(Interleaved) Extended Gabidulin Codes, More Analysis on Blockwise Rank Decoding Problem, and Their Applications to Cryptosystems

Yongcheng Song, Rongmao Chen, Fangguo Zhang, Xinyi Huang⋆, Jian Weng, and Huaxiong Wang

Abstract

In this paper, we investigate the Extended Gabidulin (EG) codes and the Interleaved EG (IEG) codes, conduct more analysis on the Blockwise Rank Decoding (BRD) problem, and obtain efficient rank-based cryptosystems.

First, we develop a general decoding algorithm for the (I)EG codes by solving the Linear Reconstruction (LR) problem. We find that the (I)EG codes can be probabilistically decoded by Welch-Berlekamp like algorithm, can achieve an arbitrarily small decoding failure rate, and can decode up to the rank Gilbert-Varshamov bound (even close to the minimal distance). Our conclusion intrinsically shows that it is not necessary to require that the generator be linearly independent as Gabidulin codes for designing decodable codes from q-polynomials. An interesting and important byproduct is that we demonstrate that decoding interleaved Gabidulin codes can be achieved *deterministically* by solving the LR problem. It has long been believed that there are only *probabilistic* decoding algorithms for interleaved Gabidulin codes (IEEE TIT 2011, DCC 2014, DCC 2024).

Second, we propose the Blockwise Puncturing (BP) approach for solving the BRD problem (Asiacrypt 2023, IEEE TIT 2025). For this purpose, we derive a tight upper bound of independent equations in the MM modeling for *general* blocks, which further addresses an open question in (Asiacrypt 2023, IEEE TIT 2025, PQC 2024). We find that the BP approach can speed up the MM modeling. When the proposed approach is applied to the BRD problem used in existing rank-based cryptosystems, such as RQC and ROLLO (IEEE TIT 2025, PQC 2024), some parameters sets are lower than the practical security strength, and the security loss is up to 25 bits; nevertheless, the schemes still preserve the claimed security level. This work further supports the hardness of the BRD problem and enhances the security and performance of cryptosystems based on the BRD problem.

Third, we apply the EG codes to the structured rank decoding encryption, namely RQC based on the BRD problem (Asiacrypt 2023, IEEE TIT 2025), and obtain the Bolckwise RQC with the EG codes (BRE). We find that the gain of using the EG codes in decoding capacity outweighs the complexity loss in solving the BRD problem with the BP approach, which still makes it possible to design more efficient schemes. As a result, BRE features a more attractive size with a bandwidth of about 1.6 KB for 128-bit security. Overall, BRE outperforms Hamming metric ones of NIST PQC Round 4 submissions, such as HQC, BIKE, and Classic McEliece, in terms of bandwidth, especially about 76% more compact than HQC selected by the NIST PQC.

Fourth, we apply the EG codes to the unstructured rank decoding encryption, namely NH-Multi-UR-AG (IEEE TIT 2024), with the homogeneous errors, and obtain the Homogeneous Unstructured Rank decoding encryption with the EG codes (HURE). The bandwidth of HURE is about 6.7 KB for 128-bit security, which is slightly shorter than NH-Multi-UR-AG. This bandwidth also outperforms lattice-based unstructured PKEs, namely FrodoKEM and Scloud$^+$, respectively about 64% and 45% more compact. We intrinsically show that it is sufficient to construct an efficient unstructured PKE scheme by only homogeneous errors, without non-homogeneous errors. This application benefits from that we derive the concise DFR for the EG codes, which allows to choose flexible parameters.

Index Terms

Rank Metric Codes, Extended Gabidulin Codes, Rank Decoding Problem, Code-Based Cryptography, NIST PQC.

⋆ Corresponding Author
Yongcheng Song is with the College of Cyber Security, Jinan University, Guangzhou, 510632, China (e-mail: yongchengsong@outlook.com).
Rongmao Chen is with the School of Computer, National University of Defense Technology, Changsha, China (e-mail: chromao@nudt.edu.cn).
Fangguo Zhang is with the School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou, China (e-mail: zhangfg@mail.sysu.edu.cn).
Xinyi Huang is with the College of Cyber Security, Jinan University, Guangzhou, 510632, China (e-mail: xyhuang81@gmail.com).
Jian Weng is with the College of Cyber Security, Jinan University, Guangzhou, 510632, China (e-mail: cryptjweng@gmail.com).
Huaxiong Wang is with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore (e-mail: hxwang@ntu.edu.sg).

CONTENTS

I Introduction 4
- I-A Our Contributions . . . 6
- I-B Technical Overview . . . 7
- I-C Comparisons With Decoding of the AG Codes . . . 9
- I-D Concurrent Work . . . 10
- I-E Organization . . . 10

II Notations 10

III Preliminaries 11
- III-A $\mathbb{F}_{q^m}$-Linear Codes with Rank Metric . . . 11
- III-B q-Polynomial and Annihilator Polynomial . . . 12
- III-C Matrix Rank and Subspace Dimension . . . 13
- III-D The RD and BRD Problems . . . 13
- III-E The MM Modelings From the RD and BRD Problems . . . 14

IV Our Results on Rank of Moore Matrix 15

V Decoding EG Codes to Solving LR Problem 17
- V-A From Decoding EG Codes to Solving NLR Problem . . . 18
- V-B From the NLR Problem to the LR Problem . . . 18

VI Decoding EG Codes 20
- VI-A Dimension of Right Kernel of the System (7) . . . 20
- VI-B Decoding Failure Rate for the Largest r . . . 21
- VI-C Decoding Capacity . . . 22
- VI-D Decoding Algorithm . . . 22
- VI-E Simulated DFR for Decoding Errors of Weight r . . . 23

VII Improved Decoding Algorithm 23
- VII-A Improved Gaussian Elimination . . . 23
- VII-B Welch-Berlekamp Like Algorithm for the EG Codes . . . 24

VIII Interleaved EG Codes 25

IX Relations with (Interleaved) Gabidulin Codes 27

X Blockwise Puncturing (BP) Approach on the BRD Problem 28
- X-A Density of the Basis for Random Errors . . . 28
- X-B Linearly Independent Equations in the MM Modeling From the BRD Problem . . . 29
- X-C The MM Modeling From BRD With the BP Approach . . . 34
- X-D Impacts on Security Strength of Cryptosystems . . . 37

XI Applications: BRE and HURE 37
- XI-A Our BRE From the EG Codes and the IBRSD Problem . . . 38
- XI-B Parameters and Performance of Our BRE . . . 39
- XI-C Our HURE From the EG Codes and the RSL Problem . . . 39
- XI-D Parameters and Performance of Our HURE . . . 41

XII Conclusion and Future Work 42

Appendix A: Omitted Lemmata, Tables, and Proofs 42
- A-A Omitted Lemmata . . . 42
- A-B Table XI for Simulated DFR by Welch-Berlekamp Like Algorithm . . . 43
- A-C The Proof of Theorem 8 . . . 43

Appendix B: Decoding Errors of Weight w $(w < r)$ for the EG Codes 44

Appendix C: Decoding Errors of Weight w $(w < r)$ for the IEG Codes 47

Appendix D: Public Key Encryption 48

Appendix E: Ideal Codes and Ideal BRSD Problem 48

Appendix F: Rank Support Learning Problem 49

References 50

Biographies 51
Yongcheng Song . . . 51
Rongmao Chen . . . 52
Fangguo Zhang . . . 52
Xinyi Huang . . . 52
Jian Weng . . . 52
Huaxiong Wang . . . 52

I. Introduction

Code-based cryptography is a promising candidate for post-quantum cryptography. Three code-based systems using Hamming metric codes, i.e., Classic McEliece, BIKE, and HQC, are advanced to the fourth round of the NIST Post-Quantum Cryptography (NIST PQC) standardization process for potential future adoption [1]. Especially, HQC recently has been selected for the final standardization. As an alternative, rank-based cryptosystems, which use rank metric error-correcting codes and are based on the rank decoding problems, offer competitive bandwidth [2]. Recent studies [3]–[6] have further explored the potential of rank metrics, demonstrating that McEliece, NTRU, and Alekhnovich approaches outperform the counterparts of Hamming metric systems in bandwidth. The typical schemes are LowMS [4], ROLLO [3], [5], and RQC [3], [5], [6], especially ROLLO and RQC whose security rely only on the hardness of the rank decoding problems. In this paper, we further analyze the security and efficiency of RQC, ROLLO, and their variants by developing rank metric error-correcting codes and more analysis on the rank decoding problem.

$\mathbb{F}_{q^m}$-Linear Codes with Rank Metric. The rank metric codes were introduced by Delsarte [7] in 1978, and later were also found by Gabidulin [8]. Since then, rank metric codes have been used for many applications: coding theory and space time coding in particular, and also for cryptography. The rank metric codes used in cryptography are compressed over an extension field $\mathbb{F}_{q^m}$ of degree m of the finite field $\mathbb{F}_q$ to save the size of cryptosystems, and are called $\mathbb{F}_{q^m}$-linear codes. Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ be a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$. Then, any random $\boldsymbol{e} = (e_1, e_1, \ldots, e_n) \in \mathbb{F}_{q^m}^n$ has an associated matrix $\mathbf{Mat}(\boldsymbol{e}) \in \mathbb{F}_q^{m\times n}$ such that $\boldsymbol{e} = \boldsymbol{\alpha}\mathbf{Mat}(\boldsymbol{e})$. The rank weight $\|\boldsymbol{e}\|_{\mathrm{R}}$ of $\boldsymbol{e}$ is defined as the rank of $\mathbf{Mat}(\boldsymbol{e})$. The support $\mathrm{Supp}(\boldsymbol{e})$ of $\boldsymbol{e}$ is the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ spanned by its coordinates. It follows from definition that $\|\boldsymbol{e}\|_{\mathrm{R}}$ equals to the dimension of $\mathrm{Supp}(\boldsymbol{e})$. The set of errors of length n and weight r is denoted by $\mathcal{S}_r^n$. We call the errors in $\mathcal{S}_r^n$ *standard (or homogeneous) errors*. If no ambiguous, we call $\mathrm{Supp}(\boldsymbol{e})$'s basis a basis of $\boldsymbol{e}$. An $\mathbb{F}_{q^m}$-linear code ($[n,k]_{q^m}$-linear 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 $k \times n$ over $\mathbb{F}_{q^m}$. Currently, the families of well-known $\mathbb{F}_{q^m}$-linear codes with rank metric are Gabidulin codes [8], Low Rank Parity Check (LRPC) codes [9], [10], and Simple codes [11]. In this paper, we focus on Gabidulin codes and its variants [6], [12]–[15].

Gabidulin Codes. An $[n,k]_{q^m}$-Gabidulin code [8] is the evaluation of q-polynomials [16] bounded degree $k-1$ on a fixed generator of weight n (or linearly independent over $\mathbb{F}_q$) with the condition $k \le n \le m$. The Gabidulin codes are Maximum Rank Distance (MRD) codes with the minimal distance $d = n-k+1$, and are viewed as the rank metric analogues of classical Reed-Solomon codes in Hamming metric. They therefore have a strong algebraic structure. The Gabidulin codes benefit from efficient decoding algorithms [13], [17]–[19] that corrects weight errors up to $\lfloor \frac{n-k}{2} \rfloor$ in a deterministic way. As is well known, there is a large gap between the decoding capacity and the Rank Gilbert-Varshamov (RGV) bound (or the minimal distance).

Extended Gabidulin Codes. Among variants of Gabidulin codes [6], [12], [14], [15], Extended Gabidulin (EG) codes [12] proposed by Berger and Ourivski in 2009 are interesting. Unlike Gabidulin codes, the EG codes include many non-MRD codes and feature a weaker algebraic structure. The EG codes still are the evaluation of q-polynomials, but with a wide parameters region. Let q, m, n, t, k be integers and $k \le t \le \min\{n, m\}$. Let $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be a generator of weight t. Let $\mathcal{L}_{\le k-1}[x]$ be the set of q-polynomials of q-degree $\le k-1$. The EG code of dimension k and length n generated by $\boldsymbol{g}$ is defined as

$$\mathrm{EG}_k(\boldsymbol{g}) = \Big\{ f(\boldsymbol{g}) = (f(g_1), f(g_2), \ldots, f(g_n)) \ : \ f(x) \in \mathcal{L}_{\le k-1}[x] \Big\}.$$

One can observe that if $m \ge n$ and $t = n$, namely the coordinates $g_1, g_2, \ldots, g_n$ of the generator $\boldsymbol{g}$ is linearly independent, the EG codes are exactly Gabidulin codes. From the Gabidulin codes to the EG codes, the main difference is that the generator is allowed to be linearly dependent, i.e., $t \le \min\{n, m\}$. For long time, the linear independence of generator has been considered as the key of successfully and deterministically decoding Gabidulin codes. The community views Gabidulin codes as the rank metric analogues of the RS codes, the linearly independent generator of Gabidulin codes corresponds to the mutually different locator of the RS codes, then adapt the decoding algorithms of the RS codes to Gabidulin codes. The linear independence is mainly used to determine the locations that the error occurs. However, once introducing the change of linear dependence, the situation is rather different, and it intuitively does not to determine the locations that the error occurs. In the case of EG codes, the following questions naturally arise:

1) How can EG codes be decoded directly?
2) What are the decoding performance characteristics of EG codes, including decoding failure rate, decoding capacity, and decoding complexity?
3) Could we adapt existing decoding algorithms for Gabidulin codes to EG codes?
4) How should the interleaved EG codes be defined and decoded?

These problems were partially raised by Berger and Ourivski [12] in 2009. One could note that the EG codes are equivalent to the Augmented Gabidulin (AG) codes [6], where the proposed decoding technique can also be adapted to the EG codes.

The technique [6] decoding the AG codes can indeed be viewed as a pioneering and specific method to decode the EG codes. We refer to Section I-C for differences with the technique decoding the AG codes in [6]. However, developing other tailored and efficient decoding techniques for the EG codes has been remained open and interesting. In this paper, our first work is to develop a tailored and efficient decoding technique for the EG codes and deal with thoroughly the above problems.

Rank Decoding Problem and Variants. Let $\boldsymbol{G}$ be a generator matrix of a random $[n,k]_{q^m}$-linear code, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, and $r \in \mathbb{N}$. The Rank Decoding (RD) problem is to find $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a standard error $\boldsymbol{e} \in \mathcal{S}_r^n$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$. Although the RD problem is not shown to be NP-complete, it is very close to the Hamming metric decoding problem which is NP-complete [20], and can be seen as a structured version of the MinRank problem which is also NP-complete [21]. Moreover, after more than three decades of study, the best known algorithms for solving the RD problem are all exponential. This makes the RD problem a promising hard problem to construct secure cryptosystems.

Recently, for designing efficient cryptosystems, a variant of the RD problem are proposed in [3], [6], [22], [23], which is called the Blockwise RD (BRD) problem [3], [23]. The main difference between the RD problem and the BRD problem consists in the definition of the error $\boldsymbol{e}$. In the BRD problem, one solves a blockwise error. Let ℓ be a positive integer, $\boldsymbol{n} = (n_1, n_2, \ldots, n_\ell)$ and $\boldsymbol{r} = (r_1, r_2, \ldots, r_\ell)$ be positive integers vectors. An error $\boldsymbol{e} \in \mathcal{S}_r^n$ with $n = \sum_{i=1}^{\ell} n_i$ and $r = \sum_{i=1}^{\ell} r_i$ is a blockwise error with parameters $\boldsymbol{n}$ and $\boldsymbol{r}$ if it can be divided into ℓ sub-vectors $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_\ell)$ such that 1) the sub-vector $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^{n_i}$ has weight r_i for all $i \in \{1..\ell\}$; and 2) the supports of these sub-vectors are in direct sum. Denote $\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ as the set of blockwise errors with parameters $\boldsymbol{n}$ and $\boldsymbol{r}$. The blockwise errors are also related to the sum-rank metric errors [24]–[26], where the error is also divided into ℓ blocks and the sum-rank weight is defined as the sum of weight of each block. The difference is that we explicitly require the ℓ blocks to have direct-sum supports and different block length, which is the generalization of the sum-rank setting.

The MM Attack on the RD and BRD Problems. There currently exist combinatorial attacks [27]–[30] and algebraic attacks [29], [31]–[33] on the RD problem. The first combinatorial attack is proposed in [27] and is significantly improved in [28] and further refined in [29], [30]. The combinatorial attacks [27], [29], [30] consist of subtly guessing the support of error and solving a linear system. The attack [28] transforms a quadratic multivariate system induced from the RD problem into a linear system by guessing some information of errors. The first algebraic attack is proposed in [29], where one solves a multivariate system induced from the RD problem based on the annihilator polynomial by linearization and Gröbner basis. In the case of cryptographic parameters, this attack is considered to be less efficient than combinatorial attacks. A breakthrough algebraic attack is proposed in [31], where the $\mathbb{F}_{q^m}$-linearity is allowed to devise a dedicated attack, i.e., the MaxMinors (MM) modeling. Then the MM modeling is refined and improved in [32] where the authors also introduced another algebraic modeling, the SupportMinors (SM) modeling. The SM modeling later is combined with the MM modeling (i.e., the SM-$\mathbb{F}_{q^m}^+$ modeling [33]). The SM and MM modelings respectively reduce the RD problem to solving a bilinear system and a linear system. The analysis in [33] shows that the cost of the SM-$\mathbb{F}_{q^m}^+$ modeling is close to those of the combinatorial attack [30] and the MM modeling [32]. The advantage of these algebraic attacks is that they are independent of the size of q. Their costs mainly depend on the number of unknowns w.r.t. the number of equations. Typically, for the MM modeling [32], the larger the value of m, the more equations there are, the faster it would be to solve the system, and the lower the cost of the attack. These combinatorial and algebraic attacks are adapted to the BRD problem in [3], [5], [23]. The MM attack can well exploit the structure of errors and perform more powerfully than the combinatorial attacks for most of the parameter regions. Thus, the MM attack has become a core tool for selecting security parameters and measuring the security strength of rank-based cryptosystems.

Rank-Based Cryptography. The first rank-based cryptosystem, the GPT cryptosystem [34], which is viewed as an adaptation of the McEliece scheme in the rank metric context, is based on masking Gabidulin codes [8]. Early versions of GPT were broken by Overbeck's attack [35]. In 2017, Loidreau's variant [36] introduced a masking technique using homogeneous matrices of a given rank, which resisted Overbeck's attack [35], except in cases of small rank, as analyzed in [37], [38]. Recently, LowMS [4] improved upon Loidreau's masking approach by multiple syndromes, achieving a bandwidth of about 5.8 KB for 128-bit security. LowMS features the smallest size among unstructured lattice- and code-based PKEs, thanks to the interleaved Gabidulin codes with high decoding capacity and negligible Decoding Failure Rate (DFR).

The second type was using LRPC codes [9] to construct cryptosystems [9], [39] by following NTRU [40] (also MDPC [41]) approach. The NTRU approach generalizes the masking technique by considering public key matrices with trapdoor. The typical cryptosystem is Lake (or Locker) [9], [39], where masks a small weight vector (define an LRPC code) by a public matrix. The security relies on the *random* RD problem together with the computational indistinguishability of the public key. Lake and Locker [9] were initially submitted to the NIST PQC standardization process in 2017. Later, with another cryptosystem Ouroboros-R [42], three are merged into ROLLO in the second round [39]. The recent work [43] optimized the bandwidth by LRPC codes with multiple syndromes. This method allows to decode errors of larger weight and decreases DFR. More recently, by using blockwise structure [3] with multiple syndromes, the work [5] reduced the bandwidth of Lake to 1.7 KB.

The Alekhnovich approach was introduced in [44] and allows the security to rely solely on the *random* RD problems. This approach early was highly inefficient. A few years later, an optimized approach was proposed with HQC, which relies

on Quasi-Cyclic codes. It has been generalized to rank metric with RQC [22], [45]. In RQC, two types of codes are used: the random ideal codes are used to ensure security, and the public Gabidulin codes are used to decrypt the ciphertext. The main advantage compared to McEliece and NTRU is that the security is completely based on the *random* RD problems and is independent of the specific codes whereas McEliece and NTRU require an additional indistinguishability assumption on a specific code for the security of the private key; however, this advantage comes at a price of the short plaintext size (low encryption rate).

RQC was proposed to the NIST PQC in 2017 with competitive sizes. The combinatorial attacks [28]–[30] were once considered to be the most efficient attacks against the parameters region of RQC. However, it turned out later that the dedicated algebraic attacks [31]–[33], particularly the MM attack, greatly undermine the concrete security strength of RQC. The main reason is that RQC must work over a large field whose extension degree m is at least length n of Gabidulin codes, while the MM attack is very powerful over such a large finite field because it is highly probable to solve an overdetermined system. It was just because of the MM attack that RQC was not selected for the third round of NIST PQC. New parameter sets [22] were proposed to provide adequate security against algebraic attacks and still remain competitive sizes. In [3], [23], the authors introduced blockwise errors into RQC to decrease the noise growth, which brings large decoding gains and saves parameters scale. The bandwidth is reduced to about 2.5 KB.

The more recent works [5], [6] enriched the designs of RQC and made a breakthrough in bandwidth. The work [6] introduced the AG codes to improve the decoding capacity, and proposed two variants of RQC. Typical schemes are Non-Homogeneous Multiple-syndromes Unstructured RQC with the AG codes (NH-Multi-UR-AG) and Non-Homogeneous Multiple-syndromes RQC with the AG codes (NH-Multi-RQC-AG). The NH-Multi-UR-AG scheme considers a long-term security and features a conservative design as it relies purely on random RD problems without any ideal structure. The NH-Multi-RQC-AG scheme is ideally suited for the AG codes and allows a tradeoff between public key size and ciphertext size. By the blockwise structure [3] and the AG codes, the work [5] ultimately decreased the bandwidth to 1.4 KB, namely RQC-Block-MS-AG. This bandwidth has outperformed latticed-based Kyber finalized by NIST PQC.

Overall, these developments highlight the promise of rank-based cryptosystems. However, two folds should be further studied:

- It is worth developing more techniques to improve performance. A very promising optimization routine is to introduce error-correcting codes with a desirable decoding performance (efficient decoding algorithm, negligible DFR, and high error-correcting capacity) into cryptosystems.
- The BRD problem [3], [5], [23] are recently proposed and their complexity needs more time to mature. It is essential to develop more attacks on this problem to support the security and performance of rank-based cryptosystems.

In this paper, our goal is to analyze the decoding algorithm of the EG codes, develop more analysis on the BRD problem, and enhance performance and security of rank metric cryptosystems such as RQC and ROLLO.

A. Our Contributions

1) We develop the decoding of the EG codes by solving the Linear Reconstruction (LR) problem. We show that the EG codes can be decoded by Welch-Berlekamp like algorithm solving the LR problem with the complexity $\mathcal{O}(n^2)$, and feature the DFR which can be made arbitrarily small. More interestingly, for appropriate code parameters, the EG codes can exactly decode up to the RGV bound (even close to the minimal distance), which outperforms Gabidulin codes. From this property, we obtain that by the EG codes, any syndrome and word can be decoded efficiently to an error of weight the RGV bound. Our work essentially shows that the decoding conditions of codes defined by q-polynomial are not necessary as strong as those of Gabidulin codes, namely, the linearly independent generator is unnecessary. For decoding the same error, the EG codes are more efficient than Gabidulin codes if allowing a DFR. Further, we introduce the Interleaved EG (IEG) codes and show that the IEG codes allow to decode more errors with a negligible DFR.
   Building on our analysis approach, we also demonstrate that decoding interleaved Gabidulin codes can be achieved *deterministically* by solving the LR problem. This addresses an open question partially unresolved in [14], where the authors provided a proof only for the specific case where the number of columns in the system equals the number of rows plus one. This limitation led to a misconception in subsequent works [4], [15], [46], which assumed that decoding interleaved Gabidulin codes required *probabilistic* algorithms.
2) By the density of the basis of random errors, we propose the Blockwise Puncturing (BP) approach to solve the BRD problem. For estimating the complexity of the BP approach, we derive a tight upper bound of independent equations in the MM modeling for general blocks. This further addresses an open question in [3], [5], [23]. The BP approach allows to transform the instances into the smaller instances and can speed up the overdetermined MM modeling. When applying the MM attack with the BP approach to existing rank-based cryptosystems based on the BRD problem, the practical security strength is undermined up to 25 bits. However, the schemes still preserve the claimed security level.
3) We apply the EG codes to improve RQC based on the BRD problem [3], [23], call BRE. The bandwidth of BRE is about 1.6 KB for 128-bit security, which is about 76% more compact than the NIST PQC selected code-based cryptosystems using the Hamming metric, namely, HQC. We apply the EG codes to improve NH-Multi-UR-AG [6]

with the homogeneous errors, call HURE. The bandwidth of HURE is about 6.7 KB for 128-bit security, which is slightly shorter than NH-Multi-UR-AG and also outperforms lattice-based unstructured PKEs, namely FrodoKEM [47] and Scloud$^+$ [48], by respectively about 64% and 45%. We intrinsically simplify the structure of NH-Multi-UR-AG, and show that it is sufficient to construct an efficient unstructured PKE scheme by using only homogeneous errors, without non-homogeneous errors. The efficient applications benefits from:

- While the MM attack with the BP approach can speed up attack, the EG codes enable the parameters to mitigate the advantage of the attacks. The gain of using the EG codes in decoding capacity outweighs the complexity loss in solving the BRD problem with the BP approach, which still makes it possible to design efficient algorithms.
- We derive the concise DFR for the EG codes, which allows to choose flexible parameters for designing cryptosystems.

B. Technical Overview

We first describe the decoding model of the EG codes. Given the EG codes of dimension k and length n with the generator $\boldsymbol{g}$ of weight t, we assume that the message q-polynomial is $f(x)$ of degree $k-1$, the error occurring at the channel is $\boldsymbol{e}$ and $\|\boldsymbol{e}\|_{\mathrm{R}} \leq r$, the received word is $\boldsymbol{y} = f(\boldsymbol{g}) + \boldsymbol{e}$. The aim of decoding EG codes is to recover $\boldsymbol{e}$ and $f(x)$ from $\boldsymbol{y}$. For any $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_{q^m}^n$, we denote the $(s+1) \times n$ Moore matrix of order s of $\boldsymbol{e}$ as

$$\mathbf{Moore}(\boldsymbol{e}, s) = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \\ e_1^q & e_2^q & \cdots & e_n^q \\ \vdots & \vdots & \ddots & \vdots \\ e_1^{q^s} & e_2^{q^s} & \cdots & e_n^{q^s} \end{bmatrix}.$$

Decoding Errors of Exact Weight r. We reduce the decoding EG codes problem to solving the Linear Reconstruction (LR) problem. We show that the decoding EG codes problem is still equivalent to solving the well-known and hard Non-Linear Reconstruction (NLR) problems, then the obtained NLR problem can be reduced to the LR problem. We first analyze the method solving the LR problem by solving a linear system. Directly decoding the EG codes consists in solving the system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$, where $\boldsymbol{A} = \left[\mathbf{Moore}(\boldsymbol{y}, r)^\top \ \ \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top\right]$. The weight value r such that the system has one-dimensional right kernel determines the decoding capacity of the EG codes. We conduct an extensive and thorough analysis on the dimension of the right kernel of the system. A key step is that we derive that the matrix $\boldsymbol{A}$ is equivalent to $\left[\mathbf{Moore}(\boldsymbol{e}, r)^\top \ \ \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top\right]$ (see Proposition 9), which greatly facilitates analysis of the right kernel. A careful reader should note that the similar problem is still evaded in previous works [13], [14], [17] because analyzing the right kernel of the linear system is rather cumbersome and challenging. We find that for appropriate code parameters, the probability that one-dimensional kernel does not occur is negligible. Eventually, the EG codes can decode up to $r = \min\left\{t-k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\}$, which exactly reaches to the RGV bound. We give a specific experiment to verify the decoding capacity and DFR. We refer to Section V and Section VI for the details.

Decoding Errors of Weight $< r$. A careful reader could note that, in the above decoding idea, we only consider the decoding the maximal-weight error. However, a crucial problem of how to decode smaller errors is omitted because the errors and their weight are unpredictable in practical channels. How to decode the smaller errors? What the sufficient and necessary condition of successful decoding is? Trivially, one could try to solve r linear systems by increasing weight values from 1 to r, but this is very cost (about $\mathcal{O}(n^4)$). We analyze this problem for the EG codes with a deep level. We show that one actually can decode smaller errors by solving only "one" linear system with the cost of about $\mathcal{O}(n^3)$. Specifically, when the error of weight w occurs ($w < r$), the successful decoding iff the right kernel of $\boldsymbol{A}$ is of dimension $r - w + 1$. Note that the similar problem is omitted in the case of Gabidulin codes (Algorithm 1 [13]), where authors did not consider the sufficient and necessary condition of successful decoding for smaller errors, instead of crudely assuming existence of non-zero right kernel. The remaining problem now is that while the decoding is easy to implement, it costs the complexity of $\mathcal{O}(n^3)$, which is less efficient and should be improved. We refer to Section VI for the details.

Improved Decoding Algorithms. We consider two methods to improve decoding complexity. The first one is the improvement of solving the system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$. By observing the structure of $\boldsymbol{A}$, its part is independent of the received word $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ and depends only on the generator $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$. This fact allows us to solve a smaller system with $r+1$ unknowns and $n-k-r$ equations. The decoding complexity is $\mathcal{O}(r^3)$. The Welch-Berlekamp like algorithm is an efficient technique [13], [17] solving the LR problem. Our second improvement is that adapting Welch-Berlekamp like algorithm [13], [17] to solve the LR problem, further decode EG codes. The decoding complexity is at most $\mathcal{O}(n^2)$. We refer to Section VII for the details of improvements.

Interleaved EG Codes and Decoding. We introduce the Interleaved EG (IEG) codes and analyze its decoding performance. Interleaving a code consists in considering several codewords at the same time, corrupted by errors sharing the same support. This specific structure allows to decode more errors. Let $\boldsymbol{y}_i = f_i(\boldsymbol{g}) + \boldsymbol{e}_i, \quad i \in [N]$ where all $\boldsymbol{e}_i$'s share the support of

dimension r. The decoding IEG codes problem is that given N words $\boldsymbol{y}_i$'s, the goal is to recover N q-polynomials $f_i(x)$ and errors $\boldsymbol{e}_i$. We reduce the decoding IEG codes problem to solving the LR problem. We show that if one receives such N words $\boldsymbol{y}_i$'s, it can correct up to $r = \min\left\{t-k, \frac{N(n-k)}{(N+1)}\right\}$ and the DFR can be made arbitrarily small. We refer to Section VIII for details.

The DFR of Interleaved Gabidulin Codes. We analyze the DFR of the interleaved Gabidulin codes by solving the LR problem with Gaussian elimination. Provided that the Gabidulin codes are the special case of the EG codes, by our DFR of the (Interleaved) EG codes, we derive that the obtained linear system has always one-dimensional right kernel, further decoding interleaved Gabidulin codes is deterministic. This problem is left in [14], where the authors only considered the vague case that the number of columns of the system is exactly equal to number of rows plus 1. This leads to a mislead that the most previous works [4], [15], [46] thought that there exists only *probabilistic* decoding algorithms for interleaved Gabidulin codes. Our DFR is based on a heuristic argument (in Theorem 3). The heuristic argument is valid. Because the interleaved Gabidulin codes cover the Gabidulin codes when $N = 1$, if our heuristic argument is invalid, then decoding Gabidulin codes by Gaussian elimination would not be deterministic. This challenges the well-known conclusion: decoding Gabidulin codes is deterministic, which has stood for about 40 years. The details are presented in Section IX.

The BP Approach on the BRD Problem. Recalled that almost all previous rank-based cryptosystems considered random errors. For a random error, the elements formimg a basis of its support are very dense. That is, for a random error $\boldsymbol{e}$ of rank weight r over $\mathbb{F}_{q^m}^n$, the vector consisting of any r elements of $\boldsymbol{e}$ could form a basis of its support with an overwhelming probability. The probability is exactly the probability that a random $r \times r$ matrix over $\mathbb{F}_q$ is non-singular, which is larger than or equal to 0.289 for $q \geq 2$. We call this property *the density of the basis*. We refer to Section X-A for the details.

Recall that $\boldsymbol{n} = (n_1, n_2, \ldots, n_\ell)$ and $\boldsymbol{r} = (r_1, r_2, \ldots, r_\ell)$ are integers vector, $n = \sum_{i=1}^{\ell} n_i$, $r = \sum_{i=1}^{\ell} r_i$. The BRD problem asks an algorithm given as inputs a generator matrix $\boldsymbol{G}$ of a random $[n,k]_{q^m}$-linear code, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, to output $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a blockwise error $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_\ell) \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$. For solving the MM modeling derived from the BRD problem, the puncturing approach is used in [3], [23], where only last p coordinates of the last block are punctured. Here, we propose to puncture on the last p_i coordinates of *each* block for appropriate p_i for $i \in [\ell]$. This is called the Blockwise Puncturing (BP) approach. Let $\boldsymbol{p} = (p_1, p_2, \ldots, p_\ell)$ be an integers vector and $p = \sum_{i=1}^{\ell} p_i$. By the BP approach, the punctured $\boldsymbol{G}$, $\boldsymbol{y}$, and $\boldsymbol{e}$ are denoted by $\boldsymbol{G}'$, $\boldsymbol{y}'$, and $\boldsymbol{e}'$, respectively. By the density of the basis for random errors, we assume that the first r_i coordinates of $\boldsymbol{e}_i$ form the basis of its support for $i \in [\ell]$. Otherwise, we can perform an invertible matrix over $\mathbb{F}_q$ on $(\boldsymbol{G}, \boldsymbol{y})$ to make the assumption hold, and apply the BP approach to the new instance. In this way, for an appropriate $\boldsymbol{p}$, we can obtain a new and smaller instance $(\boldsymbol{G}', \boldsymbol{y}')$ of the BRD problem, which asks an algorithm given as inputs a generator matrix $\boldsymbol{G}'$ of a random $[n-p,k]_{q^m}$-linear code, and a vector $\boldsymbol{y}' \in \mathbb{F}_{q^m}^n$, to output $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a blockwise error $\boldsymbol{e}' \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}-\boldsymbol{p}}$ such that $\boldsymbol{y}' = \boldsymbol{x}\boldsymbol{G}' + \boldsymbol{e}'$. Based on the assumption, solving the instance $(\boldsymbol{G}', \boldsymbol{y}')$ is equivalent to solving the instance $(\boldsymbol{G}, \boldsymbol{y})$ because the BP approach does not destroy the support of $\boldsymbol{e}$. Once $(\boldsymbol{G}', \boldsymbol{y}')$ is solved, one can obtain the support of $\boldsymbol{e}$, further can solve the original $(\boldsymbol{G}, \boldsymbol{y})$ by using the obtained support; and vice versa.

The existing combinatorial attacks and algebraic attacks can be adapted to solving the punctured problem. The gain of the algebraic attacks is significant. The combinatorial attacks are either independent of the code length or benefit from the large code length. The case of the algebraic attacks is different, especially for the MM attack. The MM attack consists in solving a linear system, whose number of unknowns and linearly independent equations determines the complexity of the attack. For the blockwise errors, the number of unknowns can be easily computed, but the computation of independent equations is very tricky. To obtain a precise complexity of the MM attack with the BP approach, one must deal with an open question left in [3], [5], [23]: how to estimate the number of independent equations are in the MM modeling from the BRD problem. In [3], [23], authors used the maximal equations $m\binom{n-k-1}{r}$ to bound the number of independent equations for the conservative complexity. In [5], authors further estimated the upper bound of independent equations in the special case of $\ell = 2$ (or $\ell = 3$) and $k = n_1 = n_2 = \cdots = n_\ell$. When applying the BP approach to the BRD problem, the BP approach would lead to the general case of parameters, such as $k < n_1$, unequal n_i's, and any ℓ. Here, we consider *such general cases* and derive a tight upper bound of independent equations. Our ideal is to estimate the number of non-zero equations in the MM modeling over $\mathbb{F}_{q^m}$. From the cases of $\ell = 2$ and $\ell = 3$ (see Theorem 9 and Theorem 10), we derive the general conclusion for any ℓ by induction in Theorem 11. We refer to Section X-B for the details.

We find that the MM attack with the BP approach is powerful for some parameters region in existing rank-based cryptosystems based on the BRD problem, such as RQC [3], [5], [6], [22], [23] and ROLLO [3], [23], [42]. The BP approach can speed up the overdetermined MM modelings, which makes the parameters sets lower than the practical security strength. We refer to Section X-C for the details.

Applications to BRE and HURE. By making a tradeoff between the complexity loss of the BRD problem and the decoding capacity of the EG codes and exploiting our concise DFR for the EG codes, it is possible to design efficient and secure rank-based cryptosystems with flexible choices of parameters.

Recall that Gabidulin codes used in the previous RQC [3], [22], [23] require $m \geq n$, which makes RQC vulnerable to the MM attack and imposes a strong limitation on security parameters. The use of the EG codes can alleviate this case. The EG codes can work over a smaller finite field and allow $m < n$, which could mitigate the advantage of the MM attack and has more degree of freedom while choosing security parameters. Eventually, a tradeoff shows that the parameters gain of using the EG codes outweighs the parameters loss of the MM attack with the BP approach for preserving the security. Thus, our first application is to improve RQC based on the BRD problem by using the EG codes. To distinguish it from the previous RQC, our improved RQC is name as Blockwise RQC with the EG codes (BRE). The resulting BRE achieves the bandwidth of 1.6 KB for 128-bit security, which outperforms Hamming metric ones of NIST PQC Round 4 submissions, such as HQC, BIKE, and Classic McEliece.

Recall that NH-Multi-UR-AG proposed in [6] uses the non-homogeneous errors with the bandwidth of about 7.1 KB for 128-bit security. The use of the non-homogeneous errors makes the structure is a little complicated. Moreover, the security is based on the Non-Homogeneous RD (NHRD) problem solving the non-homogeneous errors. Currently, the complexity of the NHRD problem seem to be insufficient. It is at least unknown if the puncturing approach can speed up the MM attack. Considering that our concise DFR for the EG codes allow to choose flexible parameters and the complexity of the RD problem is relatively mature. Thus, we try to improve NH-Multi-UR-AG by using the EG codes and the homogeneous errors. To distinguish it from NH-Multi-UR-AG, our improved scheme is name as Homogeneous Unstructured Rank decoding encryption with the EG codes (HURE). The resulting HURE achieves the bandwidth of about 6.7 KB for 128-bit security, which is slightly shorter than NH-Multi-UR-AG and also outperforms significantly lattice-based unstructured PKEs, namely FrodoKEM [47] and Scloud$^+$ [48]. It is sufficient to construct an efficient unstructured PKE scheme by using only homogeneous errors, without non-homogeneous errors. We refer to Section XI for the details.

C. Comparisons With Decoding of the AG Codes

Considering the EG codes [12] are equivalent to the Augmented Gabidulin (AG) codes [6]. In this section, we highlight some differences with the decoding technique (Proposition 2 in [6]) of the AG codes. We first stress some objective facts. For some families of codes, the DFR and the decoding complexity depends on the specific decoding techniques, instead of the equivalence property of codes. Naturally, the different decoding techniques could lead to different DFR and decoding complexity. As in [14] and [15], by different decoding techniques, authors presented different DFR and decoding complexity for interleaved Gabidulin codes. Again, for Gabidulin codes, Linearized Extended Euclidean Algorithm (LEEA) [18], Gao-like algorithm [19], and Welch-Berlekamp like algorithm [13], [17] present different decoding complexity. It hence should be encouraged to develop different techniques for decoding a family of codes.

We now recall the AG codes [6]. In the definitions of the EG codes, if we set the first t coordinates of $\boldsymbol{g}$ to be linearly independent and the last $n-t$ coordinates to be zeros, then the EG codes are exactly the AG codes. In the case of the rank metric, there exists an invertible matrix on the base field $\mathbb{F}_q$ which permits to turn a code into the other and such an invertible matrix is called an isometry. Assume that one obtains an EG code with generator $\boldsymbol{g}$ of weight t, then it is possible to apply an isometry to turn n coordinates of $\boldsymbol{g}$ into t linearly independent coordinates plus $n-t$ zero coordinates. The n new coordinates define an AG code that is equivalent to the EG code. While the work [6] can serve as a pioneering effort in providing a specific technique to decode the EG codes, developing other efficient decoding techniques is still interesting. In this paper, we adopt different decoding idea. The differences with [6] are as follows.

First, the decoding techniques are obviously different. We confirm that the technique [6] decoding the AG codes can be viewed as the first specific method to decode the EG codes. The authors in [6] considered the support erasures technique exposing errors to decode the AG codes. The decoder exposed errors on zero coordinations of the generator, derived a part of support from the exposed errors, and reduced the decoding AG code problem *with the partial support* to solving a linear system. However, it seems to be hard to improve this decoding complexity because they must solve a linear system with an implicit structure (Equation (3), [6]) due to the exploiting of partial support. Currently, it is at least unknown whether there are more efficient techniques to solve such a linear system. Differently, we do not consider any support erasures exposing errors. We reduce the decoding EG code problem to solving the LR problem, try the underlying techniques solving the LR problem, further improve decoding efficiency. While directly solving the LR problem also consists in solving a linear system by Gaussian elimination, the structure of the linear system is explicit, which is beneficial for observing the essence of decoding and developing efficient decoding algorithms. Specifically, once the EG code can be decoded by solving the LR problem, one could develop and adapt efficient algorithms solving the LR problem to decode the EG codes such as (improved) Gaussian elimination [17] and Welch-Berlekamp like algorithm [13], [17]. As a result, by solving the LR problem with (improved) Gaussian elimination and Welch-Berlekamp like algorithm, we obtain that the Gaussian elimination costs $\mathcal{O}(n^3)$, the improved cost is about $\mathcal{O}(r^3)$, and Welch-Berlekamp like algorithm costs $\mathcal{O}(n^2)$. One can note that decoding AG codes in [6] costs about $\mathcal{O}((k+2r-\varepsilon)^3)$ where ε is the dimension of the vector space generated by the support erasures, and $k+2r-\varepsilon \approx m$ for cryptographic parameters. Note that $n \geq m > r$. More importantly, the (improved) Gaussian elimination and the Welch-Berlekamp like algorithm can be easily implemented. However, demonstrating EG codes can be decoded by solving the LR problem is rather cumbersome and challenging. The previous conclusions in [13], [14], [17] are not applied directly. We refer

to Section V-B for the detailed reasons. We must deal with the right kernel of a linear system. This is still left as an open question in the setting of Gabidulin codes [13], [14], [17].

Second, our DFR formula is concise. One could find that the steps of deriving our DFR are enormous; nevertheless, these steps are necessary to show that the EG codes can be decoded by solving the LR problem and to derive a precise DFR. The resulting DFR formula only depends on parameters (q, n, t, k, r). Unlike the AG codes [6], the DFR additionally depends on the number of erasures. Our concise DFR formula allows a flexible choice of parameters when applying the EG codes to rank-based cryptosystems.

Third, we definitely show that EG codes can "exactly" decode up to the errors of weight the RGV bound, instead of "asymptotical" upper bound (means a might gap). This property is not mentioned in the case of the AG codes [6]. The codes "exactly" decoding up to the RGV bound is very interesting for code-based cryptography as such codes are one of the key techniques designing efficient code-based hash-sign signatures. For example, the low signing efficiency of code-based hash-sign signature, CFS, roots in that Goppa code only "asymptotically" decodes up to the Hamming GV bound as the upper bound, instead of "exactly". This must try to find decodable syndrome in many times to obtain a signature. Our work shows that the EG codes can overcome this obstacle since any syndrome can be decoded with an overwhelming probability. The remaining challenge is technique securely hiding EG codes. We note that an interesting hiding technique for Gabidulin codes was developed in recent work [49], which seems to be a solution to securely hiding EG codes.

Fourth, we introduce the Interleaved EG (IEG) codes and analyze decoding performance. We show that the IEG codes can correct up to $r = \min\left\{t-k, \frac{N(n-k)}{(N+1)}\right\}$ and the DFR can be made arbitrarily small. By our DFR of the (I)EG codes, we obtain the null DFR of the interleaved Gabidulin codes by solving the LR problem with Gaussian elimination. This addresses an open question left partially unresolved in [14], where the authors provided a proof only for the specific case where the number of columns in the system equals the number of rows plus one.

Overall, our work shows that the EG codes can be well decoded by solving the LR problem. This is independently interesting for the EG codes and can also be viewed as the development and complement of decoding AG codes. Meanwhile, we resolve an open question for the interleaved Gabidulin codes and reveal some interesting results for the rank metric codes.

D. Concurrent Work

In updated version [50] (March 02, 2025) of published [5] (PQC 2024), authors additionally considers the application of the AG codes to RQC based on the BRD problem. In fact, our application of the EG codes to RQC based on the BRD problem was *early* submitted to Eurocrypt 2025 (October 02, 2024). In this paper, we conduct a more analysis on the complexity of the BRD problem, consider three security levels (128, 192, 256), and choose compact parameters. The compact parameters are because our concise DFR allows more flexible parameters and our precise complexity allows to save parameters size. Moreover, we do not introduce the multiple-syndromes structure to BRE. This would enable BRE to feature more applications in the future due to its flexible structure.

E. Organization

After some notations given in Section II, we present some preliminaries used in this paper. Section IV proves some useful results for analyzing the decoding performance. We give the EG codes in Section V together with a reduction from decoding EG code problem to the LR problem. Section VI analyzes the decoding algorithm, decoding complexity, decoding failure rate, and decoding capacity. Section VII presents two improvements of decoding algorithms. Section VIII introduces and analyzes the interleaved EG codes. In Section IX, we show the relation between the interleaved EG codes and the interleaved Gabidulin codes. Section X proposes the BP approach to the MM modeling induced from the BRD problem, and analyzes its impacts on the security strength of existing rank-based cryptosystems. In Section XI, we apply the EG codes to BRE and HURE. We conclude this paper in Section XII.

II. Notations

- We denote by $\mathbb{N}$ the set of non-negative integer numbers, q prime or prime power, and $\mathbb{F}_{q^m}$ an extension of degree m of the finite field $\mathbb{F}_q$.
- We denote by $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$.
- Vectors (resp. matrices) are denoted by lower-case (resp. upper-case) bold letters.
- We use the notation $[N] := \{1, 2, \ldots, N\}$ for the first N positive integers. 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. $\boldsymbol{M}_{I,*}$). The sub-vector of a vector $\boldsymbol{m}$ formed from the indices in I is denoted by $\boldsymbol{m}_I$. $|\boldsymbol{M}|$, $|\boldsymbol{M}|_{I,J}$, and $|\boldsymbol{M}|_{*,J}$ are the determinant of the matrix $\boldsymbol{M}$, the submatrix $\boldsymbol{M}_{I,J}$, and the submatrix $\boldsymbol{M}_{*,J}$, respectively.
- The maximal minor of a matrix $\boldsymbol{C}$ of size $r \times n$ is the determinant of its submatrix $\boldsymbol{C}_{*,T}$ whose column indexes $T \subset \{1..n\}$ and $\#T = r$.

- Let $\mathbf{Diag}(\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_\ell)$ denote a block diagonal matrix whose the matrices on the diagonal are $\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_\ell$. Specially, $\mathbf{Diag}(\boldsymbol{C}, \ell)$ denotes a block diagonal matrix for $\boldsymbol{C} = \boldsymbol{C}_1 = \boldsymbol{C}_2 = \cdots = \boldsymbol{C}_\ell$.
- The Gaussian elimination of a $\mu \times \nu$ random matrix of rank ρ over an $\mathbb{F}_q$ has a complexity of $\mathcal{O}(\rho^{\omega-2}\mu\nu)$ operations in $\mathbb{F}_q$, where ω is the exponent of matrix multiplication (or linear algebra constant) with $2 \leq \omega \leq 3$, a practical value is 2.807 when there are more than a few hundred rows and columns with Strassen's algorithm.
- The Cauchy-Binet formula that computes the determinant of the product of $\boldsymbol{A} \in \mathbb{F}_{q^m}^{r\times n}$ and $\boldsymbol{B} \in \mathbb{F}_{q^m}^{n\times r}$ is expressed as $|\boldsymbol{AB}| = \sum_{T\subset[n],\#T=r} |\boldsymbol{A}|_{*,T}|\boldsymbol{B}|_{T,*}$.
- Let $\mathcal{A}$ be an algorithm. We say that $\mathcal{A}$ is a PPT algorithm if it is a probabilistic polynomial-time algorithm.

III. Preliminaries

In this section, we define some notations, and recall $\mathbb{F}_{q^m}$-linear codes, q-polynomials, annihilator polynomials, the standard/ blockwise rank decoding problems, and the MM attack.

A. $\mathbb{F}_{q^m}$-Linear Codes with Rank Metric

Definition 1 (Rank Metric) *For $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, each coordinate x_i is associated to a vector of $\mathbb{F}_q^m$ w.r.t. the basis $\boldsymbol{\alpha}$. Then $\boldsymbol{x}$ is associated to an $m \times n$ matrix given by $\mathbf{Mat}(\boldsymbol{x}) = (x_{ij})_{i\in[m],j\in[n]}$: $\boldsymbol{x} = \boldsymbol{\alpha}\mathbf{Mat}(\boldsymbol{x})$. 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 $d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y}) := \|\boldsymbol{x} - \boldsymbol{y}\|_{\mathrm{R}}$.*

Let $\langle x_1, x_2, \ldots, x_n\rangle_{\mathbb{F}_q}$ be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}$ generated by linear combinations over $\mathbb{F}_q$ of coordinates of $\boldsymbol{x}$. *The support* $\mathrm{Supp}(\boldsymbol{x})$ of $\boldsymbol{x}$ is defined as $\langle x_1, x_2, \ldots, x_n\rangle_{\mathbb{F}_q}$, i.e., $\mathrm{Supp}(\boldsymbol{x}) = \langle x_1, x_2, \ldots, x_n\rangle_{\mathbb{F}_q}$. It follows from definition that $\|\boldsymbol{x}\|_{\mathrm{R}}$ is equal to the dimension of $\mathrm{Supp}(\boldsymbol{x})$, i.e., $\|\boldsymbol{x}\|_{\mathrm{R}} = \dim(\mathrm{Supp}(\boldsymbol{x}))$. The set of such errors of weight r and length n is denoted by $\mathcal{S}_r^n$. We call the errors in $\mathcal{S}_r^n$ *standard (or homogeneous)* errors.

Support Matrix, Coefficient Matrix, and Basis of the Error. For an error $\boldsymbol{e} \in \mathcal{S}_r^n$, let $\boldsymbol{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r) \in \mathbb{F}_{q^m}^r$ 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 $\boldsymbol{e} = \boldsymbol{\varepsilon}\boldsymbol{C}$. Under the basis $\boldsymbol{\alpha}$, there exists a matrix $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ of rank r such that $\boldsymbol{\varepsilon} = \boldsymbol{\alpha}\boldsymbol{S}$. Then $\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C}$. If no ambiguous, we also call $\boldsymbol{\varepsilon}$ a *basis* of $\boldsymbol{e}$. We call $\boldsymbol{S}$ and $\boldsymbol{C}$ respectively *support matrix* and *coefficient matrix*. For a fixed error $\boldsymbol{e}$, we denote these two matrices as $\mathbf{SM}(\boldsymbol{e})$ and $\mathbf{CM}(\boldsymbol{e})$, respectively. Under the same basis $\boldsymbol{\alpha}$, $\boldsymbol{e} = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e}) = \boldsymbol{\alpha}\mathbf{SM}(\boldsymbol{e})\mathbf{CM}(\boldsymbol{e}) = \boldsymbol{\alpha}\mathbf{Mat}(\boldsymbol{e})$.

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 $\mathcal{C} = \left\{\boldsymbol{m}\boldsymbol{G} \ : \ \boldsymbol{m} \in \mathbb{F}_{q^m}^k\right\}$ and a matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is called *parity-check matrix* iff $\mathcal{C} = \left\{\boldsymbol{c} \in \mathbb{F}_{q^m}^n \ : \ \boldsymbol{H}\boldsymbol{c}^\top = \boldsymbol{0}\right\}$. The systematic forms of $\boldsymbol{G}$ and $\boldsymbol{H}$ are respectively defined as $[\boldsymbol{I}_k \ \boldsymbol{P}]$ and $\left[-\boldsymbol{P}^\top \ \boldsymbol{I}_{n-k}\right]$ where $\boldsymbol{P} \in \mathbb{F}_{q^m}^{k\times(n-k)}$.

Definition 3 (Rank Gilbert-Varshamov (RGV) Bound [11], [51]) *Let $S(q, m, n, r)$ be the number of errors of weight r in $\mathbb{F}_{q^m}^n$, which equals to the number of $m \times n$ matrices in $\mathbb{F}_q^{m\times n}$ of rank r, i.e.,*

$$S(q, m, n, r) = \begin{bmatrix} m \\ r \end{bmatrix}_q \prod_{j=0}^{r-1}(q^n - q^j) = \prod_{j=0}^{r-1}\frac{(q^m - q^j)(q^n - q^j)}{q^r - q^j}.$$

Let $\mathcal{V}(q, m, n, r)$ be the number of errors of weight $\leq r$ in $\mathbb{F}_{q^m}^n$:

$$\mathcal{V}(q, m, n, r) = \sum_{i=0}^{r} S(q, m, n, i) = \sum_{i=0}^{r}\prod_{j=0}^{i-1}\frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}.$$

The RGV bound $d_{\mathrm{RGV}}(m, n, k)$ is the smallest $r \in \mathbb{N}$ such that $\mathcal{V}(q, m, n, r) \geq q^{(n-k)m}$. When either m or n tends to infinity, $\mathcal{V}(q, m, n, r) \approx q^{r(m+n-r)}$. Let $q^{r(m+n-r)} = q^{(n-k)m}$, we have

$$d_{\mathrm{RGV}}(m, n, k) = \begin{cases} \frac{m+n-\sqrt{(m-n)^2+4km}}{2}, & m \neq n; \\ n\left(1 - \sqrt{\frac{k}{n}}\right), & m = n. \end{cases} \tag{1}$$

From Definition 3, the RGV bound for an $[n, k]_{q^m}$ code $\mathcal{C}$ with parity-check matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$, corresponds to the smallest weight r for which, for any syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$, there exists on average an error $\boldsymbol{e}$ of weight r such that $\boldsymbol{H}\boldsymbol{e}^\top = \boldsymbol{s}$. Note that the approximation $q^{r(m+n-r)}$ is very tight and is the lower bound of $\mathcal{V}(q, m, n, r)$ (see Proposition 1 of [51]):

$$q^{r(m+n-r)} \leq \mathcal{V}(q, m, n, r) \leq \gamma_q \cdot q^{r(m+n-r)},$$

where $\gamma_q = \prod_{j=1}^{\infty} \frac{1}{1-q^{-j}}$ is always greater than 1 and is monotonically decreasing in q, e.g., $\gamma_2 \approx 3.463$, $\gamma_3 \approx 1.785$, and $\gamma_4 \approx 1.452$. This means that the value r satisfying $\mathcal{V}(q,m,n,r) = q^{m(n-k)}$ must be less than or equal to one satisfying $q^{r(m+n-r)} = q^{(n-k)m}$. In other words, the accurate RGV bound must be less than or equal to the (asymptotical) RGV bound in Equation (1). Further, if the code $\mathcal{C}$ can decode up to the RGV bound in Equation (1), then its decoding capacity is actually beyond the accurate RGV bound.

Hence, we obtain that if the code $\mathcal{C}$ can efficiently decode up to the RGV bound in Equation (1), then any syndrome (resp. word) in $\mathbb{F}_{q^m}^{n-k}$ (resp. $\mathbb{F}_{q^m}^{n}$) can be decoded efficiently. The EG codes are exactly this case (see Theorem 5).

Definition 4 (Rank Singleton (RS) Bound [51], [52]) *The RS bound $d_{\mathrm{RS}}(m,n,k)$ for an $[n,k]_{q^m}$-linear code is defined as* $d_{\mathrm{RS}}(m,n,k) = \left\lfloor \frac{m(n-k)}{\max(m,n)} \right\rfloor + 1$.

The minimal distance of rank metric codes is less than or equal to the RS bound. The code with the minimal distance reaching the RS bound is called a Maximum Rank Distance (MRD) code.

B. q-Polynomial and Annihilator Polynomial

The EG code is the evaluation of q-polynomials (or linearized polynomials) introduced originally by Ore in the 1930s [16].

Definition 5 (q-Polynomials [16]) *A q-polynomial of q-degree n over $\mathbb{F}_{q^m}$ is a polynomial of the form $f(x) = \sum_{i=0}^{n} f_i x^{q^i}$ for $f_i \in \mathbb{F}_{q^m}$, $f_n \neq 0$.*

We denote the q-degree of a q-polynomial $f(x)$ by $\deg_q f(x)$. Let $\mathcal{L}[x]$ be the set of q-polynomials and $\mathcal{L}_{\leq r}[x]$ be the set of q-polynomials of q-degree $\leq r$. Let $a(x) = \sum_i a_i x^{q^i}$ and $b(x) = \sum_i b_i x^{q^i} \in \mathcal{L}[x]$:

- The addition "$+$" of $a(x)$ and $b(x)$: $a(x) + b(x) = \sum_i (a_i + b_i) x^{q^i}$;
- The symbolic product "$\circ$" of $a(x)$ and $b(x)$: $a(x) \circ b(x) = a(b(x))$.

It is well-known that the set of q-polynomials together with addition and symbolic product forms a noncommutative ring. In such a ring, the symbolic product is associative and distributive w.r.t. both right and left product. The identity element is $I(x) = x$ and there are no divisors of zero, i.e., $a(x) \circ b(x) = 0$ implies $a(x) = 0$ or $b(x) = 0$. A q-polynomial $c(x)$ is said to be symbolically right divisible by $b(x)$ if $c(x) = a(x) \circ b(x)$. When $c(x) = a(x) \circ b(x)$, we say that $c(x)$ is symbolically left divisible by $a(x)$, which is denoted by $b(x) = a(x) \setminus c(x)$.

Let $s \geq r$, $a(x) = \sum_{i=0}^{r} a_i x^{q^i}$, $b(x) = \sum_{i=0}^{s} b_i x^{q^i}$, and $c(x) = a(x) \circ b(x) = \sum_{i=0}^{s+r} c_i x^{q^i}$. One easily checks that

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{s+r} \end{bmatrix} = \underbrace{\begin{bmatrix} b_0 & 0 & \cdots & 0 \\ b_1 & b_0^q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ b_s & b_{s-1}^q & \cdots & b_{s-r}^{q^r} \\ 0 & b_s^q & \cdots & b_{s-r+1}^{q^r} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_s^{q^r} \end{bmatrix}}_{:=\mathbf{PM}(b(x),r) \in \mathbb{F}_{q^m}^{(s+r+1)\times(r+1)}} \times \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_r \end{bmatrix} = \mathbf{PM}(b(x),r) \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_r \end{bmatrix}.$$

A q-polynomial $f \in \mathcal{L}[x]$ satisfies:

- $\forall\ x_1, x_2 \in \mathbb{F}_{q^m}$, $\beta_1, \beta_2 \in \mathbb{F}_q$, $f(\beta_1 x_1 + \beta_2 x_2) = \beta_1 f(x_1) + \beta_2 f(x_2)$.
- If x_1 and x_2 are any two roots of f, then $f(x_1) = f(x_2) = f(x_1 + x_2) = 0$.

These two properties imply that all roots of a q-polynomial span an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. Proposition 1 shows that the q-degree of a q-polynomial is lower bounded by the dimension of its root space. Definition 6 shows that given an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$, there exists a unique monic q-polynomial vanishing on such an $\mathbb{F}_q$-subspace.

Proposition 1 *Let $f(x) \in \mathcal{L}[x]$ be a q-polynomial. Assume that $e_1, e_2, \ldots, e_n \in \mathbb{F}_{q^m}$ span an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension r. If $f(e_i) = 0$ for all $i \in [n]$, then either $f(x) = 0$, or $\deg_q f(x) \geqslant r$.*

Definition 6 (Annihilator Polynomial [16]) *For any $\mathbb{F}_q$-subspace E of $\mathbb{F}_{q^m}$ of dimension r, there exists a unique monic q-polynomial $\mathcal{A}_E(x)$ of q-degree r that vanishes on E, i.e., $\mathcal{A}_E(x) = 0$ for any $x \in E$. Such a monic q-polynomial is called the annihilator polynomial of E.*

Since the coordinates of any error of weight r uniquely span a r-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$, i.e., its r-dimensional support, we have Definition 7.

Definition 7 (Annihilator Polynomial of Vector) *For any $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathcal{S}_r^n$, let $\mathcal{A}_{\boldsymbol{e}}(x)$ is the annihilator polynomial of the support of $\boldsymbol{e}$. There exists a unique annihilator polynomial $\mathcal{A}_{\boldsymbol{e}}(x)$ of q-degree r that vanishes on $\boldsymbol{e}$, i.e., $\mathcal{A}_{\boldsymbol{e}}(e_i) = 0$ for all $i \in [n]$.*

Proposition 2 shows that the dimension of $\mathbb{F}_q$-subspace spanned by some roots of a q-polynomial is upper bounded by its q-degree.

Proposition 2 *Let $f(x)$ be a q-polynomial of q-degree r. Let $\{e_i : f(e_i) = 0, i \in [n]\}$ be a set consisting of any n roots of $f(x)$. Then the dimension of the $\mathbb{F}_q$-subspace spanned by such a set is at most r. In other words, if $\boldsymbol{e} = (e_1, e_2, \ldots, e_n)$, then $\|\boldsymbol{e}\|_{\mathrm{R}} \leq r$.*

C. Matrix Rank and Subspace Dimension

The linear span of a set of vectors $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m$ is denoted by $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_m \rangle$. The row space and the rank of a matrix $\boldsymbol{X} \in \mathbb{F}_q^{m \times n}$ are denoted by $\langle \boldsymbol{X} \rangle$ and $\mathsf{rank}(\boldsymbol{X})$, respectively. By definition, $\mathsf{rank}(\boldsymbol{X}) = \dim\langle \boldsymbol{X} \rangle$. It is well-known that, for any $\boldsymbol{X}, \boldsymbol{Y} \in \mathbb{F}_q^{m \times n}$, any matrices $\boldsymbol{A} \in \mathbb{F}_q^{m \times r}$ and $\boldsymbol{B} \in \mathbb{F}_q^{r \times n}$, any column full-rank matrix $\boldsymbol{S} \in \mathbb{F}_q^{m \times r}$, any row full-rank matrix $\boldsymbol{R} \in \mathbb{F}_q^{\ell \times n}$, and random matrix $\boldsymbol{T} \in \mathbb{F}_q^{r \times \ell}$, we have

$$\max\{\mathsf{rank}(\boldsymbol{X}), \mathsf{rank}(\boldsymbol{Y})\} \leq \mathsf{rank}\left(\begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix}\right) \leq \mathsf{rank}(\boldsymbol{X}) + \mathsf{rank}(\boldsymbol{Y}).$$

$$\mathsf{rank}(\boldsymbol{AB}) = \min\{\mathsf{rank}(\boldsymbol{A}), \mathsf{rank}(\boldsymbol{B})\}.$$

$$\mathsf{rank}(\boldsymbol{STR}) = \mathsf{rank}(\boldsymbol{ST}) = \mathsf{rank}(\boldsymbol{TR}) = \mathsf{rank}(\boldsymbol{T}).$$

Recall that if U and V are subspaces of some fixed vector space, then the sum $U + V = \{u + v \ : \ u \in U, v \in V\}$ is the smallest subspace that contains both U and V. Recall also that $\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$. We also make full use of the fact that $\left\langle \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix} \right\rangle = \langle \boldsymbol{X} \rangle + \langle \boldsymbol{Y} \rangle$ and thus

$$\begin{aligned}\mathsf{rank}\left(\begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix}\right) &= \dim\left(\left\langle \begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix} \right\rangle\right) = \dim\Big(\langle \boldsymbol{X} \rangle + \langle \boldsymbol{Y} \rangle\Big) = \dim\left(\langle \boldsymbol{X} \rangle\right) + \dim\left(\langle \boldsymbol{Y} \rangle\right) - \dim\left(\langle \boldsymbol{X} \rangle \cap \langle \boldsymbol{Y} \rangle\right) \\ &= \mathsf{rank}(\boldsymbol{X}) + \mathsf{rank}(\boldsymbol{Y}) - \dim\Big(\langle \boldsymbol{X} \rangle \cap \langle \boldsymbol{Y} \rangle\Big).\end{aligned}$$

D. The RD and BRD Problems

Rank-based cryptosystems are based on the well-known rank decoding assumption which can be expressed by the generator matrix and the parity-check matrix, respectively. They are called the Rank Decoding (RD) problem and the Rank Syndrome Decoding (RSD) problem, respectively. Their computational versions 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 parity-check 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 $\boldsymbol{s} = \boldsymbol{He}^\top$.

We denote the RD problem and the RSD problem by $\mathsf{RD}_{q,m,n,k,r}$ and $\mathsf{RSD}_{q,m,n,k,r}$, respectively. The hardness of two problems is equivalent. Even if the RD problem is not known to be NP-complete, there is a randomized reduction from the RD problem to an NP-complete problem [20], namely to decoding in the Hamming metric. An RD instance can also be seen as a structured version of the MinRank instance, more precisely, there exists a reduction from the RD problem to the MinRank problem [21]. The MinRank problem was proven NP-complete in [53] and is now ubiquitous in multivariate cryptography.

The BRD problem [23] is a variant of the RD problem and is proposed to improved cryptosystems. The difference mainly consists in the definition of the error $\boldsymbol{e}$. 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 8 (Blockwise Errors [23]) *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 $\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$:

$$\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}} = \left\{(\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_\ell) \in \mathbb{F}_{q^m}^n \ : \ \boldsymbol{e}_i \in \mathcal{S}_{r_i}^{n_i}, \ \dim(\mathrm{Supp}(\boldsymbol{e}_i)) = r_i, \ \dim\left(\sum_{i=1}^{\ell} \mathrm{Supp}(\boldsymbol{e}_i)\right) = \sum_{i=1}^{\ell} \dim\left(\mathrm{Supp}(\boldsymbol{e}_i)\right)\right\}.$$

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

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

From [23] (Section 4), for any $\boldsymbol{e}\in\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$, there are a basis $\boldsymbol{\varepsilon}$ and a coefficient matrix $\boldsymbol{C}$ to determine $\boldsymbol{e}$:

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

where $\boldsymbol{\varepsilon}_i\in\mathbb{F}_{q^m}^{r_i}$, and $\boldsymbol{C}_i\in\mathbb{F}_q^{r_i\times n_i}$ for $i\in[\ell]$ is of rank r_i and is in systematic form whose first r_i columns and first r_i rows form an identity matrix $\boldsymbol{I}_{r_i}$.

The blockwise RD problem is the RD problem finding a blockwise error in $\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$.

Definition 9 (Blockwise RD (BRD) Problem [23]) *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 $\boldsymbol{y}=\boldsymbol{x}\boldsymbol{G}+\boldsymbol{e}$.*

As the RSD problem, we can define the Blockwise RSD (BRSD) problem by using the parity-check matrix of the code $\mathcal{C}$. When $\ell=1$, the BRD and BRSD problems are exactly the RD and RSD problems, respectively. Different from the works [3], [23], we here slightly change the notations of the BRD and BRSD problems. We denote them by $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ and $\mathsf{BRSD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$, respectively. Like the RD and RSD problems, the hardness of two problems is equivalent.

E. The MM Modelings From the RD and BRD Problems

There currently exist combinatorial attacks [27]–[30] and algebraic attacks [29], [31]–[33] on the RD problem. The best algebraic attack on the RD problem and its variants is the MM modeling (or the MM attack). The MM modeling is proposed in [31], improved in [32], and is the most powerful algebraic attack for cryptographic parameters. The MM attack is adapted to the BRD problem in [3], [5], [23]. The MM attack can well exploit the structure of errors and still performs the most powerful algebraic attack for cryptographic parameters. Thus, the MM attack has become a core tool for selecting security parameters and measuring the security strength of rank-based cryptosystems.

The MM Modeling From the RD Problem. The modeling starts from a reduction. Solving the $\mathsf{RD}_{q,m,n,k,r}$ problem defined by a random $[n,k]_{q^m}$-linear code $\mathcal{C}$ is reduced to finding a codeword (i.e., an error in $\mathcal{S}_r^n$) in the $[n,k+1]_{q^m}$ extended code of $\mathcal{C}$.

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 $(k+1)\times n$ generator matrix $\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{G}\end{bmatrix}$. In this way, $\boldsymbol{e}=\begin{pmatrix}1 & -\boldsymbol{x}\end{pmatrix}\begin{bmatrix}\boldsymbol{y}\\ \boldsymbol{G}\end{bmatrix}\in\mathcal{S}_r^n$ is exactly a codeword of $\mathcal{C}_{\boldsymbol{y}}$. Let $\boldsymbol{H}_{\boldsymbol{y}}\in\mathbb{F}_{q^m}^{(n-k-1)\times n}$ be a parity-check matrix of $\mathcal{C}_{\boldsymbol{y}}$. Then solving the RD problem consists in finding an error $\boldsymbol{e}\in\mathcal{S}_r^n$ such that $\boldsymbol{e}\boldsymbol{H}_{\boldsymbol{y}}^\top=\boldsymbol{0}_{n-k-1}$.

Let $\boldsymbol{\varepsilon}\in\mathbb{F}_{q^m}^r$ be a basis of $\boldsymbol{e}$, $\boldsymbol{C}\in\mathbb{F}_q^{r\times n}$ be the coefficients matrix of $\boldsymbol{e}$, and $\boldsymbol{e}=\boldsymbol{\varepsilon}\boldsymbol{C}$. From $\boldsymbol{e}\boldsymbol{H}_{\boldsymbol{y}}^\top=\boldsymbol{0}_{n-k-1}$ and $\boldsymbol{e}=\boldsymbol{\varepsilon}\boldsymbol{C}$, we have $\boldsymbol{\varepsilon}\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top=\boldsymbol{0}_{n-k-1}$. The equation $\boldsymbol{\varepsilon}\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top=\boldsymbol{0}_{n-k-1}$ implies that $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top\in\mathbb{F}_{q^m}^{r\times(n-k-1)}$ is not of row full rank because a non-zero vector $\boldsymbol{\varepsilon}$ belongs to its left kernel. Then all maximal minors $\left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top\right|_{*,J}$ of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ are equal to 0 for $J\subset[n-k-1]$ and $\#J=r$. By the Cauchy-Binet formula, each $\left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top\right|_{*,J}$ can be viewed a non-zero linear combination about all non-zero maximal minors $c_T=|\boldsymbol{C}|_{*,T}$ for $T\subset[n]$ and $\#T=r$. The number of non-zero maximal minors c_T's is $\binom{n}{r}$ and the number of non-zero linear combinations is $\binom{n-k-1}{r}$. One views non-zero c_T's as unknowns and linear combinations as equations, and builds a linear system with $\binom{n}{r}$ unknowns and $\binom{n-k-1}{r}$ equations over $\mathbb{F}_{q^m}$. This builds the MM modeling over $\mathbb{F}_{q^m}$:

$$\left\{\left|\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top\right|_{*,J}=\sum_{T\subset[n],\#T=r}c_T\left|\boldsymbol{H}_{\boldsymbol{y}}^\top\right|_{T,J}=0\ :\ J\subset[n-k-1],\ \#J=r,\ \left|\boldsymbol{H}_{\boldsymbol{y}}^\top\right|_{T,J}\in\mathbb{F}_{q^m}\right\}.\tag{3}$$

One wants to solve c_T's from this linear system to determine $\boldsymbol{C}$. However, the system has many solutions due to $\binom{n-k-1}{r}<\binom{n}{r}$ whereas one wants more equations than unknowns for a unique solution. As $c_T\in\mathbb{F}_q$, to obtain more equations, one then unfolds the coefficients, namely $|\boldsymbol{H}_{\boldsymbol{y}}^\top|_{T,J}$, over $\mathbb{F}_q$ and obtains $m\binom{n-k-1}{r}$ equations. The resulting MM modeling over $\mathbb{F}_q$ includes:

Unknowns: $\binom{n}{r}$ non-zero maximal minors $c_T\in\mathbb{F}_q$,

Equations: $m\binom{n-k-1}{r}$ linearly independent equations over $\mathbb{F}_q$ in all non-zero c_T's.

Once all non-zero c_T's are solved from the MM modeling, one can determine the entries of $\boldsymbol{C}$. This point is associated to the Plücker coordinates in Grassmannian manifold (see Section 3 in [33] for a general description). Finally, one solves $\boldsymbol{\varepsilon}$ and determine $\boldsymbol{e}=\boldsymbol{\varepsilon}\boldsymbol{C}$. Note that we consider the *random* parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ for the extended code $\mathcal{C}_{\boldsymbol{y}}$, instead of a

systematic form.

One must ensure $m\binom{n-k-1}{r} \geq \binom{n}{r}$ such that the MM modeling has the rank $\binom{n}{r}-1$ and has a unique solution.

- When the MM modeling is underdetermined: $m\binom{n-k-1}{r} < \binom{n}{r}$, one uses the hybrid approach. Informally, one guesses the last a columns of $\boldsymbol{C}$, and reduces the number of unknowns to $\binom{n-a}{r}$ such that the modeling is overdetermined and the complexity solving the system is minimal.
- When the MM modeling is overdetermined: $m\binom{n-k-1}{r} \geq \binom{n}{r}$, one uses the puncturing approach. One *tries* to puncture $\mathcal{C}$ on the last p coordinates, obtains the $\mathsf{RD}_{q,m,n-p,k,r}$ problem, and applies the MM modeling to $\mathsf{RD}_{q,m,n-p,k,r}$ such that the obtained modeling remains overdetermined and the complexity solving the system is minimal.

For both two cases, the complexity of solving the $\mathsf{RD}_{q,m,n,k,r}$ problem by the MM modeling is estimated as

$$\begin{cases} \mathcal{O}\left(q^{ar} m\binom{n-k-1}{r}\left(\binom{n-a}{r}\right)^{\omega-1}\right), & m\binom{n-k-1}{r} < \binom{n}{r}, \\ \mathcal{O}\left(m\binom{n-p-k-1}{r}\left(\binom{n-p}{r}\right)^{\omega-1}\right), & m\binom{n-k-1}{r} \geq \binom{n}{r}, \end{cases}$$

where p is a positive integer such that $m\binom{n-p-k-1}{r} \geq \binom{n-p}{r} - 1$ holds and the complexity is minimal, and a is a positive such that $m\binom{n-k-1}{r} \geq \binom{n-a}{r} - 1$ holds and the complexity is minimal.

For the MM modelings from the BRD problem, the main difference is the number of unknowns and independent equations.

The MM Modeling From the BRD Problem [3], [5], [23]. In the $\mathsf{BRD}^{\ell,\boldsymbol{n},\boldsymbol{r}}_{q,m,n,k,r}$ problem, one finds a blockwise error $\boldsymbol{e} \in \mathcal{S}^{\boldsymbol{n}}_{\boldsymbol{r}}$. From Equation (2), since the coefficients matrix $\boldsymbol{C}$ of blockwise error $\boldsymbol{e}$ has the block-diagonal form, the number of non-zero maximal minors is $\prod_{i=1}^{\ell}\binom{n_i}{r_i}$. The modeling includes *at most* $m\binom{n-k-1}{r}$ linearly independent equations.

Currently, the precise number of independent equations remains open in [3], [5], [23]. In [3], [23], authors used the maximal equations $m\binom{n-k-1}{r}$ to bound the number of independent equations for the conservative complexity. In [5], authors estimated the upper bound of independent equations in the special case of $\ell = 2$ (or $\ell = 3$) and $k = n_1 = n_2 = \cdots = n_\ell$. In Section X-B, we further address this open question. We consider the general case for any ℓ, k, and n_i's, and derive a tight upper bound of independent equations. This work must also be for introducing the BP approach to the BRD problem because the BP approach would lead to the general parameters.

Lemma 1 shows that the linear dependence of equations in the MM modeling is independent of the form of the parity-check matrix $\boldsymbol{H_y}$ of the extended code $\mathcal{C}_{\boldsymbol{y}}$. This lemma is used in Remark 2.

Lemma 1 *For the structure of any error, the number of linearly independent equations in the MM modeling is independent of the (systematic or general) form of the parity-check matrix of $\mathcal{C}_{\boldsymbol{y}}$.*

Proof: We consider equations in the MM modeling (Equation (3)). Let P_J be equations obtained from $\boldsymbol{H_y}$ for $J \subset [n-k-1]$ and $\#J = r$, where $\boldsymbol{H_y}$ is any systematic parity-check matrix of $\mathcal{C}_{\boldsymbol{y}}$. Let Q_J be equations obtained from $\overline{\boldsymbol{H}}_{\boldsymbol{y}}$ for $J \subset [n-k-1]$ and $\#J = r$, where $\overline{\boldsymbol{H}}_{\boldsymbol{y}}$ is any general parity-check matrix of $\mathcal{C}_{\boldsymbol{y}}$. There clearly exists an invertible matrix $\boldsymbol{A} \in \mathbb{F}_{q^m}^{(n-k-1)\times(n-k-1)}$ such that $\overline{\boldsymbol{H}}_{\boldsymbol{y}} = \boldsymbol{A}\boldsymbol{H_y}$. For fixed $J \subset [n-k-1]$ and $\#J = r$, by Cauchy-Binet formula, we have

$$\begin{aligned} Q_J = \left|\boldsymbol{C}\overline{\boldsymbol{H}}_{\boldsymbol{y}}^{\top}\right|_{*,J} &= \sum_{T\subset[n],\#T=r} |\boldsymbol{C}|_{*,T}\left|\overline{\boldsymbol{H}}_{\boldsymbol{y}}^{\top}\right|_{T,J} = \sum_{T\subset[n],\#T=r} c_T \left|\overline{\boldsymbol{H}}_{\boldsymbol{y}}\right|_{J,T} \\ &= \sum_{T\subset[n],\#T=r} c_T \sum_{U\subset[n-k-1],\#U=r} |\boldsymbol{A}|_{J,U}\,|\boldsymbol{H_y}|_{U,T} = \sum_{U\subset[n-k-1],\#U=r} |\boldsymbol{A}|_{J,U} P_U. \end{aligned}$$

The last equality shows that Q_J are linear combinations of P_J. Thus, the equations obtained from $\boldsymbol{H_y}$ and $\overline{\boldsymbol{H}}_{\boldsymbol{y}}$ have the same linear dependence. ∎

IV. Our Results on Rank of Moore Matrix

For analyzing the decoding capacity and properties of the EG codes, in this section, we derive some results on the rank of the Moore matrix. We first recall the relation between q-polynomial and Frobenius automorphism.

The q-polynomial is essentially related to Frobenius automorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$. We denote such a Frobenius automorphism by θ:

$$\begin{aligned} \theta: \quad \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m} \\ x &\longmapsto \theta(x) := x^q. \end{aligned}$$

The Frobenius automorphism θ is an $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^m}$. We use its following properties:

- $\forall\ x_1, x_2 \in \mathbb{F}_{q^m}$, $\beta_1, \beta_2 \in \mathbb{F}_q$: $\theta(x_1x_2) = \theta(x_1)\theta(x_2)$, $\theta(\beta_1 x_1 + \beta_2 x_2) = \beta_1\theta(x_1) + \beta_2\theta(x_2)$ (linearity over $\mathbb{F}_q$),

- $\forall\ i \in \mathbb{N}$, $\theta^i(x) = \theta^{i-1}(\theta(x)) = \theta^{i-1}(x^q) = \cdots = \theta\left(x^{q^{i-1}}\right) = x^{q^i}$,
- $\forall\ i \in \mathbb{N}$, θ^i is also an Frobenius automorphism. This is because the set of all Frobenius automorphisms is a cyclic group of order m.

A q-polynomial in variable x can be viewed as a polynomial of θ acting on the variable x. The addition (resp. symbolic product "$\circ$") of two q-polynomials corresponds to the addition (resp. composition "$\bullet$") of two polynomials of θ. Let $a(x) = \sum_i a_i x^{q^i}$ and $b(x) = \sum_i b_i x^{q^i} \in \mathcal{L}[x]$. Let $a(\theta) = \sum_i a_i \theta^i$ and $b(\theta) = \sum_i b_i \theta^i$.

- $a(\theta)(x) = \left(\sum_i a_i \theta^i\right)(x) = \sum_i a_i \theta^i(x) = \sum_i a_i x^{q^i} = a(x)$,
- $(a(\theta) + b(\theta))(x) = \left(\sum_i (a_i + b_i)\,\theta^i\right)(x) = \sum_i (a_i + b_i)\, x^{q^i} = a(x) + b(x)$,
- $(a(\theta) \bullet b(\theta))(x) = a(b(\theta))(x) = a(b(x)) = a(x) \circ b(x)$.

Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. The Frobenius automorphism θ can be applied to $\boldsymbol{x}$ coordinate-wise:

$$\theta(\boldsymbol{x}) = (\theta(x_1), \theta(x_2), \ldots, \theta(x_n)) = (x_1^q, x_2^q, \ldots, x_n^q)\,.$$

Further, for any $i \in \mathbb{N}$, $\theta^i(\boldsymbol{x}) = \left(\theta^i(x_1), \theta^i(x_2), \ldots, \theta^i(x_n)\right) = \left(x_1^{q^i}, x_2^{q^i}, \ldots, x_n^{q^i}\right)$.

Definition 10 *Let $s \in \mathbb{N}$. For any $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_{q^m}^n$, we denote the Moore matrix of order s of $\boldsymbol{e}$ as*

$$\mathbf{Moore}(\boldsymbol{e}, s) = \begin{bmatrix} e_1 & e_2 & \cdots & e_n \\ e_1^q & e_2^q & \cdots & e_n^q \\ \vdots & \vdots & \ddots & \vdots \\ e_1^{q^s} & e_2^{q^s} & \cdots & e_n^{q^s} \end{bmatrix} = \begin{bmatrix} \boldsymbol{e} \\ \theta(\boldsymbol{e}) \\ \vdots \\ \theta^s(\boldsymbol{e}) \end{bmatrix} \in \mathbb{F}_{q^m}^{(s+1)\times n}.$$

Proposition 3 *Let $s \in \mathbb{N}$ and $\boldsymbol{e} \in \mathcal{S}_r^n$. Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^r$ be a basis of* $\mathrm{Supp}(\boldsymbol{e})$. *Let $\mathbf{CM}(\boldsymbol{e}) \in \mathbb{F}_q^{r\times n}$ of rank r be the coefficient matrix of $\boldsymbol{e}$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e} = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e})$. Then $\mathbf{Moore}(\boldsymbol{e}, s) = \mathbf{Moore}(\boldsymbol{\varepsilon}, s) \cdot \mathbf{CM}(\boldsymbol{e})$.*

Proof: Since for any $i \in \mathbb{N}$, θ^i is an $\mathbb{F}_q$-automorphism, $\theta^i(\boldsymbol{e}) = \theta^i\left(\boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e})\right) = \theta^i(\boldsymbol{\varepsilon})\mathbf{CM}(\boldsymbol{e})$. Thus, we have

$$\mathbf{Moore}(\boldsymbol{e}, s) = \begin{bmatrix} \boldsymbol{e} \\ \theta(\boldsymbol{e}) \\ \vdots \\ \theta^s(\boldsymbol{e}) \end{bmatrix} = \begin{bmatrix} \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e}) \\ \theta(\boldsymbol{\varepsilon})\mathbf{CM}(\boldsymbol{e}) \\ \vdots \\ \theta^s(\boldsymbol{\varepsilon})\mathbf{CM}(\boldsymbol{e}) \end{bmatrix} = \mathbf{Moore}(\boldsymbol{\varepsilon}, s) \cdot \mathbf{CM}(\boldsymbol{e}).$$

■

Proposition 4 *Let $s \in \mathbb{N}$. If $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in \mathbb{F}_{q^m}^m$ is a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$, then the rank of $\mathbf{Moore}(\boldsymbol{\alpha}, s)$ satisfies:*

$$\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\alpha}, s)\right) = \begin{cases} s+1, & \text{if } s < m; \\ m, & \text{if } s \geq m. \end{cases} \tag{4}$$

Proof: By the definition of Moore matrix in Definition 10,

$$\mathbf{Moore}(\boldsymbol{\alpha}, s) = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^s} & \alpha_2^{q^s} & \cdots & \alpha_m^{q^s} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\alpha} \\ \theta(\boldsymbol{\alpha}) \\ \vdots \\ \theta^s(\boldsymbol{\alpha}) \end{bmatrix}.$$

- **Case** $s < m$**:** If $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, s)) \leq s$, then there exist a non-zero vector $(a_0, a_1, \ldots, a_s) \in \mathbb{F}_{q^m}^s$ such that $\sum_{i=0}^s a_i \theta^i(\boldsymbol{\alpha}) = 0$. This means that there exist a q-polynomial $\sum_{i=0}^s a_i x^{q^i}$ of q-degree $\leq s$ that vanishes on $\boldsymbol{\alpha}$. Since $\|\boldsymbol{\alpha}\|_{\mathrm{R}} = m$, by Definition 7, the q-degree of annihilator polynomial of $\boldsymbol{\alpha}$ must be m. This leads a contradiction, thus $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, s)) = s+1$.
- **Case** $s = m$**:** By the case of $s < m$, we have $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m-1)) = m$, further

$$\begin{aligned} \mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m)) &= \mathsf{rank}\left(\begin{bmatrix} \mathbf{Moore}(\boldsymbol{\alpha}, m-1) \\ \theta^m(\boldsymbol{\alpha}) \end{bmatrix}\right) \\ &\geq \mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m-1)) = m. \end{aligned}$$

  Moreover, $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m)) \leq m$ because the columns of $\mathbf{Moore}(\boldsymbol{\alpha}, m)$ is m. Thus, $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m)) = m$.
- **Case** $s > m$**:** By the case of $s = m$, we have $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m)) = m$, further

$$\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, s)) = \mathsf{rank}\left(\begin{bmatrix} \mathbf{Moore}(\boldsymbol{\alpha}, m) \\ \theta^{m+1}(\boldsymbol{\alpha}) \\ \vdots \\ \theta^s(\boldsymbol{\alpha}) \end{bmatrix}\right) \geq \mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, m)) = m.$$

Similarly, $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, s)) \leq m$ because the columns of $\mathbf{Moore}(\boldsymbol{\alpha}, s)$ is m. Thus, $\mathsf{rank}(\mathbf{Moore}(\boldsymbol{\alpha}, s)) = m$. Finally, we obtain a conclusion in Equation (4). ■

Corollary 1 *Let $s \in \mathbb{N}$. Let $\boldsymbol{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r) \in \mathbb{F}_{q^m}^r$ be a basis of any r-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$. Then the rank of $\mathbf{Moore}(\boldsymbol{\varepsilon}, s)$ satisfies:*

$$\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, s)\right) = \begin{cases} s+1, & \text{if } s < r; \\ r, & \text{if } s \geq r. \end{cases} \tag{5}$$

Proposition 5 *Let $s \in \mathbb{N}$. For any $\boldsymbol{e} \in \mathcal{S}_r^n$, the rank of $\mathbf{Moore}(\boldsymbol{e}, s)$ satisfies:*

$$\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{e}, s)\right) = \begin{cases} s+1, & \text{if } s < r; \\ r, & \text{if } s \geq r. \end{cases} \tag{6}$$

Proof: Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^r$ be a basis of $\mathrm{Supp}(\boldsymbol{e})$. Let $\mathbf{CM}(\boldsymbol{e}) \in \mathbb{F}_q^{r \times n}$ of rank r be the coefficient matrix of $\boldsymbol{e}$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e} = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e})$. By Proposition 3, for any $s \in \mathbb{N}$, $\mathbf{Moore}(\boldsymbol{e}, s) = \mathbf{Moore}(\boldsymbol{\varepsilon}, s) \cdot \mathbf{CM}(\boldsymbol{e})$. Since $\mathbf{CM}(\boldsymbol{e}) \in \mathbb{F}_q^{r \times n}$ is a row full-rank matrix, we have

$$\mathsf{rank}(\mathbf{Moore}(\boldsymbol{e}, r)) = \mathsf{rank}(\mathbf{Moore}(\boldsymbol{\varepsilon}, s)) = \begin{cases} s+1, & \text{if } s < r; \\ r, & \text{if } s \geq r. \end{cases}$$

The last equality uses Corollary 1. ■

V. Decoding EG Codes to Solving LR Problem

In this section, we recall the definition of the EG codes [12], and reduce decoding EG Codes to solving LR problem. We slightly relax the conditions with a wider parameters region: the weight of a generator $\leq \min\{m, n\}$, which covers Gabidulin codes.

Definition 11 (EG Codes) *Let q, m, n, t, k be integers and $k \leq t \leq \min\{n, m\}$. Let $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be the generator of weight t. An EG code of dimension k and length n generated by $\boldsymbol{g}$ is defined as*

$$\mathrm{EG}_k(\boldsymbol{g}) = \Big\{ f(\boldsymbol{g}) = (f(g_1), f(g_2), \ldots, f(g_n)) \ : \ f(x) \in \mathcal{L}_{\leq k-1}[x] \Big\}.$$

The dimension and minimal distance of the EG codes are formally presented in Propositions 6 and 7.

Proposition 6 *The dimension of the $\mathrm{EG}_k(\boldsymbol{g})$ codes is k.*

Proof: Given any $f(x) \in \mathcal{L}_{\leq k-1}[x]$, let $f(x) = \sum_{i=0}^{k-1} f_i x^{q^i}$. Then the codeword $f(\boldsymbol{g})$ can be expressed as

$$f(\boldsymbol{g}) = (f(g_1), f(g_2), \ldots, f(g_n)) = (f_0, f_1, \ldots, f_{k-1})\, \mathbf{Moore}(\boldsymbol{g}, k-1).$$

Let $\boldsymbol{G} = \mathbf{Moore}(\boldsymbol{g}, k-1)$. Since $k - 1 < t \leq \min\{n, m\}$, from Proposition 5, we have $\mathsf{rank}(\boldsymbol{G}) = k$. Thus, the dimension of the code is k, and $\boldsymbol{G}$ is its generator matrix. ■

Proposition 7 *The minimal distance of the $\mathrm{EG}_k(\boldsymbol{g})$ codes is $t - k + 1$.*

Proof: Let $\boldsymbol{G} = \mathbf{Moore}(\boldsymbol{g}, k-1)$ be a generator matrix of the $\mathrm{EG}_k(\boldsymbol{g})$ codes. Assume that the first t coordinates of $\boldsymbol{g}$ are linearly independent; otherwise, performing an invertible matrix. Let $\boldsymbol{\tau} \in \mathbb{F}_{q^m}^t$ be a basis of $\mathrm{Supp}(\boldsymbol{g})$. Let $\mathbf{CM}(\boldsymbol{g}) \in \mathbb{F}_q^{t \times n}$ of rank t be the coefficient matrix of $\boldsymbol{g}$ under $\boldsymbol{\tau}$ such that $\boldsymbol{g} = \boldsymbol{\tau}\mathbf{CM}(\boldsymbol{g})$. There exists an invertible matrix $\boldsymbol{P} \in \mathbb{F}_q^{n \times n}$ such that the last $n - t$ columns of $\mathbf{CM}(\boldsymbol{g})$ are zeros, i.e.,

$$\mathbf{CM}(\boldsymbol{g})\boldsymbol{P} = [\boldsymbol{V} \ \ \mathbf{0}_{t \times n-t}], \qquad \boldsymbol{V} \in \mathbb{F}_q^{t \times t}.$$

Further there exists a vector $\boldsymbol{g}' = (g'_1, g'_2, ..., g'_t, 0, ..., 0) \in \mathbb{F}_{q^m}^n$ such that $\boldsymbol{g}' = \boldsymbol{\tau}\mathbf{CM}(\boldsymbol{g})\boldsymbol{P} = \boldsymbol{g}\boldsymbol{P}$ and $(g'_1, g'_2, ..., g'_t) = \boldsymbol{\tau}\boldsymbol{V}$.

We have $\boldsymbol{G}\boldsymbol{P} = \mathbf{Moore}(\boldsymbol{g}, k-1)\boldsymbol{P} = \mathbf{Moore}(\boldsymbol{g}\boldsymbol{P}, k-1) = \mathbf{Moore}(\boldsymbol{g}', k-1)$. For rank metric codes over $\mathbb{F}_{q^m}$, the invertible matrix $\boldsymbol{P}$ over the basis field is an isometry. Then the EG codes defined by $\boldsymbol{G}$ are equivalent to the codes defined by $\boldsymbol{G}\boldsymbol{P}$. The first t columns of $\boldsymbol{G}\boldsymbol{P}$ define a Gabidulin code of dimension k and length t with the minimal distance $t - k + 1$. Thus, the EG codes have the minimal distance $t - k + 1$. ■

Next, we reduce the decoding EG codes to solving the LR problem.

A. From Decoding EG Codes to Solving NLR Problem

Given the EG codes in Definition 11, we assume that the message q-polynomial is $f(x) \in \mathcal{L}_{\leq k-1}[x]$, the error occurring at the channel is $\boldsymbol{e}$ and $\|\boldsymbol{e}\|_{\mathrm{R}} \leq r$, the received word is $\boldsymbol{y} = f(\boldsymbol{g}) + \boldsymbol{e}$. The aim of decoding EG codes is to recover $\boldsymbol{e}$ and $f(x)$ from $\boldsymbol{y}$. We first define the decoding EG code problem (Definition 12).

Definition 12 (Decoding EG Code Problem $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$)
Input : $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ *and* $\|\boldsymbol{g}\|_{\mathrm{R}} = t$; $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^m}^n$.
Output : $f(x) \in \mathcal{L}[x]$ *and* $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ *such that:* 1. $\deg_q f(x) \leq k-1$; 2. $\boldsymbol{e} \neq \boldsymbol{0}_n$ *and* $\|\boldsymbol{e}\|_{\mathrm{R}} \leq r$; 3. $\boldsymbol{y} = f(\boldsymbol{g}) + \boldsymbol{e}$.

From Definition 7, we known that for any $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of weight r, there exists a unique annihilator polynomial $\mathcal{A}_{\boldsymbol{e}}(x)$ of q-degree r that vanishes on $\boldsymbol{e}$, i.e., $\mathcal{A}_{\boldsymbol{e}}(e_i) = 0$ for all $i \in [n]$. Thus, it is natural to transform the $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ problem into the Non Linear Reconstruction (NLR) problem (Definition 13).

Definition 13 (Non Linear Reconstruction Problem $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$)
Input : $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ *and* $\|\boldsymbol{g}\|_{\mathrm{R}} = t$; $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^m}^n$.
Output : $f(x), v(x) \in \mathcal{L}[x]$ *such that:* 1. $\deg_q f(x) \leq k-1$; 2. $v(x) \neq 0$ *and* $\deg_q v(x) \leq r$; 3. $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$.

Theorem 1 shows that for decoding EG code, it is sufficient to solve the NLR problem, and the maximum r solved in the NLR problem determines the decoding capacity of the EG codes.

Theorem 1 *Solving the* $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ *problem can be reduced to solving the* $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ *problem.*

Proof: Let $f(x)$ and $v(x)$ be a solution of $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$. Then $\deg_q f(x) \leq k-1$, $v(x) \neq 0$, $\deg_q v(x) \leq r$, and $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$. From $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$, we have

$$v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g}) \implies v(\boldsymbol{y}) = v(f(\boldsymbol{g})) \implies v(\boldsymbol{y} - f(\boldsymbol{g})) = \boldsymbol{0}_n.$$

We set $\boldsymbol{e} = \boldsymbol{y} - f(\boldsymbol{g}) \neq \boldsymbol{0}_n$ and have $v(\boldsymbol{e}) = \boldsymbol{0}_n$. Since $\deg_q v(x) \leq r$, from Proposition 2, we have $\|\boldsymbol{e}\|_{\mathrm{R}} \leq r$. This means that $f(x)$ and $\boldsymbol{e}$ are a solution to $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$. ■

B. From the NLR Problem to the LR Problem

A naive way to solve the NLR problem is that viewing the coefficients of $v(x)$ and $f(x)$ as two groups of unknowns, respectively, then solving a system obtained from the equation $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$. Since the related equation involves products of two groups of unknowns, one has to solve a multivariate system over $\mathbb{F}_{q^m}$. However, solving a multivariate system is an NP-hard problem on average.

Facing this challenge, to find more solvable instances, we adapt the linearized technique in [13], [17] to our NLR problem. We view $v(x) \circ f(x)$ as a new unknown q-polynomial $u(x)$ of q-degree $\leq k+r-1$, and build a linear system with unknowns in the coefficients of $v(x)$ and $u(x)$. Once $v(x)$ and $u(x)$ are solved, we can obtain $f(x)$ by left division. At this time, solving the NLR problem is reduced to solving the Linear Reconstruction (LR) problem in Definition 14.

Definition 14 (Linear Reconstruction Problem $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$)
Input : $\boldsymbol{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ *and* $\|\boldsymbol{g}\|_{\mathrm{R}} = t$; $\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{q^m}^n$.
Output : $v(x), u(x) \in \mathcal{L}[x]$ *such that:* 1. $v(x) \neq 0$ *and* $\deg_q v(x) \leq r$; 2. $u(x) \leq k+r-1$; 3. $v(\boldsymbol{y}) = u(\boldsymbol{g})$.

A solution $(f(x), v(x))$ of $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ clearly gives a solution $(v(x), v(x) \circ f(x))$ of $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$. However, the converse argument is tricky. The proof of converse argument depends on specific methods solving the LR problem. For solving this LR problem, there mainly exist two pioneering and classical methods [13], [17]: Gaussian elimination and Welch-Berlekamp like algorithm.

We start with Gaussian elimination. Solving the $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$ problem by Gaussian elimination consists in solving a linear system induced from $v(\boldsymbol{y}) = u(\boldsymbol{g})$:

$$\boldsymbol{A}\boldsymbol{x}^{\top} = \boldsymbol{0}_n \tag{7}$$

where

$$\boldsymbol{A} = \begin{bmatrix} y_1 & y_1^q & \cdots & y_1^{q^r} & g_1 & g_1^q & \cdots & g_1^{q^{k+r-1}} \\ y_2 & y_2^q & \cdots & y_2^{q^r} & g_2 & g_2^q & \cdots & g_2^{q^{k+r-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ y_n & y_n^q & \cdots & y_n^{q^r} & g_n & g_n^q & \cdots & g_n^{q^{k+r-1}} \end{bmatrix} = \begin{bmatrix} \mathbf{Moore}(\boldsymbol{y}, r)^{\top} & \mathbf{Moore}(\boldsymbol{g}, k+r-1)^{\top} \end{bmatrix}. \tag{8}$$

In this case, to deal with the converse argument: A solution $(v(x), u(x))$ of $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$ can give a solution $(f(x), v(x))$ of $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ by the left division $f(x) = v(x) \setminus u(x)$, we show that:

- The vector consisting of the coefficients of $v(x)$ and $-v(x) \circ f(x)$ must be included in the right kernel of $\boldsymbol{A}$ (see Proposition 8);

- If the right kernel of $\boldsymbol{A}$ is of dimension 1, then the LR problem can be solved up to the largest q-degree (see Theorem 2).
- The condition and probability that the right kernel of $\boldsymbol{A}$ is of dimension 1 (see Theorem 3).

We here extensively analyze the right kernel of the linear system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$ to prove the converse argument and develop decodable parameters. We first describe the technical differences with the previous work [13], [17] for the proof of the converse argument and recall some left problems.

For the proof of converse argument, a careful reader may ask why not adapt the ideas of Theorem 6 in [13] (or Proposition 2 in [17]) to the parameters of the EG codes? Our answer is that it is infeasible. Note that, to decode by solving the LR problem in the rank setting, authors in [13], [17] actually presented two pioneering and classical methods: Gaussian elimination and Welch-Berlekamp like algorithm. The reasons are as follows:

> Theorem 6 in [13] (or Proposition 2 in [17]) is proven from the perspective of roots of q-polynomial. Specifically, they use Fundamental Theorem of Algebra for q-polynomials: If a q-polynomial of q-degree $\leq n-1$ vanishes on n $\mathbb{F}_q$-linearly independent elements, then the q-polynomial must be zero q-polynomial. The conclusions only hold for the conditions $m \geq n = t$ and $r \leq \lfloor \frac{n-k}{2} \rfloor$ (i.e., parameters of Gabidulin codes).

Even if the ideas of Theorem 6 in [13] (or Proposition 2 in [17]) are forcibly adapted to the parameters of the EG codes, it would also be hard to estimate DFR.

Moreover, Theorem 6 in [13] (or Proposition 2 in [17]) allows well prove the converse argument in the case where Welch-Berlekamp like algorithm is applied to solve the LR problem. The conclusion seems only support that Welch-Berlekamp like algorithm is deterministic because the proofs of Theorem 6 (or Proposition 2) and the design of Welch-Berlekamp like algorithm are almost made from the perspective of roots of q-polynomial. In the case where Gaussian elimination is applied to solve the LR problem, the decoding performance such as DFR must be made by strictly analyzing the right kernel of the linear system. This is also necessary because the different methods could lead to different DFR.

However, analyzing the right kernel of the linear system is rather cumbersome, which is evaded and left in [13], [14], [17]. As the question left in [14] (below Proposition 1): "Now we investigate the question: when is the system of dimension 1?" The authors there provided a proof only for a specific case where the number of columns in the system equals the number of rows plus one. Again, a careful reader could also note that the works [13], [17] (Algorithm 1 [13], Decoding by Gaussian elimination) omitted two crucial problems:

- How to decode the smaller errors?
- What the sufficient and necessary condition of successful decoding is?

For the latter, the authors only assume the existence of non-zero right kernel. Our conclusion shows that this is not the case (see Subsection VI-D). And if our heuristic argument (in Theorem 3) deriving DFR is invalid, then decoding Gabidulin codes by Gaussian elimination would not be deterministic (Theorem 8). This challenges the well-known conclusion: decoding Gabidulin codes is deterministic, which has stood for about 40 years.

It is also because the authors in [13], [14], [17] did not deal with the right kernel of the linear system that many decodable parameters are missed and the EG codes are missed. We will directly analyze the right kernel of the linear system and try to answer the above open questions and develop decodable parameters.

Proposition 8 *Let $f(x)$ and $v(x)$ be a solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem defined in Definition 13. Let $\boldsymbol{A}$ be an $n \times (k+2r+1)$ matrix defined in Equation (8). The solution space of the system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$ must contain a vector consisting of the coefficients of $v(x)$ and $-v(x) \circ f(x)$.*

Proof: From Definition 13, we known that if $f(x)$ and $v(x)$ are the solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem, then $\deg_q f(x) \leq k-1$, $v(x) \neq 0$, $\deg_q v(x) \leq r$, and $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$. Let $f(x) = \sum_{i=0}^{k-1} f_i x^{q^i}$ and $v(x) = \sum_{i=0}^{r} v_i x^{q^i}$. Let $u(x) = v(x) \circ f(x) = \sum_{i=0}^{k+r-1} u_i x^{q^i}$.

From $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g}) \iff v(\boldsymbol{y}) = v(f(\boldsymbol{g})) \iff v(\boldsymbol{y} - f(\boldsymbol{g})) = \boldsymbol{0}_n$, one can check:

$$\mathbf{Moore}(\boldsymbol{y} - f(\boldsymbol{g}), r)^\top (v_0, v_1, \ldots, v_r)^\top = \boldsymbol{0}_n \tag{9}$$

$$\iff$$

$$\left[\mathbf{Moore}(\boldsymbol{y}, r)^\top \quad \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top\right] \left[\frac{\boldsymbol{I}_{(r+1)\times(r+1)}}{-\mathbf{PM}(f(x), r)}\right] (v_0, v_1, \ldots, v_r)^\top = \boldsymbol{0}_n \tag{10}$$

$$\iff$$

$$\underbrace{\left[\mathbf{Moore}(\boldsymbol{y}, r)^\top \quad \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top\right]}_{=\boldsymbol{A} \in \mathbb{F}_{q^m}^{n \times (k+2r+1)}} (v_0, v_1, \ldots, v_r, -u_0, -u_1, \ldots, -u_{k+r-1})^\top = \boldsymbol{0}_n. \tag{11}$$

From Equation (11), we can observe that the vector $(v_0, v_1, \ldots, v_r, -u_0, -u_1, \ldots, -u_{k+r-1})$ consisting of the coefficients of $v(x)$ and $-v(x) \circ f(x)$ must belong to the solution space of the linear system (7). ■

Theorem 2 *If the dimension of the right kernel of matrix $\boldsymbol{A}$ defined in Equation (8) is 1, then the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem in Definition 13 can be solved up to q-degree r.*

Proof: If the dimension of the right kernel of $\boldsymbol{A}$ is 1, then the solution to the linear system (7): $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$ is unique up to a multiplicative factor in $\mathbb{F}_{q^m}$. Let $\boldsymbol{b} = (b_0, b_1, \ldots, b_{k+2r})$ be this unique solution. We set $v'(x) = \sum_{i=0}^{r} b_i x^{q^i}$ and $u'(x) = \sum_{i=0}^{k+r-1} b_{i+r+1} x^{q^i}$. Next, we show that $v'(x)$ and $-v'(x) \setminus u'(x)$ are the solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem.

From Definition 13, if $f(x)$ and $v(x)$ is a solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem, then $\deg_q f(x) \le k-1$, $v(x) \neq 0$, $\deg_q v(x) \le r$, and $v(\boldsymbol{y}) = (v \circ f)(\boldsymbol{g})$. From Proposition 8, the vector consisting of the coefficients of $v(x)$ and $-v(x) \circ f(x)$ must belong to the solution space of the linear system (7). This means that there exists a non-zero $\beta \in \mathbb{F}_{q^m}$ such that $v'(x) = \beta \cdot v(x)$ and $u'(x) = -\beta \cdot v(x) \circ f(x)$. By left division, we have $f(x) = -v'(x) \setminus u'(x)$. It is easy to check that $v'(x) \neq 0$, $\deg_q v'(x) = \deg_q v(x) \le r$, and $v'(\boldsymbol{y}) = (v' \circ f)(\boldsymbol{g})$. Thus, $v'(x)$ and $-v'(x) \setminus u'(x)$ are exactly the solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem. ■

Theorem 2 shows that when the right kernel (denote as $\mathsf{kernel}(\boldsymbol{A})$) of $\boldsymbol{A}$ is of dimension 1, any non-zero element can determine the solution to the $\mathsf{NLR}(\boldsymbol{g}, \boldsymbol{y})$ problem for the largest q-degree r. Further, by Theorem 1, the $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ problem is solved up to errors of weight r.

At this point, we prove the converse argument and obtain decoding EG codes can perfectly reduced to solving the LR problem by Gaussian elimination. As described, the solved largest q-degree r by solving the LR problem determines decoding errors of the maximal weight r for the EG codes. The remaining issue is what is the largest q-degree r? To this end, we next must analyze when the right kernel of $\boldsymbol{A}$ is of dimension 1.

VI. Decoding EG Codes

In this section, we analyze the right kernel of the linear system (7), analyze decoding failure rate and decoding capacity, and give the decoding algorithm of the EG codes.

A. Dimension of Right Kernel of the System (7)

First, we argue that $\dim(\mathsf{kernel}(\boldsymbol{A})) > 0$ for any $\boldsymbol{g}$ and $\boldsymbol{y}$, that is, there must exist a non-zero element in $\mathsf{kernel}(\boldsymbol{A})$. By Propositions 9 and 10, we get $\mathsf{rank}(\boldsymbol{A}) \le k + 2r$. Since $\mathsf{rank}(\boldsymbol{A}) + \dim(\mathsf{kernel}(\boldsymbol{A})) = k + 2r + 1$, we must have $\dim(\mathsf{kernel}(\boldsymbol{A})) \ge 1$. Proposition 9 is a key conclusion which greatly facilitates analysis of the right kernel.

Proposition 9 *Let $f(x)$ and $\boldsymbol{e}$ be the solution to the $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ problem defined in Definition 12. Then the matrix $\boldsymbol{A}$ defined in Equation (8) is equivalent to an $n \times (k + 2r + 1)$ matrix $\boldsymbol{B}$ defined in Equation (12), where*

$$\boldsymbol{B} = \left[\begin{array}{cc} \mathbf{Moore}(\boldsymbol{e}, r)^\top & \mathbf{Moore}(\boldsymbol{g}, k + r - 1)^\top \end{array} \right]. \tag{12}$$

Proof: From Definition 12, if $f(x)$ and $\boldsymbol{e}$ are the solution to the $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ problem, then $\deg_q f(x) \le k - 1$, $\boldsymbol{e} \neq \boldsymbol{0}_n$, $\|\boldsymbol{e}\|_{\mathrm{R}} \le r$, and

$$\boldsymbol{y} = f(\boldsymbol{g}) + \boldsymbol{e} \iff \boldsymbol{y} - f(\boldsymbol{g}) = \boldsymbol{e} \iff y_i - f(g_i) = e_i \text{ for all } i \in [n].$$

Combining Equation (10), we have

$$\begin{aligned} &\left[\mathbf{Moore}(\boldsymbol{y}, r)^\top \quad \mathbf{Moore}(\boldsymbol{g}, k + r - 1)^\top\right] \left[\begin{array}{c|c} \boldsymbol{I}_{(r+1)\times(r+1)} & \boldsymbol{0}_{(r+1)\times(k+r)} \\ \hline -\mathbf{PM}(f(x), r) & \boldsymbol{I}_{(k+r)\times(k+r)} \end{array}\right] \\ = &\left[\mathbf{Moore}(\boldsymbol{y} - f(\boldsymbol{g}), r)^\top \quad \mathbf{Moore}(\boldsymbol{g}, k + r - 1)^\top\right] = \boldsymbol{B}. \end{aligned}$$

■

Proposition 10 *For any uniform and random error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = r$, if $k + r \le t \le \min\{n, m\}$ and $k + 2r \le n$, then $\mathsf{rank}(\boldsymbol{B}) \le k + 2r$.*

Proof: We consider the rank of $\boldsymbol{B}^\top$. Let

$$\boldsymbol{B}_1 = \mathbf{Moore}(\boldsymbol{e}, r), \quad \boldsymbol{B}_2 = \mathbf{Moore}(\boldsymbol{g}, k + r - 1), \quad \boldsymbol{B}^\top = \left[\begin{array}{c} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{array}\right].$$

Since $k + r \le t$, from Proposition 5, we have $\mathsf{rank}(\boldsymbol{B}_1) = r$ and $\mathsf{rank}(\boldsymbol{B}_2) = k + r$. Thus,

$$\mathsf{rank}(\boldsymbol{B}) = \mathsf{rank}\left(\boldsymbol{B}^\top\right) = \mathsf{rank}\left(\left[\begin{array}{c} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{array}\right]\right) \le \mathsf{rank}(\boldsymbol{B}_1) + \mathsf{rank}(\boldsymbol{B}_2) = k + 2r.$$

■

Propositions 9 and 10 show $\mathsf{rank}(\boldsymbol{A}) = \mathsf{rank}(\boldsymbol{B}) \leq k + 2r$. Since $\mathsf{rank}(\boldsymbol{A}) + \dim(\mathsf{kernel}(\boldsymbol{A})) = k + 2r + 1$, we must have $\dim(\mathsf{kernel}(\boldsymbol{A})) \geq 1$. Thus, there must exist a non-zero element in $\mathsf{kernel}(\boldsymbol{A})$. Next, we analyze when $\mathsf{kernel}(\boldsymbol{A})$ is one-dimensional, and derive the DFR and the decoding capacity.

B. Decoding Failure Rate for the Largest r

The decoding failure depends on the event $\dim(\mathsf{kernel}(\boldsymbol{A})) \neq 1$. In Subsection VI-A, we have got $\dim(\mathsf{kernel}(\boldsymbol{A})) \geq 1$ due to $\mathsf{rank}(\boldsymbol{A}) \leq k + 2r$ and $\mathsf{rank}(\boldsymbol{A}) + \dim(\mathsf{kernel}(\boldsymbol{A})) = k + 2r + 1$. Thus, the DFR depends on the probability of $\dim(\mathsf{kernel}(\boldsymbol{A})) > 1$, which is equivalent to $\mathsf{rank}(\boldsymbol{A}) < k + 2r$. Since $\mathsf{rank}(\boldsymbol{A}) = \mathsf{rank}(\boldsymbol{B})$ (see Proposition 9), we now analyze the probability of $\mathsf{rank}(\boldsymbol{B}) < k + 2r$.

Theorem 3 *For any uniform and random error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = r$, if $k + r \leq t \leq \min\{n, m\}$ and $k + 2r \leq n$, then*

$$\Pr[\mathsf{rank}(\boldsymbol{B}) < k + 2r] \leq \gamma_q \cdot q^{a(t+r-a-n)}, \tag{13}$$

where $a = t - k - r + 1$.

Proof: We consider $\boldsymbol{B}^\top$ and estimate $\Pr[\mathsf{rank}(\boldsymbol{B}^\top) < k+2r]$. Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^r$ be a basis of $\mathrm{Supp}(\boldsymbol{e})$. Let $\mathbf{CM}(\boldsymbol{e}) \in \mathbb{F}_q^{r\times n}$ of rank r be the coefficient matrix of $\boldsymbol{e}$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e} = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e})$. Let $\boldsymbol{\gamma} \in \mathbb{F}_{q^m}^t$ be a basis of $\mathrm{Supp}(\boldsymbol{g})$. Let $\mathbf{CM}(\boldsymbol{g}) \in \mathbb{F}_q^{t\times n}$ of rank t be the coefficient matrix of $\boldsymbol{g}$ under $\boldsymbol{\gamma}$ such that $\boldsymbol{g} = \boldsymbol{\gamma}\mathbf{CM}(\boldsymbol{g})$. Following Definition 10 and Proposition 3,

$$\begin{aligned}
\boldsymbol{B}^\top &= \left[\begin{array}{c} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{array}\right] = \left[\frac{\mathbf{Moore}(\boldsymbol{e}, r)}{\mathbf{Moore}(\boldsymbol{g}, k + r - 1)}\right] = \left[\frac{\mathbf{Moore}(\boldsymbol{\varepsilon}, r) \cdot \mathbf{CM}(\boldsymbol{e})}{\mathbf{Moore}(\boldsymbol{\gamma}, k + r - 1) \cdot \mathbf{CM}(\boldsymbol{g})}\right] \\
&= \underbrace{\left[\begin{array}{c|c} \mathbf{Moore}(\boldsymbol{\varepsilon}, r) & \mathbf{0}_{(r+1)\times t} \\ \hline \mathbf{0}_{(k+r)\times r} & \mathbf{Moore}(\boldsymbol{\gamma}, k + r - 1) \end{array}\right]}_{:=\boldsymbol{L}\in\mathbb{F}_{q^m}^{(k+2r+1)\times(r+t)}} \underbrace{\left[\frac{\mathbf{CM}(\boldsymbol{e})}{\mathbf{CM}(\boldsymbol{g})}\right]}_{:=\boldsymbol{M}\in\mathbb{F}_q^{(r+t)\times n}}.
\end{aligned} \tag{14}$$

By Corollary 1, we have $\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) = r$, and as $k + r - 1 < t$, $\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\gamma}, k + r - 1)\right) = k + r$. Thus,

$$\mathsf{rank}(\boldsymbol{L}) = \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) + \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\gamma}, k + r - 1)\right) = k + 2r \leq n.$$

As $\mathsf{rank}(\boldsymbol{B}^\top) \leq \min\{\mathsf{rank}(\boldsymbol{L}), \mathsf{rank}(\boldsymbol{M})\}$ and $\boldsymbol{M} \in \mathbb{F}_q^{(t+r)\times n}$ is defined in the basis field $\mathbb{F}_q$, we have an **Heuristic Argument**: if $\mathsf{rank}(\boldsymbol{L}) = k+2r$ and $\mathsf{rank}(\boldsymbol{M}) \geq k+2r$, then $\mathsf{rank}\left(\boldsymbol{B}^\top\right) = k+2r$. We also ran a lot of experiments to verify this argument. Please see the formal **Heuristic Argument** after the proof. Hence, we have

$$\mathsf{rank}\left(\boldsymbol{B}^\top\right) < k + 2r \implies \mathsf{rank}(\boldsymbol{M}) < k + 2r. \tag{15}$$

Moreover,

$$\begin{aligned}
\mathsf{rank}(\boldsymbol{M}) &= \mathsf{rank}\left[\begin{array}{c} \mathbf{CM}(\boldsymbol{e}) \\ \mathbf{CM}(\boldsymbol{g}) \end{array}\right] = \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle + \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big) \\
&= \mathsf{rank}\left(\mathbf{CM}(\boldsymbol{e})\right) + \mathsf{rank}\left(\mathbf{CM}(\boldsymbol{g})\right) - \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big) \\
&= r + t - \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big).
\end{aligned}$$

Let $\Delta = \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big)$, we have

$$\mathsf{rank}(\boldsymbol{M}) < k + 2r \iff \Delta > t - k - r. \tag{16}$$

Let $a = t - k - r + 1$. Finally, combining Equations (15) and (16), we have:

- When $a \leq \min\{t, r\}$,

$$\begin{aligned}
&\Pr\left[\mathsf{rank}\left(\boldsymbol{B}^\top\right) < k + 2r\right] \leq \Pr[\mathsf{rank}(\boldsymbol{M}) < k + 2r] = \Pr\left[\Delta > t - k - r\right] \\
&= \sum_{i=a}^{\min\{t,r\}} \Pr\left[\Delta = i\right] \approx \Pr\left[\Delta = a\right] \leq \gamma_q \cdot q^{a(t+r-a-n)}.
\end{aligned} \tag{17}$$

The first inequality "$\leq$" due to "$\implies$" of Equation (15). The second equation "$=$" due to "$\iff$" of Equation (16). The approximation "$\approx \Pr\left[\Delta = a\right]$" is natural. By the probability in Lemma 4 (see Appendix A), as the dimension i increases, the probability decreases significantly. Of course, one can also use upper bounds "$\leq \big(\min\{t, r\} - a + 1\big)\Pr\Big[\Delta = a\Big]$". We use the approximation because it simulates closely. The last inequality also follows Lemma 4.

- When $a > \min\{t, r\}$, it is impossible to obtain an intersection space of dimension $\geq a$. Hence,

$$\Pr\left[\mathsf{rank}\left(\boldsymbol{B}^{\top}\right) < k + 2r\right] \leq \Pr\left[\mathsf{rank}(\boldsymbol{M}) < k + 2r\right] = \Pr\left[\Delta \geq a\right] = 0. \tag{18}$$

  This means that the DFR is null and the decoding algorithm is deterministic.

■

Heuristic Argument. If $\mathsf{rank}(\boldsymbol{L}) = k + 2r$ and $\mathsf{rank}(\boldsymbol{M}) \geq k + 2r$, then $\mathsf{rank}\left(\boldsymbol{B}^{\top}\right) = \mathsf{rank}\left(\boldsymbol{L}\boldsymbol{M}\right) = k + 2r$.

To validate the heuristic argument, we provide two evidences:

- We performed an experiment. With a fixed matrix $\boldsymbol{L}$, a lot of random matrices $\boldsymbol{M}$ of rank $\geq k + 2r$ always lead to a matrix $\boldsymbol{B}^{\top}$ of rank $k + 2r$. The scripts are available online at https://github.com/RQCPKE/EGCodesRQC.
- In Section IX (Theorem 8), the heuristic argument is applied to prove the null DFR of the (Interleaved) Gabidulin codes. If our heuristic argument is invalid, then decoding Gabidulin codes would not be deterministic. This challenges the well-known conclusion: decoding Gabidulin codes is deterministic, which has stood for about 40 years.

These two evidences show that our heuristic argument is reliable, sound, and valid.

C. Decoding Capacity

Theorem 4 *The* $\mathrm{EG}_k(\boldsymbol{g})$ *codes in Definition 11 can decode errors of weight up to* $\min\left\{t - k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\}$.

Proof: For any error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = r$, from Theorem 3, we known that when $k + r \leq t$ and $k + 2r \leq n$, the $\mathrm{EG}_k(\boldsymbol{g})$ codes can decode such an error $\boldsymbol{e}$. This leads to the conclusion. ■

Theorem 5 *If* $t = m$ *and* $k = 2m - n$*, then the* $\mathrm{EG}_k(\boldsymbol{g})$ *codes in Definition 11 can decode errors of weight up to the RGV bound in Definition 3.*

Proof: From Theorem 4, we know that the $\mathrm{EG}_k(\boldsymbol{g})$ codes can decode errors of weight up to $\min\left\{t - k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\}$. Let $r = \min\left\{t - k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\}$. By the definition of the RGV bound (Definition 3), we only need to prove that such a value r satisfies $q^{r(m+n-r)} = q^{(n-k)m}$. If $t = m$ and $k = 2m - n$, then $t - k = \left\lfloor \frac{n-k}{2} \right\rfloor = n - m$. Hence, $r = \min\left\{t - k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\} = n - m$. It is easy to check that $q^{r(m+n-r)} = q^{(n-k)m} = q^{2m(n-m)}$. ■

Recall that the RGV bound in Definition 3, $q^{r(m+n-r)}$ is the lower bound of $\mathcal{V}(q, m, n, r)$. Thus, by the EG codes, any syndrome (resp. word) in $\mathbb{F}_{q^m}^{n-k}$ (resp. $\mathbb{F}_{q^m}^{n}$) can be decoded to an error of weight the RGV bound. In the experiment, for some code parameters, any syndrome (resp. word) can even decode up to a larger error than the RGV bound with an overwhelming probability.

D. Decoding Algorithm

Theorem 3 considers the errors of weight exactly r, and the decoding will fail if $\mathsf{rank}(\boldsymbol{A}) < k + 2r$. However, when an error of weight $< r$ (say weight is w) really occurs, we must have $\mathsf{rank}(\boldsymbol{A}) < k + 2r$:

$$\mathsf{rank}(\boldsymbol{L}) = \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) + \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\gamma}, k + r - 1)\right) = w + k + r < k + 2r,$$

$$\mathsf{rank}(\boldsymbol{A}) = \mathsf{rank}(\boldsymbol{B}^{\top}) \leq \min\{\mathsf{rank}(\boldsymbol{L}), \mathsf{rank}(\boldsymbol{M})\} \leq \mathsf{rank}(\boldsymbol{L}) < k + 2r,$$

where $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^{w}$ is a basis of support of the error of weight w.

Then, in this case, whether it can decode successfully, how to recover $f(x)$, and how to determine DFR? We discuss this case in Appendix B. We there show that if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)$ is controlled as $r - w + 1$, any non-zero element in $\mathsf{kernel}(\boldsymbol{A})$ can still be used to recover $f(x)$, and the DFR $\leq \gamma_q \cdot q^{a(t+w-a-n)}$. The DFR quickly decreases in w and is upper bounded by that of decoding weight r.

The resulting decoding procedure is given in Algorithm 1. We present a general decoding procedure: given an EG code decoding up to weight r, when the error of weight w occurs ($w \leq r$), if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)$ is controlled as $r - w + 1$, any non-zero element in $\mathsf{kernel}(\boldsymbol{A})$ can determine $f(x)$ by Steps 5 - 6. The DFR depends on $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)$, and Algorithm 1 returns failure if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right) \neq r - w + 1$.

Decoding Complexity. The complexity of Algorithm 1 is dominated by Step 2. The right kernel of the system $\boldsymbol{A}\boldsymbol{x}^{\top} = \boldsymbol{0}_n$ can be found in $\mathcal{O}(n^3)$ operations in $\mathbb{F}_{q^m}$ by standard Gaussian elimination. Thus, the complexity of decoding EG codes is bounded by $\mathcal{O}(n^3)$.

Algorithm 1 Decoding errors of weight w for the EG codes ($w \le r$)

Input: $q, m, n, k, t, w, r \in \mathbb{N}$, $k \le t \le \min\{n, m\}$,
$\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{g}\|_{\mathrm{R}} = t$, $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$.
Output: $f(x) \in \mathcal{L}_{\le k-1}[x]$; $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = w$

1: Compute matrices $\boldsymbol{Y}$ and $\boldsymbol{Z}$, and construct matrix $\boldsymbol{A}$:

$$\boldsymbol{Y} = \mathbf{Moore}(\boldsymbol{y}, r)^\top, \quad \boldsymbol{Z} = \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top, \quad \boldsymbol{A} = [\boldsymbol{Y} \quad \boldsymbol{Z}].$$

2: Compute the right kernel $\mathsf{kernel}(\boldsymbol{A})$. // Solve the linear system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$.
3: Let $\boldsymbol{b} = (b_0, b_1, \ldots, b_{k+2r})$ be a random non-zero element in $\mathsf{kernel}(\boldsymbol{A})$.
4: Set $v'(x) = \sum_{i=0}^{r} b_i x^{q^i}$ and $u'(x) = \sum_{i=0}^{k+r-1} b_{i+r+1} x^{q^i}$.
5: Set $f(x) = -v'(x) \setminus u'(x)$ by left division. // Holds **iff** $\dim(\mathsf{kernel}(\boldsymbol{A})) = r - w + 1$
6: **return** $f(x)$ and $\boldsymbol{e} := \boldsymbol{y} - f(\boldsymbol{g})$

E. Simulated DFR for Decoding Errors of Weight r

In Table I, we chose eight types of simulable code parameters, and set five groups of parameters for each type. We simulated DFR for each group by performing decoding algorithms (Algorithm 1) in 10^5 times. The theoretical DFR is estimated by Equations (17) and (18) with $\gamma_2 = 4$, and $\gamma_q = 2$ if $q > 2$. The theoretical DFR for the types decoding up to the RGV bound is always greater than 1, and we recorded these DFR as 1 (see No. 26 - 35). Here, d is the minimal distance (Proposition 7), d_{RGV} is the RGV bound (Definition 3), and d_{RS} is the RS bound (Definition 4). The test scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

VII. Improved Decoding Algorithm

It is clear that the cost $\mathcal{O}(n^3)$ of decoding Algorithm 1 is too much for an efficiently implementation. In this section, we provide two improvements and obtain the cost $\mathcal{O}(r^3)$ and $\mathcal{O}(n^2)$. These also show that our decoding idea starting from solving the LR problem is potential for developing efficient decoding algorithms.

A. Improved Gaussian Elimination

Here, we adapt the idea of decoding Gabidulin codes by Loidreau [17] (Section 5.1). Recall that decoding Algorithm 1 consists in solving the system (7): $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$. The first $r+1$ coordinates of $\boldsymbol{x}$ determine $v(x)$ of q-degree r and the last $k+r$ coordinates of $\boldsymbol{x}$ determine $u(x) = -v(x) \circ f(x)$ of q-degree $\le k+r-1$.

By observing $\boldsymbol{A}$, its part is independent of the received word $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ and depends only on the generator $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$. Let $\boldsymbol{y}_1 \in \mathbb{F}_{q^m}^{k+r}$ and $\boldsymbol{g}_1 \in \mathbb{F}_{q^m}^{k+r}$ be vectors consisting of the first $k+r$ coordinates of $\boldsymbol{y}$ and $\boldsymbol{g}$, respectively. Let $\boldsymbol{y}_2 \in \mathbb{F}_{q^m}^{n-k-r}$ and $\boldsymbol{g}_2 \in \mathbb{F}_{q^m}^{n-k-r}$ be vectors consisting of the last $n-k-r$ coordinates of $\boldsymbol{g}$ and $\boldsymbol{y}$, respectively. To adapt the decoding idea in [17], we assume that the coordinates of $\boldsymbol{g}_1$ are linearly independent over $\mathbb{F}_q$, i.e., $\|\boldsymbol{g}_1\|_{\mathrm{R}} = k+r$. Otherwise, we perform an invertible matrix on $\boldsymbol{g}$ and $\boldsymbol{y}$ such that the coordinates of $\boldsymbol{g}_1$ are linearly independent. We write $\boldsymbol{A}$ as

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{T}_1 & \boldsymbol{G}_1 \\ \hline \boldsymbol{T}_2 & \boldsymbol{G}_2 \end{array}\right] \in \mathbb{F}_{q^m}^{n \times (k+2r+1)},$$

where $\boldsymbol{T}_1 = \mathbf{Moore}(\boldsymbol{y}_1, r)^\top \in \mathbb{F}_{q^m}^{(k+r)\times(r+1)}$, $\boldsymbol{T}_2 = \mathbf{Moore}(\boldsymbol{y}_2, r)^\top \in \mathbb{F}_{q^m}^{(n-k-r)\times(r+1)}$, $\boldsymbol{G}_1 = \mathbf{Moore}(\boldsymbol{g}_1, k+r-1)^\top \in \mathbb{F}_{q^m}^{(k+r)\times(k+r)}$, and $\boldsymbol{G}_2 = \mathbf{Moore}(\boldsymbol{g}_2, k+r-1)^\top \in \mathbb{F}_{q^m}^{(n-k-r)\times(k+r)}$.

Let $\boldsymbol{x}_1 \in \mathbb{F}_{q^m}^{r+1}$ be a vector consisting of the first $r+1$ coordinates of $\boldsymbol{x}$. Let $\boldsymbol{x}_2 \in \mathbb{F}_{q^m}^{k+r}$ be a vector consisting of the last $k+r$ coordinates of $\boldsymbol{x}$. As $\|\boldsymbol{g}_1\|_{\mathrm{R}} = k+r$, we have $\mathsf{rank}(\boldsymbol{G}_1) = k+r$, i.e., $\boldsymbol{G}_1$ is invertible. Solving the system (7): $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$ is equivalent to solving

$$\begin{cases} \boldsymbol{T}_1\boldsymbol{x}_1^\top + \boldsymbol{G}_1\boldsymbol{x}_2^\top = \boldsymbol{0}_{k+r} \\ \boldsymbol{T}_2\boldsymbol{x}_1^\top + \boldsymbol{G}_2\boldsymbol{x}_2^\top = \boldsymbol{0}_{n-k-r} \end{cases} \iff \begin{cases} \boldsymbol{x}_2^\top = -\boldsymbol{G}_1^{-1}\boldsymbol{T}_1\boldsymbol{x}_1^\top \\ \left(\boldsymbol{T}_2 - \boldsymbol{G}_2\boldsymbol{G}_1^{-1}\boldsymbol{T}_1\right)\boldsymbol{x}_1^\top = \boldsymbol{0}_{n-k-r} \end{cases} \tag{19}$$

For decoding by solving the system (19), one *precomputes* $\boldsymbol{G}_1^{-1}$ and $\boldsymbol{G}_2\boldsymbol{G}_1^{-1}$. Once receiving $\boldsymbol{y}$, one first solves $\boldsymbol{x}_1$ from the subsystem $\left(\boldsymbol{T}_2 - \boldsymbol{G}_2\boldsymbol{G}_1^{-1}\boldsymbol{T}_1\right)\boldsymbol{x}_1^\top = \boldsymbol{0}_{n-k-r}$ with $r+1$ unknowns and $n-k-r$ equations, then computes $\boldsymbol{x}_2$. The overall complexity is $\mathcal{O}(r^3)$ in $\mathbb{F}_{q^m}$ for solving $\boldsymbol{x}_1$ when $r+1 \approx n-k-r$. This is the case of cryptographic parameters.

TABLE I
THEORETICAL AND SIMULATED DFR OF THE EG CODES FOR ERRORS OF WEIGHT r

Types	No.	Parameters (q, m, n, t, k, r)	Theoretical DFR	Simulated DFR	d	d_{RGV}	d_{RS}
Increase q $(t = m < n)$	1	$(2, 5, 7, 5, 2, 2)$	(2^{-2}) 0.2500	0.0579	4	3	4
	2	$(3, 5, 7, 5, 2, 2)$	$(2^{-5.3})$ 0.0247	0.0123	4	3	4
	3	$(5, 5, 7, 5, 2, 2)$	$(2^{-8.3})$ 0.0032	0.0016	4	3	4
	4	$(7, 5, 7, 5, 2, 2)$	$(2^{-10.2})$ 0.00085	0.00034	4	3	4
	5	$(11, 5, 7, 5, 2, 2)$	$(2^{-12.8})$ 0.00014	0.00004	4	3	4
Increase m $(t = m < n)$	6	$(2, 31, 41, 31, 9, 16)$	(2^{-5}) 0.0313	0.0154	23	19	25
	7	$(2, 32, 41, 32, 9, 16)$	(2^{-6}) 0.0156	0.0078	24	19	25
	8	$(2, 33, 41, 33, 9, 16)$	(2^{-7}) 0.0078	0.0037	25	20	26
	9	$(2, 34, 41, 34, 9, 16)$	(2^{-8}) 0.0039	0.0018	26	20	27
	10	$(2, 35, 41, 35, 9, 16)$	(2^{-9}) 0.0020	0.0009	27	20	28
Increase n $(t = m < n)$	11	$(2, 27, 41, 27, 9, 16)$	(2^{-1}) 0.5000	0.2312	19	17	22
	12	$(2, 27, 42, 27, 9, 16)$	(2^{-4}) 0.0625	0.0388	19	17	22
	13	$(2, 27, 43, 27, 9, 16)$	(2^{-7}) 0.0078	0.0052	19	18	22
	14	$(2, 27, 44, 27, 9, 16)$	(2^{-10}) 0.00098	0.00085	19	18	22
	15	$(2, 27, 45, 27, 9, 16)$	(2^{-13}) 0.00012	0.00008	19	18	22
Increase t $(t < m < n)$	16	$(2, 35, 41, 30, 9, 16)$	(2^{-4}) 0.0625	0.0300	22	20	28
	17	$(2, 35, 41, 31, 9, 16)$	(2^{-5}) 0.0313	0.0151	23	20	28
	18	$(2, 35, 41, 32, 9, 16)$	(2^{-6}) 0.0156	0.0083	24	20	28
	19	$(2, 35, 41, 33, 9, 16)$	(2^{-7}) 0.0078	0.0036	25	20	28
	20	$(2, 35, 41, 34, 9, 16)$	(2^{-8}) 0.0039	0.0018	26	20	28
Increase t $(t < n < m)$	21	$(2, 29, 26, 16, 5, 10)$	(2^{-2}) 0.0250	0.1326	12	16	22
	22	$(2, 29, 26, 17, 5, 10)$	(2^{-4}) 0.0625	0.0371	13	16	22
	23	$(2, 29, 26, 18, 5, 10)$	(2^{-6}) 0.0156	0.0098	14	16	22
	24	$(2, 29, 26, 19, 5, 10)$	(2^{-8}) 0.0039	0.0024	15	16	22
	25	$(2, 29, 26, 20, 5, 10)$	(2^{-10}) 0.00098	0.00058	16	16	22
Decoding RGV Bound $(k > r)$	26	$(2, 30, 37, 30, 23, 7)$	1	0.7122	8	7	12
	27	$(2, 30, 38, 30, 22, 8)$	1	0.7086	9	8	13
	28	$(2, 30, 39, 30, 21, 9)$	1	0.7102	10	9	14
	29	$(2, 30, 40, 30, 20, 10)$	1	0.7109	11	10	16
	30	$(2, 30, 41, 30, 19, 11)$	1	0.7142	12	11	17
Decoding RGV Bound $(k < r)$	31	$(2, 21, 34, 21, 8, 13)$	1	0.7125	14	13	17
	32	$(2, 22, 36, 22, 8, 14)$	1	0.7119	15	14	18
	33	$(2, 23, 38, 23, 8, 15)$	1	0.7118	16	15	19
	34	$(2, 24, 40, 24, 8, 16)$	1	0.7122	17	16	20
	35	$(2, 25, 42, 25, 8, 17)$	1	0.7123	18	17	21
Gabidulin Codes $(t = n \leq m)$	36	$(2, 27, 27, 27, 7, 10)$	0	0	21	14	21
	37	$(2, 28, 27, 27, 7, 10)$	0	0	21	14	21
	38	$(2, 29, 27, 27, 7, 10)$	0	0	21	14	21
	39	$(2, 30, 27, 27, 7, 10)$	0	0	21	14	21
	40	$(2, 31, 27, 27, 7, 10)$	0	0	21	15	21

B. Welch-Berlekamp Like Algorithm for the EG Codes

The Welch-Berlekamp algorithm [54] is another efficient algorithm solving the LR problem. This algorithm was adapted to decoding Gabidulin codes by Loidreau [13], [17] (called Welch-Berlekamp like algorithm). In this section, we find that the Welch-Berlekamp like algorithm can be adapted to decode EG codes.

The idea is to compute two pairs (u_0, v_0) and (u_1, v_1) of q-polynomials which satisfy the interpolation conditions of the LR problem (see Definition 14):

$$v\left(y_i\right) = u\left(g_i\right), \quad i \in [n]$$

and such that at least one of the pairs satisfies the final degree conditions:

$$\mathsf{deg}_q(u(x)) \leq \begin{cases} k + \left\lfloor \frac{n-k}{2} \right\rfloor - 1, & \text{if } n-k \text{ even} \\ k + \left\lfloor \frac{n-k}{2} \right\rfloor, & \text{if } n-k \text{ odd} \end{cases}$$
$$v(x) \neq 0; \quad \mathsf{deg}_q(v(x)) \leq r.$$

For a negligible DFR, n is often sufficient large and $\left\lfloor \frac{n-k}{2} \right\rfloor$ is often greater than r. This also is the case of cryptographic parameters. In this case, the decoding complexity is $\mathcal{O}\left(n^2\right)$ in $\mathbb{F}_{q^m}$. If we do not consider a negligible DFR, the first $2r + k$

elements of $\boldsymbol{y}$ are sufficient for successful decoding and the last $n-2r-k$ elements are redundant. We thus can tune the final degree conditions as:

$$\begin{aligned}&\mathsf{deg}_q(u(x)) \leq k+r,\\ &v(x)\neq 0;\quad \mathsf{deg}_q(v(x))\leq r.\end{aligned}$$

In this case, the overall decoding complexity is $\mathcal{O}\left((2r+k)^2\right)$.

The resulting decoding algorithm is presented in Algorithm 2. The simulated DFR is presented in Table XI (see Appendix A-B). The test scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

Algorithm 2 Decoding errors of weight $\leq r$ by the Welch-Berlekamp algorithm

Input: $q,m,n,k,r\in\mathbb{N}$, $\boldsymbol{g}\in\mathbb{F}_{q^m}^n$ and $\|\boldsymbol{g}\|_{\mathrm{R}}=t$, $\boldsymbol{y}\in\mathbb{F}_{q^m}^n$.
Output: $f(x)\in\mathcal{L}_{\leq k-1}[x]$; $\boldsymbol{e}\in\mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}}\leq r$

1: Call Algorithm 5 in [13]
2: Return (N_1,W_1)
3: Set $u(x)=N_1$ and $v(x)=W_1$
4: Compute $f(x)=v(x)\setminus u(x)$
5: **if** $\mathsf{deg}_q f(x)\leq k-1$ and $\|\boldsymbol{y}-f(\boldsymbol{g})\|_{\mathrm{R}}\leq r$:
6: **return** $f(x)$ and $\boldsymbol{e}:=\boldsymbol{y}-f(\boldsymbol{g})$
7: **else**:
8: **return** $\perp$

VIII. Interleaved EG Codes

Interleaving a code considers several codewords at the same time, corrupted by errors sharing the same support. This specific structure allows to design algorithms being able to decode more errors. In this section, we introduce the Interleaved EG (IEG) codes and analyze its decoding capacity.

Definition 15 (IEG Codes) *Let q,m,n,t,k,N be integers and $k\leq t\leq\min\{n,m\}$. Let $\boldsymbol{g}=(g_1,g_2,\ldots,g_n)\in\mathbb{F}_{q^m}^n$ be the generator of weight t. An IEG code of dimension k and length n generated by $\boldsymbol{g}$ is defined as*

$$\mathrm{IEG}_k(\boldsymbol{g})=\left\{\begin{bmatrix} f_1(\boldsymbol{g})\\ f_2(\boldsymbol{g})\\ \vdots\\ f_N(\boldsymbol{g})\end{bmatrix}\ :\ f_i(x)\in\mathcal{L}_{\leq k-1}[x],\quad i\in[N]\right\}.$$

Let $\boldsymbol{y}_i=f_i(\boldsymbol{g})+\boldsymbol{e}_i,\quad i\in[N]$ where all $\boldsymbol{e}_i$'s share the support of dimension r. We show that if one receives such a set of N words $\boldsymbol{y}_i$'s, it can decode more errors than the EG codes, specifically correct up to $r=\min\left\{t-k,\frac{N(n-k)}{(N+1)}\right\}$. We give a decoding algorithm based on solving the LR problem and bound the DFR. First, like the LR problem for decoding the EG codes (see Definition 14), we define the LR problem for decoding the IEG codes.

Definition 16 (The LR $\left(\boldsymbol{g},\{\boldsymbol{y}_i\}_{i\in[N]}\right)$ Problem for Decoding IEG Codes)
Input : $\boldsymbol{g}=(g_1,g_2,\ldots,g_n)\in\mathbb{F}_{q^m}^n$; $\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_N\in\mathbb{F}_{q^m}^n$.
Output : $v(x),u_i(x)\in\mathcal{L}[x]$ *such that:* 1. $v(x)\neq 0$ *and* $\mathsf{deg}_q v(x)\leq r$; 2. $u_i(x)\leq k+r-1$; 3. $v\left(\boldsymbol{y}_i\right)=u_i\left(\boldsymbol{g}\right)$.

Let $\boldsymbol{Z}=\mathbf{Moore}(\boldsymbol{g},k+r-1)^\top\in\mathbb{F}_{q^m}^{n\times(k+r)}$ and $\boldsymbol{Y}_i=\mathbf{Moore}(\boldsymbol{y}_i,r)^\top\in\mathbb{F}_{q^m}^{n\times(r+1)}$. Solving the $\mathsf{LR}\left(\boldsymbol{g},\{\boldsymbol{y}_i\}_{i\in[N]}\right)$ problem is equivalent to solving a linear system $\widehat{\boldsymbol{A}}\boldsymbol{x}=\boldsymbol{0}_{Nn}$ where

$$\widehat{\boldsymbol{A}}=\left[\begin{array}{c|cccc}\boldsymbol{Y}_1 & \boldsymbol{Z} & \boldsymbol{0} & \cdots & \boldsymbol{0}\\ \boldsymbol{Y}_2 & \boldsymbol{0} & \boldsymbol{Z} & \cdots & \boldsymbol{0}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{Y}_N & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{Z}\end{array}\right]:=\left[\begin{array}{c|c}\boldsymbol{Y}_1 & \\ \boldsymbol{Y}_2 & \\ \vdots & \mathbf{Diag}(\boldsymbol{Z},N)\\ \boldsymbol{Y}_N & \end{array}\right]\in\mathbb{F}_{q^m}^{nN\times[r+1+N(k+r)]}.\tag{20}$$

Let $\boldsymbol{b}=(b_0,b_1,\ldots,b_{r+N(k+r)})$ be a random non-zero element in $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$. We set $v'(x)=\sum_{i=0}^{r}b_i x^{q^i}$ and $u_i'(x)=\sum_{j=0}^{k+r-1}b_{r+1+(i-1)(k+r)+j}x^{q^j}$. If the right kernel $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$ is one-dimensional, then $f_i(x)=-v'(x)\setminus u_i'(x)$. Next, we analyze when $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$ is one-dimensional, and derive the DFR and the decoding capacity.

Let $\boldsymbol{E}_i=\mathbf{Moore}(\boldsymbol{e}_i,r)^\top\in\mathbb{F}_{q^m}^{n\times(r+1)}$ and $\boldsymbol{\Gamma}_i=-\mathbf{PM}(f_i(x),r)\in\mathbb{F}_{q^m}^{(k+r)\times(r+1)}$. Following Proposition 9, we have

$$\widehat{\boldsymbol{A}}\underbrace{\begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \boldsymbol{\Gamma}_1 & \boldsymbol{I} & \boldsymbol{0} & \cdots & \boldsymbol{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{\Gamma}_N & \boldsymbol{0} & \boldsymbol{0} & \cdots & \boldsymbol{I} \end{bmatrix}}_{\text{invertible matrix}} = \left[\begin{array}{c|c} \boldsymbol{E}_1 & \\ \boldsymbol{E}_2 & \\ \vdots & \mathbf{Diag}(\boldsymbol{Z}, N) \\ \boldsymbol{E}_N & \end{array}\right] := \widehat{\boldsymbol{B}}.$$

Thus, $\widehat{\boldsymbol{A}}$ is equivalent to $\widehat{\boldsymbol{B}}$. Next, we analyze $\dim\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right) \geq 1$.

Proposition 11 *For any N uniform and random errors $\boldsymbol{e}_i$'s sharing the same support of dimension r, if $k+r \leq t \leq \min\{n,m\}$ and $r+N(k+r) \leq nN$, then* $\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) \leq r+N(k+r)$.

Proof: We consider the rank of $\widehat{\boldsymbol{B}}^\top$. Let

$$\widehat{\boldsymbol{B}}_1 = \begin{bmatrix} \boldsymbol{E}_1^\top & \boldsymbol{E}_2^\top & \cdots & \boldsymbol{E}_N^\top \end{bmatrix}, \quad \widehat{\boldsymbol{B}}_2 = \mathbf{Diag}\left(\boldsymbol{Z}^\top, N\right), \quad \widehat{\boldsymbol{B}}^\top = \begin{bmatrix} \widehat{\boldsymbol{B}}_1 \\ \widehat{\boldsymbol{B}}_2 \end{bmatrix}.$$

Let $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_N)$ be the concatenation of $\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_N$. Then $\widehat{\boldsymbol{B}}_1 = \mathbf{Moore}(\boldsymbol{e}, r)$. Since the vector $\boldsymbol{e}$ has the rank weight r (all $\boldsymbol{e}_i$'s share the support of dimension r), from Proposition 5, we have $\mathsf{rank}\left(\widehat{\boldsymbol{B}}_1\right) = r$. Since $k+r \leq t$, from Proposition 5, we have $\mathsf{rank}\left(\boldsymbol{Z}\right) = k+r$. Further $\mathsf{rank}\left(\widehat{\boldsymbol{B}}_2\right) = N(k+r)$. Thus,

$$\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) = \mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) \leq \mathsf{rank}\left(\widehat{\boldsymbol{B}}_1\right) + \mathsf{rank}\left(\widehat{\boldsymbol{B}}_2\right) = r+N(k+r).$$

■

By Proposition 11, we have $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) = \mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) \leq r+N(k+r)$. Since $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) + \dim\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right) = r+N(k+r)+1$, we must have $\dim\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right) \geq 1$. Thus, there must exists a non-zero element in $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$.

The DFR decoding the errors of maximal weight depends on $\dim\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right) > 1$, which is equivalent to $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) < r+N(k+r)$. Since $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) = \mathsf{rank}\left(\widehat{\boldsymbol{B}}\right)$, the DFR depends on the probability of $\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) < r+N(k+r)$. This leads to Theorem 6.

Theorem 6 *For any N uniform and random errors $\boldsymbol{e}_i$'s sharing the same support of dimension r, if $k+r \leq t \leq \min\{n,m\}$ and $r+N(k+r) \leq nN$, then*

$$\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) < r+N(k+r)\right] \leq \gamma_q \cdot q^{a(Nt+r-a-Nn)}, \tag{21}$$

where $a = N(t-k-r)+1$.

Proof: We consider $\widehat{\boldsymbol{B}}^\top$ and estimate $\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < r+N(k+r)\right]$. Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^r$ be a basis of support for N errors $\boldsymbol{e}_i$'s. Let $\mathbf{CM}(\boldsymbol{e}_i) \in \mathbb{F}_q^{r\times n}$ of rank r be the coefficient matrix of $\boldsymbol{e}_i$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e}_i = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e}_i)$. Let $\boldsymbol{\gamma} \in \mathbb{F}_{q^m}^t$ be a basis of $\mathrm{Supp}(\boldsymbol{g})$. Let $\mathbf{CM}(\boldsymbol{g}) \in \mathbb{F}_q^{t\times n}$ of rank t be the coefficient matrix of $\boldsymbol{g}$ under $\boldsymbol{\gamma}$ such that $\boldsymbol{g} = \boldsymbol{\gamma}\mathbf{CM}(\boldsymbol{g})$. Let $\boldsymbol{N}_1 = \mathbf{Moore}(\boldsymbol{\varepsilon}, r) \in \mathbb{F}_{q^m}^{(r+1)\times r}$ and $\boldsymbol{N}_2 = \mathbf{Moore}(\boldsymbol{\gamma}, k+r-1) \in \mathbb{F}_{q^m}^{(k+r)\times t}$. By Definition 10 and Proposition 3,

$$\begin{aligned} \widehat{\boldsymbol{B}}^\top &= \left[\begin{array}{cccc} \boldsymbol{E}_1^\top & \boldsymbol{E}_2^\top & \cdots & \boldsymbol{E}_N^\top \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{Z}^\top, N)} \end{array}\right] = \left[\begin{array}{cccc} \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_1) & \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_2) & \cdots & \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_N) \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{N}_2\cdot\mathbf{CM}(\boldsymbol{g}), N)} \end{array}\right] \\ &= \underbrace{\left[\begin{array}{c|c} \boldsymbol{N}_1 & \boldsymbol{0} \\ \hline \boldsymbol{0} & \mathbf{Diag}(\boldsymbol{N}_2, N) \end{array}\right]}_{:=\boldsymbol{L}\in\mathbb{F}_{q^m}^{[r+N(k+r)+1]\times(r+Nt)}} \underbrace{\left[\begin{array}{cccc} \mathbf{CM}(\boldsymbol{e}_1) & \mathbf{CM}(\boldsymbol{e}_2) & \cdots & \mathbf{CM}(\boldsymbol{e}_N) \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\mathbf{CM}(\boldsymbol{g}), N)} \end{array}\right]}_{:=\boldsymbol{M}\in\mathbb{F}_q^{(r+Nt)\times Nn}}. \end{aligned} \tag{22}$$

By Corollary 1, we have $\mathsf{rank}\left(\boldsymbol{N}_1\right) = r$, and as $k+r-1 < t$, $\mathsf{rank}\left(\mathbf{Diag}(\boldsymbol{N}_2, N)\right) = N(k+r)$. Thus, $\mathsf{rank}(\boldsymbol{L}) = \mathsf{rank}\left(\boldsymbol{N}_1\right) + \mathsf{rank}\left(\mathbf{Diag}(\boldsymbol{N}_2, N)\right) = r+N(k+r) \leq Nn$.

As $\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) \leq \min\{\mathsf{rank}(\boldsymbol{L}), \mathsf{rank}(\boldsymbol{M})\}$ and $\boldsymbol{M} \in \mathbb{F}_q^{(r+Nt)\times Nn}$ is defined in the basis field $\mathbb{F}_q$, Following the Heuristic Argument presented in Theorem 3: if $\mathsf{rank}(\boldsymbol{M}) \geq r+N(k+r)$, then $\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) = r+N(k+r)$. Hence, we have

$$\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < r+N(k+r) \implies \mathsf{rank}(\boldsymbol{M}) < r+N(k+r). \tag{23}$$

Moreover, since

$$\begin{aligned}\mathsf{rank}(\boldsymbol{M}) &= \mathsf{rank}\left(\left[\begin{array}{cccc}\mathbf{CM}(\boldsymbol{e}_1) & \mathbf{CM}(\boldsymbol{e}_2) & \cdots & \mathbf{CM}(\boldsymbol{e}_N)\\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\mathbf{CM}(\boldsymbol{g}), N)}\end{array}\right]\right)\\ &= \mathsf{dim}\Big(\langle[\ \mathbf{CM}(\boldsymbol{e}_1)\quad \mathbf{CM}(\boldsymbol{e}_2)\quad \cdots\quad \mathbf{CM}(\boldsymbol{e}_N)\ ]\rangle + \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big)\\ &= r + Nt - \Delta,\end{aligned}$$

where $\Delta = \mathsf{dim}\Big(\langle[\ \mathbf{CM}(\boldsymbol{e}_1)\quad \mathbf{CM}(\boldsymbol{e}_2)\quad \cdots\quad \mathbf{CM}(\boldsymbol{e}_N)\ ]\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big)$, we have

$$\mathsf{rank}(\boldsymbol{M}) < r + N(k+r) \iff \Delta > N(t-k-r). \tag{24}$$

Let $a = N(t-k-r)+1$. Finally, combining Equations (23) and (24), we have:

- When $a \le \min\{Nt, r\}$,

$$\begin{aligned}&\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < r + N(k+r)\right] \le \Pr\left[\mathsf{rank}(\boldsymbol{M}) < r + N(k+r)\right]\\ &= \Pr\left[\Delta > N(t-k-r)\right] = \sum_{i=a}^{\min\{Nt,r\}} \Pr\left[\Delta = i\right] \approx \Pr\left[\Delta = a\right]\\ &\le \gamma_q \cdot q^{a(Nt+r-a-Nn)}.\end{aligned} \tag{25}$$

  The first inequality "$\le$" due to "$\Longrightarrow$" of Equation (23). The second equation "$=$" due to "$\Longleftrightarrow$" of Equation (24). The approximation "$\approx$" is natural. By the probability in Lemma 4 (see Appendix A), as the dimension i increases, the probability decreases significantly. The last inequality also follows Lemma 4.
- When $a > \min\{Nt, r\}$, it is impossible to obtain an intersection space of dimension $\ge a$. Hence,

$$\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < r + N(k+r)\right] \le \Pr[\mathsf{rank}(\boldsymbol{M}) < r + N(k+r)] = \Pr\left[\Delta \ge a\right] = 0. \tag{26}$$

  This means that the DFR is null and the decoding algorithm is deterministic.

■

Theorem 7 *The IEG codes can decode errors of weight up to* $r = \min\left\{t-k, \left\lfloor \frac{N(n-k)}{N+1} \right\rfloor\right\}$.

Proof: For all errors $\boldsymbol{e}_i$ sharing the same support of dimension r, from Theorem 6, we known that when $k + r \le t$ and $r + N(k+r) \le nN$, the IEG codes can decode such errors $\boldsymbol{e}_i$'s. This leads to conclusion. ■

Theorem 6 considers N errors sharing r-dimensional support, and the decoding will fail if $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) < N(k+r)+r$. However, when N errors share the support of dimension $< r$ (say dimension is w) really occurs, we must have $\mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) < N(k+r)+r$:

$$\begin{aligned}\mathsf{rank}(\boldsymbol{L}) &= \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) + \mathsf{rank}\left(\mathbf{Diag}(\boldsymbol{N}_2, N)\right) = w + N(k+r) < N(k+r) + r,\\ \mathsf{rank}\left(\widehat{\boldsymbol{A}}\right) &= \mathsf{rank}\left(\widehat{\boldsymbol{A}}^\top\right) \le \min\{\mathsf{rank}(\boldsymbol{L}), \mathsf{rank}(\boldsymbol{M})\} \le \mathsf{rank}(\boldsymbol{L}) < N(k+r) + r,\end{aligned}$$

where $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^w$ is a basis of support of the error of weight w.

Then, in this case, whether it can decode successfully, how to recover $f_i(x)$, and how to determine DFR? We discuss this case in Appendix C. We there show that if $\mathsf{dim}\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right)$ is controlled as $r - w + 1$, any non-zero element in $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$ can determine $f_i(x)$, and the DFR $\le \gamma_q \cdot q^{a(Nt+w-a-Nn)}$. The resulting decoding procedure is presented in Algorithm 3.

Decoding Complexity. The complexity of Algorithm 3 is dominated by Step 2. The right kernel of the system $\boldsymbol{A}\boldsymbol{x}^\top = \boldsymbol{0}_n$ can be found in $\mathcal{O}\left((Nn)^3\right)$ operations in $\mathbb{F}_{q^m}$ by Gaussian elimination. Thus, the complexity is bounded by $\mathcal{O}\left((Nn)^3\right)$. We leave more improvements as independent interest for further study.

IX. Relations with (Interleaved) Gabidulin Codes

In this section, building on our idea analyzing DFR for decoding EG codes, we show that decoding interleaved Gabidulin codes is deterministic by the solving LR problem. This problem is left in [14], where the authors only presented a proof in a vague case that the number of columns of the system is exactly equal to number of rows plus 1. This leads to a mislead that the most previous works [4], [15], [46], [55] thought that there exists only efficient *probabilistic* decoding algorithms for interleaved Gabidulin codes. The result covers the fact that decoding Gabidulin codes is deterministic. This work also supports the validity of our heuristic argument for Equation (15). If our heuristic argument is invalid, then decoding Gabidulin codes by the solving LR problem would not be deterministic. This challenges the well-known conclusion: decoding Gabidulin codes is deterministic, which has stood for about 40 years.

Algorithm 3 Decoding errors of weight w for the IEG codes ($w \leq r$)

Input: $q, m, n, k, t, w, r, N \in \mathbb{N}$, $k \leq t \leq \min\{n, m\}$,
$\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{g}\|_{\mathrm{R}} = t$; $\{\boldsymbol{y}_i\}_{i\in[N]} \in (\mathbb{F}_{q^m}^n)^N$.
Output: $f_i(x) \in \mathcal{L}_{\leq k-1}[x]$; $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^n$ and $\mathsf{dim}(\mathrm{Supp}(\boldsymbol{e}_i)) = w$

Compute $\boldsymbol{Y}_i = \mathbf{Moore}(\boldsymbol{y}_i, r)^\top \in \mathbb{F}_{q^m}^{n\times(r+1)}$ and $\boldsymbol{Z} = \mathbf{Moore}(\boldsymbol{g}, k+r-1)^\top \in \mathbb{F}_{q^m}^{n\times(k+r)}$, construct the matrix $\widehat{\boldsymbol{A}} \in \mathbb{F}_{q^m}^{nN\times[r+1+N(k+r)]}$ as in Equation (20).
Compute the right kernel $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$ of the linear system $\widehat{\boldsymbol{A}}\boldsymbol{x}^\top = \boldsymbol{0}_{Nn}$.
Recover message q-polynomials $f_i(x)$ and errors $\boldsymbol{e}_i$ for $i \in [N]$:
  Let $\boldsymbol{b} = (b_0, b_1, \ldots, b_{r+N(k+r)})$ be a random non-zero element in $\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)$.
  Set $v'(x) = \sum_{i=0}^{r} b_i x^{q^i}$ and $u_i'(x) = \sum_{j=0}^{k+r-1} b_{r+1+(i-1)(k+r)+j} x^{q^j}$.
  Set $f_i(x) = -v'(x) \setminus u_i'(x)$ by left division. // Holds **iff** $\mathsf{dim}\left(\mathsf{kernel}\left(\widehat{\boldsymbol{A}}\right)\right) = r - w + 1$
  if $\mathsf{deg}_q f_i(x) \leq k-1$ and $\|\boldsymbol{y}_i - f_i(\boldsymbol{g})\|_{\mathrm{R}} = w$:
    return $f_i(x)$ and $\boldsymbol{e}_i := \boldsymbol{y}_i - f_i(\boldsymbol{g})$
  else:
    return $\perp$

Definition 17 (Gabidulin Codes) *Let q, m, n, k be integers and $k \leq n \leq m$. Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be a vector of weight n, which is called a generator. A Gabidulin code of dimension k and length n generated by $\boldsymbol{g}$ is defined as*

$$\mathrm{Gab}_k(\boldsymbol{g}) = \Big\{ f(\boldsymbol{g}) = (f(g_1), f(g_2), \ldots, f(g_n)) \ : \ f(x) \in \mathcal{L}_{\leq k-1}[x] \Big\}.$$

Let $f_i(x) \in \mathcal{L}_{\leq k-1}[x]$ for $i \in [N]$ be N q-polynomials. The decoding model of the interleaved Gabidulin codes is that given

$$\boldsymbol{y}_i = f_i(\boldsymbol{g}) + \boldsymbol{e}_i, \quad i \in [N]$$

where all $\boldsymbol{e}_i$'s share the support of dimension r, one aims to recover $f_i(x)$'s and $\boldsymbol{e}_i$'s. Note that when $N = 1$, the decoding model is exactly that of the Gabidulin codes.

By the definition of the EG codes (Definition 11), when $t = n$ and $m \geq n$, the EG codes are exactly Gabidulin codes. We adapt the results of our DFR to the case of the interleaved Gabidulin codes and obtain the null DFR in Theorem 8.

Theorem 8 *For any N uniform and random errors $\boldsymbol{e}_i$'s sharing the same support of dimension r, if $r \leq \left\lfloor \frac{N(n-k)}{N+1} \right\rfloor$, then the decoding of interleaved Gabidulin codes is deterministic, i.e., the DFR is null.*

Theorem 8 can be viewed as a direct application of Theorem 6. If $r \leq \left\lfloor \frac{N(n-k)}{N+1} \right\rfloor$, then $Nn \geq N(k+r) + r$. In the case of Gabidulin codes, $a = N(t-k-r)+1 = N(n-k-r)+1 \geq r+1 > r$. This is an impossible event, hence $\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < N(k+r)+r\right] = 0$. This means that the DFR is null. We present the formal proof in Appendix A-C.

X. Blockwise Puncturing (BP) Approach on the BRD Problem

In this section, we introduce the Blockwise Puncturing (BP) approach on the BRD problem. We show that the MM attack with the BP approach is powerful to the BRD problem. We present its impact on the security of schemes based on the BRD problem in Section X-D. To show the rationality and correctness of the BP approach, we first demonstrate formally the density of the basis for random rank errors in Section X-A, then in Section X-B, we analyze the number of independent equations in the MM modeling for any BRD problem, which is an open problem in [3], [5], [23].

A. Density of the Basis for Random Errors

The behind of the BP approach consists in a property of random error: the basis of a random error is dense. This property has implicitly been used in the works [3], [23], [31], [32]. For the purpose of our attacks, this section we explicitly and formally explains this property.

Recalled that almost all previous rank metric cryptosystems considered random errors or errors block. For a random error, the elements that can form a basis of its support are very dense. We call this property ***the density of the basis***. That is, for a random error $\boldsymbol{e}$ of rank weight r over $\mathbb{F}_{q^m}^n$, the vector consisting of any r elements of $\boldsymbol{e}$ could form a basis of its support with an overwhelming probability. The probability is exactly the probability that a random $r \times r$ matrix over $\mathbb{F}_q$ is non-singular.

Specifically, the random error $\boldsymbol{e}$ in the set $\mathcal{S}_r^n$ is generated in the following way. Under the fixed basis $\boldsymbol{\alpha} \in \mathbb{F}_{q^m}^m$ of $\mathbb{F}_{q^m}$, one samples a random matrix $\boldsymbol{S} \in \mathbb{F}_q^{m\times r}$ of rank r and a random matrix $\boldsymbol{C} \in \mathbb{F}_q^{r\times n}$ of rank r, and sets $\boldsymbol{e} = \boldsymbol{\alpha}\boldsymbol{S}\boldsymbol{C}$. In this

way, the column space of $\boldsymbol{S}$ determines $\mathrm{Supp}(\boldsymbol{e})$ and $\boldsymbol{\alpha S}$ can be viewed as a basis of $\mathrm{Supp}(\boldsymbol{e})$. Then, for any $T \subset [n]$ and $\#T = r$, let $\boldsymbol{e}_T = \boldsymbol{\alpha S}(\boldsymbol{C}_{*,T})$, we have

$$\mathrm{Supp}(\boldsymbol{e}_T) = \mathrm{Supp}(\boldsymbol{e}) \iff |\boldsymbol{C}|_{*,T} \neq 0.$$

A random $r \times r$ matrix is non-singular if the first row is non-zero, which happens with probability $1 - q^{-r}$; and for each i $(2 \leq i \leq r)$, the i-th row is not in the span of the first $(i-1)$ rows, which happens with probability $1 - q^{(i-1)-r}$. Thus, the probability of being non-singular is

$$\prod_{i=1}^{r} \left(1 - q^{(i-1)-r}\right) = \prod_{i=1}^{r} \left(1 - q^{-i}\right) \geq \prod_{i=1}^{\infty} (1 - q^{-i}) = \frac{1}{\gamma_q}.$$

We then have $\Pr\left[\mathrm{Supp}(\boldsymbol{e}_T) = \mathrm{Supp}(\boldsymbol{e})\right] = \Pr\left[\ |\boldsymbol{C}|_{*,T} \neq 0\right] \geq 1/\gamma_q$. Here γ_q is defined in Lemma 3 (see Appendix A). γ_q is always greater than 1 and is monotonically decreasing in q, e.g., $\gamma_2 \approx 3.463$, $\gamma_3 \approx 1.785$, and $\gamma_4 \approx 1.452$. When $q = 2$, $\Pr\left[\mathrm{Supp}(\boldsymbol{e}_T) = \mathrm{Supp}(\boldsymbol{e})\right] \geq 1/\gamma_2 \approx 0.289$.

B. Linearly Independent Equations in the MM Modeling From the BRD Problem

To obtain a precise complexity, the difficulty of analyzing the MM modeling from the BRD problem is how to estimate precisely the number of independent equations. This also remains open in [3], [5], [23]. In [3], [5], [23], authors only considered some special cases: the maximal equations $m\binom{n-k-1}{r}$ to bound the number of independent equations [3], [23], $\ell = 2$ (or $\ell = 3$), and $k = n_1 = n_2 = \cdots = n_\ell$ [5]. Here, we consider the general case for any ℓ, k, and n_i's. We derive a tight upper bound of independent equations. This work must also be made when applying the BP approach to the BRD problem because the BP approach will lead to the general case of parameters. Our ideal is to estimate the number of non-zero equations in the MM modeling. From the cases of $\ell = 2$ and $\ell = 3$ (see Theorem 9 and Theorem 10), we derive the general conclusion for any ℓ by induction in Theorem 11. Theorems 9 and 10 cover the current cryptographic parameters. The proofs of Theorems 9-11 depend on Lemma 2.

Lemma 2 *Let $\mathbb{F}$ be any field, $w \in \mathbb{N}$, and $\ell \in \mathbb{N}$. For $i \in [\ell]$, $n_i \in \mathbb{N}$, $r_i \in \mathbb{N}$, $r_i \leq n_i$, $n = \sum_i^\ell n_i$, and $r = w + \sum_i^\ell r_i$. Let $\boldsymbol{A}_i \in \mathbb{F}^{w \times n_i}$ and $\boldsymbol{B}_i \in \mathbb{F}^{r_i \times n_i}$ be uniform and random matrices over $\mathbb{F}$ for $i \in [\ell]$. Let $\boldsymbol{M} = \left[\begin{array}{c|ccc} \boldsymbol{A}_1 & \boldsymbol{A}_2 & \cdots & \boldsymbol{A}_\ell \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{B}_1, \boldsymbol{B}_2, \ldots, \boldsymbol{B}_\ell)} \end{array}\right]$ be a $r \times n$ matrix over $\mathbb{F}$. The number of non-zero maximal minors of $\boldsymbol{M}$ is*

$$\sum_{\sum_j^\ell \nu_j = w} \prod_i^\ell \binom{n_i}{r_i + \nu_i} \tag{27}$$

where $\nu_j \in \mathbb{N}$ for $j \in [\ell]$.

Proof: We first observe the structure of $\boldsymbol{M}$. By its rows, $\boldsymbol{M}$ consists of $\ell + 1$ blocks: the first w rows shared by all columns; subsequent r_i rows for $i \in [\ell]$. By its columns, $\boldsymbol{M}$ consists of ℓ blocks: each $(\boldsymbol{A}_i, \boldsymbol{B}_i)$ corresponds one block.

To obtain a maximal minor, i.e., the determinant of $r \times r$ submatrix of $\boldsymbol{M}$, when choosing r columns, we choose k_i columns from the i-th column block for $i \in [\ell]$ such that $\sum_i^\ell k_i = r$. We denote such submatrix as $\boldsymbol{M}'$:

$$\boldsymbol{M}' = \left[\begin{array}{c|ccc} \boldsymbol{A}'_1 & \boldsymbol{A}'_2 & \cdots & \boldsymbol{A}'_\ell \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{B}'_1, \boldsymbol{B}'_2, \ldots, \boldsymbol{B}'_\ell)} \end{array}\right] \in \mathbb{F}^{r \times r},$$

where $\boldsymbol{A}'_i \in \mathbb{F}^{w \times k_i}$ is a submatrix of $\boldsymbol{A}_i$ consisting of its any k_i columns and $\boldsymbol{B}'_i \in \mathbb{F}^{r_i \times k_i}$ is a submatrix of $\boldsymbol{B}_i$ consisting of its any k_i columns.

The determinant of $\boldsymbol{M}'$ is non-zero iff $\boldsymbol{M}'$ is full rank. Then $\boldsymbol{B}'_i$ first should be row-full rank, which means that $k_i \geq r_i$ for $i \in [\ell]$. This holds for uniform and random matrix $\boldsymbol{B}_i$. Considering a map ϕ.

$$\begin{aligned} \phi: \quad \mathsf{kernel}(\boldsymbol{B}'_1) \times \mathsf{kernel}(\boldsymbol{B}'_2) \times \cdots \times \mathsf{kernel}(\boldsymbol{B}'_\ell) &\longrightarrow \mathbb{F}^w \\ (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_\ell) &\longmapsto \boldsymbol{A}'_1\boldsymbol{b}_1 + \boldsymbol{A}'_2\boldsymbol{b}_2 + \cdots + \boldsymbol{A}'_\ell\boldsymbol{b}_\ell. \end{aligned}$$

Now the determinant of $\boldsymbol{M}'$ is non-zero iff ϕ is injective. This requires $\sum_i^\ell \dim\big(\mathsf{kernel}(\boldsymbol{B}'_i)\big) \leq w$. Since $\boldsymbol{B}_i$ is row-full rank, we have $\mathsf{rank}(\boldsymbol{B}'_i) = r_i$ and $\dim\big(\mathsf{kernel}(\boldsymbol{B}'_i)\big) = k_i - r_i$. In this way, $\sum_i^\ell (k_i - r_i) \leq w$. Since $\sum_i^\ell k_i = r = w + \sum_i^\ell r_i$, $\sum_i^\ell (k_i - r_i) = w$.

Let $\nu_i = k_i - r_i$ for $i \in [\ell]$. For any $(\nu_1, \nu_2, \ldots, \nu_\ell)$ satisfying $\sum_i^\ell \nu_i = w$, choosing k_i columns from the i-th column block of $\boldsymbol{M}$ has $\binom{n_i}{r_i + \nu_i}$ cases. This leads to Equation (27). ∎

Remark 1 *For Lemma 2, we want to additionally say that: The conclusion can be extended to any ring; If $\boldsymbol{B}_i = \boldsymbol{0}$ for some $i \in [\ell]$, we set the corresponding r_i in Equation (27) as 0.*

Theorem 9 *For $\ell = 2$, with the blockwise errors, the number of linearly independent equations in the MM modeling over $\mathbb{F}_q$ is upper bounded by $\overline{E}(m,n,k,r,2,\boldsymbol{n},\boldsymbol{r})$. $\overline{E}(m,n,k,r,2,\boldsymbol{n},\boldsymbol{r})$ is:*

$$\begin{cases} m \sum\limits_{\nu_1+\nu_2=r_0-z_0} \binom{z_1}{r_1+z_0+\nu_1}\binom{n_2}{r_2+\nu_2}, & 0 < k+1 \le r_1; \\ m \sum\limits_{\nu_1+\nu_2=r_1} \binom{z_1}{\nu_1}\binom{n_2}{r_2+\nu_2}, & r_1 < k+1 \le n_1; \\ m\binom{z_2}{r}, & n_1 < k+1 \le n_1+n_2. \end{cases} \tag{28}$$

where $z_\iota = \sum_{i=0}^{\iota} n_i - (k+1)$ for $\iota \in [0,2]$, $r_0 = 0$, and $n_0 = 0$.

Proof: Recall Definition 8 in Section III-D, when $\ell = 2$, the coefficient matrix $\boldsymbol{C}$ of the blockwise error $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$:

$$\boldsymbol{C} = \mathbf{Diag}(\boldsymbol{C}_1, \boldsymbol{C}_2) \in \mathbb{F}_q^{r \times n},$$

where $\boldsymbol{C}_i \in \mathbb{F}_q^{r_i \times n_i}$ for $i \in [2]$ is of rank r_i and is in systematic form whose first r_i columns and first r_i rows form an identity matrix $\boldsymbol{I}_{r_i}$. Recall the MM modeling in Section III-E, we consider the parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ of the extended code $\mathcal{C}_{\boldsymbol{y}}$ in systematic form: $\boldsymbol{H}_{\boldsymbol{y}} = [\boldsymbol{P} \;\; \boldsymbol{I}_{n-k-1}]$ where $\boldsymbol{P} \in \mathbb{F}_{q^m}^{(n-k-1)\times(k+1)}$.

Case 1: $0 < k+1 \le r_1$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^\top = \begin{bmatrix} \boldsymbol{P}^\top \\ \boldsymbol{I}_{z_2} \end{bmatrix} = \left[\begin{array}{cc} \boldsymbol{Q} & \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{n_2} \end{array}\right] \in \mathbb{F}_{q^m}^{n \times z_2}$ where $\boldsymbol{Q} = \boldsymbol{P}^\top \in \mathbb{F}_{q^m}^{(-z_0)\times z_2}$. We write $\boldsymbol{C}_1 = \left[\begin{array}{c|c} \boldsymbol{C}_1' & \begin{matrix} \boldsymbol{C}_1'' \\ \boldsymbol{C}_1''' \end{matrix} \end{array}\right] \in \mathbb{F}_q^{r_1 \times n_1}$ where $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1 \times (-z_0)}$, $\boldsymbol{C}_1'' \in \mathbb{F}_q^{(-z_0)\times z_1}$, and $\boldsymbol{C}_1''' \in \mathbb{F}_q^{(r_1+z_0)\times z_1}$. Then

$$\boldsymbol{C}_1 \left[\begin{array}{c} \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_1} \;\; \boldsymbol{0} \end{array}\right] = \boldsymbol{C}_1'\boldsymbol{Q} + \begin{bmatrix} \boldsymbol{C}_1'' \\ \boldsymbol{C}_1''' \end{bmatrix} \begin{bmatrix} \boldsymbol{I}_{z_1} & \boldsymbol{0} \end{bmatrix} := \left[\begin{array}{c} \boldsymbol{T} \\ \hline \boldsymbol{C}_1''' \;\; \boldsymbol{0} \end{array}\right] \in \mathbb{F}_{q^m}^{r_1 \times z_2},$$

where $\boldsymbol{T} = \boldsymbol{Q} + \begin{bmatrix} \boldsymbol{C}_1'' & \boldsymbol{0} \end{bmatrix} \in \mathbb{F}_{q^m}^{(-z_0)\times z_2}$. Note that $\boldsymbol{C}_1$ is in systematic form whose first r_1 columns and first r_1 rows form an identity matrix $\boldsymbol{I}_{r_1}$. The first $-z_0$ rows of $\boldsymbol{C}_1'\boldsymbol{Q}$ form $\boldsymbol{Q}$ and the last (r_1+z_0) rows form $\boldsymbol{0}$ due to $-z_0 \le r_1$. In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top = \left[\begin{array}{cc} \boldsymbol{T} & \\ \hline \boldsymbol{C}_1''' & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{C}_2 \end{array}\right] \in \mathbb{F}_{q^m}^{r \times z_2}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ is $\sum\limits_{\nu_1+\nu_2=r_0-z_0} \binom{z_1}{r_1+z_0+\nu_1}\binom{n_2}{r_2+\nu_2}$.

Case 2: $r_1 < k+1 \le n_1$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^\top = \begin{bmatrix} \boldsymbol{P}^\top \\ \boldsymbol{I}_{z_2} \end{bmatrix} = \left[\begin{array}{cc} \boldsymbol{Q} & \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{n_2} \end{array}\right] \in \mathbb{F}_{q^m}^{n \times z_2}$ where $\boldsymbol{Q} = \boldsymbol{P}^\top \in \mathbb{F}_{q^m}^{(-z_0)\times z_2}$. We write $\boldsymbol{C}_1 = \left[\begin{array}{c|c} \boldsymbol{C}_1' & \boldsymbol{C}_1'' \end{array}\right] \in \mathbb{F}_q^{r_1 \times n_1}$ where $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1 \times (-z_0)}$ and $\boldsymbol{C}_1'' \in \mathbb{F}_q^{r_1 \times z_1}$. Then

$$\boldsymbol{C}_1 \left[\begin{array}{c} \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_1} \;\; \boldsymbol{0} \end{array}\right] = \boldsymbol{C}_1'\boldsymbol{Q} + \boldsymbol{C}_1'' \begin{bmatrix} \boldsymbol{I}_{z_1} & \boldsymbol{0} \end{bmatrix} := \boldsymbol{T} \in \mathbb{F}_{q^m}^{r_1 \times z_2}.$$

In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top = \left[\begin{array}{cc} \boldsymbol{Q} & \\ \hline \boldsymbol{0} & \boldsymbol{C}_2 \end{array}\right] \in \mathbb{F}_{q^m}^{r \times z_2}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ is $\sum\limits_{\nu_1+\nu_2=r_1} \binom{z_1}{\nu_1}\binom{n_2}{r_2+\nu_2}$.

Case 3: $n_1 < k+1 \le n_1 + r_2$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^\top = \begin{bmatrix} \boldsymbol{P}^\top \\ \boldsymbol{I}_{z_2} \end{bmatrix} = \left[\begin{array}{c} \boldsymbol{P}_1 \\ \hline \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_2} \end{array}\right] \in \mathbb{F}_{q^m}^{n \times z_3}$ where $\boldsymbol{P}_1 \in \mathbb{F}_{q^m}^{n_1 \times z_2}$ and $\boldsymbol{Q} \in \mathbb{F}_{q^m}^{(-z_1)\times z_2}$. We write $\boldsymbol{C}_2 = \left[\begin{array}{c|c} \boldsymbol{C}_2' & \begin{matrix} \boldsymbol{C}_2'' \\ \boldsymbol{C}_2''' \end{matrix} \end{array}\right] \in \mathbb{F}_q^{r_2 \times n_2}$ where $\boldsymbol{C}_2' \in \mathbb{F}_q^{r_2 \times (-z_1)}$, $\boldsymbol{C}_2'' \in \mathbb{F}_q^{(-z_1)\times z_2}$, and $\boldsymbol{C}_2''' \in \mathbb{F}_q^{(r_2+z_1)\times z_2}$. Then

$$\boldsymbol{C}_2 \left[\begin{array}{c} \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_2} \end{array}\right] = \boldsymbol{C}_2'\boldsymbol{Q} + \begin{bmatrix} \boldsymbol{C}_2'' \\ \boldsymbol{C}_2''' \end{bmatrix} \boldsymbol{I}_{z_2} := \left[\begin{array}{c} \boldsymbol{T} \\ \hline \boldsymbol{C}_2''' \end{array}\right] \in \mathbb{F}_{q^m}^{r_2 \times z_2},$$

where $\boldsymbol{T} = \boldsymbol{Q} + \begin{bmatrix} \boldsymbol{C}_2'' & \boldsymbol{0} \end{bmatrix} \in \mathbb{F}_{q^m}^{(-z_1)\times z_2}$. Note that $\boldsymbol{C}_2$ is in systematic form whose first r_2 columns and first r_2 rows form an identity matrix $\boldsymbol{I}_{r_2}$. The first $-z_1$ rows of $\boldsymbol{C}_2'\boldsymbol{Q}$ form $\boldsymbol{Q}$ and the last (r_2+z_1) rows form $\boldsymbol{0}$ due to $-z_1 \le r_2$. In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top = \left[\begin{array}{c} \boldsymbol{C}_1\boldsymbol{P}_1 \\ \hline \boldsymbol{T} \\ \hline \boldsymbol{C}_2''' \end{array}\right] \in \mathbb{F}_{q^m}^{r \times z_2}.$$

Obviously, $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ does not contain large zero submatrices. Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is around $\sum_{\nu_2=r_1-z_1} \binom{z_2}{r_2+z_1+\nu_2} = \binom{z_2}{r}$.

Case 4: $n_1+r_2 < k+1 \le n_1+n_2$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{P}^{\top} \\ \boldsymbol{I}_{z_2} \end{array}\right] = \left[\begin{array}{c} \boldsymbol{P}_1 \\ \hline \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_2} \end{array}\right] \in \mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{P}_1 \in \mathbb{F}_{q^m}^{n_1\times z_2}$ and $\boldsymbol{Q} \in \mathbb{F}_{q^m}^{(-z_1)\times z_2}$. We write $\boldsymbol{C}_2 = \left[\begin{array}{c|c} \boldsymbol{C}_2' & \boldsymbol{C}_2'' \end{array}\right] \in \mathbb{F}_q^{r_2\times n_2}$ where $\boldsymbol{C}_2' \in \mathbb{F}_q^{r_2\times(-z_1)}$ and $\boldsymbol{C}_2'' \in \mathbb{F}_q^{r_2\times z_2}$. Then

$$\boldsymbol{C}_2\left[\begin{array}{c} \boldsymbol{Q} \\ \hline \boldsymbol{I}_{z_2} \end{array}\right] = \boldsymbol{C}_2'\boldsymbol{Q} + \boldsymbol{C}_2''\boldsymbol{I}_{z_2} := \boldsymbol{T} \in \mathbb{F}_{q^m}^{r_2\times z_2}.$$

In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{C}_1\boldsymbol{P}_1 \\ \hline \boldsymbol{T} \end{array}\right] \in \mathbb{F}_{q^m}^{r\times z_2}.$$

Obviously, $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ does not contain large zero submatrices. Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is around $\sum_{\nu_2=r_1+r_2} \binom{z_2}{\nu_2} = \binom{z_2}{r}$.

In **Cases** 1-4, we analyze the number of non-zero equations of the MM modeling over $\mathbb{F}_{q^m}$ and obtain an upper bound of linearly independent equations. By unfolding these equations over $\mathbb{F}_q$, we can obtain a factor m, which leads to $\overline{E}(m,n,k,r,2,\boldsymbol{n},\boldsymbol{r})$. ■

Theorem 10 *For $\ell = 3$, with the blockwise errors, the number of linearly independent equations in the MM modeling over $\mathbb{F}_q$ is upper bounded by $\overline{E}(m,n,k,r,3,\boldsymbol{n},\boldsymbol{r})$. $\overline{E}(m,n,k,r,3,\boldsymbol{n},\boldsymbol{r})$ is:*

$$\begin{cases} m \sum\limits_{\nu_1+\nu_2+\nu_3=r_0-z_0} \binom{z_1}{r_1+z_0+\nu_1}\binom{n_2}{r_2+\nu_2}\binom{n_3}{r_3+\nu_3}, & 0 < k+1 \le r_1; \\ m \sum\limits_{\nu_1+\nu_2+\nu_3=r_1} \binom{z_1}{\nu_1}\binom{n_2}{r_2+\nu_2}\binom{n_3}{r_3+\nu_3}, & r_1 < k+1 \le n_1; \\ m \sum\limits_{\nu_2+\nu_3=r_1-z_1} \binom{z_2}{r_2+z_1+\nu_2}\binom{n_3}{r_3+\nu_3}, & n_1 < k+1 \le n_1+r_2; \\ m \sum\limits_{\nu_2+\nu_3=r_1+r_2} \binom{z_2}{\nu_2}\binom{n_3}{r_3+\nu_3}, & n_1+r_2 < k+1 \le n_1+n_2; \\ m\binom{z_3}{r}, & n_1+n_2 < k+1 \le n_1+n_2+n_3. \end{cases} \tag{29}$$

where $z_\iota = \sum_{i=0}^{\iota} n_i - (k+1)$ for $\iota \in [0,3]$, $r_0 = 0$, and $n_0 = 0$.

Proof: Recall Definition 8 in Section III-D, when $\ell = 3$, the coefficient matrix $\boldsymbol{C}$ of the blockwise error $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$:

$$\boldsymbol{C} = \mathbf{Diag}(\boldsymbol{C}_1, \boldsymbol{C}_2, \boldsymbol{C}_3) \in \mathbb{F}_q^{r\times n},$$

where $\boldsymbol{C}_i \in \mathbb{F}_q^{r_i\times n_i}$ for $i \in [3]$ is of rank r_i and is in systematic form whose first r_i columns and first r_i rows form an identity matrix $\boldsymbol{I}_{r_i}$. Recall the MM modeling in Section III-E, we consider the parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ of the extended code $\mathcal{C}_{\boldsymbol{y}}$ in systematic form: $\boldsymbol{H}_{\boldsymbol{y}} = [\boldsymbol{P} \;\; \boldsymbol{I}_{n-k-1}]$ where $\boldsymbol{P} \in \mathbb{F}_{q^m}^{(n-k-1)\times(k+1)}$.

Case 1: $0 < k+1 \le r_1$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{P}^{\top} \\ \boldsymbol{I}_{z_3} \end{array}\right] = \left[\begin{array}{ccc} \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{n_2} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{n_3} \end{array}\right] \in \mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{Q} = \boldsymbol{P}^{\top} \in \mathbb{F}_{q^m}^{(-z_0)\times z_3}$. We write $\boldsymbol{C}_1 = \left[\begin{array}{c|c} \boldsymbol{C}_1' & \begin{array}{c}\boldsymbol{C}_1'' \\ \boldsymbol{C}_1'''\end{array} \end{array}\right] \in \mathbb{F}_q^{r_1\times n_1}$ where $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1\times(-z_0)}$, $\boldsymbol{C}_1'' \in \mathbb{F}_q^{(-z_0)\times z_1}$, and $\boldsymbol{C}_1''' \in \mathbb{F}_q^{(r_1+z_0)\times z_1}$. Then

$$\boldsymbol{C}_1\left[\begin{array}{ccc} \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] = \boldsymbol{C}_1'\boldsymbol{Q} + \left[\begin{array}{c} \boldsymbol{C}_1'' \\ \boldsymbol{C}_1''' \end{array}\right]\left[\begin{array}{ccc} \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] := \left[\begin{array}{ccc} \multicolumn{3}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{C}_1''' & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] \in \mathbb{F}_{q^m}^{r_1\times z_3},$$

where $\boldsymbol{T} = \boldsymbol{Q} + \left[\begin{array}{ccc} \boldsymbol{C}_1'' & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] \in \mathbb{F}_{q^m}^{(-z_0)\times z_3}$. Note that $\boldsymbol{C}_1$ is in systematic form whose first r_1 columns and first r_1 rows form an identity matrix $\boldsymbol{I}_{r_1}$. The first $-z_0$ rows of $\boldsymbol{C}_1'\boldsymbol{Q}$ form $\boldsymbol{Q}$ and the last (r_1+z_0) rows form $\boldsymbol{0}$ due to $-z_0 \le r_1$. In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{ccc} \multicolumn{3}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{C}_1''' & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{C}_2 & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{C}_3 \end{array}\right] \in \mathbb{F}_{q^m}^{r\times z_3}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is $\sum_{\nu_1+\nu_2+\nu_3=r_0-z_0} \binom{z_1}{r_1+z_0+\nu_1}\binom{n_2}{r_2+\nu_2}\binom{n_3}{r_3+\nu_3}$.

Case 2: $r_1 < k+1 \leq n_1$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{P}^{\top} \\ \boldsymbol{I}_{z_3} \end{array}\right] = \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{I}_{n_2} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{I}_{n_3} \end{array}\right] \in \mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{Q} = \boldsymbol{P}^{\top} \in \mathbb{F}_{q^m}^{(-z_0)\times z_3}$. We write $\boldsymbol{C}_1 = \left[\begin{array}{c|c} \boldsymbol{C}_1' & \boldsymbol{C}_1'' \end{array}\right] \in \mathbb{F}_q^{r_1\times n_1}$ where $\boldsymbol{C}_1' \in \mathbb{F}_q^{r_1\times(-z_0)}$ and $\boldsymbol{C}_1'' \in \mathbb{F}_q^{r_1\times z_1}$. Then

$$\boldsymbol{C}_1\left[\begin{array}{c|ccc} \multicolumn{4}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] = \boldsymbol{C}_1'\boldsymbol{Q} + \boldsymbol{C}_1''\left[\begin{array}{ccc} \boldsymbol{I}_{z_1} & \boldsymbol{0} & \boldsymbol{0} \end{array}\right] := \boldsymbol{T} \in \mathbb{F}_{q^m}^{r_1\times z_3}.$$

In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c|ccc} \multicolumn{4}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{0} & \boldsymbol{C}_2 & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{C}_3 \end{array}\right] \in \mathbb{F}_{q^m}^{r\times z_3}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is $\sum_{\nu_1+\nu_2+\nu_3=r_1} \binom{z_1}{\nu_1}\binom{n_2}{r_2+\nu_2}\binom{n_3}{r_3+\nu_3}$.

Case 3: $n_1 < k+1 \leq n_1+r_2$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{P}^{\top} \\ \boldsymbol{I}_{z_3} \end{array}\right] = \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{P}_1} \\ \hline \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_2} & \boldsymbol{0} & \\ \boldsymbol{0} & \boldsymbol{I}_{n_3} & \end{array}\right] \in \mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{P}_1 \in \mathbb{F}_{q^m}^{n_1\times z_3}$ and $\boldsymbol{Q} \in \mathbb{F}_{q^m}^{(-z_1)\times z_3}$. We write $\boldsymbol{C}_2 = \left[\begin{array}{c|c} \boldsymbol{C}_2' & \begin{array}{c}\boldsymbol{C}_2'' \\ \boldsymbol{C}_2'''\end{array} \end{array}\right] \in \mathbb{F}_q^{r_2\times n_2}$ where $\boldsymbol{C}_2' \in \mathbb{F}_q^{r_2\times(-z_1)}$, $\boldsymbol{C}_2'' \in \mathbb{F}_q^{(-z_1)\times z_2}$, and $\boldsymbol{C}_2''' \in \mathbb{F}_q^{(r_2+z_1)\times z_2}$. Then

$$\boldsymbol{C}_2\left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_2} & \boldsymbol{0} & \end{array}\right] = \boldsymbol{C}_2'\boldsymbol{Q} + \left[\begin{array}{c}\boldsymbol{C}_2'' \\ \boldsymbol{C}_2'''\end{array}\right]\left[\begin{array}{cc} \boldsymbol{I}_{z_2} & \boldsymbol{0} \end{array}\right] := \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{C}_2''' & \boldsymbol{0} & \end{array}\right] \in \mathbb{F}_{q^m}^{r_2\times z_3},$$

where $\boldsymbol{T} = \boldsymbol{Q} + \left[\begin{array}{cc} \boldsymbol{C}_2'' & \boldsymbol{0} \end{array}\right] \in \mathbb{F}_{q^m}^{(-z_1)\times z_3}$. Note that $\boldsymbol{C}_2$ is in systematic form whose first r_2 columns and first r_2 rows form an identity matrix $\boldsymbol{I}_{r_2}$. The first $-z_1$ rows of $\boldsymbol{C}_2'\boldsymbol{Q}$ form $\boldsymbol{Q}$ and the last (r_2+z_1) rows form $\boldsymbol{0}$ due to $-z_1 \leq r_2$. In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{C}_1\boldsymbol{P}_1} \\ \hline \multicolumn{3}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{C}_2''' & \boldsymbol{0} & \\ \boldsymbol{0} & \boldsymbol{C}_3 & \end{array}\right] \in \mathbb{F}_{q^m}^{r\times z_3}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is $\sum_{\nu_2+\nu_3=r_1-z_1} \binom{z_2}{r_2+z_1+\nu_2}\binom{n_3}{r_3+\nu_3}$.

Case 4: $n_1+r_2 < k+1 \leq n_1+n_2$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c} \boldsymbol{P}^{\top} \\ \boldsymbol{I}_{z_3} \end{array}\right] = \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{P}_1} \\ \hline \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_2} & \boldsymbol{0} & \\ \boldsymbol{0} & \boldsymbol{I}_{n_3} & \end{array}\right] \in \mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{P}_1 \in \mathbb{F}_{q^m}^{n_1\times z_3}$ and $\boldsymbol{Q} \in \mathbb{F}_{q^m}^{(-z_1)\times z_3}$. We write $\boldsymbol{C}_2 = \left[\begin{array}{c|c} \boldsymbol{C}_2' & \boldsymbol{C}_2'' \end{array}\right] \in \mathbb{F}_q^{r_2\times n_2}$ where $\boldsymbol{C}_2' \in \mathbb{F}_q^{r_2\times(-z_1)}$ and $\boldsymbol{C}_2'' \in \mathbb{F}_q^{r_2\times z_2}$. Then

$$\boldsymbol{C}_2\left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{Q}} \\ \hline \boldsymbol{I}_{z_2} & \boldsymbol{0} & \end{array}\right] = \boldsymbol{C}_2'\boldsymbol{Q} + \boldsymbol{C}_2''\left[\begin{array}{cc} \boldsymbol{I}_{z_2} & \boldsymbol{0} \end{array}\right] := \boldsymbol{T} \in \mathbb{F}_{q^m}^{r_2\times z_3}.$$

In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top} = \left[\begin{array}{c|cc} \multicolumn{3}{c}{\boldsymbol{C}_1\boldsymbol{P}_1} \\ \hline \multicolumn{3}{c}{\boldsymbol{T}} \\ \hline \boldsymbol{0} & \boldsymbol{C}_3 & \end{array}\right] \in \mathbb{F}_{q^m}^{r\times z_3}.$$

Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^{\top}$ is $\sum_{\nu_2+\nu_3=r_1+r_2} \binom{z_2}{\nu_2}\binom{n_3}{r_3+\nu_3}$.

Case 5: $n_1+n_2<k+1\le n_1+n_2+r_3$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^\top=\left[\begin{array}{c}\boldsymbol{P}^\top\\ \boldsymbol{I}_{z_3}\end{array}\right]=\left[\begin{array}{c}\boldsymbol{P}_1\\ \hline \boldsymbol{P}_2\\ \hline \boldsymbol{Q}\\ \hline \boldsymbol{I}_{z_3}\end{array}\right]\in\mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{P}_1\in\mathbb{F}_{q^m}^{n_1\times z_3}$, $\boldsymbol{P}_2\in\mathbb{F}_{q^m}^{n_2\times z_3}$, and $\boldsymbol{Q}\in\mathbb{F}_{q^m}^{(-z_2)\times z_3}$. We write $\boldsymbol{C}_3=\left[\begin{array}{c|c}\boldsymbol{C}_3' & \begin{array}{c}\boldsymbol{C}_3''\\ \boldsymbol{C}_3'''\end{array}\end{array}\right]\in\mathbb{F}_q^{r_3\times n_3}$ where $\boldsymbol{C}_3'\in\mathbb{F}_q^{r_3\times(-z_2)}$, $\boldsymbol{C}_3''\in\mathbb{F}_q^{(-z_2)\times z_3}$, and $\boldsymbol{C}_3'''\in\mathbb{F}_q^{(r_3+z_2)\times z_3}$. Then

$$\boldsymbol{C}_3\left[\begin{array}{c}\boldsymbol{Q}\\ \hline \boldsymbol{I}_{z_3}\end{array}\right]=\boldsymbol{C}_3'\boldsymbol{Q}+\left[\begin{array}{c}\boldsymbol{C}_3''\\ \boldsymbol{C}_3'''\end{array}\right]\boldsymbol{I}_{z_3}:=\left[\begin{array}{c}\boldsymbol{T}\\ \hline \boldsymbol{C}_3'''\end{array}\right]\in\mathbb{F}_{q^m}^{r_3\times z_3},$$

where $\boldsymbol{T}=\boldsymbol{Q}+\boldsymbol{C}_3''\in\mathbb{F}_{q^m}^{(-z_2)\times z_3}$. Note that $\boldsymbol{C}_3$ is in systematic form whose first r_3 columns and first r_3 rows form an identity matrix $\boldsymbol{I}_{r_3}$. The first $-z_2$ rows of $\boldsymbol{C}_3'\boldsymbol{Q}$ form $\boldsymbol{Q}$ and the last (r_3+z_2) rows form $\boldsymbol{0}$ due to $-z_2\le r_3$. In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top=\left[\begin{array}{c}\boldsymbol{C}_1\boldsymbol{P}_1\\ \hline \boldsymbol{C}_2\boldsymbol{P}_2\\ \hline \boldsymbol{T}\\ \hline \boldsymbol{C}_3'''\end{array}\right]\in\mathbb{F}_{q^m}^{r\times z_3}.$$

Obviously, $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ does not contain large zero submatrices. Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ is around $\sum_{\nu_3=r_1+r_2-z_2}\binom{z_3}{r_3+z_2+\nu_3}=\binom{z_3}{r}$.

Case 6: $n_1+n_2+r_3<k+1\le n_1+n_2+n_3$.

We write $\boldsymbol{H}_{\boldsymbol{y}}^\top=\left[\begin{array}{c}\boldsymbol{P}^\top\\ \boldsymbol{I}_{z_3}\end{array}\right]=\left[\begin{array}{c}\boldsymbol{P}_1\\ \hline \boldsymbol{P}_2\\ \hline \boldsymbol{Q}\\ \hline \boldsymbol{I}_{z_3}\end{array}\right]\in\mathbb{F}_{q^m}^{n\times z_3}$ where $\boldsymbol{P}_1\in\mathbb{F}_{q^m}^{n_1\times z_3}$, $\boldsymbol{P}_2\in\mathbb{F}_{q^m}^{n_2\times z_3}$, and $\boldsymbol{Q}\in\mathbb{F}_{q^m}^{(-z_2)\times z_3}$. We write $\boldsymbol{C}_3=\left[\begin{array}{c|c}\boldsymbol{C}_3' & \boldsymbol{C}_3''\end{array}\right]\in\mathbb{F}_q^{r_3\times n_3}$ where $\boldsymbol{C}_3'\in\mathbb{F}_q^{r_3\times(-z_2)}$ and $\boldsymbol{C}_3''\in\mathbb{F}_q^{r_3\times z_3}$. Then

$$\boldsymbol{C}_3\left[\begin{array}{c}\boldsymbol{Q}\\ \hline \boldsymbol{I}_{z_3}\end{array}\right]=\boldsymbol{C}_3'\boldsymbol{Q}+\boldsymbol{C}_3''\boldsymbol{I}_{z_3}:=\boldsymbol{T}\in\mathbb{F}_{q^m}^{r_3\times z_3}.$$

In this way,

$$\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top=\left[\begin{array}{c}\boldsymbol{C}_1\boldsymbol{P}_1\\ \hline \boldsymbol{C}_2\boldsymbol{P}_2\\ \hline \boldsymbol{T}\end{array}\right]\in\mathbb{F}_{q^m}^{r\times z_3}.$$

Obviously, $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ does not contain large zero submatrices. Then, by Lemma 2, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ is around $\sum_{\nu_3=r}\binom{z_3}{\nu_3}=\binom{z_3}{r}$.

In **Cases** 1-6, we analyze the number of non-zero equations of the MM modeling over $\mathbb{F}_{q^m}$ and obtain an upper bound of linearly independent equations. By unfolding these equations over $\mathbb{F}_q$, we can obtain a factor m, which leads to $\overline{E}(m,n,k,r,3,\boldsymbol{n},\boldsymbol{r})$. ■

Theorem 11 *For general ℓ, with the blockwise errors, the number of linearly independent equations in the MM modeling over $\mathbb{F}_q$ is upper bounded by $\overline{E}(m,n,k,r,\ell,\boldsymbol{n},\boldsymbol{r})$. $\overline{E}(m,n,k,r,\ell,\boldsymbol{n},\boldsymbol{r})$ is*

$$\begin{cases} m\sum\limits_{\sum_{i=\ell-j+1}^{\ell}\nu_i=\sum_{i=0}^{\ell-j}r_i-z_{\ell-j}}\binom{z_{\ell-j+1}}{r_{\ell-j+1}+z_{\ell-j}+\nu_{\ell-j+1}}\prod\limits_{i=\ell-j+2}^{\ell}\binom{n_i}{r_i+\nu_i}, & \sum_{i=0}^{\ell-j}n_i<k+1\le\sum_{i=0}^{\ell-j}n_i+r_{\ell-j+1};\\ m\sum\limits_{\sum_{i=\ell-j+1}^{\ell}\nu_i=\sum_{i=0}^{\ell-j+1}r_i}\binom{z_{\ell-j+1}}{\nu_{\ell-j+1}}\prod\limits_{i=\ell-j+2}^{\ell}\binom{n_i}{r_i+\nu_i}, & \sum_{i=0}^{\ell-j}n_i+r_{\ell-j+1}<k+1\le\sum_{i=0}^{\ell-j+1}n_i. \end{cases} \tag{30}$$

where $j\in[\ell]$, $z_\iota=\sum_{i=0}^{\iota}n_i-(k+1)$ for $\iota\in[0,\ell]$, $r_0=0$, and $n_0=0$. We denote $\prod_{i=\ell-j+2}^{\ell}\binom{n_i}{r_i+\nu_i}=1$ if $\ell-j+2>\ell$.

Proof: Recall Definition 8 in Section III-D, for general ℓ, the coefficient matrix $\boldsymbol{C}$ of $\boldsymbol{e}\in\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$:

$$\boldsymbol{C}=\mathbf{Diag}(\boldsymbol{C}_1,\boldsymbol{C}_2,\boldsymbol{C}_3,\ldots,\boldsymbol{C}_\ell)\in\mathbb{F}_q^{r\times n},$$

where $\boldsymbol{C}_i\in\mathbb{F}_q^{r_i\times n_i}$ for $i\in[\ell]$ is of rank r_i and is in systematic form whose first r_i columns and first r_i rows form an identity matrix $\boldsymbol{I}_{r_i}$. Recall the MM modeling in Section III-E, we consider the parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ of the extended code $\mathcal{C}_{\boldsymbol{y}}$ in systematic form: $\boldsymbol{H}_{\boldsymbol{y}}=[\boldsymbol{P}\ \ \boldsymbol{I}_{n-k-1}]$ where $\boldsymbol{P}\in\mathbb{F}_{q^m}^{(n-k-1)\times(k+1)}$.

We can generalize the proof of Theorem 10 and obtain $\overline{E}(m,n,k,r,\ell,\boldsymbol{n},\boldsymbol{r})$. This can be done naturally by induction. ■

Simulations. We here give some experiments on simulable parameters to verify the correctness and tightness of our derived upper bound. We simulate two types of the BRD instances, i.e., $\ell = 2$ and $\ell = 3$. The simulated results are presented in Table II. Form Table II, we can conclude that

- Our bound is correct. We can observe SLIE $\leq$ TNE for all parameters.
- Our bound is tight. We can observe that as k continues to increase, TNE is getting closer to SLIE; after some point where k is about n_1, TNE is exactly SLIE. $k = n_1$ is also the case of current cryptographic parameters.
- TNE is a lower bound of the non-zero equations in the MM modeling over $\mathbb{F}_{q^m}$. In Theorem 9 and Theorem 10, one can find that we do not point out whether we obtained an upper bound or a lower bound. By our experiments, we can observe SNE $\geq$ TNE. This shows that we obtain a lower bound. We have SLIE $\leq$ TNE $\leq$ SNE.

TABLE II
SIMULATED UPPER BOUND ON LINEARLY INDEPENDENT EQUATIONS.

ℓ	(q,m,n,k,r)	$\boldsymbol{n}$	$\boldsymbol{r}$	SME	SNE	SLIE	TNE	TME
2	$(2,9,12,1,4)$	$(6,6)$	$(2,2)$	210	185	160	185	210
	$(2,9,12,2,4)$	$(6,6)$	$(2,2)$	126	120	114	120	126
	$(2,9,12,3,4)$	$(6,6)$	$(2,2)$	70	70	70	70	70
	$(2,9,12,4,4)$	$(6,6)$	$(2,2)$	35	35	35	35	35
	$(2,9,12,5,4)$	$(6,6)$	$(2,2)$	15	15	15	15	15
	$(2,9,12,3,4)$	$(8,4)$	$(2,2)$	70	70	53	53	70
	$(2,9,12,4,4)$	$(8,4)$	$(2,2)$	35	35	31	31	35
	$(2,9,12,5,4)$	$(8,4)$	$(2,2)$	15	15	15	15	15
3	$(2,9,15,1,6)$	$(5,5,5)$	$(2,2,2)$	1716	1100	792	1100	1716
	$(2,9,15,2,6)$	$(5,5,5)$	$(2,2,2)$	924	700	588	700	924
	$(2,9,15,3,6)$	$(5,5,5)$	$(2,2,2)$	462	400	369	400	462
	$(2,9,15,4,6)$	$(5,5,5)$	$(2,2,2)$	210	200	195	200	210
	$(2,9,15,5,6)$	$(5,5,5)$	$(2,2,2)$	84	84	84	84	84
	$(2,9,15,6,6)$	$(5,5,5)$	$(2,2,2)$	28	28	28	28	28
	$(2,9,15,7,6)$	$(5,5,5)$	$(2,2,2)$	7	7	7	7	7
	$(2,9,15,6,6)$	$(6,5,4)$	$(2,2,2)$	28	28	28	28	28
	$(2,9,15,7,6)$	$(7,5,3)$	$(2,2,2)$	7	7	7	7	7
	$(2,9,17,8,6)$	$(8,5,4)$	$(2,2,2)$	28	28	28	28	28
	$(2,9,17,8,6)$	$(8,6,3)$	$(2,2,2)$	28	28	25	25	28
	$(2,9,17,8,6)$	$(8,7,2)$	$(2,2,2)$	28	28	15	15	28
	$(2,9,20,7,6)$	$(14,3,3)$	$(2,2,2)$	924	172	172	172	924
	$(2,9,20,8,6)$	$(14,3,3)$	$(2,2,2)$	462	121	121	121	462
	$(2,9,20,9,6)$	$(14,3,3)$	$(2,2,2)$	210	79	79	79	210
	$(2,9,20,10,6)$	$(14,3,3)$	$(2,2,2)$	84	46	46	46	84
	$(2,9,20,7,6)$	$(3,3,14)$	$(2,2,2)$	924	172	172	924	924
	$(2,9,20,8,6)$	$(3,3,14)$	$(2,2,2)$	462	121	121	462	462
	$(2,9,20,9,6)$	$(3,3,14)$	$(2,2,2)$	210	79	79	210	210
	$(2,9,20,10,6)$	$(3,3,14)$	$(2,2,2)$	84	46	46	84	84

SME: Simulated Maximal Equations. SNE: Simulated Non-zero Equations. SLIE: Simulated Linearly Independent Equations. TNE: Theoretical Non-zero Equations $\overline{E}(m,n,k,r,\ell,\boldsymbol{n},\boldsymbol{r})/m$. TME: Theoretical Maximal Equations $\binom{n-k-1}{r}$. The scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

Remark 2 *For the computation of $\overline{E}(m,n,k,r,\ell,\boldsymbol{n},\boldsymbol{r})$, we want to additionally explain three points:*

1) *For a tighter bound, we should sort n_i's for $i \in [\ell]$ such that $n_1 \geq n_2 \geq \cdots \geq n_\ell$ if $r_1 = r_2 = \cdots = r_\ell$. In the proofs of Theorem 9 and Theorem 10, we can observe that as $k+1$ continues to increase and exceeds $n_1, n_1+n_2, ...$, the number of non-zero maximal minors of $\boldsymbol{C}\boldsymbol{H}_{\boldsymbol{y}}^\top$ will be estimated up to* TME*: $\binom{n-k-1}{r}$. Thus, we hope $n_1 \geq n_2 \geq \cdots \geq n_\ell$ to slow down the speed at which $k+1$ exceeds $n_1, n_1+n_2, ...$ and obtain more zero maximal minors. In the last eight groups of parameters in Table II, one can observe that if $\boldsymbol{n} = (3,3,14)$, (*SME, SNE, SLIE*) keeps unchanged, and* TNE *is equal to* TME.
2) *Similarly, for a tighter bound, we should sort r_i's for $i \in [\ell]$ if $n_1 = n_2 = \cdots = n_\ell$.*
3) *Generally, for a tighter bound, we should permute pair (n_i, r_i) for $i \in [\ell]$ if the values of both n_i's and r_i's are general.*

The reasons that the above arguments hold are as follows.

1) *From Lemma 1, we known that the linear dependence of equations in the MM modeling is independent of the form of the parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$ of $\mathcal{C}_{\boldsymbol{y}}$. Then, in the proofs of Theorem 9 and Theorem 10, in the systematic parity-check matrix $\boldsymbol{H}_{\boldsymbol{y}}$, we can assume that any $n-k-1$ columns constitute the identity matrix $\boldsymbol{I}_{n-k-1}$.*
2) *Given an instance $(\boldsymbol{G},\boldsymbol{y},\boldsymbol{e})$ of the $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem, one can apply a permutation matrix $\boldsymbol{P}$ to the instance and obtain the instance $(\boldsymbol{G}\boldsymbol{P},\boldsymbol{y}\boldsymbol{P},\boldsymbol{e}\boldsymbol{P})$. Because $\boldsymbol{e}\boldsymbol{P}$ keeps the support of $\boldsymbol{e}$, solving $(\boldsymbol{G},\boldsymbol{y},\boldsymbol{e})$ is equivalent to solving $(\boldsymbol{G}\boldsymbol{P},\boldsymbol{y}\boldsymbol{P},\boldsymbol{e}\boldsymbol{P})$. This means that the complexity of problems is independent of the order of $\boldsymbol{e}_1, \boldsymbol{e}_2, ..., \boldsymbol{e}_\ell$.*

C. The MM Modeling From BRD With the BP Approach

The puncturing approach is proposed in [32] for solving the MM modeling from the RD problem. For solving the MM modeling derived from the BRD problem, the puncturing approach is also used in [3]. The goal of the puncturing approach

is to reducing the decoding complexity. The idea is to puncture the instance of the decoding problem, then apply the MM modeling to the punctured instance.

One could note that the puncturing approach in [3] only considers the puncturing of the last p coordinates of the last error block. Here, we propose to puncture on the last p_i coordinates of each error block for appropriate p_i for $i \in [\ell]$. This is also the reason that the method is called the Blockwise Puncturing (BP) approach. The soundness and correctness of the BP approach are presented in Theorem 12. Solving the BRD problem is equivalent to solving its punctured version. The best attack on the punctured version is the MM modeling. We recall the MM modeling derived from the BRD problem in Section III-E.

Recall that $\boldsymbol{n} = (n_1, n_2, \ldots, n_\ell)$ and $\boldsymbol{r} = (r_1, r_2, \ldots, r_\ell)$ are integers vector, $n = \sum_{i=1}^{\ell} n_i$, $r = \sum_{i=1}^{\ell} r_i$. The $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem asks an algorithm given as inputs a generator matrix $\boldsymbol{G}$ of a random $[n,k]_{q^m}$-linear code $\mathcal{C}$, and a vector $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$, to output $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ and a blockwise error $\boldsymbol{e} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_\ell) \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$.

By the block length $\boldsymbol{n}$, we split $\boldsymbol{y}$ as $(\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_\ell)$ and split $\boldsymbol{G}$ as $[\boldsymbol{G}_1, \boldsymbol{G}_2, \ldots, \boldsymbol{G}_\ell]$ by columns. Let $\boldsymbol{p} = (p_1, p_2, \ldots, p_\ell)$ be an integers vector and $p = \sum_{i=1}^{\ell} p_i$. Let $\mathbf{BP}^{\boldsymbol{p}}(\cdot)$ be the BP operation. Applying $\mathbf{BP}^{\boldsymbol{p}}(\cdot)$ to $\boldsymbol{e}$, $\boldsymbol{y}$, and $\boldsymbol{G}$, let

$$\begin{aligned}
\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e}) &= \left(\mathbf{BP}^{p_1}(\boldsymbol{e}_1), \mathbf{BP}^{p_2}(\boldsymbol{e}_2), \ldots, \mathbf{BP}^{p_\ell}(\boldsymbol{e}_\ell)\right) \in \mathbb{F}_{q^m}^{n-p}, \\
\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}) &= \left(\mathbf{BP}^{p_1}(\boldsymbol{y}_1), \mathbf{BP}^{p_2}(\boldsymbol{y}_2), \ldots, \mathbf{BP}^{p_\ell}(\boldsymbol{y}_\ell)\right) \in \mathbb{F}_{q^m}^{n-p}, \\
\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}) &= \left[\mathbf{BP}^{p_1}(\boldsymbol{G}_1), \mathbf{BP}^{p_2}(\boldsymbol{G}_2), \ldots, \mathbf{BP}^{p_\ell}(\boldsymbol{G}_\ell)\right] \in \mathbb{F}_{q^m}^{k\times(n-p)},
\end{aligned}$$

where $\mathbf{BP}^{p_i}(\boldsymbol{e}_i)$ (resp. $\mathbf{BP}^{p_i}(\boldsymbol{y}_i)$) is the operation puncturing on the last p_i coordinates of $\boldsymbol{e}_i$ (resp. $\boldsymbol{y}_i$), and $\mathbf{BP}^{p_i}(\boldsymbol{G}_i)$ is the operation puncturing on the last p_i columns of $\boldsymbol{G}_i$.

After applying the $\mathbf{BP}^{\boldsymbol{p}}(\cdot)$ operation to the instance $(\boldsymbol{G}, \boldsymbol{y})$ of the $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem, we have $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}) = \boldsymbol{x}\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}) + \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e})$. Based on this observation, we have Theorem 12.

Theorem 12 *Assume that the first r_i coordinates of $\boldsymbol{e}_i$ are linearly independent over $\mathbb{F}_q$ for $i \in [\ell]$. If $n_i - p_i \geq r_i$ and $n - p > k$, then solving the instance $(\boldsymbol{G}, \boldsymbol{y})$ of the $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem is equivalent to solving the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$ of the $\mathsf{BRD}_{q,m,n-p,k,r}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}$ problem.*

Proof: Since $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ is a random matrix, $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}) \in \mathbb{F}_{q^m}^{k\times(n-p)}$ is also a random matrix. Then $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}) \in \mathbb{F}_{q^m}^{k\times(n-p)}$ can be viewed as a generator matrix of a random $[n-p,k]_{q^m}$-linear codes due to $n - p > k$.

Since $p_i \leq n_i - r_i$ and the first r_i coordinates of $\boldsymbol{e}_i$ are linearly independent over $\mathbb{F}_q$ for $i \in [\ell]$, we have that $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e})$ and $\boldsymbol{e}$ share the same support and $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e})$ is still a blockwise error and is in the set $\mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}-\boldsymbol{p}}$.

Thus, $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$ is an instance of the $\mathsf{BRD}_{q,m,n-p,k,r}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}$ problem. Then, once the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$ is solved, one can obtain the support of $\boldsymbol{e}$, further can solve the instance $(\boldsymbol{G}, \boldsymbol{y})$ by using the obtained support; and vice versa. ∎

Remark 3 *The behind of attack is that the BP approach does not destroy the support of $\boldsymbol{e}$.*

- *By the density of the basis for random errors (see Section X-A), the assumption that the first r_i coordinates of $\boldsymbol{e}_i$ are linearly independent over $\mathbb{F}_q$ for $i \in [\ell]$ holds with an overwhelming probability.*
- *When solving $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$ fails, it might imply that the first r_i coordinates of $\boldsymbol{e}_i$ are linearly dependent over $\mathbb{F}_q$ for $i \in [\ell]$. In this case, we can perform a block diagonal invertible matrix*

$$\boldsymbol{P} = \mathbf{Diag}(\boldsymbol{P}_1, \boldsymbol{P}_2, \ldots, \boldsymbol{P}_\ell), \qquad \boldsymbol{P}_i \text{ is an invertible matrix of size } n_i \times n_i \text{ over } \mathbb{F}_q$$

on $(\boldsymbol{G}, \boldsymbol{y})$ to solve an instance $(\boldsymbol{G}\boldsymbol{P}, \boldsymbol{y}\boldsymbol{P})$ whose solution is $\boldsymbol{e}\boldsymbol{P} = (\boldsymbol{e}_1\boldsymbol{P}_1, \boldsymbol{e}_2\boldsymbol{P}_2, \ldots, \boldsymbol{e}_\ell\boldsymbol{P}_\ell) \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$. We require that $\boldsymbol{P}$ make the first r_i coordinates of $\boldsymbol{e}_i\boldsymbol{P}_i$ to be linearly independent over $\mathbb{F}_q$ for $i \in [\ell]$. Such $\boldsymbol{P}$ can be easily found in the rank metric setting.

By Theorem 12, for solving the $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem, one can first solve the $\mathsf{BRD}_{q,m,n-p,k,r}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}$ problem. The existing combinatorial attacks and algebraic attacks in [23] can be adapted to solving the $\mathsf{BRD}_{q,m,n-p,k,r}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}$ problem. The combinatorial attacks do not bring a significant gain because they either are independent of the code length or benefit from the large code length. One can observe that the BP approach only reduce the code length. The case of the algebraic attacks is different, especially for the MM attack. The MM attack can exploit the special structure of error to speed up attack. In the MM modeling derived from the $\mathsf{BRD}_{q,m,n-p,k,r}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}$ problem, the number of independent equations and unknowns is respectively

$$\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}), \qquad \prod_{i=1}^{\ell} \binom{n_i - p_i}{r_i}.$$

If there exists an appropriate $\boldsymbol{p}$ such that $\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i - p_i}{r_i} - 1$, one can

1) Solve the MM modeling to obtain $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e})$ and its support;

2) Solve the instance $(\boldsymbol{G}, \boldsymbol{y})$ by the obtained support, and recover error $\boldsymbol{e}$.

The complexity is concluded in Theorem 13. The computation of $\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r})$ follows Theorem 11, especially Theorem 9 for $\ell = 2$ and Theorem 10 for $\ell = 3$. We want to say that this complexity could be conservatively low because $\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r})$ is an upper bound of independent equations. A more precise complexity requires a tighter upper bound of independent equations. Nevertheless, the complexity difference should be slight because our derived bound of independent equations is tight. The specific attack steps are presented in Algorithm 4. For large ℓ, searching appropriate $\boldsymbol{a}$ and $\boldsymbol{p}$ is usually time-consuming for the computation of complexity. As described in Remark 2, $n_1 \geq n_2 \geq \cdots \geq n_\ell$ allows to compute the tighter number of independent equations. Thus, by symmetry, we can only search $(p_1, p_2, \ldots, p_\ell)$ satisfying $p_1 \leq p_2 \leq \cdots \leq p_\ell$ to speed up the computation of complexity.

Algorithm 4 Solve BRD by the MM modeling with the BP Approach

Input: $q, m, n, k, r, \ell, \boldsymbol{n} = (n_1, n_2, \ldots, n_\ell), \boldsymbol{r} = (r_1, r_2, \ldots, r_\ell)$;
$\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$, $\boldsymbol{y} \in \mathbb{F}_{q^m}^{n}$.
Output: $\boldsymbol{x} \in \mathbb{F}_{q^m}^{k}$ and $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{n}}^{\boldsymbol{r}}$ such that $\boldsymbol{y} = \boldsymbol{x}\boldsymbol{G} + \boldsymbol{e}$

Search $\boldsymbol{p} = (p_1, p_2, \ldots, p_\ell)$ and compute $p = \sum_{i=1}^{\ell} p_i$ such that

$$n_i - p_i \geq r_i, \quad n - p - k - 1 \geq r, \quad \overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i - p_i}{r_i} - 1$$

Store $\boldsymbol{p}$ into the list List
if List is non-empty // Allow overdetermined MM modeling
  Choose $\boldsymbol{p} \in$ List that minimizes the complexity (Theorem 13)
  Construct the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$
  Apply the MM modeling to the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}))$
  Solve an *overdetermined* MM modeling to obtain the support of $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e})$
  if the MM modeling has no solution:
    Sample a block diagonal invertible matrix $\boldsymbol{P}$ over $\mathbb{F}_q$
    Construct the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}\boldsymbol{P}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}\boldsymbol{P}))$
    Apply the MM modeling to the instance $(\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{G}\boldsymbol{P}), \mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{y}\boldsymbol{P}))$
    Solve an *overdetermined* MM modeling to obtain the support of $\mathbf{BP}^{\boldsymbol{p}}(\boldsymbol{e}\boldsymbol{P})$
  Solve the instance $(\boldsymbol{G}, \boldsymbol{y})$ by the obtained support, and recover $\boldsymbol{e}$
  Compute $\boldsymbol{x}$ from $\boldsymbol{y} - \boldsymbol{e}$ and $\boldsymbol{G}$ by solving a linear system
  return $\boldsymbol{x}$ and $\boldsymbol{e}$
else: // Allow underdetermined MM modeling
  Apply the MM modeling to the instance $(\boldsymbol{G}, \boldsymbol{y})$
  Solve an *underdetermined* MM modeling to obtain $\boldsymbol{e}$
  Compute $\boldsymbol{x}$ from $\boldsymbol{y} - \boldsymbol{e}$ and $\boldsymbol{G}$ by solving the linear system
  return $\boldsymbol{x}$ and $\boldsymbol{e}$

Theorem 13 *Let $\boldsymbol{a} = (a_1, a_2, \ldots, a_\ell)$ and $\boldsymbol{p} = (p_1, p_2, \ldots, p_\ell)$ be two integers vectors and $p = \sum_{i=1}^{\ell} p_i$. With the BP approach, the MM modeling solves the $\mathsf{BRD}_{q,m,n,k,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}$ problem with a complexity*

$$\mathcal{O}\left(q^{\sum_{i=1}^{\ell} a_i r_i} \overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \left(\prod_{i=1}^{\ell} \binom{n_i - p_i - a_i}{r_i} \right)^{\omega - 1} \right), \tag{31}$$

where $\boldsymbol{a}$, $\boldsymbol{p}$, and p such that $\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i - p_i - a_i}{r_i} - 1$ holds and the complexity is minimal.

The complexity can be seen as the merge of the following overdetermined and underdetermined cases

$$\begin{cases} \mathcal{O}\left(\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \left(\prod_{i=1}^{\ell} \binom{n_i - p_i}{r_i} \right)^{\omega - 1} \right), & \overline{E}(m, n, k, r, \ell, \boldsymbol{n}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i}{r_i}; \\ \mathcal{O}\left(q^{\sum_{i=1}^{\ell} a_i r_i} \overline{E}(m, n, k, r, \ell, \boldsymbol{n}, \boldsymbol{r}) \left(\prod_{i=1}^{\ell} \binom{n_i - a_i}{r_i} \right)^{\omega - 1} \right), & \overline{E}(m, n, k, r, \ell, \boldsymbol{n}, \boldsymbol{r}) < \prod_{i=1}^{\ell} \binom{n_i}{r_i}. \end{cases} \tag{32}$$

where $\boldsymbol{p}$ and p such that $\overline{E}(m, n-p, k, r, \ell, \boldsymbol{n}-\boldsymbol{p}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i - p_i}{r_i} - 1$ holds and the complexity is minimal; $\boldsymbol{a}$ such that $\overline{E}(m, n, k, r, \ell, \boldsymbol{n}, \boldsymbol{r}) \geq \prod_{i=1}^{\ell} \binom{n_i - a_i}{r_i} - 1$ holds and the complexity is minimal.

We should note that the BP approach could transform an instance $\mathsf{BRD}^{\ell,\boldsymbol{n},\boldsymbol{r}}_{q,m,n,k,r}$ inducing the underdetermined MM modeling into an instance $\mathsf{BRD}^{\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}}_{q,m,n-p,k,r}$ inducing the overdetermined one. When the MM modeling is "slight"-underdetermined, the BP approach could still have chance to find an appropriate $\boldsymbol{p}$ such that $\overline{E}(m,n-p,k,r,\ell,\boldsymbol{n}-\boldsymbol{p},\boldsymbol{r}) \geq \prod_{i=1}^{\ell}\binom{n_i-p_i}{r_i}-1$ holds.

D. Impacts on Security Strength of Cryptosystems

In this section, we estimate the security strength of cryptosystems based on the BRD problem by the MM attack with the BP approach. We consider four typical rank-based cryptosystems: RQC, Locker (ROLLO-II), and Ouroboros-R (ROLLO-III) improved in [3], [23]; RQC-Block-MS-AG proposed in [5]. Please see Tables III - VI for security loss. We find that some parameters sets are lower than the current security strength and the security loss is up to 25 bits. However, the attack does not weaken the claimed security level.

- RQC. The scheme uses Gabidulin codes in the decryption step and the security relies on the hardness of two types of the BRD problems. We refer to [23] for the details of RQC. Under the MM attack with the BP approach, the security strength is estimated in Table III. From Table III, we can observe that the BP approach is powerful for the $\mathsf{BRD}^{3,(n,n,n),(w_{\boldsymbol{r}_1},w_{\boldsymbol{e}},w_{\boldsymbol{r}_2})}_{q,m,3n,n,w_{\boldsymbol{r}_1}+w_{\boldsymbol{e}}+w_{\boldsymbol{r}_2}}$ problem. The security loss is up to 25 bits for 128-bit security.
- Locker (ROLLO-II). The scheme uses the blockwise LRPC codes in the decryption step and the security relies on the hardness of two types of the BRD problems. We refer to [23] for the details of Locker. Under the MM attack with the BP approach, the security strength is estimated in Table IV. From Table IV, we can observe that the BP approach is powerful for the $\mathsf{BRD}^{2,(n-d,n),(d_1,d_2)}_{q,m,2n-d,n-d,d_1+d_2}$ problem. The security loss is up to 19 bits for 192-bit security.
- Ouroboros-R (ROLLO-III). The scheme uses the blockwise LRPC codes in the decryption step and the security relies on the hardness of two types of the BRD problems. We refer to [23] for the details of Ouroboros-R. Under the MM attack with the BP approach, the security strength is estimated in Table V. From Table V, we can observe that the BP approach is powerful for the $\mathsf{BRD}^{3,(n,n,n),(r_3,r_1,r_2)}_{q,m,3n,n,r_1+r_2+r_3}$ problem. The security loss is about 11 bits for 128-bit security.
- RQC-Block-MS-AG. The scheme uses the AG codes in the decryption step and the security relies on the hardness of two types of the BRD problems. We refer to [5] for the details of RQC-Block-MS-AG. Under the MM attack with the BP approach, the security strength is estimated in Table VI. From Table VI, we can observe that the BP approach is powerful for the $\mathsf{BRD}^{3,(n_2,n_2,n_2),(w_{\boldsymbol{r}_1},w_{\boldsymbol{e}},w_{\boldsymbol{r}_2})}_{q,m,3n_2,n_2,w_{\boldsymbol{r}_1}+w_{\boldsymbol{e}}+w_{\boldsymbol{r}_2}}$ problem. The security loss is about 12 bits for 128-bit security.

We do not consider Lake [23] because its structure is same as Locker. All in all, using the blockwise errors is still a nice alternative for designing rank-based cryptosystems.

TABLE III
SECURITY LOSS OF **RQC BASED ON THE BRD PROBLEM** (IEEE TIT [23], 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-$2n$ $(\xi,a_1,a_2,\boldsymbol{p},\xi',\mathbb{C}',\mathbb{C})$	Attack-$3n$ $(\xi,\boldsymbol{a},p_1,p_2,p_3,\xi',\mathbb{C}',\mathbb{C})$	λ
2	83	79	7	4	4	4	4	4	2.5	$(0.86,0,3,\boldsymbol{0},1.01,2^{127},2^{127})$	$(6.86,\boldsymbol{0},0,0,68,1.28,2^{\mathbf{138}},2^{163})$	128
2	127	113	3	5	5	5	5	5	5.3	$(0.36,0,21,\boldsymbol{0},1.04,2^{253},2^{253})$	$(3.90,\boldsymbol{0},0,0,56,1.00,2^{213},2^{213})$	192
2	139	137	3	5	5	6	6	7	7.1	$(0.42,0,22,\boldsymbol{0},1.03,2^{267},2^{267})$	$(1.06,\boldsymbol{0},1,1,1,1.01,2^{288},2^{288})$	256

The public key size (pks): $\left(\lceil\frac{mn}{8}\rceil+40\right)$ bytes, the ciphertext size (cts): $\left(2\lceil\frac{mn}{8}\rceil\right)$ bytes, the bandwidth (total) = pks + cts. "Attacks-$2n$" represents attacking the $\mathsf{BRD}^{2,(n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}_{q,m,2n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}$ problem and "Attacks-$3n$" represents attacking the $\mathsf{BRD}^{3,(n,n,n),(w_{\boldsymbol{r}_1},w_{\boldsymbol{e}},w_{\boldsymbol{r}_2})}_{q,m,3n,n,w_{\boldsymbol{r}_1}+w_{\boldsymbol{e}}+w_{\boldsymbol{r}_2}}$ problem. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$" (resp. "$\mathbb{C}$") represents the practical security strength, namely the complexity of the MM attacks with (resp. without) with the BP approach. "λ" represents the claimed security level.

TABLE IV
SECURITY LOSS OF **LOCKER** (ROLLO-II, IEEE TIT [23]) BASED ON THE BRD PROBLEM

q	m	n	r_1	r_2	d_1	d_2	DFR	total (KB)	Structural attack $\boldsymbol{y}-\boldsymbol{x}\boldsymbol{h}=\boldsymbol{0}$ $(\xi,a_1,a_2,\boldsymbol{p},\xi',\mathbb{C}',\mathbb{C})$	Message attack $\boldsymbol{c}=\boldsymbol{e}_1+\boldsymbol{h}\boldsymbol{e}_2$ $(\xi,a_1,a_2,p_1,p_2,\xi',\mathbb{C}',\mathbb{C})$	λ
2	83	173	4	4	5	5	2^{-133}	3.6	$(0.86,0,5,\boldsymbol{0},1.03,2^{\mathbf{189}},2^{190})$	$(1.03,0,0,0,1,1.00,2^{141},2^{141})$	128
2	97	179	4	5	5	6	2^{-129}	4.4	$(0.53,0,17,\boldsymbol{0},1.00,2^{\mathbf{262}},2^{281})$	$(0.65,1,14,0,0,1.01,2^{229},2^{229})$	192
2	101	191	5	5	5	6	2^{-134}	4.8	$(0.57,0,17,\boldsymbol{0},1.04,2^{\mathbf{265}},2^{279})$	$(0.33,0,38,0,0,1.02,2^{359},2^{359})$	256

The public key size (pks): $\lceil\frac{mn}{8}\rceil$ bytes, the ciphertext size (cts): $\left(\lceil\frac{mn}{8}\rceil+64\right)$ bytes, the bandwidth (total) = pks + cts. "Structural attack" represents attacking the $\mathsf{BRD}^{2,(n-d,n),(d_1,d_2)}_{q,m,2n-d,n-d,d_1+d_2}$ problem with a zero syndrome, where $d=\left\lfloor\frac{n}{\min\{d_1,d_2\}}\right\rfloor$. Note that for this problem with the zero-syndrome, we should tune $k+1$ of formula in Theorem 9 as $n-d$ because the code $\mathcal{C}_{\boldsymbol{y}}$ building the MM modeling has dimension $n-d$. "Message attack" represents attacking the $\mathsf{BRD}^{2,(n,n),(r_1,r_2)}_{q,m,2n,n,r_1+r_2}$ problem. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$" (resp. "$\mathbb{C}$") represents the practical security strength, namely the complexity of the MM attacks with (resp. without) with the BP approach. "λ" represents the claimed security level.

XI. APPLICATIONS: BRE AND HURE

In this section, we make two applications on the public key encryption (PKE) schemes by exploiting advantages of the EG codes:

TABLE V
SECURITY LOSS OF **OUROBOROS-R** (ROLLO-III, IEEE TIT [23]) BASED ON THE BRD PROBLEM

q	m	n	r_1	r_2	r_3	d_1	d_2	DFR	total (KB)	Attack-$2n$ $(\xi, a_1, a_2, \boldsymbol{p}, \xi', \mathbb{C}', \mathbb{C})$	Attack-$3n$ $(\xi, \boldsymbol{a}, \boldsymbol{p}, \xi', \mathbb{C}', \mathbb{C})$	λ
2	59	73	4	4	5	4	4	2^{-33}	1.6	$(0.60, 0, 9, \mathbf{0}, 1.02, 2^{147}, 2^{147})$	$(3.35, \mathbf{0}, 0, 0, 44, 1.02, 2^{\mathbf{160}}, 2^{171})$	128
2	89	101	6	6	6	4	5	2^{-33}	3.3	$(0.52, 0, 15, \mathbf{0}, 1.00, 2^{193}, 2^{195})$	$(0.85, 0, 0, 3, \mathbf{0}, 1.02, 2^{272}, 2^{266})$	192
2	97	109	6	6	7	5	5	2^{-42}	3.9	$(0.28, 0, 25, \mathbf{0}, 1.04, 2^{270}, 2^{270})$	$(0.66, 1, 3, 3, \mathbf{0}, 1.01, 2^{314}, 2^{305})$	256

The public key size (pks): $\left(\lceil \frac{mn}{8} \rceil + 40\right)$ bytes, the ciphertext size (cts): $\left(2\lceil \frac{mn}{8} \rceil\right)$ bytes, the bandwidth (total) = pks + cts. "Attacks-$2n$" represents attacking the $\mathsf{BRD}^{2,(n,n),(d_1,d_2)}_{q,m,2n,n,d_1+d_2}$ problem and "Attacks-$3n$" represents attacking the $\mathsf{BRD}^{3,(n,n,n),(r_3,r_1,r_2)}_{q,m,3n,n,r_1+r_2+r_3}$ problem. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$" (resp. "$\mathbb{C}$") represents the practical security strength, namely the complexity of the MM attacks with (resp. without) with the BP approach. "λ" represents the claimed security level.

TABLE VI
SECURITY LOSS OF **RQC-BLOCK-MS-AG** (PQC [5])) BASED ON THE BRD PROBLEM

q	m	n_2	k	ε	n_1	$w_{\boldsymbol{x}}$	$w_{\boldsymbol{y}}$	$w_{\boldsymbol{r}_1}$	$w_{\boldsymbol{r}_2}$	$w_{\boldsymbol{e}}$	DFR	total (KB)	Attack-$2n_2$ $(\xi, a_1, a_2, \boldsymbol{p}, \xi', \mathbb{C}', \mathbb{C})$	Attack-$3n_2$ $(\xi, \boldsymbol{a}, p_1, p_2, p_3, \xi', \mathbb{C}', \mathbb{C})$	λ
2	43	52	3	32	2	4	4	4	4	4	2^{-145}	1.43	$(0.37, 0, 12, \mathbf{0}, 1.11, 2^{145}, 2^{145})$	$(3.07, \mathbf{0}, 0, 0, 24, 1.01, 2^{\mathbf{141}}, 2^{153})$	128
2	67	70	3	45	2	5	5	5	5	6	2^{-196}	2.98	$(0.15, 0, 22, \mathbf{0}, 1.10, 2^{234}, 2^{232})$	$(1.24, \mathbf{0}, 0, 2, 3, 1.00, 2^{207}, 2^{207})$	192

The public key size (pks): $\left(\lceil \frac{mn_2}{8} \rceil + \frac{2\lambda}{8}\right)$, the ciphertext size (cts): $\left(2\lceil \frac{mn_2n_1}{8} \rceil\right)$, the bandwidth (total) = pks + cts. "Attacks-$2n_2$" represents attacking the $\mathsf{BRD}^{2,(n_2,n_2),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}_{q,m,2n_2,n_2,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}$ problem and "Attacks-$3n_2$" represents attacking the $\mathsf{BRD}^{3,(n_2,n_2,n_2),(w_{\boldsymbol{r}_1},w_{\boldsymbol{e}},w_{\boldsymbol{r}_2})}_{q,m,3n_2,n_2,w_{\boldsymbol{r}_1}+w_{\boldsymbol{e}}+w_{\boldsymbol{r}_2}}$ problem. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$" (resp. "$\mathbb{C}$") represents the practical security strength, namely the complexity of the MM attacks with (resp. without) with the BP approach. "λ" represents the claimed security level.

1) We apply the EG codes to RQC based on the BRD problem (Asiacrypt 2023, IEEE TIT 2025) and obtain the Bolckwise RQC with the EG codes (BRE). While RQC based on the BRD problem in Table III remains an attractive bandwidth, we still hope to further improve it. We use the EG codes for decryption, and still base the security on the ideal BRD problem, precisely the Ideal BRSD (IBRSD) problem. We obtain a bandwidth of 1.6 KB for 128-bit security. Unlike RQC-Block-MS-AG, we do not introduce the multiple-syndromes structure to base the security on the Rank Support Learning (RSL) problem. This would enable BRE feature more applications in the further due to its flexible structure.
2) We apply the EG codes to NH-Multi-UR-AG (IEEE TIT 2024 [6]) with the standard (or homogeneous) errors and obtain Homogeneous Unstructured Rank decoding Encryption (HURE). We use the EG codes for decryption, and base the security on the RSL problem. The bandwidth of HURE is slightly shorter than NH-Multi-UR-AG. The bandwidth also outperforms lattice-based unstructured PKEs, namely FrodoKEM [47] and Scloud$^+$ [48]. We intrinsically show that it is sufficient to construct an efficient PKE scheme based on unstructured rank decoding problem by using homogeneous errors, without the non-homogeneous errors.

All efficient applications benefit from that (1) The decoding capacity of the EG codes. The EG codes allow to work over a small finite field, which enables our scheme to mitigate the advantage of the MM attack with the BP approach and brings a gain of parameter size; (2) We derive the concise DFR for the EG codes, which allows to choose flexible parameters. The definition of PKE is recalled in Appendix D. The IBRSD problem is recalled in Appendix E. The RSL problem is recalled in Appendix F.

A. Our BRE From the EG Codes and the IBRSD Problem

Our BRE uses three codes:

- A public $[n,k]_{q^m}$-EG code with generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k\times n}$ generated by $\boldsymbol{g} \in \mathbb{F}_{q^m}^{n}$ of weight t. This EG code can correct up to weight $\min\left\{\left\lfloor \frac{n-k}{2} \right\rfloor, t-k\right\}$ by a probabilistic decoding algorithm. We denote its decoding algorithm by $\mathsf{EG.Decode}$.
- A random $[2n,n]_{q^m}$-ideal code with parity-check matrix $\begin{bmatrix} \boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{h})^\top \end{bmatrix}$.
- A random $[3n,n]_{q^m}$-ideal code with parity-check matrix $\begin{bmatrix} \boldsymbol{I}_n & \mathbf{0} & \mathcal{IM}(\boldsymbol{h})^\top \\ \mathbf{0} & \boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{s})^\top \end{bmatrix}$.

The EG code is used for the decryption step. Two random ideal codes are used to ensure the security of the scheme. Our BRE scheme is described in Figure 1.

Correctness. In the decryption step, $\boldsymbol{v} - \boldsymbol{u}\cdot\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{x}\cdot\boldsymbol{r}_2 + \boldsymbol{e} - \boldsymbol{r}_1\cdot\boldsymbol{y}$. The term $\boldsymbol{x}\cdot\boldsymbol{r}_2 + \boldsymbol{e} - \boldsymbol{r}_1\cdot\boldsymbol{y}$ is viewed an error and $\|\boldsymbol{x}\cdot\boldsymbol{r}_2 + \boldsymbol{e} - \boldsymbol{r}_1\cdot\boldsymbol{y}\|_{\mathrm{R}} \le w_{\boldsymbol{x}}w_{\boldsymbol{r}_2} + w_{\boldsymbol{y}}w_{\boldsymbol{r}_1} + w_{\boldsymbol{e}}$. Let $r = w_{\boldsymbol{x}}w_{\boldsymbol{r}_2} + w_{\boldsymbol{y}}w_{\boldsymbol{r}_1} + w_{\boldsymbol{e}}$. To obtain $\boldsymbol{m}$, one applies $\mathsf{EG.Decode}$ to $\boldsymbol{v} - \boldsymbol{u}\cdot\boldsymbol{y}$. Thus, one must ensure that the weight $r \le \min\left\{\left\lfloor \frac{n-k}{2} \right\rfloor, t-k\right\}$ and $\boldsymbol{m}$ can be decoded by $\mathsf{EG.Decode}$. Moreover, one also ensures that the DFR (Theorem 3) decoding errors of weight r is small enough. For the requirements of NIST PQC, DFR $\le 2^{-\lambda}$.

$\underline{\mathsf{BRE.KGen}(\lambda)}$:

- Sample $\boldsymbol{g} \xleftarrow{\theta_1} \mathcal{S}_t^n$ and $\boldsymbol{h} \xleftarrow{\theta_1} \mathbb{F}_{q^m}^n$ from a seed θ_1 of 40 bytes
- Sample $(\boldsymbol{x}, \boldsymbol{y}) \xleftarrow{\theta_2} \mathcal{S}_{(w_{\boldsymbol{x}}, w_{\boldsymbol{y}})}^{(n,n)}$ from a seed θ_2 of 40 bytes
- Compute $\boldsymbol{s} = \boldsymbol{x} + \boldsymbol{h} \cdot \boldsymbol{y}$
- Output a public key $pk = (\boldsymbol{g}, \boldsymbol{h}, \boldsymbol{s})$ and a private key $sk = (\boldsymbol{x}, \boldsymbol{y})$

$\underline{\mathsf{BRE.Enc}(pk, \boldsymbol{m})}$:

- Input the public key pk and a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$
- Compute the generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$ of $[n, k]_{q^m}$-EG code defined by $\boldsymbol{g}$
- Sample $(\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{e}) \xleftarrow{\$} \mathcal{S}_{(w_{\boldsymbol{r}_1}, w_{\boldsymbol{r}_1}, w_{\boldsymbol{e}})}^{(n,n,n)}$
- Compute $\boldsymbol{u} = \boldsymbol{r}_1 + \boldsymbol{h} \cdot \boldsymbol{r}_2$ and $\boldsymbol{v} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s} \cdot \boldsymbol{r}_2 + \boldsymbol{e}$
- Output a ciphertext $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v})$

$\underline{\mathsf{BRE.Dec}(sk, \boldsymbol{c})}$:

- Input the private key sk and the ciphertext $\boldsymbol{c}$
- Output the plaintext $\boldsymbol{m} := \mathsf{EG.Decode}(\boldsymbol{v} - \boldsymbol{y} \cdot \boldsymbol{u})$

Fig. 1. Description of our BRE PKE scheme

Theorem 14 *Under the* $\mathsf{DIBRSD}_{q,m,2n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}^{2,(n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}$ *and* $\mathsf{DIBRSD}_{q,m,3n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}+w_{\boldsymbol{e}}}^{3,(n,n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}},w_{\boldsymbol{e}})}$ *problems (see Appendix E), our BRE in Figure 1 is IND-CPA secure. Concretely, for any PPT algorithm* $\mathcal{A}$*, there is a PPT algorithm* $\mathcal{B}$ *such that the advantage that* $\mathcal{A}$ *against the* IND-CPA *experiment defined by our BRE is bounded as*

$$\mathsf{Adv}_{\mathsf{BRE},\mathcal{A}}^{\mathsf{IND\text{-}CPA}}(\lambda) \leq 2\left(\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DIBRSD}_{q,m,2n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}^{2,(n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}}(\lambda) + \mathsf{Adv}_{\mathcal{B}}^{\mathsf{DIBRSD}_{q,m,3n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}+w_{\boldsymbol{e}}}^{3,(n,n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}},w_{\boldsymbol{e}})}}(\lambda)\right).$$

Proof: The proof is similar to [22] with $\mathsf{IBRSD}_{q,m,2n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}}^{2,(n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}})}$ and $\mathsf{IBRSD}_{q,m,3n,n,w_{\boldsymbol{x}}+w_{\boldsymbol{y}}+w_{\boldsymbol{e}}}^{3,(n,n,n),(w_{\boldsymbol{x}},w_{\boldsymbol{y}},w_{\boldsymbol{e}})}$ instances. Two instances are defined as

$$\boldsymbol{x} + \boldsymbol{h} \cdot \boldsymbol{y} = \boldsymbol{s} \iff \begin{bmatrix} \boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{h})^\top \end{bmatrix} \begin{bmatrix} \boldsymbol{x}^\top \\ \boldsymbol{y}^\top \end{bmatrix} = \boldsymbol{s}^\top,$$

$$\begin{matrix} \boldsymbol{r}_1 + \boldsymbol{h} \cdot \boldsymbol{r}_2 = \boldsymbol{u} \\ \boldsymbol{m}\boldsymbol{G} + \boldsymbol{s} \cdot \boldsymbol{r}_2 + \boldsymbol{e} = \boldsymbol{v} \end{matrix} \iff \begin{bmatrix} \boldsymbol{I}_n & \boldsymbol{0} & \mathcal{IM}(\boldsymbol{h})^\top \\ \boldsymbol{0} & \boldsymbol{I}_n & \mathcal{IM}(\boldsymbol{s})^\top \end{bmatrix} \begin{bmatrix} \boldsymbol{r}_1^\top \\ \boldsymbol{e}^\top \\ \boldsymbol{r}_2^\top \end{bmatrix} = \begin{bmatrix} \boldsymbol{u}^\top \\ \boldsymbol{v}^\top - (\boldsymbol{m}\boldsymbol{G})^\top \end{bmatrix}.$$

■

B. Parameters and Performance of Our BRE

The parameters are chosen in three principles. First, the complexity of solving decoding problems is ensured to reach the target security level 2^λ for the target security level parameter λ. Second, the decoding capacity of the EG codes is ensured to satisfy the decryption correctness condition. The EG codes must be designed to correct errors of weight up to r. Third, one must ensure that the decoding failure rate (DFR) correcting errors of weight up to r (Theorem 3 for DFR) is less than $2^{-\lambda}$.

In Table VII, we list the security parameters and compute the complexity of best attacks on the IBRSD problems. The best attack is the MM attack with the BP approach. One can verify the complexity of the MM attack by the optimal $\boldsymbol{a}$ and $\boldsymbol{p}$.

In Table VIII, we compute bandwidths and provide reference timings for our BRE. We can observe that the parameter m is smaller than that in Table III, which leads to a smaller bandwidth. The timings are roughly 1000 times greater than when running on C language. Thus, the efficiency is quite practical. These benefits from the gain of the EG codes in decoding capacity. The EG codes allow to work over a small finite field, which enables our BRE to mitigate the advantage of the MM attack with the BP approach and brings a gain of parameter size. As a result, the gain of using the EG codes outweighs the complexity loss in solving the BRD problem, and it is possible to design an efficient PKE by the blockwise errors and the EG codes.

C. Our HURE From the EG Codes and the RSL Problem

The HURE uses three codes:

- A public $[N_1N_2, k]_{q^m}$-EG code with generator matrix $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times N_1N_2}$ generated by $\boldsymbol{g} \in \mathbb{F}_{q^m}^{N_1N_2}$ of weight t. This EG code can correct up to weight $\min\left\{\left\lfloor \frac{N_1N_2-k}{2} \right\rfloor, t-k\right\}$ by a probabilistic decoding algorithm denoted by $\mathsf{EG.Decode}$.
- A random $[2n, n]_{q^m}$-linear code with parity-check matrix $\begin{bmatrix} \boldsymbol{I}_n & \boldsymbol{H} \end{bmatrix}$.

TABLE VII
SECURITY PARAMETERS AND SECURITY STRENGTH OF OUR **BRE**

q	m	n	t	k	$w_{\boldsymbol{x}}$	$w_{\boldsymbol{y}}$	$w_{\boldsymbol{r}_1}$	$w_{\boldsymbol{r}_2}$	$w_{\boldsymbol{e}}$	r	$P(X)$	Attack-$2n$ $(\xi, a_1, a_2, \boldsymbol{p}, \xi', \mathbb{C}')$	Attack-$3n$ $(\xi, \boldsymbol{a}, p_1, p_2, p_3, \xi', \mathbb{C}')$	λ
2	47	89	47	3	4	4	4	4	4	36	$X^{89}+X^{38}+1$	$(0.51, 0, 14, \boldsymbol{0}, 1.02, 2^{172})$	$(4.00, \boldsymbol{0}, 0, 0, 53, 1.02, 2^{163})$	128
2	59	113	59	4	4	5	4	5	5	45	$X^{113}+X^{9}+1$	$(0.36, 1, 20, \boldsymbol{0}, 1.00, 2^{239})$	$(2.69, \boldsymbol{0}, 0, 0, 48, 1.01, 2^{204})$	192
2	73	137	73	4	5	5	5	5	7	57	$X^{137}+X^{21}+1$	$(0.22, 0, 36, \boldsymbol{0}, 1.05, 2^{333})$	$(1.36, \boldsymbol{0}, 1, 1, 8, 1.01, 2^{261})$	256

We set the weight t of generator $\boldsymbol{g}$ of the EG codes as m. $P(X)$ is a polynomial of degree n in $\mathbb{F}_q[X]$, and is used to build the ring $\mathcal{R} = \mathbb{F}_{q^m}[X]/\langle P(X)\rangle$ and construct the ideal codes (see Appendix E). $P(X)$ is set to be an irreducible polynomial for resisting the folding attack [56]. Moreover, to decrease the computational costs, $P(X)$ is suggested to be sparse. We choose minimal weight $P(X)$ with the SageMath 9.5 software. For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant ω) is set as 2.81. "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 and "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. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$" represents the practical security strength, namely the complexity of the MM attacks with the BP approach.

TABLE VIII
SIZES, DFR, AND TIMINGS OF OUR **BRE**

pts	sks	pks	cts	total	DFR	KGen (ms)	Enc (ms)	Dec (ms)	λ
141	40	563	1046	1609	2^{-133}	81	83	205	128
236	40	874	1668	2542	2^{-218}	120	124	386	192
292	40	1291	2502	3793	2^{-258}	183	188	710	256

The plaintext size (pts): mk bits, the private key size (sts): a seed of 40 bytes, the public key size (pks): $\left(\left\lceil \frac{mn}{8} \right\rceil + 40\right)$ bytes, the ciphertext size (cts): $\left(2\left\lceil \frac{mn}{8} \right\rceil\right)$ bytes, total=pks + cts. The DFR is estimated by Equation (17) with $\gamma_q = 4$. The schemes are implemented on SageMath 9.5. The benchmark is Ubuntu-22.04 + WSL + Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz with SageMath 9.5. The test scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

- A random $[2n+N_1, n]_{q^m}$-linear code with parity-check matrix $\begin{bmatrix} \boldsymbol{I}_n & \boldsymbol{0} & \boldsymbol{H}^\top \\ \boldsymbol{0} & \boldsymbol{I}_{N_1} & \boldsymbol{S}^\top \end{bmatrix}$.

The EG code is used for the decryption step. Two random linear codes are used to ensure the security of the scheme. Our HURE scheme is described in Figure 2.

The HURE uses two operations:

- Fold: It takes as input a vector of length N_1N_2 and output a matrix of size $N_1 \times N_2$ by a specific rule.
- UnFold: The inverse operation of Fold. It takes as input a matrix of size $N_1 \times N_2$ and output a vector of length N_1N_2 by the specific rule as in the operation Fold.

The HURE uses two sets of small weight matrices:

- $\mathcal{S}^{2n\times N_1}_{w_1,1} = \left\{ \boldsymbol{X} = \begin{bmatrix} \boldsymbol{X}_1 \\ \boldsymbol{X}_2 \end{bmatrix} \in \mathbb{F}^{2n\times N_1}_{q^m} \ : \ \boldsymbol{X}_1 \in \mathbb{F}^{n\times N_1}_{q^m}, \boldsymbol{X}_2 \in \mathbb{F}^{n\times N_1}_{q^m}, \|\boldsymbol{X}\|_{\mathrm{R}} = w_1, 1 \in \mathrm{Supp}(\boldsymbol{X}) \right\}$.
- $\mathcal{S}^{(2n+N_1)\times N_2}_{w_2} = \left\{ \boldsymbol{X} = \begin{bmatrix} \boldsymbol{X}_1 \\ \boldsymbol{X}_2 \\ \boldsymbol{X}_3 \end{bmatrix} \in \mathbb{F}^{(2n+N_1)\times N_2}_{q^m} \ : \ \boldsymbol{X}_1 \in \mathbb{F}^{n\times N_2}_{q^m}, \boldsymbol{X}_2 \in \mathbb{F}^{N_1\times N_2}_{q^m}, \boldsymbol{X}_3 \in \mathbb{F}^{n\times N_2}_{q^m}, \|\boldsymbol{X}\|_{\mathrm{R}} = w_2 \right\}$.

HURE.KGen(λ):
- Sample $\boldsymbol{g} \xleftarrow{\theta_1} \mathcal{S}^{N_1N_2}_t$ and $\boldsymbol{H} \xleftarrow{\theta_1} \mathbb{F}^{n\times n}_{q^m}$ from a seed θ_1 of 40 bytes
- Sample $\begin{bmatrix} \boldsymbol{X} \\ \boldsymbol{Y} \end{bmatrix} \xleftarrow{\theta_2} \mathcal{S}^{2n\times N_1}_{w_1,1}$ by a seed θ_2 of 40 bytes
- Compute $\boldsymbol{S} = \boldsymbol{X} + \boldsymbol{HY} \in \mathbb{F}^{n\times N_1}_{q^m}$
- Output the public key $pk = (\boldsymbol{g}, \boldsymbol{H}, \boldsymbol{S})$ and the private key $sk = \boldsymbol{Y}$.

HURE.Enc($pk, \boldsymbol{m} \in \mathbb{F}^k_{q^m}$):
- Input the public key pk and a plaintext $\boldsymbol{m} \in \mathbb{F}^k_{q^m}$
- Compute the generator matrix $\boldsymbol{G} \in \mathbb{F}^{k\times N_1N_2}_{q^m}$ of $[N_1N_2, k]_{q^m}$-EG code defined by $\boldsymbol{g}$
- Sample $\begin{bmatrix} \boldsymbol{R}_1 \\ \boldsymbol{E} \\ \boldsymbol{R}_2 \end{bmatrix} \xleftarrow{\$} \mathcal{S}^{(2n+N_1)\times N_2}_{w_2}$
- Compute $\boldsymbol{U} = \boldsymbol{R}_1 + \boldsymbol{H}^\top \boldsymbol{R}_2 \in \mathbb{F}^{n\times N_2}_{q^m}$ and $\boldsymbol{V} = \mathsf{Fold}(\boldsymbol{mG}) + \boldsymbol{E} + \boldsymbol{S}^\top \boldsymbol{R}_2 \in \mathbb{F}^{N_1\times N_2}_{q^m}$
- Output the ciphertext $\boldsymbol{C} = (\boldsymbol{U}, \boldsymbol{V})$.

HURE.Dec($sk, \boldsymbol{C}$):
- Input the private key sk and the ciphertext $\boldsymbol{C}$
- Output the plaintext $\boldsymbol{m} := \mathsf{EG.Decode}\left(\mathsf{UnFold}\left(\boldsymbol{V} - \boldsymbol{Y}^\top \boldsymbol{U}\right)\right)$.

Fig. 2. Description of our HURE PKE scheme.

Correctness. In the decryption step,

$$\mathsf{UnFold}\left(\boldsymbol{V}-\boldsymbol{Y}^{\top}\boldsymbol{U}\right)=\boldsymbol{m}\boldsymbol{G}+\mathsf{UnFold}\left(\boldsymbol{X}^{\top}\boldsymbol{R}_2-\boldsymbol{Y}^{\top}\boldsymbol{R}_1+\boldsymbol{E}\right).$$

The term $\mathsf{UnFold}\left(\boldsymbol{X}^{\top}\boldsymbol{R}_2-\boldsymbol{Y}^{\top}\boldsymbol{R}_1+\boldsymbol{E}\right)$ is viewed as an error of length N_1N_2 and

$$\left\|\mathsf{UnFold}\left(\boldsymbol{X}^{\top}\boldsymbol{R}_2-\boldsymbol{Y}^{\top}\boldsymbol{R}_1+\boldsymbol{E}\right)\right\|_{\mathrm{R}}\leq w_1w_2.$$

Let $r=w_1w_2$. To obtain $\boldsymbol{m}$, one applies $\mathsf{EG.Decode}$ to $\mathsf{UnFold}\left(\boldsymbol{V}-\boldsymbol{Y}^{\top}\boldsymbol{U}\right)$. Thus, one must ensure that the weight $r\leq\min\left\{\left\lfloor\frac{N_1N_2-k}{2}\right\rfloor,t-k\right\}$ and $\boldsymbol{m}$ can be decoded by $\mathsf{EG.Decode}$. Moreover, one also ensures that the DFR (Theorem 3) decoding errors of weight r is small enough. For the requirements of NIST PQC, DFR $\leq 2^{-\lambda}$.

Theorem 15 *Under the* $\mathsf{DRSL}_{q,m,2n,n,w_1,N_1}$ *and* $\mathsf{DRSL}_{q,m,2n+N_1,n,w_2,N_2}$ *problems (see Appendix F), our HURE in Figure 2 is IND-CPA secure. Concretely, for any PPT algorithm* $\mathcal{A}$*, there is a PPT algorithm* $\mathcal{B}$ *such that the advantage that* $\mathcal{A}$ *against the* IND-CPA *experiment defined by our HURE is bounded as*

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{HURE},\mathcal{A}}(\lambda)\leq 2\left(\mathsf{Adv}^{\mathsf{DRSL}_{q,m,2n,n,w_1,N_1}}_{\mathcal{B}}(\lambda)+\mathsf{Adv}^{\mathsf{DRSL}_{q,m,2n+N_1,n,w_2,N_2}}_{\mathcal{B}}(\lambda)\right).$$

Proof: The proof is similar to [22] with $\mathsf{DRSL}_{q,m,2n,n,w_1,N_1}$ and $\mathsf{DRSL}_{q,m,2n+N_1,n,w_2,N_2}$ instances. Two instances are defined as

$$\boldsymbol{X}+\boldsymbol{H}\boldsymbol{Y}=\boldsymbol{S}\iff\begin{bmatrix}\boldsymbol{I}_n & \boldsymbol{H}\end{bmatrix}\begin{bmatrix}\boldsymbol{X}\\ \boldsymbol{Y}\end{bmatrix}=\boldsymbol{S},$$

$$\begin{array}{l}\boldsymbol{R}_1+\boldsymbol{H}^{\top}\boldsymbol{R}_2=\boldsymbol{U}\\ \mathsf{Fold}(\boldsymbol{m}\boldsymbol{G})+\boldsymbol{E}+\boldsymbol{S}^{\top}\boldsymbol{R}_2=\boldsymbol{V}\end{array}\iff\begin{bmatrix}\boldsymbol{I}_n & \boldsymbol{0} & \boldsymbol{H}^{\top}\\ \boldsymbol{0} & \boldsymbol{I}_{N_1} & \boldsymbol{S}^{\top}\end{bmatrix}\begin{bmatrix}\boldsymbol{R}_1\\ \boldsymbol{E}\\ \boldsymbol{R}_2\end{bmatrix}=\begin{bmatrix}\boldsymbol{U}\\ \boldsymbol{V}-\mathsf{Fold}(\boldsymbol{m}\boldsymbol{G})\end{bmatrix}.$$

■

D. Parameters and Performance of Our HURE

As the BRE scheme, the parameters are chosen in three principles. In Table IX, we list the security parameters and compute the complexity of the MM attacks on the RSD problem. One can verify the complexity by the optimal a and p. While the complexity of the RSL problem decreases as N_1 and N_2 increases, in our case N_1 and N_2 are small and the complexity loss can be negligible compared to the RSD problem (see Appendix F for the hardness of the RSL problem).

In Table X, we compute bandwidths and provide reference timings for our HURE. The bandwidth is slightly shorter than NH-Multi-UR-AG (IEEE TIT 2024 [6]). The timings are roughly 1000 times greater than when running on C language. The efficiency is practical. These benefit from the advantage of EG codes. The EG code can decode over the small field with a negligible DFR and our concise DFR allows to choose flexible parameters.

TABLE IX
PARAMETERS AND SECURITY STRENGTH OF OUR **HURE**

q	m	n	t	k	N_1	N_2	w_1	w_2	r	Attak-N_1 $(\xi,a,p,\xi',\mathbb{C}')$	Attack-N_2 $(\xi,a,p,\xi',\mathbb{C}')$	λ
2	67	30	67	3	10	13	7	8	56	$(0.27,10,0,1.05,2^{144})$	$(0.44,7,0,1.06,2^{145})$	128
2	83	38	83	3	12	14	8	9	72	$(0.17,15,0,1.09,2^{208})$	$(0.30,11,0,1.06,2^{203})$	192
2	113	45	113	3	13	15	9	10	90	$(0.11,19,0,1.08,2^{272})$	$(0.21,18,0,1.08,2^{268})$	256

For all estimations of complexity, the exponent of matrix multiplication (or linear algebra constant ω) is set as 2.81. "Attack-N_1" represents attacking the $\mathsf{RSD}_{q,m,2n,n,w_1,N_1}$ problem and "Attack-N_2" represents attacking the $\mathsf{RSD}_{q,m,2n+N_1,n,w_2,N_2}$ problem. "ξ" (resp. "ξ'") represents the (resp. updated) rate of equations and unknowns. "$\mathbb{C}'$", represents the practical security strength, namely the complexity of the MM attack [32]. As analyzed in [6], [11], the RSL problem is as almost hard as the RSD problem for a small number of syndromes N_1 and N_2, typically $< kr$.

TABLE X
SIZES, DFR, AND TIMINGS OF OUR **HURE**

pts	sks	pks	cts	total	DFR	KGen (ms)	Enc (ms)	Dec (ms)	λ
201	40	2553	4355	6908	2^{-142}	385	448	699	128
249	40	4771	7263	12034	2^{-196}	689	531	1270	192
339	40	8304	12289	20593	2^{-271}	1310	851	2230	256

The plaintext size (pts): mk bits, the private key size (sks): a seed of 40 bytes, the public key size (pts): $\left(\left\lceil\frac{mnN_1}{8}\right\rceil+40\right)$ bytes, the ciphertext size (cts): $\left\lceil\frac{(N_2n+N_1N_2)m}{8}\right\rceil$ bytes, total=pks + cts. The DFR is estimated by Equation (17) with $\gamma_q=4$. The schemes are implemented on SageMath 9.5. The benchmark is Ubuntu-22.04 + WSL + Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz with SageMath 9.5. The test scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

XII. Conclusion and Future Work

In this paper, we investigated the (I) EG codes by solving the LR problem, developed the BP approach for solving the BRD problem, and applied the EG codes to improve rank-based cryptosystems: RQC based on the BRD problem and NH-Multi-UR-AG. The (I)EG codes feature a nice decoding performance. We also proved the null DFR of the interleaved Gabidulin codes. The BP approach can speed up the MM modelings. The MM attack with the BP approach lowers the security strength of most rank-based cryptosystems based on the BRD problem. We exploited the decoding gains of the EG codes to improve the bandwidth, efficiency, and structure of cryptosystems. Compared to HQC, FrodoKEM, and Scloud$^+$, our improvements offers a very competitive bandwidth. Our work provided a broad space for enriching coding theory and designing rank-based cryptosystems. In the future, we would like to conduct more study.

- We hope the heuristic argument deriving DFR is well proven.
- Adapt other decoding algorithms of Gabidulin codes, such as Linearized Extended Euclidean Algorithm (LEEA) [18] and Gao-like algorithm [19], to decode the EG codes and derive the decoding performance.
- Study the list decoding of the EG codes for the radius τ: $\min\left\{t-k, \left\lfloor \frac{n-k}{2} \right\rfloor\right\} \leq \tau \leq m$.
- Generalize the EG codes over fields of any characteristic.
- Apply the EG codes to matrix/subspace codes in random network coding [57].
- Study the structure of the parity-check matrix for the EG code.
- Mask EG codes and try to improve LowMS [4] and MinRank-McEliece cryptosystems [49], even design full domain Hash-and-Sign signatures.
- Apply the IEG codes to improve and design the rank-based cryptosystems.
- Derive the tighter upper bound of independent equations in the MM modeling from the BRD problem for general blocks.
- Develop other rank errors to mitigate the MM attack with the BP approach.

Acknowledgement

We would like to thank the anonymous reviewers from Eurocrypt & Crypto 2025 on the (interleaved) EG codes, to thank Philippe Gaborit, Pierre Briaud, Diego Napp, and Yu Li for the inspiration and suggestions during communication.

Appendix A
Omitted Lemmata, Tables, and Proofs

A. Omitted Lemmata

Lemma 3 *Let $q, n, r \in \mathbb{N}$ and $n \geq r$. $q^{r(n-r)} \leq \begin{bmatrix} n \\ r \end{bmatrix}_q < \gamma_q \cdot q^{r(n-r)}$.*

Proof: By definition of Gaussian binomials, we have

$$\begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{i=0}^{r-1} \frac{q^n - q^i}{q^r - q^i} = q^{r(n-r)} \prod_{i=0}^{r-1} \frac{1-q^{i-n}}{1-q^{i-r}}.$$

Since $n \geq r$, we get $\prod_{i=0}^{r-1} \frac{1-q^{i-n}}{1-q^{i-r}} \geq 1$ which yields the left-hand inequality. To get the other inequality, we bound the product:

$$\prod_{i=0}^{r-1} \frac{1-q^{i-n}}{1-q^{i-r}} \leq \prod_{i=0}^{r-1} \frac{1}{1-q^{i-r}} = \prod_{k=0}^{r-1} \frac{1}{1-\frac{1}{q^{k+1}}} < \prod_{j=1}^{\infty} \frac{1}{1-\frac{1}{q^j}}.$$

The right-hand inequality is obtained by taking $\gamma_q = \prod_{j=1}^{\infty} \frac{1}{1-q^{-j}}$. Note that γ_q is always greater than 1 and is monotonically decreasing in q, e.g., $\gamma_2 \approx 3.463$, $\gamma_3 \approx 1.785$, and $\gamma_4 \approx 1.452$. ∎

Lemma 4 is to quantify the probability that the fixed subspace U and the random subspace V have an intersection of a certain dimension. We will use it to estimate the decoding failure rate. We found a trace of this probability in [58] (Proposition 3.2) and its application in [11] (Lemma 5). Here, we provide a concise proof and precise upper bound.

Lemma 4 *Let $t, r, a \in \mathbb{N}$ and $a \leq \min\{r, t\}$. Let U be a fixed t-dimensional subspace of $\mathbb{F}_q^n$. Let V be a random r-dimensional subspace of $\mathbb{F}_q^n$. Then*

$$\Pr\left[\dim(U \cap V) = a\right] \leq \gamma_q \cdot q^{a(t+r-a-n)}.$$

Proof: By Lemma 7 in [59], given subspace U of dimension t, there are $\begin{bmatrix} t \\ a \end{bmatrix}_q$ ways to choose an a-dimensional subspace W of U. For a fixed W, the number of r-dimensional subspaces V such that $U \cap V = W$ is

$$\frac{\left(q^n - q^t\right)\left(q^n - q^{t+1}\right)\cdots\left(q^n - q^{t+r-a-1}\right)}{\left(q^r - q^a\right)\left(q^r - q^{a+1}\right)\cdots\left(q^r - q^{r-1}\right)} = \begin{bmatrix} n-t \\ r-a \end{bmatrix}_q q^{(r-a)(t-a)}.$$

The total number of r-dimensional subspace V of $\mathbb{F}_q^n$ is $\begin{bmatrix} n \\ r \end{bmatrix}_q$. Thus, we have

$$\Pr\left[\dim(U \cap V) = a\right] = \frac{\begin{bmatrix} t \\ a \end{bmatrix}_q \begin{bmatrix} n-t \\ r-a \end{bmatrix}_q q^{(r-a)(t-a)}}{\begin{bmatrix} n \\ r \end{bmatrix}_q} \leq \gamma_q \cdot q^{a(t+r-a-n)}.$$

The inequality follows the conclusion in Lemma 3. ∎

B. Table XI for Simulated DFR by Welch-Berlekamp Like Algorithm

In Table XI, we test five types of simulable code parameters, and set five groups of parameters for each type. We simulated DFR for each group by performing decoding algorithms (Algorithm 2) in 10^5 times. The theoretical DFR is estimated by Equations (17) and (18) with $\gamma_2 = 4$, and $\gamma_q = 2$ if $q > 2$. The theoretical DFR for the types decoding up to the RGV bound is always greater than 1, and we recorded these DFR as 1 (see No. 16 - 25). Here, d is the minimal distance (Proposition 7), d_{RGV} is the RGV bound (Definition 3), and d_{RS} is the RS bound (Definition 4). The test scripts are available online at https://github.com/RQCPKE/EGCodesRQC.

TABLE XI
THEORETICAL AND SIMULATED DFR OF THE EG CODES FOR ERRORS OF WEIGHT r USING **WELCH-BERLEKAMP LIKE ALGORITHM**

Types	No.	Parameters (q, m, n, t, k, r)	Theoretical DFR	Simulated DFR	d	d_{RGV}	d_{RS}
Increase m $(t = m < n)$	1	$(2, 31, 41, 31, 9, 16)$	(2^{-5}) 0.0313	0.0150	13	19	25
	2	$(2, 32, 41, 32, 9, 16)$	(2^{-6}) 0.0156	0.0076	14	19	25
	3	$(2, 33, 41, 33, 9, 16)$	(2^{-7}) 0.0078	0.0038	15	20	26
	4	$(2, 34, 41, 34, 9, 16)$	(2^{-8}) 0.0039	0.0017	16	20	27
	5	$(2, 35, 41, 35, 9, 16)$	(2^{-9}) 0.0020	0.0008	17	20	28
Increase t $(t < m < n)$	6	$(2, 35, 41, 30, 9, 16)$	(2^{-4}) 0.0625	0.0310	22	20	28
	7	$(2, 35, 41, 31, 9, 16)$	(2^{-5}) 0.0313	0.0150	23	20	28
	8	$(2, 35, 41, 32, 9, 16)$	(2^{-6}) 0.0156	0.0084	24	20	28
	9	$(2, 35, 41, 33, 9, 16)$	(2^{-7}) 0.0078	0.0036	25	20	28
	10	$(2, 35, 41, 34, 9, 16)$	(2^{-8}) 0.0039	0.0018	26	20	28
Increase t $(t < n < m)$	11	$(2, 29, 26, 16, 5, 10)$	(2^{-2}) 0.0250	0.1320	11	16	22
	12	$(2, 29, 26, 17, 5, 10)$	(2^{-4}) 0.0625	0.0372	13	16	22
	13	$(2, 29, 26, 18, 5, 10)$	(2^{-6}) 0.0156	0.0098	14	16	22
	14	$(2, 29, 26, 19, 5, 10)$	(2^{-8}) 0.0039	0.0025	15	16	22
	15	$(2, 29, 26, 20, 5, 10)$	(2^{-10}) 0.00098	0.00058	16	16	22
Decoding RGV Bound $(k > r)$	16	$(2, 30, 37, 30, 23, 7)$	1	0.7120	8	7	12
	17	$(2, 30, 38, 30, 22, 8)$	1	0.7087	9	8	13
	18	$(2, 30, 39, 30, 21, 9)$	1	0.7100	10	9	14
	19	$(2, 30, 40, 30, 20, 10)$	1	0.7105	11	10	16
	20	$(2, 30, 41, 30, 19, 11)$	1	0.7141	12	11	17
Decoding RGV Bound $(k < r)$	21	$(2, 21, 34, 21, 8, 13)$	1	0.7124	14	13	17
	22	$(2, 22, 36, 22, 8, 14)$	1	0.7120	15	14	18
	23	$(2, 23, 38, 23, 8, 15)$	1	0.7118	16	15	19
	24	$(2, 24, 40, 24, 8, 16)$	1	0.7120	17	16	20
	25	$(2, 25, 42, 25, 8, 17)$	1	0.7125	18	17	21

C. The Proof of Theorem 8

Proof: We adapt the proof of Theorem 6, consider $\widehat{\boldsymbol{B}}^\top$, and estimate $\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < r + N(k+r)\right]$. Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^r$ be a basis of support for N errors $\boldsymbol{e}_i$'s. Let $\mathbf{CM}(\boldsymbol{e}_i) \in \mathbb{F}_q^{r\times n}$ of rank r be the coefficient matrix of $\boldsymbol{e}_i$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e}_i = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e}_i)$. Differently, $\boldsymbol{g}$ has weight n. Let $\boldsymbol{\gamma} \in \mathbb{F}_{q^m}^n$ be a basis of $\mathrm{Supp}(\boldsymbol{g})$. Let $\mathbf{CM}(\boldsymbol{g}) \in \mathbb{F}_q^{n\times n}$ of rank n be the coefficient matrix of $\boldsymbol{g}$ under $\boldsymbol{\gamma}$ such that $\boldsymbol{g} = \boldsymbol{\gamma}\mathbf{CM}(\boldsymbol{g})$. Let $\boldsymbol{N}_1 = \mathbf{Moore}(\boldsymbol{\varepsilon}, r) \in \mathbb{F}_{q^m}^{(r+1)\times r}$ and $\boldsymbol{N}_2 = \mathbf{Moore}(\boldsymbol{\gamma}, k+r-1) \in \mathbb{F}_{q^m}^{(k+r)\times n}$. By Equation (22), let $t = n$, we have

$$\begin{aligned}
\widehat{\boldsymbol{B}}^\top &= \left[\begin{array}{cccc} \boldsymbol{E}_1^\top & \boldsymbol{E}_2^\top & \cdots & \boldsymbol{E}_N^\top \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{Z}^\top, N)} \end{array}\right] = \left[\begin{array}{cccc} \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_1) & \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_2) & \cdots & \boldsymbol{N}_1\cdot\mathbf{CM}(\boldsymbol{e}_N) \\ \hline \multicolumn{4}{c}{\mathbf{Diag}(\boldsymbol{N}_2\cdot\mathbf{CM}(\boldsymbol{g}), N)} \end{array}\right] \\
&= \underbrace{\left[\begin{array}{c|c} \boldsymbol{N}_1 & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{Diag}(\boldsymbol{N}_2, N) \end{array}\right]}_{:=\boldsymbol{L}\in\mathbb{F}_{q^m}^{[r+N(k+r)+1]\times(r+Nn)}} \underbrace{\left[\begin{array}{c} \mathbf{CM}(\boldsymbol{e}_1) \quad \mathbf{CM}(\boldsymbol{e}_2) \quad \cdots \quad \mathbf{CM}(\boldsymbol{e}_N) \\ \hline \mathbf{Diag}(\mathbf{CM}(\boldsymbol{g}), N) \end{array}\right]}_{:=\boldsymbol{M}\in\mathbb{F}_q^{(r+Nn)\times Nn}}.
\end{aligned}$$

By Corollary 1, we have $\mathsf{rank}\left(\boldsymbol{N}_1\right) = r$, and as $k + r - 1 < n$, we have $\mathsf{rank}\left(\mathbf{Diag}(\boldsymbol{N}_2, N)\right) = N(k+r)$. Thus,

$$\mathsf{rank}(\boldsymbol{L}) = \mathsf{rank}\left(\boldsymbol{N}_1\right) + \mathsf{rank}\left(\mathbf{Diag}(\boldsymbol{N}_2, N)\right) = r + N(k+r) \leq Nn.$$

As $\boldsymbol{M} \in \mathbb{F}_q^{(r+Nn)\times Nn}$ and $\mathsf{rank}(\mathbf{CM}(\boldsymbol{g})) = n$, we have

$$\left\langle \left[\begin{array}{cccc} \mathbf{CM}(\boldsymbol{e}_1) & \mathbf{CM}(\boldsymbol{e}_2) & \cdots & \mathbf{CM}(\boldsymbol{e}_N) \end{array} \right] \right\rangle \subset \left\langle \mathbf{Diag}(\mathbf{CM}(\boldsymbol{g}), N) \right\rangle.$$

Hence,

$$\begin{aligned} \mathsf{rank}(\boldsymbol{M}) &= \dim\Big(\left\langle \left[\begin{array}{cccc} \mathbf{CM}(\boldsymbol{e}_1) & \mathbf{CM}(\boldsymbol{e}_2) & \cdots & \mathbf{CM}(\boldsymbol{e}_N) \end{array} \right] \right\rangle + \left\langle \mathbf{Diag}(\mathbf{CM}(\boldsymbol{g}), N) \right\rangle \Big) \\ &= r + Nn - r = Nn. \end{aligned}$$

If $r \leq \left\lfloor \frac{N(n-k)}{N+1} \right\rfloor$, then $Nn \geq N(k+r) + r$, further $\Pr\left[\mathsf{rank}(\boldsymbol{M}) < N(k+r) + r\right] = 0$. Following the Heuristic Argument presented in Theorem 3, we have

$$\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < N(k+r) + r \implies \mathsf{rank}(\boldsymbol{M}) < N(k+r) + r.$$

$$\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}^\top\right) < N(k+r) + r\right] \leq \Pr\left[\mathsf{rank}(\boldsymbol{M}) < N(k+r) + r\right] = 0.$$

■

APPENDIX B
DECODING ERRORS OF WEIGHT w ($w < r$) FOR THE EG CODES

Assume that the value r is the maximum q-degree solved in the LR problem. In this case, the EG codes can decode up to weight r. Let $w < r$. Now, we analyze how to decode when the error of weight w occurs, and show the relation between the solutions of the decoding problem and LR problem.

Theorem 16 *Assume that the* LR *problem can be solved up to q-degree r. Let $f(x)$ be a fixed q-polynomial of q-degree $\leq k-1$. Let $(\boldsymbol{g}, \boldsymbol{y})$ be the instance of the* $\mathsf{DecEGCode}(\boldsymbol{g}, \boldsymbol{y})$ *problem with $\boldsymbol{y} = f(\boldsymbol{g}) + \boldsymbol{e}$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = w$. Let $\mathcal{A}_{\boldsymbol{e}}(x)$ be the annihilator polynomial of $\boldsymbol{e}$. The solutions of the* $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$ *problem are included in a set $\mathcal{V}_w^r$:*

$$\mathcal{V}_w^r = \left\{ \big(v(x),\ -v(x) \circ f(x)\big) \ :\ v(x) = z(x) \circ \mathcal{A}_{\boldsymbol{e}}(x),\ z(x) \in \mathcal{L}_{\leq r-w}[x] \right\}.$$

Then the set $\mathcal{V}_w^r$ is isomorphic to a linear space over $\mathbb{F}_{q^m}$ of dimension $r - w + 1$.

Proof: It is clear that any $\big(v(x),\ -v(x) \circ f(x)\big) \in \mathcal{V}_w^r$ satisfies

$$-v\left(\boldsymbol{y}\right) = -v(f\left(\boldsymbol{g}\right) + \boldsymbol{e}) = -v(f\left(\boldsymbol{g}\right)) + z \circ \mathcal{A}_{\boldsymbol{e}}(\boldsymbol{e}) = -v(f\left(\boldsymbol{g}\right)) = -\left(v \circ f\right)\left(\boldsymbol{g}\right).$$

When $z(x) \neq 0$, $v(x) = z(x) \circ \mathcal{A}_{\boldsymbol{e}}(x) \neq 0$, $\deg_q v(x) \leq r$, and $\deg_q(-v \circ f)(x) \leq k + r - 1$, such $\big(v(x),\ -v(x) \circ f(x)\big)$ exactly is the solution to the $\mathsf{LR}(\boldsymbol{g}, \boldsymbol{y})$ problem. We denote a map by

$$\begin{aligned} \varphi :\quad \mathcal{L}_{\leq r}[x] &\ \to\ \mathbb{F}_{q^m}^{r+1} \\ b(x) = \sum_{i=0}^{r} b_i x^{q^i} &\ \mapsto\ (b_0, b_1, \ldots, b_r). \end{aligned}$$

By some abuse of notation, we also denote by φ its natural extension to $\mathcal{V}_w^r$:

$$\begin{aligned} \varphi :\quad \mathcal{V}_w^r &\ \to\ \mathbb{F}_{q^m}^{k+2r+1} \\ \big(v(x),\ -v(x) \circ f(x)\big) &\ \mapsto\ \Big(\varphi(v(x)), \varphi\left(-v(x) \circ f(x)\right)\Big) \end{aligned}$$

Let $v(x) = z(x) \circ \mathcal{A}_{\boldsymbol{e}}(x) = \sum_{i=0}^{r} v_i x^{q^i}$ and $u(x) = -v(x) \circ f(x) = \sum_{i=0}^{k+r-1} u_i x^{q^i}$. Let $f(x) = \sum_{i=0}^{k-1} f_i x^{q^i}$, and $\mathcal{A}_{\boldsymbol{e}}(x) = \sum_{i=0}^{w} a_i x^{q^i}$, $(a_w = 1)$. Let $z(x) = \sum_{i=0}^{r-w} z_i x^{q^i}$. One easily checks equations:

$$\left(u_0, u_1, \ldots, u_{k+r-1}\right)^\top = -\mathbf{PM}(f(x), r)\left(v_0, v_1, \ldots, v_r\right)^\top \tag{33}$$

$$\left(v_0, v_1, \ldots, v_r\right)^\top = \mathbf{PM}\left(\mathcal{A}_{\boldsymbol{e}}(x), r - w\right)\left(z_0, z_1, \ldots, z_{r-w}\right)^\top. \tag{34}$$

Therefore, we have

$$\begin{aligned}&\Big(\varphi\big(v(x),\ -v(x)\circ f(x)\big)\Big)^{\top}=\Big(\varphi(v(x)),\varphi\left(-v(x)\circ f(x)\right)\Big)^{\top}\\&=\left(v_0,v_1,\ldots,v_r,u_0,u_1,\ldots,u_{k+r-1}\right)^{\top}\\&=\underbrace{\left[\begin{array}{c}\boldsymbol{I}_{(r+1)\times(r+1)}\\\hline -\mathbf{PM}(f(x),r)\end{array}\right]}_{:=\boldsymbol{F}\in\mathbb{F}_{q^m}^{(k+2r+1)\times(r+1)}}\underbrace{\mathbf{PM}\left(\mathcal{A}_{\boldsymbol{e}}(x),r-w\right)}_{:=\boldsymbol{W}\in\mathbb{F}_{q^m}^{(r+1)\times(r-w+1)}}\left(z_0,z_1,\ldots,z_{r-w}\right)^{\top}.\end{aligned}\tag{35}$$

In Equation (35), $\boldsymbol{F}$ is fixed and is column full-rank (rank $r+1$), and $\boldsymbol{W}$ is fixed and is of rank $r-w+1$ due to $a_r=1$. Thus, $\boldsymbol{FW}$ is a column full-rank $(k+2r+1)\times(r-w+1)$ matrix over $\mathbb{F}_{q^m}$. This shows that under the map φ, the set $\mathcal{V}_w^r$ is isomorphic to a linear space $\langle(\boldsymbol{FW})^{\top}\rangle$ over $\mathbb{F}_{q^m}$ of dimension $r-w+1$. ■

By Theorem 16, we can get that in $\mathcal{V}_w^r$, any no-zero pair $(v(x),u(x))$ satisfies $-v(x)\backslash u(x)=f(x)$. Thus, once the set $\mathcal{V}_w^r$ is determined, we can obtain the solution to the $\mathsf{LR}(\boldsymbol{g},\boldsymbol{y})$ problem.

Theorem 17 *Let $f(x)$ be a fixed q-polynomial of $\deg_q f(x)\le k-1$. Let $\boldsymbol{y}=f(\boldsymbol{g})+\boldsymbol{e}$ and $\|\boldsymbol{e}\|_{\mathrm{R}}=w$. Let $\mathsf{LR}(\boldsymbol{g},\boldsymbol{y})$ be the instance of the LR problem. If the dimension of the right kernel $\mathsf{kernel}(\boldsymbol{A})$ of matrix $\boldsymbol{A}$ defined in Equation (8) is $r-w+1$, then $\mathsf{kernel}(\boldsymbol{A})$ is isomorphic to $\mathcal{V}_w^r$ defined in Theorem 16.*

Proof: If $f(x)$ and $(v\circ f)(x)$ are the solution to the $\mathsf{LR}(\boldsymbol{g},\boldsymbol{y})$ problem, then $v(x)\neq 0$, $\deg_q v(x)\le r$, $\deg_q(v\circ f)(x)\le k+r-1$, and

$$v\left(\boldsymbol{y}\right)=\left(v\circ f\right)\left(\boldsymbol{g}\right)\iff v\left(\boldsymbol{y}\right)=v(f\left(\boldsymbol{g}\right))\iff v\left(\boldsymbol{y}-f(\boldsymbol{g})\right)=\mathbf{0}_n\iff v\left(\boldsymbol{e}\right)=\mathbf{0}_n.$$

Then $v(x)$ must have the form of $v(x)=z(x)\circ\mathcal{A}_{\boldsymbol{e}}(x)$, where $z(x)\in\mathcal{L}[x]$ is random, $\deg_q z(x)\le r-w$, and $\mathcal{A}_{\boldsymbol{e}}(x)$ is the annihilator polynomial of $\boldsymbol{e}$ (Definition 7, $\mathcal{A}_{\boldsymbol{e}}(x)$ is unique and monic, $\deg_q\mathcal{A}_{\boldsymbol{e}}(x)=w$, and $\mathcal{A}_{\boldsymbol{e}}(\boldsymbol{e})=\mathbf{0}_n$).

Let $f(x)=\sum_{i=0}^{k-1}f_i x^{q^i}$ and $v(x)=z(x)\circ\mathcal{A}_{\boldsymbol{e}}(x)=\sum_{i=0}^{r}v_i x^{q^i}$. Let $\mathcal{A}_{\boldsymbol{e}}(x)=\sum_{i=0}^{w}a_i x^{q^i}$ $(a_w=1)$ and $z(x)=\sum_{i=0}^{r-w}z_i x^{q^i}$. From $v\left(\boldsymbol{y}-f(\boldsymbol{g})\right)=\mathbf{0}_n$, combing Equation (9), we have

$$\begin{gathered}\mathbf{Moore}(\boldsymbol{y}-f(\boldsymbol{g}),r)^{\top}\left(v_0,v_1,\ldots,v_r\right)^{\top}=\mathbf{0}_n\\\Longleftrightarrow\\\boldsymbol{A}\left[\begin{array}{c}\boldsymbol{I}_{(r+1)\times(r+1)}\\\hline -\mathbf{PM}(f(x),r)\end{array}\right]\left(v_0,v_1,\ldots,v_r\right)^{\top}=\mathbf{0}_n\\\Longleftrightarrow\end{gathered}$$

$$\boldsymbol{A}\underbrace{\left[\begin{array}{c}\boldsymbol{I}_{(r+1)\times(r+1)}\\\hline -\mathbf{PM}(f(x),r)\end{array}\right]}_{:=\boldsymbol{F}\in\mathbb{F}_{q^m}^{(k+2r+1)\times(r+1)}}\underbrace{\mathbf{PM}\left(\mathcal{A}_{\boldsymbol{e}}(x),r-w\right)}_{:=\boldsymbol{W}\in\mathbb{F}_{q^m}^{(r+1)\times(r-w+1)}}\left(z_0,z_1,\ldots,z_{r-w}\right)^{\top}=\mathbf{0}_n\tag{36}$$

In Equation (36), $\boldsymbol{F}$ is fixed and is a column full-rank (rank $r+1$), and $\boldsymbol{W}$ is fixed and is of rank $r-w+1$ due to $a_w=1$. Thus, $\boldsymbol{FW}$ is a column full-rank $(k+2r+1)\times(r-w+1)$ matrix over $\mathbb{F}_{q^m}$. This shows that $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)=r-w+1$ and $\left\langle(\boldsymbol{FW})^{\top}\right\rangle=\mathsf{kernel}(\boldsymbol{A})$.

Consider the linear system

$$\boldsymbol{A}\boldsymbol{x}^{\top}=\mathbf{0}_n.\tag{37}$$

Combing Equation (35), we clearly have that if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)=r-w+1$, then $\mathsf{kernel}(\boldsymbol{A})$ is isomorphic to $\mathcal{V}_w^r$. ■

By Theorem 16 and Theorem 17, if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)=r-w+1$, for any non-zero solution $\boldsymbol{x}=(v_0,v_1,\ldots,v_r,u_0,u_1,\ldots,u_{k+r-1})$ to the system (37), let $v(x)=\sum_{i=0}^{r}v_i x^{q^i}$ and $u(x)=\sum_{i=0}^{k+r-1}u_i x^{q^i}$, then $f(x)=-v(x)\backslash u(x)$. Such $(v(x),f(x))$ is solution to the $\mathsf{NLR}(\boldsymbol{g},\boldsymbol{y})$ problem. This means that, given the EG codes decoding weight up to r, any error of weight $w\le r$ can decoded by solving the $\mathsf{LR}(\boldsymbol{g},\boldsymbol{y})$ problem if $\dim\left(\mathsf{kernel}(\boldsymbol{A})\right)=r-w+1$.

Proposition 12 *Assume that the LR problem can be solved up to q-degree r. For any error $\boldsymbol{e}\in\mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}}=w$, if $k+r\le t\le\min\{n,m\}$ and $k+2r\le n$, then $\mathsf{rank}(\boldsymbol{B})\le k+r+w$.*

Proof: Recall that when the LR problem can be solved up to q-degree r, following Proposition 9, the matrix $\boldsymbol{A}$ is equivalent to $\boldsymbol{B}$ in Equation (12).

$$\boldsymbol{B}=\left[\begin{array}{cc}\mathbf{Moore}(\boldsymbol{e},r)^{\top} & \mathbf{Moore}(\boldsymbol{g},k+r-1)^{\top}\end{array}\right].$$

We consider the rank of $\boldsymbol{B}^\top$. Let

$$\boldsymbol{B}_1 = \mathbf{Moore}(\boldsymbol{e}, r), \quad \boldsymbol{B}_2 = \mathbf{Moore}(\boldsymbol{g}, k+r-1), \quad \boldsymbol{B}^\top = \begin{bmatrix} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{bmatrix}.$$

Since $k+r \le t$, from Proposition 5, we have $\mathsf{rank}(\boldsymbol{B}_1) = w$ and $\mathsf{rank}(\boldsymbol{B}_2) = k+r$. Thus,

$$\mathsf{rank}(\boldsymbol{B}) = \mathsf{rank}\left(\boldsymbol{B}^\top\right) = \mathsf{rank}\left(\begin{bmatrix} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{bmatrix}\right) \le \mathsf{rank}(\boldsymbol{B}_1) + \mathsf{rank}(\boldsymbol{B}_2) \le k+r+w.$$

■

From Theorem 17, the DFR of decoding weight $w < r$ depends on the probability that $\dim(\mathsf{kernel}(\boldsymbol{A})) \neq r-w+1$. Proposition 12 shows $\mathsf{rank}(\boldsymbol{A}) = \mathsf{rank}(\boldsymbol{B}) \le k+r+w$, since $\mathsf{rank}(\boldsymbol{A}) + \dim(\mathsf{kernel}(\boldsymbol{A})) = k+2r+1$, we have $\Pr[\dim(\mathsf{kernel}(\boldsymbol{A})] \ge r-w+1$. Thus, the DFR depends on probability of $\dim(\mathsf{kernel}(\boldsymbol{A})) > r-w+1$, which is equivalent to $\mathsf{rank}(\boldsymbol{A}) < k+r+w$. We next analyze the probability of $\mathsf{rank}(\boldsymbol{A}) < k+r+w$ (or $\mathsf{rank}(\boldsymbol{B}) < k+r+w$) in Theorem 18.

Theorem 18 *For any uniform and random error $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ and $\|\boldsymbol{e}\|_{\mathrm{R}} = w$, if $k+r \le t \le \min\{n,m\}$ and $k+2r \le n$, then*

$$\Pr[\mathsf{rank}(\boldsymbol{B}) < w+k+r] \le \gamma_q \cdot q^{a(t+w-a-n)}, \tag{38}$$

where $a = t-k-r+1$.

Proof: We consider $\boldsymbol{B}^\top$ and estimate $\Pr[\mathsf{rank}(\boldsymbol{B}^\top) < w+k+r]$. Let $\boldsymbol{\varepsilon} \in \mathbb{F}_{q^m}^w$ be a basis of $\mathrm{Supp}(\boldsymbol{e})$. Let $\mathbf{CM}(\boldsymbol{e}) \in \mathbb{F}_q^{w\times n}$ of rank w be the coefficient matrix of $\boldsymbol{e}$ under $\boldsymbol{\varepsilon}$ such that $\boldsymbol{e} = \boldsymbol{\varepsilon}\mathbf{CM}(\boldsymbol{e})$. Let $\boldsymbol{\gamma} \in \mathbb{F}_{q^m}^t$ be a basis of $\mathrm{Supp}(\boldsymbol{g})$. Let $\mathbf{CM}(\boldsymbol{g}) \in \mathbb{F}_q^{t\times n}$ of rank t be the coefficient matrix of $\boldsymbol{g}$ under $\boldsymbol{\gamma}$ such that $\boldsymbol{g} = \boldsymbol{\gamma}\mathbf{CM}(\boldsymbol{g})$. Following Definition 10 and Proposition 3,

$$\begin{aligned}
\boldsymbol{B}^\top &= \begin{bmatrix} \boldsymbol{B}_1 \\ \boldsymbol{B}_2 \end{bmatrix} = \left[\begin{array}{c} \mathbf{Moore}(\boldsymbol{e}, r) \\ \hline \mathbf{Moore}(\boldsymbol{g}, k+r-1) \end{array}\right] = \left[\begin{array}{c} \mathbf{Moore}(\boldsymbol{\varepsilon}, r)\cdot\mathbf{CM}(\boldsymbol{e}) \\ \hline \mathbf{Moore}(\boldsymbol{\gamma}, k+r-1)\cdot\mathbf{CM}(\boldsymbol{g}) \end{array}\right] \\
&= \underbrace{\left[\begin{array}{c|c} \mathbf{Moore}(\boldsymbol{\varepsilon}, r) & \mathbf{0}_{(r+1)\times t} \\ \hline \mathbf{0}_{(k+r)\times r} & \mathbf{Moore}(\boldsymbol{\gamma}, k+r-1) \end{array}\right]}_{:=\boldsymbol{L}\in\mathbb{F}_{q^m}^{(k+2r+1)\times(t+w)}} \underbrace{\left[\begin{array}{c} \mathbf{CM}(\boldsymbol{e}) \\ \hline \mathbf{CM}(\boldsymbol{g}) \end{array}\right]}_{:=\boldsymbol{L}\in\mathbb{F}_q^{(t+w)\times n}}.
\end{aligned} \tag{39}$$

By Corollary 1, as $w < r$, we have $\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) = w$, and as $k+r-1 < t$, we have $\mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\gamma}, k+r-1)\right) = k+r$. Thus,

$$\mathsf{rank}(\boldsymbol{L}) = \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\varepsilon}, r)\right) + \mathsf{rank}\left(\mathbf{Moore}(\boldsymbol{\gamma}, k+r-1)\right) = w+k+r.$$

As $\mathsf{rank}\left(\boldsymbol{B}^\top\right) \le \min\left\{\mathsf{rank}(\boldsymbol{L}), \mathsf{rank}(\boldsymbol{M})\right\}$ and $\boldsymbol{M} \in \mathbb{F}_q^{(t+w)\times n}$ is defined in the basis field $\mathbb{F}_q$, we have a similar heuristic argument: if $\mathsf{rank}(\boldsymbol{M}) \ge w+k+r$, then $\mathsf{rank}\left(\boldsymbol{B}^\top\right) = w+k+r$. Hence, we have

$$\mathsf{rank}\left(\boldsymbol{B}^\top\right) < w+k+r \implies \mathsf{rank}(\boldsymbol{M}) < w+k+r. \tag{40}$$

Moreover,

$$\begin{aligned}
\mathsf{rank}(\boldsymbol{M}) &= \mathsf{rank}\begin{bmatrix} \mathbf{CM}(\boldsymbol{e}) \\ \mathbf{CM}(\boldsymbol{g}) \end{bmatrix} = \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle + \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big) \\
&= \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle\Big) + \dim\Big(\langle\mathbf{CM}(\boldsymbol{g})\rangle\Big) - \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big) \\
&= w + t - \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big).
\end{aligned}$$

Let $\Delta = \dim\Big(\langle\mathbf{CM}(\boldsymbol{e})\rangle \cap \langle\mathbf{CM}(\boldsymbol{g})\rangle\Big)$, we have

$$\mathsf{rank}(\boldsymbol{M}) < w+k+r \iff \Delta > t-k-r. \tag{41}$$

Let $a = t-k-r+1$. Finally, combining Equations (40) and (41), we have:

- When $a \le \min\{t, w\}$,

$$\begin{aligned}
&\Pr\left[\mathsf{rank}\left(\boldsymbol{B}^\top\right) < w+k+r\right] \le \Pr\left[\mathsf{rank}(\boldsymbol{M}) < w+k+r\right] = \Pr\left[\Delta > t-k-r\right] \\
&= \sum_{i=a}^{\min\{t,w\}} \Pr\left[\Delta = i\right] \approx \Pr\left[\Delta = a\right] \le \gamma_q \cdot q^{a(t+w-a-n)}.
\end{aligned} \tag{42}$$

The first inequality "$\le$" due to "$\implies$" of Equation (40). The second equation "$=$" due to "$\iff$" of Equation (41). The approximation "$\approx$" is natural. By the probability in Lemma 4 (see Appendix A), as the dimension i increases, the probability decreases significantly. The last inequality also follows Lemma 4.

- When $a > \min\{t, w\}$, it is impossible to obtain an intersection space of dimension $\geq a$. Hence,

$$\Pr\left[\mathsf{rank}\left(\boldsymbol{B}^{\top}\right) < w + k + r\right] \leq \Pr\left[\mathsf{rank}(\boldsymbol{M}) < w + k + r\right] = \Pr\left[\Delta \geq a\right] = 0. \tag{43}$$

This means that DFR is null and the decoding algorithm is deterministic.

■

Theorem 18 shows that the DFR quickly decreases in w and is upper bounded by $\gamma_q \cdot q^{a(t+r-a-n)}$. The probability $\gamma_q \cdot q^{a(t+r-a-n)}$ is exactly one of decoding weight r. Thus, given EG codes decoding up to weight r, such EG codes can decode errors of weight $\leq r$ with the maximum DFR: $\gamma_q \cdot q^{a(t+r-a-n)}$. The decoding procedure is given in Algorithm 1.

Simulated DFR for Decoding Errors of Weight $w \leq r$. In Table XII, we chose four types of simulable code parameters, and set five groups of parameters for each type. We simulated DFR for each group by performing decoding algorithms (Algorithm 1) in 10^5 times. The theoretical DFR is estimated by Equations (42) and (43) with $\gamma_2 = 4$, and $\gamma_q = 2$ if $q > 2$. From Table XII, we can observe that the theoretical and simulated DFR are close, and the theoretical DFR is always greater than the simulated one. These show the correctness of our theoretical DFR.

TABLE XII
THEORETICAL AND SIMULATED DFR OF THE EG CODES FOR ERRORS OF WEIGHT $w \leq r$

Types	No.	Parameters (q, m, n, t, k, r, w)	Theoretical DFR	Simulated DFR	d_{RGV}	d_{RS}
Decrease w ($t = m < n$)	1	$(2, 27, 41, 27, 9, 16, 16)$	(2^{-1}) 0.5000	0.2312	17	22
	2	$(2, 27, 41, 27, 9, 16, 15)$	(2^{-4}) 0.0625	0.0380	17	22
	3	$(2, 27, 41, 27, 9, 16, 14)$	(2^{-7}) 0.0078	0.0050	17	22
	4	$(2, 27, 41, 27, 9, 16, 13)$	(2^{-10}) 0.00098	0.00062	17	22
	5	$(2, 27, 41, 27, 9, 16, 12)$	(2^{-13}) 0.00012	0.00007	17	22
Decrease w ($t < n < m$)	6	$(2, 29, 26, 16, 5, 10, 10)$	(2^{-2}) 0.0250	0.1326	16	22
	7	$(2, 29, 26, 16, 5, 10, 9)$	(2^{-4}) 0.0625	0.0362	16	22
	8	$(2, 29, 26, 16, 5, 10, 8)$	(2^{-6}) 0.0156	0.0097	16	22
	9	$(2, 29, 26, 16, 5, 10, 7)$	(2^{-8}) 0.0039	0.0026	16	22
	10	$(2, 29, 26, 16, 5, 10, 6)$	(2^{-10}) 0.00098	0.00069	16	22
Decrease w (Decoding RGV Bound $k > r$)	11	$(2, 30, 37, 30, 23, 7, 7)$	(2^{1}) 2	0.7122	7	12
	12	$(2, 30, 37, 30, 23, 7, 6)$	(2^{0}) 1	0.4197	7	12
	13	$(2, 30, 37, 30, 23, 7, 5)$	(2^{-1}) 0.5000	0.2217	7	12
	14	$(2, 30, 37, 30, 23, 7, 4)$	(2^{-2}) 0.2500	0.1145	7	12
	15	$(2, 30, 37, 30, 23, 7, 3)$	(2^{-3}) 0.1250	0.0549	7	12
Decrease w (Decoding RGV Bound $k < r$)	16	$(2, 21, 34, 21, 8, 13, 13)$	(2^{1}) 2	0.7125	13	17
	17	$(2, 21, 34, 21, 8, 13, 12)$	(2^{0}) 1	0.4234	13	17
	18	$(2, 21, 34, 21, 8, 13, 11)$	(2^{-1}) 0.5000	0.2312	13	17
	19	$(2, 21, 34, 21, 8, 13, 10)$	(2^{-2}) 0.2500	0.1203	13	17
	20	$(2, 21, 34, 21, 8, 13, 9)$	(2^{-3}) 0.1250	0.0608	13	17

APPENDIX C
DECODING ERRORS OF WEIGHT w $(w < r)$ FOR THE IEG CODES

Assume that the value r is the maximum q-degree solved in the LR problem (Definition 16) obtained from the decoding IEG codes. In this case, the IEG codes can decode up to weight r. Let $w < r$. Now, we analyze how to decode when N errors $\boldsymbol{e}_i$'s share the same w-dimensional support, and show the relation between the solutions of the decoding problem and LR problem. Adapting theorems and propositions in Appendix B, we can easily obtain the following Theorems 19-21 and Proposition 13.

Theorem 19 *Assume that the* LR *problem defined in Definition 16 can be solved up to q-degree r. Let $f_i(x)$'s be fixed q-polynomials of q-degree $\leq k-1$. Let $\left(\boldsymbol{g}, \{\boldsymbol{y}_i\}_{i\in[N]}\right)$ be the instance of decoding IEG codes problem with $\boldsymbol{y}_i = f_i(\boldsymbol{g}) + \boldsymbol{e}_i$ and $\boldsymbol{e}_i$ of sharing w-dimensional support E. Let $\mathcal{A}_E(x)$ be the annihilator polynomial of E. The solutions of the* LR $\left(\boldsymbol{g}, \{\boldsymbol{y}_i\}_{i\in[N]}\right)$ *problem are included in a set $\mathcal{V}_w^{N,r}$:*

$$\mathcal{V}_w^{N,r} = \left\{\left(v(x),\ \{-v(x) \circ f_i(x)\}_{i\in[N]}\right)\ :\ v(x) = z(x) \circ \mathcal{A}_E(x),\ z(x) \in \mathcal{L}_{\leq r-w}[x]\right\}.$$

Then the set $\mathcal{V}_w^{N,r}$ is isomorphic to a linear space over $\mathbb{F}_{q^m}$ of dimension $r - w + 1$.

Theorem 20 *Let $f_i(x)$ be fixed q-polynomials of q-degree $\leq k-1$. Let $\boldsymbol{y}_i = f_i(\boldsymbol{g}) + \boldsymbol{e}_i$ and $\boldsymbol{e}_i$ of sharing w-dimensional support E. Let* LR $\left(\boldsymbol{g}, \{\boldsymbol{y}_i\}_{i\in[N]}\right)$ *be the instance of the* LR *problem defined in Definition 16. If the dimension of the right kernel* kernel $\left(\widehat{\boldsymbol{A}}\right)$ *of matrix $\widehat{\boldsymbol{A}}$ defined in Equation (20) is $r - w + 1$, then* kernel $\left(\widehat{\boldsymbol{A}}\right)$ *is isomorphic to $\mathcal{V}_w^{N,r}$ defined in Theorem 19.*

Proposition 13 *Assume that the LR problem defined in Definition 16 can be solved up to q-degree r. For any error $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^n$ sharing w-dimensional support, if $k+r \le t \le \min\{n,m\}$ and $r+N(k+r) \le nN$, then* $\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) \le w + N(k+r)$.

Theorem 21 *For any N uniform and random errors $\boldsymbol{e}_i \in \mathbb{F}_{q^m}^n$ sharing w-dimensional support, if $k+r \le t \le \min\{n,m\}$ and $r+N(k+r) \le nN$, then*

$$\Pr\left[\mathsf{rank}\left(\widehat{\boldsymbol{B}}\right) \le w + N(k+r)\right] \le \gamma_q \cdot q^{a(Nt+w-a-Nn)},$$

where $a = N(t-k-r)+1$.

Appendix D
Public Key Encryption

Definition 18 (Public Key Encryption) *A Public Key Encryption (PKE) scheme* $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ *consists of three polynomial-time algorithms:*

- KGen*: The key generation algorithm that takes the security parameter λ as input and outputs a public key pk and a private key sk. It is denoted as $(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$.*
- Enc*: The encryption algorithm that takes pk and a plaintext M as inputs and outputs a ciphertext C. It is denoted as $C \leftarrow \mathsf{Enc}(pk, M)$.*
- Dec*: The decryption algorithm that takes sk and C as inputs and outputs a plaintext M. It is denoted as $M \leftarrow \mathsf{Dec}(sk, C)$.*

The correctness of PKE requires that for all $(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$, any plaintext M, and any $C \leftarrow \mathsf{Enc}(pk, M)$, the equation $M = \mathsf{Dec}(sk, C)$ hold with overwhelming probability.

An IND-CPA secure PKE scheme is defined by the experiment $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}}(\lambda)$ between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

1) $\mathcal{A}$ takes λ as inputs.
2) $\mathcal{C}$ computes $(pk, sk) \leftarrow \mathsf{KGen}(1^\lambda)$, gives pk to $\mathcal{A}$, and keeps sk to itself.
3) $\mathcal{A}$ outputs two equal length plaintexts M_0, M_1. $\mathcal{C}$ randomly chooses a bit $b^* \in \{0,1\}$ and returns the challenge ciphertext $C^* = \mathsf{Enc}(pk, M_{b^*})$ to $\mathcal{A}$.
4) $\mathcal{A}$ outputs a guess $b \in \{0,1\}$. If $b = b^*$, $\mathcal{C}$ outputs 1, else outputs 0.

Definition 19 (IND-CPA Security) *A PKE scheme is Indistinguishability under Chosen Plaintext Attacks (IND-CPA) if for any* PPT *adversary $\mathcal{A}$, its advantage*

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\mathsf{PKE},\mathcal{A}}(\lambda) = 1\right] - \frac{1}{2}\right| \le \mathsf{negl}(\lambda).$$

Appendix E
Ideal Codes and Ideal BRSD Problem

To apply the ideal variants of the BRSD problem to RQC, in this section, we recall the definitions of ideal codes.

Let $P(X)$ be a polynomial of degree n in $\mathbb{F}_q[X]$ and $\mathcal{R} = \mathbb{F}_{q^m}[X]/\langle P(X)\rangle$. By the map $\psi : \mathbb{F}_{q^m}^n \to \mathcal{R}$, the element of $\mathbb{F}_{q^m}^n$ is viewed as one of $\mathcal{R}$ and vice versa. The polynomial associated the vector $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_{q^m}^n$ is defined as $\boldsymbol{u}(X) = \sum_{i=0}^{n-1} u_i X^i \in \mathcal{R}$. The vector $(1, 0, \ldots, 0) \in \mathbb{F}_{q^m}^n$ corresponds to the identity $\mathbf{1}$ of $\mathcal{R}$. For $\boldsymbol{u} \in \mathbb{F}_{q^m}^n$ and $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$, the product $\boldsymbol{u} \cdot \boldsymbol{v}$ is defined as the vector of coefficients of $\boldsymbol{u}(X)\boldsymbol{v}(X) \mod P(X)$, i.e., $\psi^{-1}\big(\boldsymbol{u}(X)\boldsymbol{v}(X) \mod P(X)\big)$.

Definition 20 (Ideal Matrix) *The ideal matrix generated by $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ is defined as an $n \times n$ matrix:*

$$\mathcal{IM}(\boldsymbol{v}) = \begin{bmatrix} \psi^{-1}\big(\boldsymbol{v}(X)\big) \\ \psi^{-1}\big(X\boldsymbol{v}(X) \mod P(X)\big) \\ \vdots \\ \psi^{-1}\big(X^{n-1}\boldsymbol{v}(X) \mod P(X)\big) \end{bmatrix}.$$

With the ideal matrix, the product $\boldsymbol{u} \cdot \boldsymbol{v}$ is equivalent to the vector-matrix product

$$\boldsymbol{u} \cdot \boldsymbol{v} = \psi^{-1}\big(\boldsymbol{u}(X)\boldsymbol{v}(X) \mod P(X)\big) = \psi^{-1}\left(\sum_{i=0}^{n-1} u_i X^i \boldsymbol{v}(X) \mod P(X)\right)$$
$$= \psi^{-1}\left(\sum_{i=0}^{n-1} u_i \left(X^i \boldsymbol{v}(X) \mod P(X)\right)\right) = (u_0, \ldots, u_{n-1})\,\mathcal{IM}(\boldsymbol{v}) = \boldsymbol{u}\mathcal{IM}(\boldsymbol{v}).$$

Thus, $\boldsymbol{u} \cdot \boldsymbol{v} = \boldsymbol{u}\mathcal{IM}(\boldsymbol{v}) = \boldsymbol{v}\mathcal{IM}(\boldsymbol{u}) = \boldsymbol{v} \cdot \boldsymbol{u}$. It is clear that, for any $\boldsymbol{h}_1$, $\boldsymbol{h}_2$, $\boldsymbol{e}_1$, and $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^n$,

$$\boldsymbol{h}_1 \cdot \boldsymbol{e}_1 + \boldsymbol{h}_2 \cdot \boldsymbol{e}_2 = \boldsymbol{s} \iff \begin{bmatrix}\boldsymbol{h}_1 & \boldsymbol{h}_2\end{bmatrix} \cdot \begin{bmatrix}\boldsymbol{e}_1 \\ \boldsymbol{e}_2\end{bmatrix} = \boldsymbol{s} \iff \begin{bmatrix}\mathcal{IM}(\boldsymbol{h}_1)^\top & \mathcal{IM}(\boldsymbol{h}_2)^\top\end{bmatrix} \begin{bmatrix}\boldsymbol{e}_1^\top \\ \boldsymbol{e}_2^\top\end{bmatrix} = \boldsymbol{s}^\top$$

To reduce the size of rank-based cryptosystems, the family of ideal codes is introduced in rank-based cryptography. The ideal codes are codes with a systematic generator matrix consisting of blocks of ideal matrices.

Definition 21 (Ideal Codes [9], [42]) *Let $P(X)$ be a polynomial of degree n in $\mathbb{F}_q[X]$. An $[n\ell, nt]_{q^m}$ code $\mathcal{C}$ is an (ℓ, t)-ideal code if its generator matrix under the systematic form is of the form*

$$\boldsymbol{G} = \begin{bmatrix} & \mathcal{IM}(\boldsymbol{g}_{1,1}) & \dots & \mathcal{IM}(\boldsymbol{g}_{1,\ell-t}) \\ \boldsymbol{I}_{tn} & \vdots & \ddots & \vdots \\ & \mathcal{IM}(\boldsymbol{g}_{t,1}) & \dots & \mathcal{IM}(\boldsymbol{g}_{t,\ell-t}) \end{bmatrix}$$

where $(\boldsymbol{g}_{i,j})_{i\in[t],j\in[\ell-t]}$ are vectors of $\mathbb{F}_{q^m}^n$.

It has been proven that if m and n are two different prime numbers and $P(X)$ is irreducible, then a non-zero ideal matrix is always non-singular [22]. In this case, the generator matrix of ideal codes can be always reduced to the systematic form. We only use $[\ell n, n]_{q^m}$-ideal codes with the systematic parity-check matrix

$$\boldsymbol{H} = \begin{bmatrix} & \mathcal{IM}(\boldsymbol{h}_1)^\top \\ \boldsymbol{I}_{(\ell-1)n} & \vdots \\ & \mathcal{IM}(\boldsymbol{h}_{\ell-1})^\top \end{bmatrix} \in \mathbb{F}_{q^m}^{(\ell-1)n\times \ell n}. \tag{44}$$

Definition 22 (Ideal BRSD (IBRSD) Problem) *Let $\boldsymbol{H}$ be a systematic parity-check matrix of a random $[\ell n, n]_{q^m}$-ideal code and $\boldsymbol{s} \in \mathbb{F}_{q^m}^{(\ell-1)n}$. The problem is to find a blockwise error $\boldsymbol{e} \in \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}$ such that $\boldsymbol{s} = \boldsymbol{H}\boldsymbol{e}^\top$.*

This is called the computational IBRSD problem. In security proof of cryptosystems, the decisional version is often used.

Definition 23 (Decisional IBRSD (DIBRSD) Problem) *Let $\boldsymbol{H}$ be a systematic parity-check matrix of a random $[\ell n, n]_{q^m}$-ideal code. The $\mathsf{DIBRSD}_{q,m,\ell n,n}^{\boldsymbol{n},\boldsymbol{r}}$ problem is hard, if for any PPT adversary $\mathcal{B}$, the following advantage is negligible:*

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DIBRSD}_{q,m,\ell n,n,r}^{\ell,\boldsymbol{n},\boldsymbol{r}}}(\lambda) := \left|\Pr\left[\mathcal{B}(\boldsymbol{H}, \boldsymbol{s}) = 1 \ : \ \boldsymbol{s} \xleftarrow{\$} \mathbb{F}_{q^m}^{(\ell-1)n}\right] - \Pr\left[\mathcal{B}\left(\boldsymbol{H}, \boldsymbol{H}\boldsymbol{e}^\top\right) = 1 \ : \ \boldsymbol{e} \xleftarrow{\$} \mathcal{S}_{\boldsymbol{r}}^{\boldsymbol{n}}\right]\right|.$$

As hardness assumptions [39], [42] of the ideal versions of the RSD problem,

- The IBRSD problem is as hard as the BRSD problem and there is no known significant improvement on the complexity of solving the ideal version, typically choosing a $P(X)$ with many small factors to resist the folding attack [56] and in our case, $P(X)$ is set as an irreducible polynomial;
- The attacks on the decisional IBRSD problem remain the direct attacks on the computational IBRSD problem, thus decisional and computational versions have an equivalent complexity.

Appendix F
Rank Support Learning Problem

The Rank Support Learning (RSL) problem consists of N distinct RSD instances whose errors share the same support. The RSL problem is related to homogeneous matrices. We extend the support and weight definitions of vectors to matrices, and recall homogenous matrices.

Definition 24 (Homogeneous Matrix) *A matrix $\boldsymbol{E} \in \mathbb{F}_{q^m}^{n\times N}$ is a homogeneous matrix if its entries span an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ of dimension r, i.e., $\mathsf{dim}(\mathrm{Supp}(\boldsymbol{E})) = \|\boldsymbol{E}\|_{\mathrm{R}} = r$.*

We denote the set of such homogeneous matrices by $\mathcal{S}_r^{n\times N}$:

$$\mathcal{S}_r^{n\times N} = \left\{\boldsymbol{E} \in \mathbb{F}_{q^m}^{n\times N} \ : \ \mathsf{dim}(\mathrm{Supp}(\boldsymbol{E})) = \|\boldsymbol{E}\|_{\mathrm{R}} = r\right\}.$$

We present the equivalent variant of the RSL problem, in which we require that one recover the whole homogeneous matrix, instead of its support.

Definition 25 (RSL Problem) *Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity-check matrix of a random $[n, k]_{q^m}$-linear code and $\boldsymbol{S} \in \mathbb{F}_{q^m}^{(n-k)\times N}$. The* RSL *problem is to find a matrix $\boldsymbol{E} \in \mathcal{S}_r^{n\times N}$ such that $\boldsymbol{H}\boldsymbol{E} = \boldsymbol{S}$.*

We denote the RSL problem by $\mathsf{RSL}_{q,m,n,k,r,N}$.

Definition 26 (Decisional RSL (DRSL) Problem) *Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity-check matrix of a random $[n, k]_{q^m}$-linear code. The decisional* RSL *problem is hard, if for any PPT adversary $\mathcal{B}$, the following advantage is negligible:*

$$\mathsf{Adv}_{\mathcal{B}}^{\mathsf{DRSL}_{q,m,n,k,r,N}}(\lambda) := \left|\Pr\left[\mathcal{B}(\boldsymbol{H}, \boldsymbol{S}) = 1 \ : \ \boldsymbol{S} \xleftarrow{\$} \mathbb{F}_{q^m}^{(n-k)\times N}\right] - \Pr\left[\mathcal{B}(\boldsymbol{H}, \boldsymbol{H}\boldsymbol{E}) = 1 \ : \ \boldsymbol{E} \xleftarrow{\$} \mathcal{S}_r^{n\times N}\right]\right|.$$

The hardness of the RSL and DRSL problems is analyzed in [6], [11], [52], [60]:

- In [11], the authors introduced the RSL problem and analyzed firstly its complexity of the combinatorial attack by adapting the AGHT attack. When $N \geq nr$, the RSL problem can be solved in polynomial time. For the case $1 < N < nr$, the authors reduced the RSL problem to the problem finding a codeword of weight r in a code of same length and dimension containing q^N words of the weight r, and conjectured that the complexity is reduced by at most a factor q^N compared to the case $N = 1$. The complexity gain in fact is lower due to the deep correlation of codewords. Moreover, the authors showed that the attacks on the decisional DRSL problem remain the direct attacks on the computational RSL problem, and the decisional and computational versions have equivalent hardness.
- In [52], the authors showed that the condition $N \leq kr$ should be satisfied in order to avoid subexponential time attack.
- In [60], the authors introduced the algebraic attacks on the RSL problem by adapting the MM modeling. In [6], the authors further clarified the algebraic attacks proposed in [60] and showed that the attacks are valid only when $N > n - k - r$. Moreover, the work [6] decreased the threshold where the RSL problem starts to be solvable in polynomial time and showed that when $N > kr$, the RSL problem actually leads to a polynomial time attack by the proposed new combinatorial attack.

Overall, the RSL problem is as almost hard as the RSD problem for a small number of syndromes N, typically $N < kr$ and $N < n - k - r$.

REFERENCES

[1] NIST, "Status report on the third round of the NIST post-quantum cryptography standardization process." NIST, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8413, 2022. [Online]. Available: https://doi.org/10.6028/NIST.IR.8413-upd1 4

[2] ——, "Status report on the second round of the NIST post-quantum cryptography standardization process." NIST, Gaithersburg, MD, USA, Tech. Rep. NIST IR 8309, 2020. [Online]. Available: https://doi.org/10.6028/NIST.IR.8309 4

[3] Y. Song, J. Zhang, X. Huang, and W. Wu, "Blockwise rank decoding problem and LRPC codes: Cryptosystems with smaller sizes," in *Advances in Cryptology - ASIACRYPT*, vol. 14444. Springer, 2023, pp. 284–316. 4, 5, 6, 8, 9, 14, 15, 28, 29, 34, 35, 37

[4] N. Aragon, V. Dyseryn, P. Gaborit, P. Loidreau, J. Renner, and A. Wachter-Zeh, "LowMS: a new rank metric code-based KEM without ideal structure," *Designs, Codes and Cryptography*, vol. 92, no. 4, pp. 1075–1093. 4, 5, 6, 8, 27, 42

[5] N. Aragon, P. Briaud, V. Dyseryn, P. Gaborit, and A. Vinçotte, "The blockwise rank syndrome learning problem and its applications to cryptography," in *Post-Quantum Cryptography (PQCrypto)*, vol. 14771. Springer, 2024, pp. 75–106. 4, 5, 6, 8, 10, 14, 15, 28, 29, 37, 38

[6] L. Bidoux, P. Briaud, M. Bros, and P. Gaborit, "RQC revisited and more cryptanalysis for rank-based cryptography," *IEEE Transactions on Information Theory*, vol. 70, no. 3, pp. 2271–2286, 2024. 4, 5, 6, 8, 9, 10, 38, 41, 49, 50

[7] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory*, vol. 25, no. 3, pp. 226–241, 1978. 4

[8] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy peredachi informatsii*, vol. 21, no. 1, pp. 3–16, 1985. 4, 5

[9] N. Aragon, P. Gaborit, A. Hauteville, O. Ruatta, and G. Zémor, "Low rank parity check codes: New decoding algorithms and applications to cryptography," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 7697–7717, 2019. 4, 5, 49

[10] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *The Workshop on Coding and Cryptography (WCC)*. [Online]. Available: http://www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf 4

[11] P. Gaborit, A. Hauteville, D. H. Phan, and J. Tillich, "Identity-based encryption from codes with rank metric," in *Advances in Cryptology - CRYPTO*, vol. 10403. Springer, 2017, pp. 194–224. 4, 11, 41, 42, 49, 50

[12] T. P. Berger and A. Ourivski, "Construction of new MDS codes from Gabidulin codes," in *Proceedings of ACCT*, 2009, pp. 40–47. 4, 9, 17

[13] D. Augot, P. Loidreau, and G. Robert, "Generalized Gabidulin codes over fields of any characteristic," *Designs, Codes and Cryptography*, vol. 86, no. 8, pp. 1807–1848, 2018. 4, 7, 9, 10, 18, 19, 24, 25

[14] P. Loidreau, "Decoding rank errors beyond the error-correcting capability," in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, 2006, pp. 168–190. 4, 6, 7, 8, 9, 10, 19, 27

[15] V. Sidorenko, L. Jiang, and M. Bossert, "Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 621–632, 2011. 4, 6, 8, 9, 27

[16] O. Ore, "On a special class of polynomials," *Transactions of the American Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933. 4, 12

[17] P. Loidreau, "A Welch-Berlekamp like algorithm for decoding Gabidulin codes," in *International Workshop on Coding and Cryptography (WCC)*, vol. 3969. Springer, 2005, pp. 36–45. 4, 7, 9, 10, 18, 19, 23, 24

[18] A. Wachter, V. Sidorenko, and M. Bossert, "A fast linearized Euclidean algorithm for decoding Gabidulin codes," in *Proceedings of ACCT*, 2010, pp. 298–303. 4, 9, 42

[19] A. Wachter-Zeh, V. B. Afanassiev, and V. Sidorenko, "Fast decoding of Gabidulin codes," *Designs, Codes and Cryptography*, vol. 66, no. 1-3, pp. 57–73, 2013. 4, 9, 42

[20] P. Gaborit and G. Zémor, "On the hardness of the decoding and the minimum distance problems for rank codes," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7245–7252, 2016. 5, 13

[21] J. Faugère, F. Levy-dit-Vehel, and L. Perret, "Cryptanalysis of MinRank," in *Advances in Cryptology - CRYPTO*, vol. 5157. Springer, 2008, pp. 280–296. 5, 13

[22] C. A. Melchor, N. Aragon, S. Bettaieb, and et al., "RQC," Second round submission to the NIST post-quantum cryptography call, 2020. [Online]. Available: http://pqc-rqc.org/ 5, 6, 8, 9, 39, 41, 49

[23] Y. Song, J. Zhang, X. Huang, and W. Wu, "Blockwise rank decoding problem and LRPC codes: Cryptosystems with smaller sizes," *IEEE Transactions on Information Theory*, vol. 71, no. 6, pp. 4806–4838, 2025. 5, 6, 8, 9, 13, 14, 15, 28, 29, 35, 37, 38

[24] E. Byrne, H. Gluesing-Luerssen, and A. Ravagnani, "Fundamental properties of sum-rank-metric codes," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6456–6475, 2021. 5

[25] S. Puchinger, J. Renner, and J. Rosenkilde, "Generic decoding in the sum-rank metric," *IEEE Transactions on Information Theory*, vol. 68, no. 8, pp. 5075–5097, 2022. 5

[26] T. Jerkovits, H. Bartz, and A. Wachter-Zeh, "Support-guessing decoding algorithms in the sum-rank metric," *arXiv preprint*, 2024. [Online]. Available: https://arxiv.org/abs/2410.15806 5

[27] F. Chabaud and J. Stern, "The cryptographic security of the syndrome decoding problem for rank distance codes," in *Advances in Cryptology - ASIACRYPT*, vol. 1163. Springer, 1996, pp. 368–381. 5, 14

[28] A. V. Ourivski and T. Johansson, "New technique for decoding codes in the rank metric and its cryptography applications," *Problems of Information Transmission*, vol. 38, no. 3, pp. 237–246, 2002. 5, 6, 14

[29] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the rank syndrome decoding problem," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 1006–1019, 2016. 5, 6, 14

[30] N. Aragon, P. Gaborit, A. Hauteville, and J. Tillich, "A new algorithm for solving the rank syndrome decoding problem," in *International Symposium on Information Theory (ISIT)*. IEEE, 2018, pp. 2421–2425. 5, 6, 14

[31] M. Bardet, P. Briaud, M. Bros, P. Gaborit, V. Neiger, O. Ruatta, and J. Tillich, "An algebraic attack on rank metric code-based cryptosystems," in *Advances in Cryptology - EUROCRYPT*, vol. 12107. Springer, 2020, pp. 64–93. 5, 6, 14, 28

[32] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J. Tillich, and J. A. Verbel, "Improvements of algebraic attacks for solving the rank decoding and MinRank problems," in *Advances in Cryptology - ASIACRYPT*, vol. 12491. Springer, 2020, pp. 507–536. 5, 6, 14, 28, 34, 41

[33] M. Bardet, P. Briaud, M. Bros, P. Gaborit, and J. Tillich, "Revisiting algebraic attacks on MinRank and on the rank decoding problem," *Designs, Codes and Cryptography*, vol. 91, no. 11, pp. 3671–3707, 2023. 5, 6, 14

[34] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a non-commutative ring and their applications in cryptology," in *Advances in Cryptology - EUROCRYPT*, vol. 547. Springer, 1991, pp. 482–489. 5

[35] R. Overbeck, "Structural attacks for public key cryptosystems based on Gabidulin codes," *Journal of Cryptology*, vol. 21, no. 2, pp. 280–301, 2008. 5

[36] P. Loidreau, "A new rank metric codes based encryption scheme," in *Post-Quantum Cryptography (PQCrypto)*, vol. 10346. Springer, 2017, pp. 3–17. 5

[37] D. Coggia and A. Couvreur, "On the security of a Loidreau rank metric code based encryption scheme," *Designs, Codes and Cryptography*, vol. 88, no. 9, pp. 1941–1957, 2020. 5

[38] A. Ghatak, "Extending Coggia-Couvreur attack on Loidreau's rank-metric cryptosystem," *Designs, Codes and Cryptography*, vol. 90, no. 1, pp. 215–238, 2022. 5

[39] C. A. Melchor, N. Aragon, M. Bardet, and et al., "ROLLO," Second round submission to the NIST post-quantum cryptography call, 2020. [Online]. Available: https://pqc-rollo.org/ 5, 49

[40] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Third International Symposium on Algorithmic Number Theory (ANTS-III)*, vol. 1423. Springer, 1998, pp. 267–288. 5

[41] R. Misoczki, J. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2013, pp. 2069–2073. 5

[42] N. Aragon, O. Blazy, J. Deneuville, P. Gaborit, and G. Zémor, "Ouroboros: An efficient and provably secure KEM family," *IEEE Transactions on Information Theory*, vol. 68, no. 9, pp. 6233–6244, 2022. 5, 8, 49

[43] C. A. Melchor, N. Aragon, V. Dyseryn, P. Gaborit, and G. Zémor, "LRPC codes with multiple syndromes: Near ideal-size KEMs without ideals," in *Post-Quantum Cryptography (PQCrypto)*, vol. 13512. Springer, 2022, pp. 45–68. 5

[44] M. Alekhnovich, "More on average case vs approximation complexity," in *Proceedings of the 44th Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 2003, pp. 298–307. 5

[45] C. A. Melchor, O. Blazy, J. Deneuville, P. Gaborit, and G. Zémor, "Efficient encryption from random quasi-cyclic codes," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3927–3943, 2018. 6

[46] A. Wachter-Zeh and A. Zeh, "List and unique error-erasure decoding of interleaved Gabidulin codes with interpolation techniques," *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 547–570, 2014. 6, 8, 27

[47] E. Alkim, J. W. Bos, L. Ducas, and et al., "FrodoKEM: Learning with errors key encapsulation - preliminary standardization proposal," 2024. [Online]. Available: https://frodokem.org/ 7, 9, 38

[48] A. Wang, Z. Zheng, C. Zhao, Z. Qiu, G. Zeng, Y. Yuan, C. Mu, and X. Wang, "Scloud$^+$: An efficient LWE-based KEM without ring/module structure," in *the 9th International Conference on Security Standardisation Research (SSR)*, vol. 15559. Springer, 2024, pp. 147–174. 7, 9, 38

[49] N. Aragon, A. Couvreur, V. Dyseryn, P. Gaborit, and A. Vinçotte, "MinRank Gabidulin encryption scheme on matrix codes," in *Advances in Cryptology - ASIACRYPT*, vol. 15487. Springer, 2024, pp. 68–100. 10, 42

[50] N. Aragon, P. Briaud, V. Dyseryn, P. Gaborit, and A. Vinotte, "The blockwise rank syndrome learning problem and its applications to cryptography," Cryptology ePrint Archive, Paper 2023/1875, 2023. [Online]. Available: https://eprint.iacr.org/2023/1875 10

[51] P. Loidreau, "Asymptotic behaviour of codes in rank metric over finite fields," *Designs, Codes and Cryptography.*, vol. 71, no. 1, pp. 105–118, 2014. 11, 12

[52] T. Debris-Alazard and J. Tillich, "Two attacks on rank metric code-based schemes: RankSign and an IBE Scheme," in *Advances in Cryptology - ASIACRYPT*, vol. 11272. Springer, 2018, pp. 62–92. 12, 49, 50

[53] J. F. Buss, G. S. Frandsen, and J. O. Shallit, "The computational complexity of some problems of linear algebra," *Journal of Computer and System Sciences*, vol. 58, no. 3, pp. 572–596, 1999. 13

[54] P. Gemmell and M. Sudan, "Highly resilient correctors for polynomials," *Information Processing Letters*, vol. 43, no. 4, pp. 169–174, 1992. 24

[55] A. Couvreur and M. Bombar, "Right-hand side decoding of Gabidulin codes and applications," in *International Workshop on Coding and Cryptography (WCC)*, 2022. 27

[56] A. Hauteville and J. Tillich, "New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem," in *IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 2747–2751. 40, 49

[57] D. Silva, F. R. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, 2008. 42

[58] A. Hauteville, "Décodage en métrique rang et attaques sur un système de chiffrement à base de codes LRPC," Master's thesis, University of Limoges, September, 2014. 42

[59] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, 2011. 42

[60] M. Bardet and P. Briaud, "An algebraic approach to the rank support learning problem," in *Post-Quantum Cryptography (PQCrypto)*, vol. 12841. Springer, 2021, pp. 442–462. 49, 50

Yongcheng Song received the Ph.D. degree in College of Mathematics and Informatics, Fujian Normal University, China, in 2020. He is currently a lecturer with the College of Cyber Security, Jinan University, Guangzhou, China. His research interests mainly include post-quantum cryptography, public key cryptography,

code-based cryptography, and coding theory.

Rongmao Chen received the PhD degree in computer science from the University of Wollongong, Australia. He is now an associate professor with the College of Computer Science and Technology, National University of Defense Technology in China. His major research interests include applied cryptography and cybersecurity. He has published more than 50 research papers in refereed international conferences and journals, such as CRYPTO, ASIACRYPT, PKC, and CT-RSA. He has served as the program committee member on various international conferences such as ASIACRYPT, ACMCCS, and PKC. He received the prestigious Young Elite Scientists Sponsorship by CAST (2017), Rising Star Award by ACM SIGSAC CHINA(2020), and Distinguished Young Scholars by National Natural Science Foundation of China (2021).

Fangguo Zhang received his Ph.D. from the School of Communication Engineering, Xidian University in 2001. He is currently a Professor at the School of Computer Science and Engineering of Sun Yat-sen University, China. He is the co-director of Guangdong Province Key Laboratory of Information Security Technology. His research mainly focuses on cryptography and its applications. Specific interests are elliptic curve cryptography, secure obfuscation, blockchain, anonymity and privacy, etc.

Xinyi Huang received the PhD degree from the School of Computer Science and Software Engineer-ing, University of Wollongong, Australia. He is cur-rently a professor with the College of Cyber Security, Jinan University, China. He has authored more than 100 research papers in refereed international confer-ences and journals. His work has been cited more than 13000 times at Google Scholar (H-index: 59). His research interests include applied cryptography and network security.

Jian Weng (Senior Member, IEEE) received the BS and MS degrees in computer science and engineering from the South China University of Technology, Guangzhou, China, in 2000 and 2004, respectively, and the PhD degree in computer science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2008. From 2008 to 2010, he held a postdoctoral position with the School of Information Systems, Singapore Management University. He is currently a professor with the College of Cyber Security, Jinan University, Guangzhou, China. He has authored or coauthored more than 100 papers in cryptography and security conferences and journals, such as CRYPTO, EUROCRYPT, ASIACRYPT, TCC, PKC, TPAMI, TIFS, and TDSC. His research interests include public key cryptography, cloud security, and blockchain. He was the PC co-chairs or PC member for more than 30 international conferences.

Huaxiong Wang received the Ph.D. degree in mathematics from the University of Haifa, Israel, in 1996, and the Ph.D. degree in computer science from the University of Wollongong, Australia, in 2001. Since 2006, he has been with Nanyang Technological University (NTU), Singapore, where he is currently a Professor with the Division of Mathematical Sciences. He is also the Co-Director of the National Centre for Research in Digital Trust and the Deputy Director of the Strategic Centre for Research in Privacy-Preserving Technologies and Systems, NTU. Prior to NTU, he was a Faculty Member with Macquarie University and the University of Wollongong, Australia. He was also a Visiting Researcher with ENS de Lyon, France, City University of Hong Kong, the National University of Singapore, and Kobe University, Japan. His research interests include cryptography and cybersecurity. He was the Program Co-Chair of Asiacrypt 2020 and 2021.