 \le m$, $\boldsymbol{T}_j$ is row full-rank with overwhelming probability. Then

$$\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j = \boldsymbol{0}_{m\times m} \implies \boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j] = \boldsymbol{0}_{m\times(k+2)} \qquad \forall\, j \in \{1,\ldots,n-k-1\}.$$

Consequently,

$$\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{A}_2] = \boldsymbol{0}_{m\times n} \iff \boldsymbol{S}\boldsymbol{C} = \boldsymbol{0}_{m\times n} \iff \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C} = \boldsymbol{e} = \boldsymbol{0}_n.$$

These two arguments demonstrate that the IOJ attack proposed in [27,28] can be safely ignored in realistic random decoding scenarios. In Sections 5.3 and 7.2 we further show, by direct comparison, that the complexity estimates derived from the IOJ modeling are overly optimistic.

5 The OJ Attack on the RD Problem

The original complexity formulas [24] of the OJ attack are restricted by special parameter regions, and we here apply the OJ modeling refined in Section 4.2 to the RD problem and obtain general and tight formulas for *general parameters*.

5.1 Complexity of the OJ Attack on the RD Problem

In Section 4.3, we have obtained the complexity of the basis enumeration since the basis enumeration is independent of the structure of errors (see Theorem 2). However, the coordinate enumeration strictly depends on the structure of errors, thus we here derive the complexity of the coordinate enumeration.

Theorem 3. *With $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (6), by the coordinate enumeration, the OJ attack solves the RD problem with complexity over $\mathbb{F}_q$*

$$\mathcal{O}\left((mN)^{\omega} q^{(r-1)(N+k+1-r)}\right)$$

where $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$ and $N \leq n-k-1$.

Proof. From Equation (6), $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \left[\boldsymbol{I}_r \ \boldsymbol{C}'\right],$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-r)}$. Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By Equation (19), for all $j \in J$,

$$P_j = \boldsymbol{\alpha}\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right]\begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = 0.$$

Case 1: $0 < k+1 \leq r$
Let $\{k+2..r\} - (k+1) \subset J$. At this point, $\boldsymbol{a}_1^*$ and $\boldsymbol{A}_1^*$ are constant matrices. We can observe that $\boldsymbol{a}_2^*(j)$ has $N-r+k+1$ unknown entries; $\boldsymbol{A}_2^*(j)$ has $(r-1)(N-r+k+1)$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(N-r+k+1)r$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the unknown entries of $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(N-r+k+1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(N-r+k+1) \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(r-1)(N+k+1-r)}\right)$.

Case 2: $r < k+1 \leq n$.
We can observe that $\boldsymbol{a}_1^*$ and $\boldsymbol{a}_2^*(j)$ have $N+k+1-r$ unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r-1)(N+k+1-r)$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(N+k+1-r)r$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, one can obtain a linear system with mN equations and $m(r-1)+(N+k+1-r)$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(N+k+1-r) \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(r-1)(N+k+1-r)}\right)$. □

5.2 Generality of Our Complexity

Compared to the complexity in [24], our complexity is universal. Recall that in [24], the basis enumeration is estimated as $\mathcal{O}\left((nr+m)^{\omega}q^{(r-1)(m-r)}\right)$ and the coordinate enumeration is estimated as $\mathcal{O}\left((mr)^{\omega}q^{(r-1)(k+1)}\right)$. For the basis enumeration, the complexity keeps the same exponent parts as Theorem 2, and the difference of the polynomial parts is limited for any code parameters.

However, the case is different for the coordinate enumeration. By our complexity in Theorem 3:

- When $0 < k \leq m-1$, we have $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil = \left\lceil \frac{(m-1)(r-1)+k}{m-1} \right\rceil = r$ and the complexity is $\mathcal{O}\left((mr)^{\omega}q^{(r-1)(k+1)}\right)$. This is consistent with the complexity obtained in the work [24].
- When $\beta \geq 1$ and $\beta(m-1) < k \leq (\beta+1)(m-1)$, we have $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil = \left\lceil \frac{(m-1)(r-1)+k}{m-1} \right\rceil = r+\beta$ and the complexity is $\mathcal{O}\left((m(r+\beta))^{\omega}q^{(r-1)(k+\beta+1)}\right)$.

Therefore, our coordinate enumeration is general for any code parameters. The coordinate enumeration in the work [24] is underestimated for sufficiently large dimension k.

5.3 Comparison with the IOJ Attack

The complexity of the IOJ attack on the RD problem is derived in Appendix A. Theorem 9 gives the complexity of basis enumeration, which retains the same exponent as the OJ basis enumeration in Theorem 2. Theorem 10 gives the complexity of coordinate enumeration. We show there that the IOJ attack runs in polynomial time when $0 < k+1 \leq r$; when $r < k+1 \leq n$, the exponent term is $q^{(r-1)(k+2-r)}$. Compared with the OJ complexity in Theorem 3, this yields a gain of about $(r-1)^2$ bits. While this gain would allow the IOJ attack to break the parameter sets of RYDE [9,10,11], the underlying assumptions are overly optimistic, and thus the attack does not represent a realistic threat.

5.4 Security of Cryptosystems Based on the RD Problem

In this section, we estimate the security strength of cryptosystems based on the RD problem by the AGHT and OJ attacks. We consider three typical rank-based cryptosystems: Multi-UR-AG [8], LowMS [2], and RYDE [9,10,11]. We observe that the OJ attack has chance to become more powerful than the AGHT attack.

Illustrations: To be precise, Multi-UR-AG and LowMS are based on the Rank Support Learning (RSL) problem consisting of N distinct RSD instances whose errors share a support. As analyzed in [8], the RSL problem is considered to be as almost hard as the RSD problem for a small N. Thus, we use the complexity of the NHRSD problem to describe that of the NHRSL problem. "λ" represents the claimed security level. "AGHT" and "OJ" represent the complexity using the AGHT and OJ attacks, respectively. The bold complexity is the best one.

Table 1. Multi-UR-AG (IEEE TIT 2024 [8])

q	m	n'	n	n_1	n_2	k	ε	w	w_1	total (KB)	Attack-w (AGHT, OJ)	Attack-w_1 (AGHT, OJ)	λ
2	97	96	24	14	15	3	83	8	11	11.0	$(2^{225}, 2^{\mathbf{201}})$	$(2^{227}, 2^{\mathbf{201}})$	128
2	127	126	35	15	16	3	93	9	12	21.1	$(2^{352}, 2^{\mathbf{316}})$	$(2^{353}, 2^{\mathbf{316}})$	192

"Attack-w" represents attacking the $\mathsf{RD}_{q,m,2n,n,w}$ problem. "Attack-w_1" represents attacking the $\mathsf{RD}_{q,m,2n+n_1,n,w_1}$ problem. For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant) ω is set as 2.81.

Table 2. LowMS (DCC 2024 [2])

q	m	n	k	r	ℓ	DFR	total (KB)	AGHT	OJ	λ
2	61	50	25	7	6	2^{-242}	5.91	2^{192}	$2^{\mathbf{180}}$	128
2	101	74	37	8	2	2^{-301}	18.21	2^{331}	$2^{\mathbf{293}}$	192
2	101	88	44	9	5	2^{-503}	27.22	2^{400}	$2^{\mathbf{387}}$	256

Attacking the $\mathsf{RD}_{q,m,n,k,r}$ problem. For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant) ω is set as 2.81.

Table 3. RYDE (Version 2.0.0, NIST PQC 2023 [9] and DCC 2025 [10])

q	m	n	k	r	AGHT	OJ	λ
2	31	33	15	10	$2^{\mathbf{147}}$	2^{160}	128
2	37	41	18	13	$2^{\mathbf{216}}$	2^{245}	192
2	43	47	18	17	$2^{\mathbf{283}}$	2^{323}	256

Attacking the $\mathsf{RD}_{q,m,n,k,r}$ problem. For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant ω) is conservatively set as 2.

Table 4. RYDE (Version 2.1.0, NIST PQC 2025 [11])

q	m	n	k	r	AGHT	OJ	λ
2	53	53	45	4	$2^{\mathbf{148}}$	2^{153}	128
2	61	61	51	5	$2^{\mathbf{217}}$	2^{224}	192
2	61	57	44	7	2^{301}	$2^{\mathbf{287}}$	256

Attacking the $\mathsf{RD}_{q,m,n,k,r}$ problem. For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant ω) is conservatively set as 2.

6 The OJ Attack on the NHRD Problem

In this section, we apply the OJ modeling refined in Section 4.2 to the NHRD problem and show that the OJ attack has a significantly lower complexity than the adapted AGHT attack proposed in [8].

6.1 Complexity of the OJ Attack on the NHRD Problem

In Section 4.3, we have obtained the complexity of the basis enumeration since the basis enumeration is independent of the structure of errors (see Theorem 2).

However, the coordinate enumeration strictly depends on the structure of errors. For the non-homogeneous error, the OJ attack could benefit from the coefficient matrix in the form of Equation (8) or Equation (9). With these two coefficient matrices, the complexity is respectively analyzed in Theorem 4 and Theorem 5.

Theorem 4. *With $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (8), by the coordinate enumeration, the OJ attack solves the NHRD problem with complexity over $\mathbb{F}_q$:*

$$\begin{cases} \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N+k+1-r_1)}\right), & 0 < k+1 \le n_1+r_2; \\ \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N+k+1-r_1)+r_2(k+1-r_2)}\right), & n_1+r_2 < k+1 \le n_1+n_2; \\ \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N+k+1-r_1)+r_2(n_2-r_2)}\right), & n_1+n_2 < k+1 \le n_1+n_2+n_3, \end{cases}$$

where $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$.

Proof. From Equation (8), $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}_1'] & \boldsymbol{C}_2' & \boldsymbol{C}_3' \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}_4'] & \boldsymbol{0} \end{bmatrix},$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$, $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1\times(n_1-r_1)}$, $\boldsymbol{C}_2' \in \mathbb{F}_q^{r_1\times n_2}$, $\boldsymbol{C}_3' \in \mathbb{F}_q^{r_1\times n_3}$, and $\boldsymbol{C}_4' \in \mathbb{F}_q^{r_2\times(n_2-r_2)}$. Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By Equation (19), for all $j \in J$,

$$P_j = \boldsymbol{\alpha}\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right]\begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = 0.$$

We consider five cases.
Case 1: $0 < k+1 \le r_1$.
Let $(\{k+2..r_1\} \cup \{n_1+1..n_1+r_2\}) - (k+1) \subset J$ and $\{n_1+r_2..n_2\} - (k+1) \nsubseteq J$. At this point, $\boldsymbol{a}_1^*$ and $\boldsymbol{A}_1^*$ are constant matrices. We can observe that $\boldsymbol{a}_2^*(j)$ has $N - r_1 + k + 1$ unknown entries; $\boldsymbol{A}_2^*(j)$ has $(r_1-1)(N-r_1+k+1)$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r_1(N-r_1+k+1)$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+N-r_1+k+1$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r_1)+N \le mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N+k+1-r_1)}\right)$.

Case 2: $r_1 < k+1 \le n_1$.
Let $\{n_1+1..n_1+r_2\} - (k+1) \subset J$ and $\{n_1+r_2..n_2\} - (k+1) \nsubseteq J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r_1-1)(k+1-r_1)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and

$m(r-1)+r_1(k+1-r_1)+r_1N$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r_1)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r_1)+N \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(N+k+1-r_1)}\right)$.

Case 3: $n_1 < k+1 \leq n_1+r_2$.
Let $\{k+2..n_1+r_2\}-(k+1) \subset J$ and $\{n_1+r_2..n_2\}-(k+1) \nsubseteq J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r_1-1)(k+1-r_1)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r_1(k+1-r_1)+r_1N$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r_1)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r_1)+N \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(N+k+1-r_1)}\right)$.

Case 4: $n_1+r_2 < k+1 \leq n_1+n_2$.
Let $\{k+2..n_1+n_2\}-(k+1) \nsubseteq J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r_1-1)(k+1-r_1)+r_2(k+1-r_2)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r_1(k+1-r_1)+r_2(k+1-r_2)+r_1N$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r_1)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r_1)+N \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(N+k+1-r_1)+r_2(k+1-r_2)}\right)$.

Case 5: $n_1+n_2 < k+1 \leq n_1+n_2+n_3$.
We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r_1-1)(k+1-r_1)+r_2(n_2-r_2)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r_1(k+1-r_1)+r_2(n_2-r_2)+r_1N$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r_1)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r_1)+N \leq mN$, then the sys-

tem could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r_1}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N+k+1-r_1)+r_2(n_2-r_2)}\right)$.

Cases 1-3 can be merged into one case for $0 < k+1 \leq n_1 + r_2$, we finally obtain the conclusion. □

Theorem 5. *With $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (9), by the coordinate enumeration, the OJ attack solves the NHRD problem with complexity over $\mathbb{F}_q$:*

$$\begin{cases} \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N-r+k+1)}\right), & 0 < k+1 \leq r; \\ \mathcal{O}\left((mN)^{\omega} q^{(r-1)(k+1-r)+(r_1-1)N}\right), & r < k+1 \leq n_2; \\ \mathcal{O}\left((mN)^{\omega} q^{(r-1)(n_2-r)+(r_1-1)(N+k+1-n_2)}\right), & n_2 < k+1 \leq n_1+n_2+n_3, \end{cases}$$

where $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$.

Proof. From Equation (9), $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S'} \end{array}\right], \qquad \boldsymbol{C} = \left[\begin{array}{cc|cc} \boldsymbol{I}_r & \boldsymbol{C}'_2 & \boldsymbol{C}'_1 & \boldsymbol{C}'_3 \\ \hline & & \boldsymbol{0} & \boldsymbol{0} \end{array}\right],$$

where $\boldsymbol{S'} \in \mathbb{F}_q^{m\times(r-1)}$, $\boldsymbol{C}'_2 \in \mathbb{F}_q^{r\times(n_2-r)}$, $\boldsymbol{C}'_1 \in \mathbb{F}_q^{r_1\times n_1}$, and $\boldsymbol{C}'_3 \in \mathbb{F}_q^{r_1\times n_3}$. Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By Equation (19), for all $j \in J$,

$$P_j = \boldsymbol{\alpha}\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s'}\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s'}\boldsymbol{A}_2^*(j) \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S''}\boldsymbol{A}_1^* & \boldsymbol{S''}\boldsymbol{A}_2^*(j) \end{array}\right]\left[\begin{array}{c} \boldsymbol{r}_j \\ -1 \end{array}\right] = 0.$$

We consider three cases.
Case 1: $0 < k+1 \leq r$.
Let $\{k+2..r\} - (k+1) \subset J$ and $\{r+1..n_2\} - (k+1) \nsubseteq J$. At this point, $\boldsymbol{a}_1^*$ and $\boldsymbol{A}_1^*$ are constant matrices. We can observe that $\boldsymbol{a}_2^*(j)$ has $N-r+k+1$ unknown entries; $\boldsymbol{A}_2^*(j)$ has $(r_1-1)(N-r+k+1)$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and *at most* $m(r-1)+r_1(N-r+k+1)$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+N-r+k+1$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+N-r+k+1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(N-r+k+1)}\right)$.

Case 2: $r < k+1 \leq n_2$.
Let $\{k+2..n_2\}-(k+1) \nsubseteq J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r-1)(k+1-r)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r(k+1-r)+r_1N$ variables in the entries

of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r)+N \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r-1)(k+1-r)+(r_1-1)N}\right)$.

Case 3: $n_2 < k+1 \leq n_1+n_2+n_3$.
We can observe that $\boldsymbol{a}_1^*$ has $k+1-r$ unknown entries; $\boldsymbol{a}_2^*(j)$ has N unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r-1)(k+1-r)+(r_1-1)(k+1-n_2)+(r_1-1)N$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+r(k+1-r)+(r_1-1)(k+1-n_2)+r_1N$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(k+1-r)+N$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(k+1-r)+N \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+k+1-r}{m-1} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r-1)(n_2-r)+(r_1-1)(N+k+1-n_2)}\right)$. □

6.2 Security of Cryptosystems Based on the NHRD Problem

In this section, we estimate the security strength of cryptosystems based on the NHRD problem by combinatorial attacks: the OJ and AGHT attacks. We consider two typical cryptosystems: NH-Multi-RQC-AG and NH-Multi-UR-AG [8].

- For NH-Multi-RQC-AG, the OJ attack in Theorem 4 is more powerful than one in Theorem 5. This shows that the OJ attack benefits from the original NHRD instance whose coefficients matrix is in the form of Equation (8). However, for NH-Multi-UR-AG, the case is the opposite. The OJ attack benefits from the permuted NHRD instance whose coefficient matrix is in the form of Equation (9).
- For NH-Multi-RQC-AG, the OJ attack is less powerful than the adapted AGHT attack [8]. However, for NH-Multi-UR-AG, the case is different. The OJ attack is much more powerful than the adapted AGHT attack and the complexity gain is up to 100 bits. This is because the exponent of the OJ attack is independent of m and benefits from a small dimension k, whereas the adapted AGHT attack benefits from a small dimension m and k.

Illustrations: To be precise, NH-Multi-RQC-AG and NH-Multi-UR-AG are based on the Non-Homogeneous Rank Support Learning (NHRSL) problem consisting of N distinct NHRSD instances whose errors share the same support. We here estimate the complexity of the NHRSD (equivalently, NHRD) problem. As analyzed in [8], the NHRSL problem is considered to be almost as hard as the NHRSD problem for a small N. Thus, we use the complexity of the NHRSD

problem to describe that of the NHRSL problem. The complexity of the adapted AGHT (AGHT-NHRD) attack follows the conclusion in [8] (Section 5). The complexity of th OJ attack is estimated by Theorems 4 and 5, respectively. Following work [8], for all complexity estimations, we set the matrix multiplication exponent (or linear algebra constant) ω as 2.81 for a fair comparison. "λ" represents the claimed security level. "AGHT" and "OJ" represent the complexity using the adapted AGHT (AGHT-NHRD) and OJ attacks, respectively. The bold complexity is the best one.

Table 5. NH-Multi-RQC-AG [8] based on the NHRSD problem

q	m	n'	n_1	n_2	k	ε	w	w_1	w_2	DFR	total (KB)	AGHT	OJ (Theorem 4)	OJ (Theorem 5)	λ
2	61	60	3	50	3	51	7	7	5	2^{-158}	2.7	$2^{\mathbf{193}}$	2^{363}	2^{523}	128
2	79	78	2	95	5	65	8	8	5	2^{-238}	4.7	$2^{\mathbf{277}}$	2^{743}	2^{1118}	192

The AGHT-NHRD and OJ attacks against the $\mathsf{NHRSD}^{(n_2,n_2,n_2),(w_1,w_2)}_{q,m,3n_2,n_2}$ problem.

Table 6. NH-Multi-UR-AG [8] based on the NHRSD problem

q	m	n'	n	n_1	n_2	k	ε	w	w_1	w_2	DFR	total (KB)	AGHT	OJ (Theorem 4)	OJ (Theorem 5)	λ
2	73	72	22	13	14	2	66	8	8	4	2^{-133}	7.1	2^{264}	2^{217}	$2^{\mathbf{193}}$	128
2	97	96	30	14	14	3	77	9	9	4	2^{-214}	12.6	2^{389}	2^{309}	$2^{\mathbf{281}}$	192

The AGHT-NHRD and OJ attacks against the $\mathsf{NHRSD}^{(n,n_1,n),(w_1,w_2)}_{q,m,2n+n_1,n}$ problem.

7 The OJ Attack on the BRD Problem

In this section, we apply the OJ modeling refined in Section 4.2 to the BRD problem and derive general and tight complexity for general blocks.

7.1 Complexity of the OJ Attack on the BRD Problem

In Section 4.3, we have obtained the complexity of the basis enumeration since it is independent of the structure of errors (see Theorem 2). The coordinate enumeration strictly depends on the structure of errors. For the blockwise errors, when $\boldsymbol{S}$ and $\boldsymbol{C}$ are in the form of Equation (11), the coordinate enumeration has the lowest complexity. The complexity is very various because we must choose an appropriate J such that the unknowns of the linear system include all entries of $\boldsymbol{S}$ and the complexity is the lowest. Moreover, for general ℓ, it is also tricky to find a universal way to present complexity. In Theorem 6, we consider the

case of $\ell = 2$. In Theorem 7, we consider the case of $\ell = 3$. Then we derive the general conclusion for any ℓ by induction in Theorem 8.

Theorem 6. *When $\ell = 2$, with $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (11), by the coordinate enumeration, the OJ attack solves the BRD problem with complexity over $\mathbb{F}_q$*

$$\begin{cases} \mathcal{O}\left((mN)^{\omega} q^{(N-r_1-r_2+k+1)\gamma}\right), & 0 < k+1 \le r_1; \\ \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(k+1-r_1)+(N-r_2)\gamma}\right), & r_1 < k+1 \le n_1; \\ \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(n_1-r_1)+(N-n_1-r_2+k+1)\gamma}\right), & n_1 < k+1 \le n_1+r_2; \\ \mathcal{O}\left((mN)^{\omega} q^{(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+N\gamma}\right), & n_1+r_2 < k+1 \le n_1+n_2, \end{cases}$$

where $\gamma = \min\left\{r_i : i \in \{1,2\}\right\}$ *and* $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$.

Proof. From Equation (11), when $\ell = 2$, $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}_1'] & \boldsymbol{0} \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}_2'] \end{bmatrix}$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}_i' \in \mathbb{F}_q^{r_i\times(n_i-r_i)}$ for $i \in \{1,2\}$. Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By Equation (19), for all $j \in J$,

$$P_j = \boldsymbol{\alpha} \left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right] \begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = 0.$$

We consider four cases.
Case 1: $0 < k+1 \le r_1$.
Let $(\{k+2..r_1\} \cup \{n_1+1..n_1+r_2\}) - (k+1) \subset J$. At this point, $\boldsymbol{a}_1^*$ and $\boldsymbol{A}_1^*$ are constant matrices. We can observe that the $\boldsymbol{a}_2^*(j)$ has *at most* $n_1 - r_1$ unknown entries; $\boldsymbol{A}_2^*(j)$ has *at leat* $(N - r_1 - r_2 + k + 1)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1) + n_1 - r_1 + (N - r_1 - r_2 + k + 1)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1) + n_1 - r_1$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1) + n_1 - r_1 \le Nm$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^{\omega} q^{(N-r_1-r_2+k+1)\gamma}\right)$.

Case 2: $r_1 < k+1 \le n_1$.
Let $\{n_1+1..n_1+r_2\} - (k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has *at most* $n_1 - (k+1)$ unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at leat* $(r_1-1)(k+1-r_1) + (N-r_2)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1) + (k+1-r_1)r_1 + n_1 - (k+1) + (N-r_2)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can

obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(n_1-r_1) \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(k+1-r_1)+(N-r_2)\gamma}\right)$.

Case 3: $n_1 < k+1 \leq n_1+r_2$.
Let $\{k+2..n_1+r_2\}-(k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \boldsymbol{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at leat* $(r_1-1)(n_1-r_1)+(N-n_1-r_2+k+1)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(n_1-r_1)r_1+(N-n_1-r_2+k+1)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(N-n_1-r_2+k+1)\gamma}\right)$.

Case 4: $n_1+r_2 < k+1 \leq n_1+n_2$.
We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \boldsymbol{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at leat* $(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+N\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(n_1-r_1)r_1+(k+1-n_1-r_2)r_2+N\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+N\gamma}\right)$. □

Theorem 7. *When $\ell = 3$, with $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (11), by the coordinate enumeration, the OJ attack solves the BRD problem with complexity over $\mathbb{F}_q$*

$$\begin{cases} \mathcal{O}\left((mN)^\omega q^{(N-r_1-r_2-r_3+k+1)\gamma}\right), & 0 < k+1 \leq r_1; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(k+1-r_1)+(N-r_2-r_3)\gamma}\right), & r_1 < k+1 \leq n_1; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(N-n_1-r_2-r_3+k+1)\gamma}\right), & n_1 < k+1 \leq n_1+r_2; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+(N-r_3)\gamma}\right), & n_1+r_2 < k+1 \leq n_1+n_2; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(N-n_1-n_2-r_3+k+1)\gamma}\right), & n_1+n_2 < k+1 \leq n_1+n_2+r_3; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(k+1-n_1-n_2-r_3)r_3+N\gamma}\right), & n_1+n_2+r_3 < k+1 \leq n_1+n_2+n_3, \end{cases}$$

where $\gamma = \min\left\{r_i : i \in \{1..3\}\right\}$ *and* $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$.

Proof (Theorem 7). From Equation (11), when $\ell = 3$, $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \mathbf{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}'_1] & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}'_2] & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & [\boldsymbol{I}_{r_3}\ \boldsymbol{C}'_3] \end{bmatrix},$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}'_i \in \mathbb{F}_q^{r_i\times(n_i-r_i)}$ for $i \in \{1..3\}$. Let $J \subset \{1..n-k-1\}$ and $\#J = N$. By Equation (19), for all $j \in J$,

$$P_j = \boldsymbol{\alpha}\left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \hline \mathbf{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right]\begin{bmatrix} \boldsymbol{r}_j \\ -1 \end{bmatrix} = 0.$$

We consider six cases.

Case 1: $0 < k+1 \le r_1$.
Let $(\{k+2..r_1\} \cup \{n_1+1..n_1+r_2\} \cup \{n_1+n_2+1..n_1+n_2+r_3\})-(k+1) \subset J$. At this point, $\boldsymbol{a}_1^*$ and $\boldsymbol{A}_1^*$ are constant matrices. We can observe that $\boldsymbol{a}_2^*(j)$ has *at most* n_1-r_1 unknown entries; $\boldsymbol{A}_2^*(j)$ has *at least* $(N-r_1-r_2-r_3+k+1)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+n_1-r_1+(N-r_1-r_2-r_3+k+1)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+n_1-r_1$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \le mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+(n_1-r_1)}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(N-r_1-r_2-r_3+k+1)\gamma}\right)$.

Case 2: $r_1 < k+1 \le n_1$.
Let $(\{n_1+1..n_1+r_2\} \cup \{n_1+n_2+1..n_1+n_2+r_3\}) - (k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has $k+1-r_1$ unknown entries; $\boldsymbol{a}_2^*(j)$ has *at most* $n_1-(k+1)$ unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at least* $(r_1-1)(k+1-r_1)+(N-r_2-r_3)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(k+1-r_1)r_1+n_1-(k+1)+(N-r_2-r_3)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+(n_1-r_1) \le mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(k+1-r_1)+(N-r_2-r_3)\gamma}\right)$.

Case 3: $n_1 < k+1 \le n_1+r_2$.
Let $(\{k+2..n_1+r_2\} \cup \{n_1+n_2+1..n_1+n_2+r_3\}) - (k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \mathbf{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at least* $(r_1-1)(n_1-r_1)+(N-n_1-r_2-r_3+k+1)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and *at most*

$m(r-1)+(n_1-r_1)r_1+(N-n_1-r_2-r_3+k+1)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(N-n_1-r_2-r_3+k+1)\gamma}\right)$.

Case 4: $n_1+r_2 < k+1 \leq n_1+n_2$.
Let $\{n_1+n_2+1..n_1+n_2+r_3\}-(k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \boldsymbol{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at least* $(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+(N-r_3)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(n_1-r_1)r_1+(k+1-n_1-r_2)r_2+(N-r_3)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(k+1-n_1-r_2)r_2+(N-r_3)\gamma}\right)$.

Case 5: $n_1+n_2 < k+1 \leq n_1+n_2+r_3$.
Let $\{k+2..n_1+n_2+r_3\}-(k+1) \subset J$. We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \boldsymbol{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at least* $(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(N-n_1-n_2-r_3+k+1)\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(n_1-r_1)r_1+(n_2-r_2)r_2+(N-n_1-n_2-r_3+k+1)\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(N-n_1-n_2-r_3+k+1)\gamma}\right)$.

Case 6: $n_1+n_2+r_3 < k+1 \leq n_1+n_2+n_3$.
We can observe that $\boldsymbol{a}_1^*$ has n_1-r_1 unknown entries; $\boldsymbol{a}_2^* = \boldsymbol{0}$; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have *at least* $(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(k+1-n_1-n_2-r_3)r_3+N\gamma$ unknown entries. The OJ modeling gives a quadratic multivariate system with mN polynomials and $m(r-1)+(n_1-r_1)r_1+(n_2-r_2)r_2+(k+1-n_1-n_2-r_3)r_3+N\gamma$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations and $m(r-1)+(n_1-r_1)$ unknowns in the entries of $\boldsymbol{S}$ and $\boldsymbol{a}_1^*$. If the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and $m(r-1)+n_1-r_1 \leq mN$, then the system could be solved uniquely

and we would obtain $\boldsymbol{S}$. Let $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. The complexity is estimated as $\mathcal{O}\left((mN)^\omega q^{(r_1-1)(n_1-r_1)+(n_2-r_2)r_2+(k+1-n_1-n_2-r_3)r_3+N\gamma}\right)$. □

Theorem 8. *For general ℓ, with $\boldsymbol{S}$ and $\boldsymbol{C}$ in Equation (11), by the coordinate enumeration, the BRD problem can be solved with complexity over $\mathbb{F}_q$*

$$\begin{cases} \mathcal{O}\left((mN)^\omega q^{(N-\sum_{i=1}^{\ell} r_i+k+1)\gamma}\right), & 0 < k+1 \le r_1; \\ \mathcal{O}\left((mN)^\omega q^{(r_1-1)(k+1-r_1)+(N-\sum_{i=2}^{\ell} r_i)\gamma}\right), & r_1 < k+1 \le n_1; \\ \mathcal{O}\left((mN)^\omega q^{\sum_{i=1}^{j} r_i(n_i-r_i)-(n_1-r_1)+(N-\sum_{i=1}^{j} n_i-\sum_{i=j+1}^{\ell} r_i+k+1)\gamma}\right), & \sum_{i=1}^{j} n_i < k+1 \le \sum_{i=1}^{j} n_i + r_{j+1}; \\ \mathcal{O}\left((mN)^\omega q^{\sum_{i=1}^{j} r_i(n_i-r_i)-(n_1-r_1)+\left(k+1-\sum_{i=1}^{j} n_i-r_{j+1}\right)r_{j+1}+(N-\sum_{i=j+2}^{\ell} r_i)\gamma}\right), & \sum_{i=1}^{j} n_i + r_{j+1} < k+1 \le \sum_{i=1}^{j+1} n_i, \end{cases}$$

where $\gamma = \min\left\{r_i : i \in \{1..\ell\}\right\}$, $j \in \{1..\ell-1\}$, and $N = \left\lceil \frac{m(r-1)+n_1-r_1}{m} \right\rceil$. We denote $\sum_{i=j+2}^{\ell} r_i = 0$ if $j+2 > \ell$.

Proof. From Equation (11), for general ℓ, $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\frac{1}{\boldsymbol{0}_{(m-r)\times 1}} \middle| \boldsymbol{S}'\right], \qquad \boldsymbol{C} = \begin{bmatrix} [\boldsymbol{I}_{r_1}\ \boldsymbol{C}'_1] & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{0} & [\boldsymbol{I}_{r_2}\ \boldsymbol{C}'_2] & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{0} & \boldsymbol{0} & & [\boldsymbol{I}_{r_\ell}\ \boldsymbol{C}'_\ell] \end{bmatrix},$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}'_i \in \mathbb{F}_q^{r_i\times(n_i-r_i)}$ for $i \in \{1..\ell\}$.

We can generalize the proof of Theorem 7 and can obtain the conclusion. This can be done naturally by induction. □

Remark 1. For the complexity, we additionally give the following explanations:

- For general parameters, our complexity is slightly optimistic because we set $\gamma = \min\left\{r_i : i \in \{1..\ell\}\right\}$. Our complexity is precise for $n_1 = n_2 = \cdots = n_\ell$ and $r_1 = r_2 = \cdots = r_\ell$, which is the case of most cryptographic parameters.
- The complexity is independent of the order of $\boldsymbol{e}_1, \boldsymbol{e}_2, ..., \boldsymbol{e}_\ell$. Given an instance $(\boldsymbol{G}, \boldsymbol{y}, \boldsymbol{e})$ of the $\mathsf{BRD}^{\ell,\boldsymbol{n},\boldsymbol{r}}_{q,m,n,k,r}$ problem, one can apply a permutation matrix $\boldsymbol{P}$ to the instance and obtain the instance $(\boldsymbol{GP}, \boldsymbol{yP}, \boldsymbol{eP})$. Because $\boldsymbol{eP}$ keeps the support of $\boldsymbol{e}$, solving $(\boldsymbol{G}, \boldsymbol{y}, \boldsymbol{e})$ amounts to solving $(\boldsymbol{GP}, \boldsymbol{yP}, \boldsymbol{eP})$.
- The complexity increases as k becomes larger. The attack cost is mainly determined by the number of unknown entries included in $\boldsymbol{A}_1$. As k becomes larger, $\boldsymbol{A}_1$ will include more unknown entries of the coefficients matrix $\boldsymbol{C}$, which means that we must guess more unknown entries to solve the OJ modeling by the coordinate enumeration.
- If $n_1 = n_2 = \cdots = n_\ell$, we should sort r_i's for $i \in [\ell]$ such that $r_1 \le r_2 \le \cdots \le r_\ell$ to obtain the minimal complexity. The attack cost is mainly determined by the number of unknown entries included in $\boldsymbol{A}_1$. When $r_1 \le r_2 \le \cdots \le r_\ell$, $\boldsymbol{A}_1$ has a chance to include fewer unknown entries.

– If both n_i's and r_i's are general, we should permute pair (n_i, r_i) for $i \in [\ell]$ to compute the minimal complexity.

7.2 Comparison with Combinatorial Attacks on the BRD Problem

In this section, we compare four combinatorial attacks against the BRD problem: IOJ, OJ, AGHT, and PRR. We show that the IOJ attack [28] previously underestimated the complexity of the RD problem by approximately γ^2 bits in the exponent, where $\gamma = \min\{r_i : i \in [\ell]\}$. Our OJ attack remains a candidate for the most powerful combinatorial attack when $m > k$.

In Table 7, we recall the complexities of combinatorial attacks: AGHT, PRR, and OJ. We only list the exponential terms of complexities. For clarity, in Table 7, we denote the types of these attacks as follows.

– The AGHT attack: AGHT-S and AGHT-C. AGHT-S for guessing a subspace containing the support (equivalently the column space of the support matrix) and AGHT-C for guessing a subspace containing the row space of the coefficient matrix. AGHT-S and AGHT-C respectively correspond to AGHT-1 and AGHT-2 in [28].
– The PRR attack: PRR-S and PRR-C. PRR-S for blockwise guessing a subspace containing the support (equivalently the column space of the support matrix) and PRR-C for blockwisely guessing a subspace containing the row space of coefficient matrix. PRR-S and PRR-C respectively correspond to PRR-1 and PRR-2 in [28].
– The IOJ attack: IOJ-S and IOJ-C. IOJ-S for the basis enumeration (guessing the support matrix) and IOJ-C for the coordinate enumeration. IOJ-S and IOJ-C respectively correspond to OJ-1 and OJ-2 in [28].
– **Our OJ attack**: OJ-S and OJ-C. OJ-S for the basis enumeration (guessing the support matrix) and OJ-C for the coordinate enumeration.

Table 7. Complexities of solving the BRD problem by the combinatorial attacks

Attacks	Types	$\mathsf{BRD}^{\ell,\boldsymbol{n},\boldsymbol{r}}_{q,m,n,k,r}$
AGHT [28]	AGHT-S	$q^{r\left\lceil\frac{(k+1)m}{n}\right\rceil-m}$
	AGHT-C	$q^{r(k+1)}$
PRR [28]	PRR-S	$q^{\min\{\sum_{i=1}^{\ell} r_i(m-t_i)-m\}}$
	PRR-C	$q^{\min\{\sum_{i=1}^{\ell} r_i(n_i-t'_i)\}}$
IOJ [28]	IOJ-S	$q^{(m-r)(r-1)}$
	IOJ-C	$q^{(r_1-1)(k-r_1)+\gamma}$ $(k=n_1)$
Our OJ	OJ-S	$q^{(m-r)(r-1)}$
	OJ-C	$q^{(r_1-1)(k-r_1)+r_1\gamma}$ $(k=n_1)$

We simulate complexities in Figure 1. For observing changes, we still adopt the parameter regions in [28]: $\ell = 2$, $q = 2$, $m < n$, $k = n_1 = n_2 = n/2$

with two cases $m < n/2$ and $m > n/2$. In Figure 1: (a), $m < n/2$, the BRD instances are estimated with $(q, m, n, k, n_1, n_2) = (2, 53, 134, 67, 67, 67)$. In Figure 1: (b), $m > n/2$, the BRD instances are estimated with $(q, m, n, k, n_1, n_2) = (2, 73, 134, 67, 67, 67)$. Both cases have various weight $(r_1, r_2) = (4, 4), (5, 5), (6, 6), (7, 7), (4, 6), (3, 7), (2, 8), (8, 2), (7, 3), (6, 4)$. The pair $(5, 5)$ and the last six pairs are possible decompositions of weight $r = r_1 + r_2 = 10$. Since the AGHT-S attack is significantly more powerful than the AGHT-C attack as m is smaller than n, we only consider the AGHT-S attack in Figure 1. Since the IOJ attack can be avoided, we only consider the OJ attack of this paper. Compared to Figure 1 of [28], only the green line is changed.

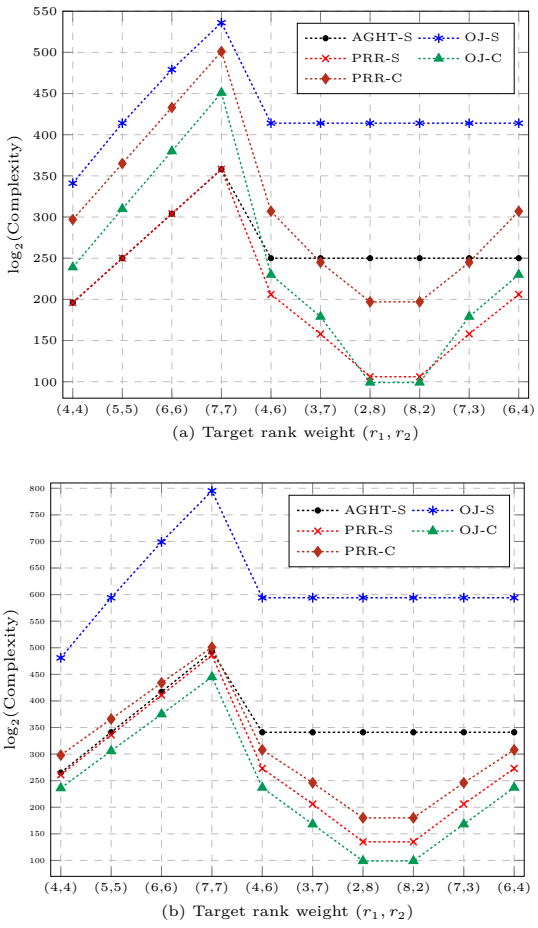


Fig. 1. Comparison of combinatorial attacks on the BRD problem

Comparisons. From Table 7, we can observe that the IOJ-C attack is underestimated by $(r_1 - 1)\gamma$ bits in the exponential term compared to the OJ-C attack.

From Figure 1, we can observe that the OJ-S attack is less powerful than other attacks. For the blockwise errors with a fixed weight, the complexities of the AGHT-S and OJ-S attacks remain unchanged, which means that the blockwise structure does not bring a gain for these two attacks.

When $m < n/2$, the PRR-S attack reflects the trend of complexity. From Figure 1 (a), we observe that:

- If the weight is divided equally ($r_1 = r_2$), the AGHT-S and PRR-S attacks are close and are superior to the other attacks.
- If r_1 and r_2 are not equal, the OJ-C and PRR-S attacks are close and are superior to the AGHT-S and PRR-C attacks. The more r_1 and r_2 are different, the lower the complexities are.

When $m > n/2$, the OJ-C attack is the most powerful. From Figure 1 (b), we observe that:

- If the weight is divided equally ($r_1 = r_2$), the AGHT-S and PRR-S attacks are close and less powerful than the OJ-C attack.
- If r_1 and r_2 are not equal, the more r_1 and r_2 are different, the lower the complexities are. The AGHT-S attack is less powerful than the PRR and OJ-C attacks

Whether $m < n/2$ and $m > n/2$, for the fixed weight decompositions ($r_1 + r_2 = 10$), the PRR and OJ-C attacks are independent of the order of r_1 and r_2.

7.3 Security of Cryptosystems Based on the BRD Problem

In this section, we estimate the security strength of cryptosystems based on the BRD problem by the combinatorial attacks: the AGHT, PRR, and OJ attacks. We consider two typical *blockwise* cryptosystems in [27,28]: Blockwise RQC (BRQC) and Blockwise Ouroboros-R (BOuroboros-R). Please see Table 8 and 9. For the parameters of BRQC, the OJ attack is the most powerful among the AGHT and PRR attacks because m is larger than the code dimension in two instances of the BRD probelm. Their quantum security strength is determined by the OJ attack. For the parameters of BOuroboros-R, the OJ attack is not the best, but it has a chance to become more powerful than the AGHT or PRR attack. The attack does not lower the claimed security level.

Illustrations: Following works [27,28], for all complexity estimations, we set linear algebra constant ω as 2.81 for a fair comparison. "λ" represents the claimed security level. AGHT = min{AGHT-S, AGHT-C}, PRR = min{PRR-S, PRR-C}, and OJ = min{OJ-S, OJ-C}. "AGHT", "PRR", and "OJ" represent the complexity using the AGHT, PRR, and OJ attacks, respectively. The bold complexity is the best one for an instance of the BRSD problem.

8 Conclusion

In this work, we revisited the OJ and IOJ attacks on the RD, NHRD, and BRD problems, and established a unified framework for their modeling and complexity analysis. We derived explicit and tight complexity bounds that cover general

Table 8. BRQC based on the BRSD problem [28] (DFR = Null)

q	m	n	k	$w_{\boldsymbol{x}}$	$w_{\boldsymbol{y}}$	$w_{\boldsymbol{r}_1}$	$w_{\boldsymbol{r}_2}$	$w_{\boldsymbol{e}}$	total (KB)	Attack-$2n$ (AGHT, PRR, OJ)	Attack-$3n$ (AGHT, PRR, OJ)	λ
2	83	79	7	4	4	4	4	4	2.5	$(2^{296}, 2^{292}, 2^{\mathbf{271}})$	$(2^{303}, 2^{353}, 2^{\mathbf{272}})$	128
2	127	113	3	5	5	5	5	5	5.3	$(2^{561}, 2^{556}, 2^{\mathbf{490}})$	$(2^{559}, 2^{605}, 2^{\mathbf{492}}$	192
2	139	137	3	5	5	6	6	7	7.1	$(2^{610}, 2^{605}, 2^{\mathbf{587}})$	$(2^{796}, 2^{864}, 2^{\mathbf{728}})$	256

"Attack-$2n$" represents attacking the $\mathsf{BRSD}^{2,(n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}_{q,m,2n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}$ problem. "Attack-$3n$" represents attacking the $\mathsf{BRSD}^{3,(n,n,n),(w_{\boldsymbol{r}_1},w_{\boldsymbol{e}},w_{\boldsymbol{r}_2})}_{q,m,3n,n,w_{\boldsymbol{r}_1}+w_{\boldsymbol{e}}+w_{\boldsymbol{r}_2}}$ problem.

Table 9. BOuroboros-R based on the BRSD problem [28]

q	m	n	r_1	r_2	r_3	d_1	d_2	DFR	total (KB)	Attack-$2n$ (AGHT, PRR, OJ)	Attack-$3n$ (AGHT, PRR, OJ)	λ
2	59	73	4	4	5	4	4	2^{-33}	1.6	$(2^{\mathbf{214}}, 2^{\mathbf{214}}, 2^{256})$	$(2^{\mathbf{237}}, 2^{327}, 2^{258})$	128
2	89	101	6	6	6	4	5	2^{-33}	3.3	$(2^{352}, 2^{\mathbf{312}}, 2^{342})$	$(2^{\mathbf{490}}, 2^{646}, 2^{553})$	192
2	97	109	6	6	7	5	5	2^{-42}	3.9	$(2^{\mathbf{430}}, 2^{\mathbf{430}}, 2^{479})$	$(2^{\mathbf{570}}, 2^{695}, 2^{593})$	256

"Attack-$2n$" represents attacking the $\mathsf{BRSD}^{2,(n,n),(d_1,d_2)}_{q,m,2n,n,d_1+d_2}$ problem. "Attack-$3n$" represents attacking the $\mathsf{BRSD}^{3,(n,n,n),(r_3,r_1,r_2)}_{q,m,3n,n,r_1+r_2+r_3}$ problem.

block structures and arbitrary code parameters, resolving several open questions raised in prior work. Our analysis further clarified the distinct roles of basis and coordinate enumeration, showing that the former is error-structure independent while the latter is highly sensitive to it. Two practical consequences follow. First, we proved that the IOJ attack rests on overly optimistic assumptions that do not hold in real random decoding scenarios, and therefore its apparent advantage over OJ, e.g., the $(r-1)^2$-bit gain on the RD problem, should be disregarded in conservative security assessments. Second, we demonstrated that the original OJ attack is the most powerful known combinatorial attack for the NHRD problem (saving up to 100 bits over AGHT-NHRD) and, for the BRD problem, outperforms both AGHT and PRR in large-m, small-k regions, with a gap of about γ^2 bits compared to earlier IOJ estimates. Concretely, the improvement over PRR reaches 136 bits for certain 256-bit BRQC instances. Our results provide a reliable foundation for evaluating the (quantum) security of rank-based cryptosystems and demonstrate that a careful re-examination of classic attacks can yield sharp, practically relevant bounds.

Acknowledgement

We are grateful to Diego Napp for valuable discussions on the soundness of IOJ attack, which motivated us to refine a general and tight OJ modeling for the RD problem and its variants.

References

1. Aragon, N., Briaud, P., Dyseryn, V., Gaborit, P., Vinçotte, A.: The blockwise rank syndrome learning problem and its applications to cryptography. In: Post-Quantum Cryptography (PQCrypto). vol. 14771, pp. 75–106. Springer (2024) 2, 3, 5, 6
2. Aragon, N., Dyseryn, V., Gaborit, P., Loidreau, P., Renner, J., Wachter-Zeh, A.: LowMS: a new rank metric code-based KEM without ideal structure. Designs, Codes and Cryptography **92**(4), 1075–1093 (2024) 2, 19, 20
3. Aragon, N., Gaborit, P., Hauteville, A., Tillich, J.: A new algorithm for solving the rank syndrome decoding problem. In: International Symposium on Information Theory (ISIT). pp. 2421–2425. IEEE (2018) 3, 4, 5
4. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Neiger, V., Ruatta, O., Tillich, J.: An algebraic attack on rank metric code-based cryptosystems. In: Advances in Cryptology - EUROCRYPT. vol. 12107, pp. 64–93. Springer (2020) 3, 4, 5, 9
5. Bardet, M., Briaud, P., Bros, M., Gaborit, P., Tillich, J.: Revisiting algebraic attacks on MinRank and on the rank decoding problem. Designs, Codes and Cryptography **91**(11), 3671–3707 (2023) 3, 4, 5
6. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In: Advances in Cryptology - ASIACRYPT. vol. 12491, pp. 507–536. Springer (2020) 3, 4, 5, 9
7. Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the inherent intractability of certain coding problems (corresp.). IEEE Transactions on Information Theory **24**(3), 384–386 (1978) 7
8. Bidoux, L., Briaud, P., Bros, M., Gaborit, P.: RQC revisited and more cryptanalysis for rank-based cryptography. IEEE Transactions on Information Theory **70**(3), 2271–2286 (2024) 2, 3, 4, 5, 8, 19, 20, 24, 25
9. Bidoux, L., Chi-Domínguez, J., Feneuil, T., Gaborit, P., Joux, A., Rivain, M., Vinçotte, A.: RYDE specifications (2023), https://pqc-ryde.org/index.html 2, 3, 19, 20
10. Bidoux, L., Chi-Domínguez, J., Feneuil, T., Gaborit, P., Joux, A., Rivain, M., Vinçotte, A.: RYDE: a digital signature scheme based on rank syndrome decoding problem with MPC-in-the-head paradigm. Designs, Codes and Cryptography **93**(5), 1451–1486 (2025) 2, 3, 19, 20
11. Bidoux, L., Chi-Domínguez, J., Feneuil, T., Gaborit, P., Joux, A., Rivain, M., Vinçotte, A.: RYDE specifications (2025), https://pqc-ryde.org/index.html 2, 3, 19, 20
12. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences **58**(3), 572–596 (1999) 7
13. Byrne, E., Gluesing-Luerssen, H., Ravagnani, A.: Fundamental properties of sum-rank-metric codes. IEEE Transactions on Information Theory **67**(10), 6456–6475 (2021) 4
14. Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: Advances in Cryptology - ASIACRYPT. vol. 1163, pp. 368–381. Springer (1996) 3, 4, 5
15. Faugère, J., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of MinRank. In: Advances in Cryptology - CRYPTO. vol. 5157, pp. 280–296. Springer (2008) 7

16. Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Transactions on Information Theory **62**(2), 1006–1019 (2016) 3, 4, 5
17. Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Transactions on Information Theory **62**(12), 7245–7252 (2016) 7
18. Jerkovits, T., Bartz, H., Wachter-Zeh, A.: Support-guessing decoding algorithms in the sum-rank metric. arXiv preprint (2024), https://arxiv.org/abs/2410.15806 4
19. Melchor, C.A., Aragon, N., Bettaieb, S., et al.: RQC. Second round submission to the NIST post-quantum cryptography call (2020), http://pqc-rqc.org/ 2, 8
20. Melchor, C.A., Aragon, N., Bettaieb, S., et al.: HQC. Fourth round submission to the NIST post-quantum cryptography call (2022), http://pqc-hqc.org 2
21. NIST: Status report on the second round of the NIST post-quantum cryptography standardization process. NIST, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8309 (2020), https://doi.org/10.6028/NIST.IR.8309 2
22. NIST: Status report on the fourth round of the NIST post-quantum cryptography standardization process. NIST, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8545 (2025), https://doi.org/10.6028/NIST.IR.8545 2
23. NIST: Status report on the second round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. NIST, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8610 (2026), https://doi.org/10.6028/NIST.IR.8610 3
24. Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission **38**(3), 237–246 (2002) 3, 4, 5, 6, 9, 17, 19
25. Puchinger, S., Renner, J., Rosenkilde, J.: Generic decoding in the sum-rank metric. IEEE Transactions on Information Theory **68**(8), 5075–5097 (2022) 3, 4, 5
26. Song, Y., Chen, R., Zhang, F., Huang, X., Weng, J., Wang, H.: (Interleaved) extended Gabidulin codes, more analysis on blockwise rank decoding problem, and their applications to cryptosystems. Cryptology ePrint Archive, Paper 2025/668 (2025), https://eprint.iacr.org/2025/668 2, 5, 6
27. Song, Y., Zhang, J., Huang, X., Wu, W.: Blockwise rank decoding problem and LRPC codes: Cryptosystems with smaller sizes. In: Advances in Cryptology - ASIACRYPT. vol. 14444, pp. 284–316. Springer (2023) 2, 5, 6, 9, 17, 33
28. Song, Y., Zhang, J., Huang, X., Wu, W.: Blockwise rank decoding problem and LRPC codes: Cryptosystems with smaller sizes. IEEE Transactions on Information Theory **71**(6), 4806–4838 (2025) 2, 3, 4, 5, 6, 7, 8, 9, 17, 31, 32, 33, 34

Appendix for Section 5

A The IOJ Attack on the RD Problem (Section 5.3)

Theorem 9. *With $\boldsymbol{S}$ and $\boldsymbol{C}$ in the form of Equation (5), by the basis enumeration, the IOJ attack solves the RD problem with complexity over $\mathbb{F}_q$*

$$\mathcal{O}\left(((k+1)r)^{\omega}\, q^{(m-r)(r-1)}\right).$$

Proof. From Equation (5), $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{C}' \end{array}\right],$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{(m-r)\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-1)}$.

By the IOJ modeling in Equation (20), for any $j \in \{1..n-k-1\}$, we have

$$\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j = \left[\begin{array}{c|c} \boldsymbol{I}_r \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right][\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j = \boldsymbol{0}_{m\times m}. \tag{21}$$

For any j, we can observe that $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$ includes $(k+1)r$ entries. The modeling gives a quadratic multivariate system with m^2 equations and $(m-r)(r-1)+kr+r$ variables in entries of $\boldsymbol{S}$, $\boldsymbol{A}_1$, and $\boldsymbol{a}_j$.

By first guessing the entries of $\boldsymbol{S}'$, we can obtain a linear system with m^2 equations and $(k+1)r$ unknowns in the entries of $[\boldsymbol{A}_1\ \boldsymbol{a}_j]$. Since $(k+1)r \ll m^2$ for any code parameters, if $(m-r)(r-1)$ entries of $\boldsymbol{S}'$ are correctly guessed, then the system can be solved uniquely, we would obtain $\boldsymbol{S}$, further could determine $\boldsymbol{e}$ from Equation (4). The complexity is bounded by $\mathcal{O}\left(((k+1)r)^{\omega} q^{(m-r)(r-1)}\right)$. □

Theorem 10. *With $\boldsymbol{S}$ and $\boldsymbol{C}$ in the form of Equation (6), by the coordinate enumeration, the IOJ attack solves the RD problem with complexity over $\mathbb{F}_q$:*

$$\begin{cases} \mathcal{O}\left((m(r-1))^{\omega}\right), & 0 < k+1 \le r; \\ \mathcal{O}\left((m(r-1)+(k+2-r))^{\omega} q^{(r-1)(k+2-r)}\right), & r < k+1 \le n. \end{cases}$$

Proof. From Equation (6), $\boldsymbol{S}$ and $\boldsymbol{C}$ have the form:

$$\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \\ \hline \boldsymbol{0}_{(m-r)\times 1} & \boldsymbol{S}' \end{array}\right], \qquad \boldsymbol{C} = \left[\boldsymbol{I}_r\ \boldsymbol{C}'\right],$$

where $\boldsymbol{S}' \in \mathbb{F}_q^{m\times(r-1)}$ and $\boldsymbol{C}' \in \mathbb{F}_q^{r\times(n-r)}$.

Let $\boldsymbol{S} = \left[\begin{array}{c|c} 1 & \boldsymbol{s}' \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}'' \end{array}\right] \in \mathbb{F}_q^{m\times r}$ where $\boldsymbol{s}' = \boldsymbol{S}_{\{1\},\{2..r\}} \in \mathbb{F}_q^{1\times(r-1)}$ and $\boldsymbol{S}'' = \boldsymbol{S}_{\{2..m\},\{2..r\}} \in \mathbb{F}_q^{(m-1)\times(r-1)}$. Recall that $\boldsymbol{C} = [\boldsymbol{A}_1\ \boldsymbol{A}_2]$ where $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$ are the first $k+1$ columns and the last $n-k-1$ columns of $\boldsymbol{C}$. Let

$$\boldsymbol{A}_1 = \left[\begin{array}{c|c} 1 & \boldsymbol{a}_1^* \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{A}_1^* \end{array}\right] \in \mathbb{F}_q^{r\times(k+1)}, \qquad \boldsymbol{A}_2 = \left[\begin{array}{c} \boldsymbol{a}_2^* \\ \hline \boldsymbol{A}_2^* \end{array}\right] \in \mathbb{F}_q^{r\times(n-k-1)}$$

where $\boldsymbol{a}_1^* = \boldsymbol{C}_{\{1\},\{2..k+1\}} \in \mathbb{F}_q^{1\times k}$, $\boldsymbol{A}_1^* = \boldsymbol{C}_{\{2..r\},\{2..k+1\}} \in \mathbb{F}_q^{(r-1)\times k}$, $\boldsymbol{a}_2^* = \boldsymbol{C}_{\{1\},\{k+2..n\}} \in \mathbb{F}_q^{1\times(n-k-1)}$, and $\boldsymbol{A}_2^* = \boldsymbol{C}_{\{2..r\},\{k+2..n\}} \in \mathbb{F}_q^{(r-1)\times(n-k-1)}$.

For any $j \in \{1..n-k-1\}$, recall that $\boldsymbol{a}_j$ is the j-th column of $\boldsymbol{A}_2$. Let $\boldsymbol{a}_j = \left[\begin{array}{c} \boldsymbol{a}_2^*(j) \\ \hline \boldsymbol{A}_2^*(j) \end{array}\right]$ where $\boldsymbol{a}_2^*(j) \in \mathbb{F}_q$ is the j-th column of $\boldsymbol{a}_2^*$ and $\boldsymbol{A}_2^*(j) \in \mathbb{F}_q^{r-1}$ is the j-th column of $\boldsymbol{A}_2^*$. By the IOJ modeling in Equation (20), we have

$$\begin{aligned}\boldsymbol{S}[\boldsymbol{A}_1\ \boldsymbol{a}_j]\boldsymbol{T}_j &= \left[\begin{array}{c|c} 1 & \boldsymbol{s}' \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}'' \end{array}\right] \left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* & \boldsymbol{a}_2^*(j) \\ \hline \boldsymbol{0}_{(r-1)\times 1} & \boldsymbol{A}_1^* & \boldsymbol{A}_2^*(j) \end{array}\right] \boldsymbol{T}_j \\ &= \left[\begin{array}{c|c|c} 1 & \boldsymbol{a}_1^* + \boldsymbol{s}'\boldsymbol{A}_1^* & \boldsymbol{a}_2^*(j) + \boldsymbol{s}'\boldsymbol{A}_2^*(j) \\ \hline \boldsymbol{0}_{(m-1)\times 1} & \boldsymbol{S}''\boldsymbol{A}_1^* & \boldsymbol{S}''\boldsymbol{A}_2^*(j) \end{array}\right] \boldsymbol{T}_j = \boldsymbol{0}_{m\times m}. \end{aligned} \tag{22}$$

The OJ modeling gives a quadratic multivariate system with m^2 quadratic polynomials whose variables are the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with mN equations whose unknowns are the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. If the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, and unknowns $\leq m^2$, the system can be solved uniquely to obtain the entries of $\boldsymbol{S}$. The complexity is determined by the cost of solving the linear system and guessing $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$.

Case 1: $0 < k+1 \leq r$
Let $j \in \{k+2..r\} - (k+1)$. At this point, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$ are constant matrices. The IOJ modeling gives a linear system with m^2 equations and $m(r-1)$ unknowns in the entries of $\boldsymbol{S}$. Since $m(r-1) \leq m^2$ for code parameters, the system could be solved uniquely in polynomial time and we would obtain $\boldsymbol{S}$. The complexity is bounded by $\mathcal{O}\left((m(r-1))^\omega\right)$.

Case 2: $r < k+1 \leq n$.
We can observe that $\boldsymbol{a}_1^*$ and $\boldsymbol{a}_2^*(j)$ have $(k+1-r+1)$ unknown entries; $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ have $(r-1)(k+1-r+1)$ unknown entries. The IOJ modeling gives a quadratic multivariate system with m^2 polynomials and $m(r-1)+(k+2-r)r$ variables in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, $\boldsymbol{A}_1^*$, $\boldsymbol{a}_2^*(j)$, and $\boldsymbol{A}_2^*(j)$. By guessing the entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$, we can obtain a linear system with m^2 equations and $m(r-1)+(k+2-r)$ unknowns in the entries of $\boldsymbol{S}$, $\boldsymbol{a}_1^*$, and $\boldsymbol{a}_2^*(j)$. Since $m(r-1)+(k+2-r) \leq m^2$ for code parameters, if the unknown entries of $\boldsymbol{A}_1^*$ and $\boldsymbol{A}_2^*(j)$ are correctly guessed, then the system could be solved uniquely and we would obtain $\boldsymbol{S}$. The complexity is bounded by $\mathcal{O}\left((m(r-1)+(k+2-r))^\omega q^{(r-1)(k+2-r)}\right)$. □