Algebraic Study of Some Recent Asymmetric Cryptosystems

Dissertation

zur

Erlangung der naturwissenschaftlichen Doktorwürde
(Dr.sc.nat)

vorgelegt der

Mathematisch-naturwissenschaftlichen Fakultät

der

Universität Zürich

von

Khathuria Karan

aus

Indien

Promotionskommission

Prof. Dr. Joachim Rosenthal (Vorsitz)
Prof. Dr. Andrew Kresch
Prof. Dr. Elisa Gorla

Zürich, 2020

Abstract

In this dissertation, we apply various algebraic techniques to: develop some code-based cryptosystems; break some noncommutative cryptographic protocols; and theoretically analyze some multivariate cryptosystems.

Code-based encryption schemes, such as the McEliece cryptosystem, face a problem of having large key sizes. In the first part of the thesis, we propose new cryptosystems that aim to reduce the key sizes. We present two new variants of the McEliece cryptosystem: the first one is based on using shortened expanded Reed–Solomon codes, and the second one is based on using Reed-Solomon codes masked by constant row weight two matrix. Both the proposed cryptosystems show remarkable improvements on the key sizes and at the same time counter all the existing algebraic attacks.

In the second part, we cryptanalyze the protocols based on the noncommutative ring of matrices $E_p^{(m)}$. In particular, we study the intrinsic $\mathbb{Z}/p^m\mathbb{Z}$-module structure of the ring $E_p^{(m)}$. Using this intrinsic structure, solving a linear system over $E_p^{(m)}$ becomes computationally equivalent to solving a linear system over $\mathbb{Z}/p^m\mathbb{Z}$. As an application, we efficiently break all the cryptographic protocols based on the semigroup action problem and the Diffie–Hellman decomposition problem over $E_p^{(m)}$.

Currently, most of the multivariate schemes are based on systems of quadratic polynomials, mainly because they are smaller compared to higher degree constructions and hence more efficient. In quadratic constructions, one of the most successful family of attacks is the MinRank attack. It exploits the existence of a low-rank linear combination of the matrices representing the quadratic forms of the public polynomials. A natural way to avoid this attack is to use cubic polynomials. This leads to several questions: Is there a notion of rank for cubic forms? Can we extend the MinRank attack to cubic constructions? What are the implications of low-rank cubic constructions? In the last part of the thesis, we address all these questions by taking a general perspective of cubic multivariate schemes.

Acknowledgements

First, I would like to thank my supervisor, Prof. Dr. Joachim Rosenthal, for giving me the opportunity to pursue the doctoral degree. I would also like to thank him for his support and encouragement throughout the entire period of my studies.

I would like to show my gratitude to my Ph.D. committee, including Prof. Dr. Elisa Gorla and Prof. Dr. Andrew Kresch. I am also grateful to the anonymous referees that have read my thesis and provided valuable comments and suggestions.

The list of people that I would like to thank is very long, and there are not enough words that can express my gratitude towards them.

Starting with my office mates, Alessandro, Gianira, Julia, Octopussy, Raul, Simran, and Violetta, who tolerated me for more than three years. Thank you, Alessandro for the most valuable research discussions I had during my Ph.D., I always learned something from each of those discussions. Thank you, Gianira for always being kind and for all the wonderful time we had right from the morning coffees to teaching together to all the brainstorming sessions. Thank you, Violetta, my academic twin, for always showing me a better path through your optimism, for always backing me in every situation and for all the work we did (and going to do) together.

I am truly grateful to have worked with some of the great researchers: Daniel C., Daniel E., Giacomo, Gianira, Javier, Joachim, John, Paolo and Violetta. I would especially like to thank all my Colombian collaborators, Daniel C., Daniel E., Javier and John, for inviting me to Colombia for the research visit, which will always remain a special highlight of my Ph.D.

I am also very grateful to all the secretaries and the IT team of the math department. Thanks to them, I never had to worry about any bureaucratic or IT troubles and could focus on my research properly.

My heartfelt thanks to all my friends from all around the world. For all the memorable time and wonderful evenings that I had in Zurich, I would like to thank all my friends in Zurich: Alessandro, Andrés, Benedetta, Céline, Davide, Genta,

Gian, Gianira, Jacopo, Julia, Krishna, Nicola, Ödül, Petra, Raul, Saskia, Severin, Simon, Simone, Simran, Violetta and many more. A special thanks to some of my true and closest friends Anurag, Balwant, Chaitanya, Saket, Somendu, Tinku and Vishal.

Finally and most importantly, I would like to thank my family: my grandparents; my parents; and my sister (also my best friend) Sneh. Words are not enough to thank them for everything they have done for me, therefore I dedicate this thesis to them.

Contents

Chapter 1

Introduction

In the modern era, *cryptography* refers to the study of techniques for secure communication, identity authentication, data confidentiality, digital signatures, interactive proofs, secure computation, etc. In this thesis we focus on the most common form of modern cryptography that concerns with secure communication between two parties assuming the presence of third parties called adversaries.

A general protocol for secure communication involves two steps: encryption and decryption. During *encryption* the secret message, called *plaintext*, is transformed into an incomprehensible form, called *ciphertext*. On the other hand, *decryption* is the process of converting the ciphertext back to the original plaintext. Both the encryption and decryption processes are operated by using a *key*. The protocols for secure communication can be divided into two categories: symmetric and asymmetric. *Symmetric cryptosystems* use the same secret key for encrypting and decrypting a message. Whereas, in *asymmetric cryptosystems* (or *public-key cryptosystems*) a message is encrypted using a publicly known key and it is decrypted using a private key.

Symmetric cryptosystems are widely used for secure communication, mainly because of their efficiency and enhanced security. The famous AES (Advanced Encryption Standard) is an example of a symmetric cryptosystem. One main disadvantage of symmetric algorithms is that it requires both the parties to have the same secret key. Before the arrival of asymmetric cryptosystems in 1976, the shared secret key was communicated via a physically secure channel. However, physically communicatig the secret key is not always possible. Moreover, the key management becomes a nightmare if many parties are involved in the communication. In 1976, Diffie and Hellman [56] proposed the notion of public-key cryptography, by presenting the Diffie–Hellman key exchange protocol, which is now widely used to securely

communicate the shared secret key.

The Diffie–Hellman key exchange protocol showed that public-key cryptography is indeed possible. As a consequence, in 1978, Rivest, Shamir and Adleman [140] developed one of the first public-key cryptosystems, commonly known as RSA cryptosystem. Other notable public-key cryptosystems include the ElGamal cryptosystem [61], Cramer–Shoup cryptosystem [53], elliptic curve based cryptosystems [99, 121].

Besides secure communication and key exchange, public-key cryptography has been applied for many other purposes. For example:

- *Digital signatures*: to verify the authenticity of digital documents.
- *Identification systems*: that allows one party to prove its identity to another party.
- *Non-repudiation systems*: assures that someone cannot deny having performed a particular action.
- *Digital currencies*: which insures anonymity of the users.
- *Electronic voting*: to ensure confidentiality and correctness of votes.

The security of public-key cryptosystems is often based on the computational complexity of hard problems arising from different fields of mathematics. For example, the security of RSA is connected to the problem of factoring large integers, Diffie–Hellman and ElGamal are connected to the discrete logarithm problem over the underlying group, and elliptic curve cryptography (ECC) is connected to elliptic curve discrete logarithm problem.

The research field of cryptography took a sharp turn in 1994 when Shor [147] presented a polynomial-time algorithm for factoring integers on a hypothetical quantum computer. Shor's algorithm can be trivially generalized for the discrete logarithm problem over an arbitrary finite cyclic group. Moreover, the algorithm was later extended to solve also the elliptic curve discrete logarithm problem. This means that the commonly used public-key cryptosystems such as RSA, Diffie–Hellman and ECC can efficiently be broken, assuming a sufficiently large quantum computer is built. As a consequence, the cryptographers have shifted their focus on designing quantum secure cryptographic primitives, the area is more commonly known as *post-quantum cryptography*. The threat of quantum computers are mostly towards

public-key protocols, as symmetric cryptosystems are considered to be relatively safe against quantum attacks.

Over the past ten years, significant efforts have been put in developing post-quantum public-key protocols. Consequently, in December 2016, National Institute of Standards and Technology (NIST) initiated the ongoing process of standardization of quantum-resistant public-key cryptographic algorithms. The standardization process is currently in its second phase, which involves 17 candidates for public-key encryption schemes and 9 candidates for digital signature schemes. All these candidates can be categorized into five categories, where category relies on the computational complexity of distinct hard problems:

- *Code-based cryptography*: relies on the hardness of decoding a random linear code.
  - Protocols from NIST standardization process: classical McEliece cryptosystem [30], BIKE (Bit flipping key encapsulation) [7], ROLLO [116] (Rank-Ouruboros, LAKE and LOCKER), RQC [1] (Rank quasi-cyclic), HQC [1] (Hamming quasi-cyclic), LEDAcrypt [14] and NTS-KEM [3].
  - Advantages: classical McEliece scheme resisted cryptanalysis since 1978; fast encryption and decryption.
  - Disadvantages: large key sizes (but significant improvements have been made in the last decade); no secure signature schemes.
- *Hash-based cryptography*: relies on the security of the underlying hash functions.
  - Protocols from NIST standardization process: SPHINCS$^+$ [29] signature scheme.
  - Advantages: security is well understood, very efficient.
  - Disadvantages: only signature schemes; large signatures.
- *Lattice-based cryptography*: relies on certain computationally hard lattice problems, such as finding a short vector in a lattice of high dimension.
  - Protocols from NIST standardization process: FrodoKEM [37], NTRU [83], NTRU Prime [28], NewHope [5], Round5 [12] based on the general learning with rounding (GLWR) problem, SABER based on learning with rounding (LWR) problem, ThreeBears [78] based on module learning with error

(MLWE) problem, CRYSTALS-Kyber [11] based on MLWE problem, FALCON [71] (fast-Fourier lattice-based compact signatures over NTRU) and qTESLA [35] signature scheme.

- Advantages: various applications: encryption, digital signatures, key exchange, fully homomorphic encryption; many schemes are proven secure under worst-case hardness assumptions.
- Disadvantages: the overall security provided by shortest vector problems is not completely understood, as some theoretical attacks have significantly weakened the security.

- *Multivariate cryptography*: relies on the difficulty of solving a system of multivariate polynomial equations.
  - Protocols from NIST standardization process: GeMSS [41] (Great multivariate short signature) scheme, LUOV [34] (Lifted Unbalanced oil and vinegar) signature scheme, Rainbow [59, 137] signature scheme, and MQDSS [43] signature scheme.
  - Advantages: short signatures; very efficient.
  - Disadvantages: large key sizes; no secure encryption schemes.

- *Super-singular elliptic curve isogeny-based cryptography*: relies on the problem of finding the isogeny map between two super-singular elliptic curves.
  - Protocols from NIST standardization process: SIKE [89] (supersingular isogeny key encapsulation); based on SIDH [54] (super-singular isogeny Diffie–Hellman) key exchange,
  - Advantages: SIDH provides perfect forward secrecy; small key sizes.
  - Disadvantages: relatively slow speed.

1.1 Overview of the Thesis

This thesis covers three different areas of cryptography, namely code-based cryptography, noncommutative cryptography and multivariate cryptography. Each of these areas can be seen as an application of distinct algebraic structures to cryptography. Code-based cryptography can be viewed as application of linear algebra, as the primary object involved here is a linear code over a finite field $\mathbb{F}_q$, which

are linear subspaces of $\mathbb{F}_q^n$. Noncommutative cryptography, as the name suggests, is based on the noncommutative algebraic structures such as semigroups, groups and rings. Multivariate cryptography involves, as the main object, a system of non-linear polynomials in multiple variables.

Code-Based Cryptography

Code-based cryptography dates back to 1978 when McEliece [114] presented an encryption scheme based on the hardness of decoding a linear error-correcting code.

A generic design of a code-based asymmetric encryption scheme uses linear codes for public and private keys. The private key is a linear code having a specific structure that is endowed with efficient decoding capabilities. The corresponding public key is a disguised form of the private code, so that the public code behaves like a random linear code. The encryption is done by first encoding the plaintext into a codeword of the public code and then adding to it certain amount of errors. During the decryption these errors are removed using the decoding capability of the private code, and the plaintext is recovered.

While the public-key encryption scheme is the most common form of code-based cryptography, other primitives of code-based cryptography include: signature and identification schemes [48, 8, 55], random number generators [70, 72], cryptographic hash functions [10].

In Chapter 2, we present two new code-based encryption schemes. The schemes are two distinct variants of the McEliece cryptosystem based on two distinct ways of hiding the structure of Reed–Solomon (RS) codes. In the past many cryptographers have proposed to use RS codes in the McEliece's setting, but most of them failed to hide the underlying algebraic structure of RS codes. In the two proposed cryptosystems, we show that the new approaches of hiding the structure of RS codes are immune against all the existing algebraic attacks. Moreover, we obtain much lower key sizes compared to the original McEliece scheme.

Noncommutative Cryptography

Noncommutative cryptography is a broad field of research that aims to develop new cryptosystems and key exchange protocols based on noncommutative algebraic structures.

Most of the attempts in developing noncommutative cryptographic primitives can be seen as a generalization of the Diffie–Hellman key exchange and the ElGamal protocol that are based on the following underlying problems:

- *Conjugacy search problem*: Given two elements x, y in a group G, find an element $z \in G$ such that $x = z^{-1}yz$.
- *Decomposition problem*: Given two elements x, y in a semigroup G, find $z_1, z_2 \in G$ such that $x = z_1 y z_2$.
- *Semi-group action problem*: Let G be a finite semigroup acting on a set S. Given $a, b \in S$ such that $b = x \cdot a$ for some $x \in G$, find $x' \in G$ such that $b = x' \cdot a$.

Some examples of nonabelian groups which are considered: braid groups [6, 97, 96], matrix groups [157], Thompson's group [148], Solvable groups [149].

Chapter 3 is devoted to the cryptanalysis of certain cryptographic schemes based on the semigroup action problem and the decomposition problem. In [47], Climent and López-Ramos proposed three protocols using a special noncommutative ring of matrices, called $E_p^{(m)}$. We present an algebraic technique to break all three protocols in polynomial-time.

Multivariate Cryptography

Multivariate cryptography is the study of public-key cryptosystems based on the difficulty of solving a system of multivariate polynomials over a finite field.

A generic design of a multivariate public-key scheme uses systems of multivariate polynomials for public and private keys. The private key is a system of polynomials that is easy to invert. The corresponding public key is obtained by disguising the private polynomials using some affine transformations. The encryption is done by simply evaluating the public polynomials in the plaintext. Whereas the decryption uses the knowledge of private polynomials to invert the ciphertext back to the plaintext.

Historically, multivariate cryptography have been more promising in developing signature schemes than encryption schemes. This is mainly because an encryption scheme requires the public key map to be injective, whereas signature schemes requires surjectivity. Some of the most famous examples of multivariate signature

schemes include: Matsumoto–Imai (MI) cryptosystem [110], Hidden Field Equations (HFE) [132], Unbalanced Oil and Vinegar (UOV) signature scheme [133, 94], Rainbow signature scheme [59].

Chapter 4 presents a foundation theory for the analysis of multivariate cryptosystems that are based on cubic polynomials. Currently, most of the multivariate schemes are constructed using quadratic polynomials, and their security is based on the multivariate quadratic problem (to solve a system of multivariate quadratic polynomials). However, by relating quadratic forms with matrices, many of the multivariate quadratic schemes have been attacked using the MinRank attack. Hence, a natural countermeasure is to use cubic polynomials. In this thesis, we extend the notion of the MinRank attack to the cubic polynomial setting. In particular, we gather appropriate literature to frame the discussion of rank of cubic forms.

Chapter 2

Code-Based Public-Key Encryption Schemes

This chapter concerns the area of code-based cryptography. It is an area of cryptology that deals with cryptographic primitives based on the hardness of decoding a random linear code. In this chapter, we will deal with code-based public-key encryption schemes.

The chapter is based on the following two papers:

- Karan Khathuria, Joachim Rosenthal, and Violetta Weger. "Weight Two Masking of the Reed-Solomon Structure in Conjugation with List Decoding". In: Proceedings of the 23rd International Symposium on Mathematical Theory of Networks and Systems – MTNS. 2018. DOI: 10.5167/uzh-168132
  This paper proposes a variant of the McEliece cryptosystem which uses, as a secret code, a Reed–Solomon code masked by a constant row weight two matrix. The cryptosystem also uses the technique of list decoding for decryption to obtain lower key sizes.

- Karan Khathuria, Joachim Rosenthal, and Violetta Weger. "Encryption Scheme Based on Expanded Reed-Solomon Codes". In: *Advances in Mathematics of Communications* (2019). ISSN: 1930-5346. DOI: 10.3934/amc.2020053
  This paper proposes a variant of the McEliece cryptosystem which uses shortened expanded Reed–Solomon codes. The cryptosystem can also be viewed as a generalization of the classical McEliece cryptosystem.

2.1 Introduction

In 1978 McEliece [114] presented the first code-based public-key cryptosystem. It belongs to the family of a very few public-key cryptosystems which are unbroken since decades. The hard problem the McEliece system relies on, is the difficulty of decoding a random (-like) linear code having no visible structure. The famous cryptosystem RSA [140] was also introduced in the same year, which is based on the difficulty of factoring integers. However, due to large key sizes the McEliece cryptosystem never gained much traction.

The motivation to study code-based cryptography is due to the advent of quantum computers. In 1994, Peter Shor [146] developed a polynomial time quantum algorithm for factoring integers and solving discrete logarithm problems. This means that most of the currently popular cryptosystems, such as RSA and ECC, will be broken in an era of quantum computers. In the ongoing process of the standardization of quantum-resistant public-key cryptographic algorithms by the National Institute of Standards and Technology (NIST) [2], code-based cryptosystems are one of the most promising candidates. At the time of this writing there are seven code-based cryptosystems included in NIST's standardization process: BIKE [7] based on quasi-cyclic MDPC codes, classic McEliece [30] based on binary Goppa codes, ROLLO [116] based on quasi-cyclic LRPC codes, RQC [1] based on rank metric quasi-cyclic codes, HQC [1] based on Hamming metric quasi-cyclic codes, LEDAcrypt [14] based on quasi-cyclic LDPC codes and NTS-KEM [3] based on binary Goppa codes.

As mentioned before, code-based cryptography relies on the hardness of decoding a random (-like) linear code. In 1978, Berlekamp, McEliece and van Tilborg [25] showed that decoding a random linear binary code is an NP-complete problem. Until today two main methods for solving this problem have been proposed: information set decoding (ISD) and the generalized birthday algorithm (GBA). The ISD is more efficient if the decoding problem has only a small number of solutions, whereas GBA is efficient when there are many solutions. In code-based cryptography, we mainly encounter the case of having a unique solution and hence ISD algorithms act as a tool to determine the parameters of the cryptosystem for a given security level.

A Brief History of Code-Based Public-Key Cryptography: McEliece originally proposed to use binary Goppa codes for the encryption scheme, which resisted

cryptanalysis so far. However, due to the low error-correcting capacity of Goppa codes, the cryptosystem results in large public key sizes. Many variants of the McEliece scheme have been proposed in order to reduce the key sizes. These variants can be divided in two categories: one is based on changing the underlying code, and the other is based on changing the metric.

Several variants have been proposed that uses alternative families of codes. The most famous family of codes considered is the Reed–Solomon codes. In 1985, Niederreiter [128] proposed an equivalent dual version of the McEliece cryptosystem and replaced the underlying code by a Reed–Solomon code. This improved the key sizes, however in 1992 Sidelnikov and Shestakov [152] provided a polynomial time key recovery attack. Since then many researchers have tried to hide the algebraic structure of Reed–Solomon codes [15, 16, 18, 23, 36, 93], but most of them were unsuccessful due to the square code based key recovery attacks [49, 52, 162]. Other families of codes that were proposed are: non-binary Goppa codes [32], algebraic geometric codes [88], LDPC and MDPC codes [17, 123], Reed-Muller codes [150] and convolutional codes [106]. Yet again the codes having algebraicc structures were mostly unsuccessful in hiding the structure of the private code [50, 51, 101, 122, 129].

The second category of McEliece variants is based on replacing the Hamming metric by other metrics, like the rank metric and the Lee metric. In the ongoing NIST's standardization there are two schemes based on rank metric codes: ROLLO [116] and RQC [1]. The schemes based on rank metric codes delivers the lowest key sizes for a given security level. However, schemes using rank metric codes have not been cryptanalyzed as rigorously as in the Hamming metric case. Recently, [84, 160, 161] presented the potential of using the Lee metric as an alternative.

Overview of the Chapter: In this chapter we present two variants of the McEliece cryptosystem by using two distinct ways of hiding the algebraic structure of Reed–Solomon codes. The proposed variants aim to improve the key sizes and at the same time counter the existing algebraic attacks. Both the methods used to hide the Reed–Solomon codes can also be applied to other algebraic codes that have been attacked using the square code technique.

- The first variant uses expanded Reed–Solomon (RS) codes. A linear $[n, k]$ code defined over an extension field $\mathbb{F}_{q^m}$ can be expanded, over the base field $\mathbb{F}_q$, to an $[mn, mk]$ linear code by expanding each codeword with respect to a

fixed $\mathbb{F}_q$-linear isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$. In the proposed cryptosystem we hide the structure of an expanded RS code by puncturing and permuting the columns of its parity check matrix and multiplying by an invertible block diagonal matrix. In order to decode a large number of non-codewords, we use a burst of errors during the encryption step, i.e., we consider error vectors having support in sub-vectors of size λ. This error pattern comes with a disadvantage: it can be used to speed up the ISD algorithms. However, for a small degree of extension m, the key sizes turn out to be remarkably competitive.

- In the second variant we use Reed–Solomon codes as secret codes and hide their structure using a matrix of constant row weight two. In addition, we use list decoding in the decryption process, in order to allow more errors and subsequently improve the key sizes. The idea of using a weight-two masking on Reed–Solomon codes was first introduced in [36], but without a thorough security analysis. In this work, we provide some theoretical and experimental evidence for the security of the cryptosystem against some known attacks.

The chapter is organized as follows. In Section 2.2, we give the preliminaries regarding coding theory and code-based cryptography. In Section 2.3, we describe and cryptanalyze the first proposed cryptosystem which is based on the shortening of an expanded generalized Reed–Solomon code. In Section 2.4, we describe and cryptanalyze the second proposed cryptosystem which is based on the weight two masking of generalized Reed–Solomon codes. Section 2.5 compares the performance of the two proposed cryptosystems with other variants of the McEliece system , including the classical McEliece scheme.

2.2 Background

2.2.1 Coding Theory

In this thesis, we deal with linear codes with particular interest in their application to cryptography.

Let $\mathbb{F}_q$ be a finite field with q elements. For the vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, the *Hamming distance* between x and y is defined to be the number of coordinates where x and y differ, i.e., $d(x, y) := |\{1 \leq i \leq n : x_i \neq y_i\}|$. The

Hamming weight of x is defined as the number of non-zero coordinates in x, i.e., $\mathrm{wt}(x) := d(x, 0)$.

The Hamming distance is a metric on $\mathbb{F}_q^n$, as one can verify easily.

Definition 2.1. Let $\mathbb{F}_q$ be a finite field with q elements. An $[n, k, d]_q$ *linear code* $\mathcal{C}$ is a k dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ having *minimum distance* d, i.e., $d := \min\{d(x, y) : x, y \in \mathcal{C} \text{ with } x \neq y\}$.

The minimum distance of a code $\mathcal{C}$ is related to the error detection and correction capability of the code $\mathcal{C}$, i.e., the number of errors that the code is able to detect and correct. In particular, an $[n, k, d]_q$ code can detect up to $d - 1$ errors and can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

A *generator matrix* of an $[n, k, d]_q$ code $\mathcal{C}$ is a $k \times n$ matrix over $\mathbb{F}_q$ whose rows span $\mathcal{C}$, i.e., $\mathcal{C} = \{xG : x \in \mathbb{F}_q^k\}$. A *parity-check matrix* of $\mathcal{C}$ is an $(n-k) \times n$ matrix over $\mathbb{F}_q$ such that $\mathcal{C}$ is the right kernel of H, i.e., $\mathcal{C} = \ker(H) = \{c \in \mathbb{F}_q^n : Hc^\intercal = 0\}$.

Definition 2.2. Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Then the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined as the code generated by the rows of a parity-check matrix H of $\mathcal{C}$.

It follows immediately from the rank-nullity theorem that $\mathcal{C}^\perp$ is an $[n, n-k]$ code, and $\left(\mathcal{C}^\perp\right)^\perp = \mathcal{C}$.

One of the important problems in coding theory is to construct codes whose dimension and minimum distance are large, for a given length and alphabet $\mathbb{F}_q$. However, the following relation between the dimension and the minimum distance imposes some restrictions.

Proposition 2.3 (Singleton bound)**.** *Let $\mathcal{C}$ be an $[n, k, d]_q$ code over $\mathbb{F}_q$. Then*

$$d \leq n - k + 1.$$

Proof. Let $\mathcal{E}$ be the linear subspace of $\mathbb{F}_q^n$ given by

$$\mathcal{E} = \{(a_1, \ldots, a_n) : a_i = 0 \text{ for all } i \geq d\}.$$

Then $\mathcal{E} \cap \mathcal{C} = \{0\}$, as $\mathrm{wt}(a) \leq d-1$ for all $a \in \mathcal{E}$. Now, since the $\dim(\mathcal{E}) = d-1$, we obtain

$$\begin{aligned} k + d - 1 &= \dim(\mathcal{C}) + \dim(\mathcal{E}) \\ &= \dim(\mathcal{C} + \mathcal{E}) \leq n. \end{aligned}$$

□

Codes that achieve the Singleton bound, i.e., satisfy $d = n - k + 1$, are called *maximum distance separable (MDS) codes.*

In the following, we introduce some important classes of codes and some coding theory concepts that will be used in this thesis.

Generalized Reed–Solomon Codes

Definition 2.4. Let $\mathbb{F}_q$ be a finite field and let $1 \leq k < n \leq q$ be integers. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ be an n-tuple of distinct elements and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_q^n$ be an n-tuple of nonzero elements, then the *generalized Reed–Solomon (GRS) code* $\mathrm{GRS}_{n,k}(\alpha, \beta)$ of dimension k is the set of vectors $(\beta_1 p(\alpha_1), \ldots, \beta_n p(\alpha_n))$, where p ranges over all polynomials of degree less than k, having coefficients in $\mathbb{F}_q$. Thus

$$\mathrm{GRS}_{n,k}(\alpha, \beta) = \left\{ (\beta_1 p(\alpha_1), \ldots, \beta_n p(\alpha_n)) \;\middle|\; p \in \mathbb{F}_q[x],\ \deg(p) < k \right\}.$$

The GRS code has the minimum distance $d = n - k + 1$, i.e., it is an MDS code. As a consequence, GRS codes can uniquely correct upto $d/2$ errors, using efficient algorithms such as the Berlekamp–Massey algorithm [26, 109].

The GRS codes have the following properties:

- $\mathrm{GRS}_{n,k}(\alpha, \beta)^{\perp} = \mathrm{GRS}_{n,n-k}(\alpha, \beta')$ for a certain $\beta' \in \mathbb{F}_q^n$.
- A generator matrix of $\mathrm{GRS}_{n,k}(\alpha, \beta)$ can be described in the following form:

$$V_k(\alpha, \beta) := \begin{pmatrix} \beta_1 & \beta_2 & \cdots & \beta_n \\ \beta_1\alpha_1 & \beta_2\alpha_2 & \cdots & \beta_n\alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1\alpha_1^{k-1} & \beta_2\alpha_2^{k-1} & \cdots & \beta_n\alpha_n^{k-1} \end{pmatrix}.$$

Alternant Codes

Definition 2.5. Let $\mathcal{C}$ be an $[n, k]$ code over $\mathbb{F}_{q^m}$. Then the *subfield subcode* $\mathcal{C}|_{\mathbb{F}_q}$ of $\mathcal{C}$ over $\mathbb{F}_q$ is a linear code over $\mathbb{F}_q$ defined as $\mathcal{C} \cap \mathbb{F}_q$.

Let H be an $(n-k) \times n$ parity-check matrix of an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_{q^m}$. Let γ be a primitive element in $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, associated with the $\mathbb{F}_q$-linear isomorphism $\phi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ given by $\sum_{i=0}^{m-1} a_i\gamma^i \mapsto (a_0, \ldots, a_{m-1})$. Then a parity-check matrix of $\mathcal{C}|_{\mathbb{F}_q}$ can be obtained by replacing each entry β of H by the column vector $\phi(\beta)^\intercal$. This also implies that $\mathcal{C}|_{\mathbb{F}_q}$ is an $[n, k', d']$ code with $k' \geq n - m(n-k)$ and $d' \geq d$.

Definition 2.6. Let $GRS_{n,k}(\alpha, \beta)$ be a GRS code over $\mathbb{F}_{q^m}$. The subfield subcode of $GRS_{n,k}(\alpha, \beta)$ over $\mathbb{F}_q$ is the *alternant code* $A_{n,k}(\alpha, \beta)$.

A subclass of alternant codes, having cryptographic importance, is the classical Goppa codes.

Definition 2.7. Let $g(x)$ be a polynomial in $\mathbb{F}_{q^m}[x]$ of degree $r \leq n$, and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$ be a tuple of n distinct elements such that $g(\alpha_i) \neq 0$ for all $i \in \{1, \ldots, n\}$. The *Goppa code* $\mathcal{G}(g, \alpha)$ with *Goppa polynomial* $g(x)$ and *support* α is the alternant code $A_{n,r}(\alpha, \beta)$, where $\beta = \big(g^{-1}(\alpha_1), \ldots, g^{-1}(\alpha_n)\big)$.

Using the bounds on the dimension and the minimum distance of subfield subcodes, we infer that the dimension of $\mathcal{G}(g, \alpha)$ is $k \geq n - mr$, and the minimum distance $d \geq r + 1$. In the special case of binary Goppa codes, i.e., $q = 2$, the minimum distance is $d \geq 2r + 1$.

Expanded Codes

Let q be a prime power and let m be an integer. Let γ be a primitive element of the field $\mathbb{F}_{q^m}$, i.e., $\mathbb{F}_{q^m} \cong \mathbb{F}_q(\gamma)$. The field $\mathbb{F}_{q^m}$ can also be seen as an $\mathbb{F}_q$-vector space of dimension m via the following $\mathbb{F}_q$-linear isomorphism

$$\begin{aligned} \phi : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q^m, \\ a_0 + a_1\gamma + \cdots + a_{m-1}\gamma^{m-1} &\longmapsto (a_0, a_1, \ldots, a_{m-1}). \end{aligned}$$

We extend this isomorphism for vectors over $\mathbb{F}_{q^m}$ in the following way:

$$\begin{aligned}\phi_n : \mathbb{F}_{q^m}^n &\longrightarrow \mathbb{F}_q^{mn},\\ (\alpha_1, \alpha_2, \ldots, \alpha_n) &\longmapsto (\phi(\alpha_1), \phi(\alpha_2), \ldots, \phi(\alpha_n)).\end{aligned}$$

This is clearly an $\mathbb{F}_q$-linear isomorphism. Hence this gives us a way to obtain a linear code over $\mathbb{F}_q$ from a linear code over $\mathbb{F}_{q^m}$.

Definition 2.8. Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_{q^m}$. The *expanded code* of $\mathcal{C}$ with respect to a primitive element $\gamma \in \mathbb{F}_{q^m}$ is a linear code over the base field $\mathbb{F}_q$ defined as

$$\widehat{\mathcal{C}} := \{\phi_n(c) : c \in \mathcal{C}\},$$

where ϕ_n is the $\mathbb{F}_q$-linear isomorphism defined by γ as above.

Remark 2.9. It is easy to see that the expanded code $\widehat{\mathcal{C}}$ is a linear code of length mn and dimension mk, because ϕ_n is an $\mathbb{F}_q$-linear isomorphism and $|\widehat{\mathcal{C}}| = |\mathcal{C}| = (q^m)^k = q^{mk}$.

Given a code $\mathcal{C}$ with its generator matrix and parity-check matrix, the following lemma gives a way to construct a generator matrix and a parity-check matrix of the expanded code $\widehat{\mathcal{C}}$.

Lemma 2.10. *Let $\mathcal{C}$ be a linear code in $\mathbb{F}_{q^m}^n$.*

1. *Let $\mathcal{C}$ have a generator matrix $G = [g_1, g_2, \ldots, g_k]^\intercal$, where $g_1, g_2, \ldots, g_k$ are vectors in $\mathbb{F}_{q^m}^n$. Then the expanded code of $\mathcal{C}$ over $\mathbb{F}_q$ with respect to a primitive element $\gamma \in \mathbb{F}_{q^m}$ has the expanded generator matrix*

$$\begin{aligned}\widehat{G} := [\phi_n(g_1), \phi_n(\gamma g_1), \ldots, \phi_n(\gamma^{m-1} g_1), &\phi_n(g_2), \phi_n(\gamma g_2), \ldots, \phi_n(\gamma^{m-1} g_2), \ldots,\\ &\phi_n(g_k), \phi_n(\gamma g_k) \ldots, \phi_n(\gamma^{m-1} g_k)]^\intercal.\end{aligned}$$

2. *Let $\mathcal{C}$ have a parity-check matrix $H = [h_1^\intercal, h_2^\intercal, \ldots, h_n^\intercal]$, where $h_1, h_2, \ldots, h_n$ are vectors in $\mathbb{F}_{q^m}^{n-k}$. Then the expanded code of $\mathcal{C}$ over $\mathbb{F}_q$ with respect to a primitive element $\gamma \in \mathbb{F}_{q^m}$ has the expanded parity-check matrix*

$$\begin{aligned}\widehat{H} := [&\phi_{n-k}(h_1)^\intercal, \phi_{n-k}(\gamma h_1)^\intercal, \ldots, \phi_{n-k}(\gamma^{m-1} h_1)^\intercal, \phi_{n-k}(h_2)^\intercal, \phi_{n-k}(\gamma h_2)^\intercal,\\ &\ldots, \phi_{n-k}(\gamma^{m-1} h_2)^\intercal, \ldots, \phi_{n-k}(h_n)^\intercal, \phi_{n-k}(\gamma h_n)^\intercal \ldots, \phi_{n-k}(\gamma^{m-1} h_n)^\intercal].\end{aligned}$$

Proof. 1. Let $B = \{\phi_n(\gamma^i g_j) : 0 \leq i \leq m-1, 1 \leq j \leq k\}$. Then, by the definition of the expanded code $\widehat{\mathcal{C}}$, we have that $\mathrm{Span}_{\mathbb{F}_q}(B) \subseteq \widehat{\mathcal{C}}$.

Now let $\phi_n(c)$ be an arbitrary element in $\widehat{\mathcal{C}}$, for some $c \in \mathcal{C}$. Since G is a generator matrix of $\mathcal{C}$, there exists $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_{q^m}$ such that

$$c = \sum_{j=1}^{k} \lambda_j g_j.$$

Moreover, as γ is a primitive element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, for each j we can write $\lambda_j = \sum_{i=0}^{m-1} \lambda_j^{(i)} \gamma^i$ for some $\lambda_j^{(0)}, \ldots, \lambda_j^{(m-1)} \in \mathbb{F}_q$. Putting all together, we obtain

$$\begin{aligned}
\phi_n(c) &= \sum_{j=1}^{k} \phi_n\left(\lambda_j g_j\right) \\
&= \sum_{j=1}^{k} \sum_{i=0}^{m-1} \phi_n\left(\lambda_j^{(i)} \gamma^i g_j\right) \\
&= \sum_{j=1}^{k} \sum_{i=0}^{m-1} \lambda_j^{(i)} \phi_n\left(\gamma^i g_j\right) \in \mathrm{Span}_{\mathbb{F}_q}(B).
\end{aligned}$$

2. Let $h^{(\ell)} = (h_{1\ell}, h_{2\ell}, \ldots, h_{n\ell})$ be the ℓ-th row of H and $c = (c_1, c_2, \ldots, c_n)$ be a codeword in $\mathcal{C}$. Then observe that

$$\begin{aligned}
h^{(\ell)} c^{\intercal} &= \sum_{j=1}^{n} h_{j\ell} c_j \\
&= \sum_{j=1}^{n} h_{j\ell} \sum_{i=0}^{m-1} c_j^{(i)} \gamma^i \\
&= \sum_{j=1}^{n} \sum_{i=0}^{m-1} c_j^{(i)} \gamma^i h_{j\ell},
\end{aligned}$$

where $\left(c_j^{(0)}, c_j^{(1)}, \ldots, c_j^{(m-1)}\right) = \phi(c_j)$ for all $j \in \{1, \ldots, n\}$. Applying ϕ to above equation we get

$$\phi(h^{(\ell)} c^{\intercal}) = \phi\left(\sum_{j=1}^{n} \sum_{i=0}^{m-1} c_j^{(i)} \gamma^i h_{j\ell}\right) = \sum_{j=1}^{n} \sum_{i=0}^{m-1} c_j^{(i)} \phi(\gamma^i h_{j\ell}).$$

Now since $h^{(\ell)}c^\intercal = 0$, it follows that

$$\left[\phi(h_{1\ell})^\intercal, \phi(\gamma h_{1\ell})^\intercal, \ldots, \phi(\gamma^{m-1}h_{1\ell})^\intercal, \ldots, \right.$$
$$\left. \phi(h_{n\ell})^\intercal, \phi(\gamma h_{n\ell})^\intercal, \ldots, \phi(\gamma^{m-1}h_{n\ell})^\intercal\right] \phi(c)^\intercal = 0.$$

□

Proposition 2.11. *Let $\mathcal{C}$ be a linear code in $\mathbb{F}_{q^m}^n$ having a generator matrix $G = [g_1, g_2, \ldots, g_k]^\intercal$ and a parity-check matrix $H = [h_1^\intercal, h_2^\intercal, \ldots, h_n^\intercal]$. Let $\widehat{G}$ and $\widehat{H}$ be the expanded generator matrix and expanded parity-check matrix of $\widehat{\mathcal{C}}$, respectively. Then*

1. *$\phi_n(xG) = \phi_k(x)\widehat{G}$ for all $x \in \mathbb{F}_{q^m}^k$,*
2. *$\phi_{n-k}(Hy^\intercal) = \widehat{H}(\phi_n(y))^\intercal$ for all $y \in \mathbb{F}_{q^m}^n$.*

Proof. Let $x = (x_1, x_2, \ldots, x_k) \in \mathbb{F}_{q^m}^k$ and let $x_i = \sum_{j=0}^{m-1} x_{ij}\gamma^j$ for all $i \in \{1, 2, \ldots, k\}$. Then

$$\begin{aligned}
\phi_k(x)\widehat{G} &= \sum_{i=1}^{k}\sum_{j=0}^{m-1} x_{ij}\phi_n(\gamma^j g_i) \\
&= \sum_{i=1}^{k} \phi_n\left(\sum_{j=0}^{m-1} x_{ij}\gamma^j g_i\right) \\
&= \phi_n\left(\sum_{i=1}^{k} x_i g_i\right) \\
&= \phi_n(xG).
\end{aligned}$$

Similarly, $\phi_{n-k}(Hy^\intercal) = \widehat{H}(\phi_n(y))^\intercal$ for all $y \in \mathbb{F}_{q^m}^n$. □

Remark 2.12. $\widehat{\mathcal{C}}$ can also be determined by the commutativity of the following diagram (as $\mathbb{F}_q$-linear maps):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{F}_{q^m}^k & \xrightarrow{G} & \mathbb{F}_{q^m}^n & \xrightarrow{H^\intercal} & \mathbb{F}_{q^m}^{n-k} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_k} & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \phi_{n-k}} & & \\
0 & \longrightarrow & \mathbb{F}_q^{mk} & \xrightarrow{\widehat{G}} & \mathbb{F}_q^{mn} & \xrightarrow{\widehat{H}^\intercal} & \mathbb{F}_q^{m(n-k)} & \longrightarrow & 0
\end{array}$$

Schur Product and Square Codes

Definition 2.13. Let $x, y \in \mathbb{F}_q^n$. We denote by the *Schur product* of x and y their component-wise product

$$x \star y = (x_1 y_1, \ldots, x_n y_n).$$

Remark 2.14. The Schur product is symmetric and bilinear.

Definition 2.15. Let $\mathcal{A}, \mathcal{B}$ be two codes of length n. The *Schur product* of two codes is the vector space spanned by all $a \star b$ with $a \in \mathcal{A}$ and $b \in \mathcal{B}$:

$$\langle \mathcal{A} \star \mathcal{B} \rangle = \langle \{ a \star b \mid a \in \mathcal{A}, b \in \mathcal{B} \} \rangle.$$

If $\mathcal{A} = \mathcal{B}$, then we call $\langle \mathcal{A} \star \mathcal{A} \rangle$ the *square code* of $\mathcal{A}$ and denote it by $\langle \mathcal{A}^2 \rangle$.

Definition 2.16. Let G be a $k \times n$ matrix, with rows $(g_i)_{1 \leq i \leq k}$. The *Schur matrix* of G, denoted by $S(G)$, consists of the rows $g_i \star g_j$ for $1 \leq i \leq j \leq k$.

We observe by Remark 2.14, that if G is a generator matrix of a code $\mathcal{C}$ then its Schur matrix $S(G)$ is a generator matrix of the square code of $\mathcal{C}$. Let s be the following map

$$\begin{aligned} s : \mathbb{N} &\to \mathbb{N}, \\ k &\mapsto \frac{1}{2}\left(k^2 + k\right). \end{aligned}$$

For a $k \times n$ matrix A, we observe that $S(A)$ has the size $s(k) \times n$.

The dimension of the square code of a code $\mathcal{C}$ provides information about how much Reed–Solomon type algebraic structure is present in $\mathcal{C}$. It is easy to see that for an $[n, k]$ code $\mathcal{C}$ having large enough length,

$$2k - 1 \leq \dim \langle \mathcal{C} \rangle^2 \leq s(k).$$

The lower bound is attained by GRS codes, since

$$\langle GRS_{n,k}(\alpha, \beta) \rangle^2 = GRS_{n,2k-1}(\alpha, \beta \star \beta).$$

In contrast to GRS codes, for a randomly chosen $[n, k]$ linear code $\mathcal{C}$ having length $n \geq s(k)$ the dimension of $\langle \mathcal{C} \rangle^2$ is $s(k)$, with high probability (see [42]).

List Decoding

In 1999, Guruswami and Sudan [77] published a polynomial time list decoding algorithm for Reed–Solomon codes that can correct errors beyond the $d/2$ error-correcting bound.

The Guruswami–Sudan (GS) decoding algorithm has an internal parameter m, called the interpolation multiplicity. The bound on the number of errors the GS algorithm can correct is associated to m, which is given by

$$t_m = n\left(1 - \sqrt{R\left(\frac{m+1}{m}\right)}\right),$$

where n is the length of the Reed–Solomon code and R is its rate (the *rate* of a linear code is given by $R = k/n$, where k is the dimension of the code).

Let $\mathcal{C}$ be a Reed–Solomon code $RS_{n,k}(\alpha)$ of length n and dimension k over a finite field $\mathbb{F}_q$. Given $z = (z_1, \ldots, z_n)$ a word over $\mathbb{F}_q$, the GS algorithm finds all the polynomials $p(x)$ of degree less than k such that the codeword $(p(\alpha_1), \ldots, p(\alpha_n))$ has Hamming distance is less than or equal to t_m from z. The GS algorithm involves two major steps:

1. (Interpolation step) Construct a bivariate polynomial $Q(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ such that Q has a zero of multiplicity m at each of the points (α_i, z_i), and the $(1, k-1)$-weighted degree of $Q(x, y)$ is minimal.

2. (Factorization step) Compute the factors of $Q(x, y)$ of the form $y - p(x)$ with degree of $p(x)$ less than k.

The output of the algorithm is a list $\mathcal{L}_m$ of codewords of $\mathcal{C}$, which includes all the codewords with Hamming distance is less than or equal to t_m from z. The size of the list is bounded above by

$$\ell_m = \left(m + \frac{1}{2}\right)\sqrt{\frac{n}{k-1}}.$$

In [77], the main aim of Guruswami and Sudan was to show the existence of a polynomial-time list decoding algorithm, and not the efficiency of the algorithm. However, several authors have contributed to improve the efficiency of the key steps in the GS algorithm. Some noteworthy contributions are by Kötter, described by McEliece in [115], for the interpolation step and by Roth–Ruckenstein [141] for the

factorization step. Using Kötter's improvement, inspired by the Feng–Tzeng algorithm [68], the interpolation algorithm takes $\mathcal{O}(n^2m^4)$ field operations. Whereas the factorization algorithm, using the Roth–Ruckenstein improvement, takes $\mathcal{O}(n^2m^2)$ field operations. Hence the overall complexity of the GS algorithm is $\mathcal{O}(n^2m^4)$ field operations. For more details on the GS algorithm and improvements by Kötter and Roth–Ruckenstein we refer the reader to [115].

2.2.2 McEliece Cryptosystem and Variants

Code-based cryptography first came up with the McEliece cryptosystem, which dates back to 1978. The original cryptosystem uses binary Goppa codes. However, the protocol can be generalized to make use of an arbitrary linear code. The security of the cryptosystem heavily relies of the choice of this linear code.

The McEliece Cryptosystem

We describe the general structure of the McEliece public-key crypotsystem, which involves three algorithms:

- **Key generation:** Let G be a generator matrix of an $[n,k]_q$ linear code $\mathcal{C}$ which can efficiently correct up to t errors. Choose a random $k \times k$ invertible matrix S and a random $n \times n$ permutation matrix P.

  The private key is then (S, G, P) and the public key is $(G' := SGP^{-1}, t)$.

- **Encryption:** Let $y \in \mathbb{F}_q^k$ be a message that we want to encrypt. The cipher text is given by $c = yG' + e$, where $e \in \mathbb{F}_q^n$ is a random error vector with Hamming weight $\mathrm{wt}(e) \leq t$.

- **Decryption:** For the decryption we first multiply the cipher text by P, i.e.,

$$cP = yG'P + eP = ySG + eP.$$

  Since $\mathrm{wt}(eP) = \mathrm{wt}(e) \leq t$, we decode cP to obtain yS, and then multiply by S^{-1} to retrieve the original message y.

The security of a McEliece cryptosystem is based on two types of attacks:

1. Key recovery attack: given the public key (G', t) recover the private key (S, G, P). These attacks exploit the algebraic structure of the hidden private code.

2. Ciphertext attack: given a cipher text c recover the original message y. The difficulty of this attack is related to the general decoding problem. We will discuss more about general decoding problem later in this section.

If a McEliece cryptosystem resists both these types of attacks, one can use general procedure to obtain a CCA2 (adaptive chosen-ciphertext attack) secure cryptosystem (see for example [98]). Note that in the CCA2 secure variants of the McEliece encryption schemes the public key G' can be represented in the systematic form (row reduced echelon form), which reduces the public key size.

The Niederreiter Cryptosystem

In 1985, Niederreiter presented a version of the McEliece cryptosystem that uses the parity-check matrix instead of the generator matrix. The Niederreiter version has been proved to be completely equivalent in terms of security [104].

- **Key generation:** Let H be a parity-check matrix of an $[n,k]_q$ linear code $\mathcal{C}$ which can efficiently correct up to t errors. Choose a random $(n-k)\times(n-k)$ invertible matrix S and a random $n \times n$ permutation matrix P.

  The private key is then (S, H, P) and the public key is $(H' := SHP, t)$.

- **Encryption:** Let $y \in \mathbb{F}_q^n$ be a message such that its Hamming weight $\mathrm{wt}(y) \leq t$. The cipher text is given by the syndrome of y, i.e., $c = H'y^\intercal$.

- **Decryption:** For the decryption we first multiply the cipher text by S^{-1}, i.e.,

$$S^{-1}c = S^{-1}H'y^\intercal = HPy^\intercal.$$

  Since $\mathrm{wt}(yP^\intercal) = \mathrm{wt}(y) \leq t$, we decode $S^{-1}c$ to obtain $yP^\intercal$, and then multiply by $(P^\intercal)^{-1}$ to retrieve the original message y.

Variants and Vulnerabilities

Since the origin of the McEliece cryptosystem, many variants have been proposed using different codes or different ways of hiding the private code. We present some those variants and their vulnerabilities.

- Neiderreiter, in the same article [128] as the famous Niederreiter cryptosystem, proposed to use the generalised Reed–Solomon codes instead of Goppa codes.

This proposal was then attacked by Sidelnikov and Shestakov in [153], where they used the fact, that the public matrix is still a generator matrix of a GRS code and they were able to recover the evaluation points and hence the GRS structure of the public matrix.

- Various McEliece cryptosystems based on modifications of GRS codes have been proposed [15, 16, 18, 23, 36, 128]. Most of them have been proved to be fully (or partially) insecure due to the infamous distinguisher attack [49, 52, 73]. The distinguisher attack exploits the fact that the dimension of the square code of GRS codes is very low compared to a random linear code of the same dimension.

- Moreover, other families of codes have also been shown to be vulnerable against the distinguisher attack. In [50], Couvreur et al. presented a general attack against cryptosystems based on algebraic geometric codes and their subcodes. In [66] Faugère et al. showed that high rate binary Goppa codes can be distinguished from a random code. In [51], Couvreur et al. presented a polynomial time attack against cryptosystems based on non-binary Goppa codes defined over quadratic extensions.

- At the time of this writing there are seven code-based cryptosystems included in NIST's standardization process: BIKE [7] based on quasi-cyclic MDPC codes, classic McEliece [30] based on binary Goppa codes, ROLLO [116] based on quasi-cyclic LRPC codes, RQC [1] based on rank metric quasi-cyclic codes, HQC [1] based on Hamming metric quasi-cyclic codes, LEDAcrypt [14] based on quasi-cyclic LDPC codes and NTS-KEM [3] based on binary Goppa codes.

Information Set Decoding

The overall security of a McEliece cryptosystem is related to the general decoding problem.

Definition 2.17 (General decoding problem)**.** Given an $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ and $x \in \mathbb{F}_q^n$, find $c \in \mathcal{C}$ such that $d(x, c)$ is minimum.

Note that if $d(x, c) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, then this problem has a unique solution. Here d is the minimum distance of $\mathcal{C}$. This problem, over the binary field, was proved to be NP-complete by Berlekamp, McEliece and van Tilborg in [25]. An equivalent

formulation of this problem is using a parity-check matrix, and is called the syndrome decoding problem.

Definition 2.18 (Syndrome decoding problem)**.** Given a parity-check matrix H for an $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$, a vector $s \in \mathbb{F}_q^{n-k}$ and a positive integer w. Then find $e \in \mathbb{F}_q^n$ such that $eH^\intercal = s$ and $\mathrm{wt}(e) \leq w$.

Using the following Gilbert–Varshamov distance d_0, we notice that the syndrome decoding problem has a unique solution if $w < d_0$.

Definition 2.19. Let q be a prime power and $0 \leq k \leq n$ be integers. Then the *Gilbert–Varshamov distance* is the largest integer $d_0(n, k)$ such that

$$\sum_{i=0}^{d_0(n,k)-1} \binom{n}{i} (q-1)^i \leq q^{n-k}.$$

In cryptographic schemes, the weight of an error is much smaller than the Gilbert–Varshamov distance as it is within the error-correction capacity. In the case of $w < d_0(n, k)$, information set decoding (ISD) algorithms are the best known algorithms for decoding a general linear code. ISD algorithms were introduced by Prange [139] in 1962, it is also known as the plain ISD algorithm.

Plain ISD Algorithm: The plain ISD algorithm first chooses an information set I, which is a size k subset of $\{1, 2, \ldots, n\}$ such that the restriction of the generator matrix on the columns indexed by the set I is non-singular. Then Gaussian elimination brings the generator matrix in a standard form and assuming that the errors are outside of the information set, these row operations will exploit the corresponding error vector. The algorithm terminates when the weight of the corresponding error vector does not exceed the given error correction capacity. See Algorithm 1 for details.

Notations used in Algorithm 1: Let $x \in \mathbb{F}_q^n$, G be a $k \times n$ matrix over $\mathbb{F}_q$, and $I \subseteq \{1, \ldots, n\}$ be a subset of size k. Then x_I denotes the subvector of x with entries indexed by I, and G_I denotes the $k \times k$ submatrix of G with columns indexed by I.

Algorithm 1 Plain ISD algorithm over $\mathbb{F}_q$

Input: a vector $x \in \mathbb{F}_q^n$, a generator matrix G of an $[n, k]$ linear code $\mathcal{C}$, a positive integer w.
Output: $e \in \mathbb{F}_q^n$ such that $x + e \in \mathcal{C}$ and $\mathrm{wt}(e) = w$.

1: Choose an information set I.
2: Compute $x' = x - x_I G_I^{-1} G$.
3: **if** $\mathrm{wt}(x') = w$ **then**
4: output $e := x'$
5: **else**
6: go to Step 1.

The running time of the plain ISD algorithm can be given by the product of the cost of one iteration and the expected number of iterations, which is

$$\text{Cost of the plain ISD} = \mathcal{O}\left(k^3 \cdot \left(\frac{\binom{n-k}{w}}{\binom{n}{w}}\right)^{-1}\right).$$

A Brief History of ISD Improvements: Even though the cost of one iteration of Prange's plain ISD algorithm is very low, the algorithm is still coming with a huge complexity due to the number of iterations needed. In order to improve the time complexity, many improvements have been suggested to Prange's simplest form of ISD. All the improvements focus on a more elaborate and more likely weight distribution of the error vector, which results in a higher cost of one iteration, but less iterations have to be performed. The improvements were splitting from an early time on into two directions:

The first direction is following the splitting of Lee and Brickell [102] into the information set and the redundant set, i.e., they ask for v errors in the information set and $t - v$ outside. In 1988, the same year as Lee and Brickell proposed their algorithm, Leon [103] introduced a zero window inside the redundant set of size ℓ, where no error are allowed. In 1993 Stern [156] kept this zero window and proposed to partition the information set into two sets and asks for v errors in each part and $t - 2v$ errors outside the information set. The generalization of both Lee–Brickell and Stern's algorithm to a general finite field $\mathbb{F}_q$ were performed by Peters [135] in 2010. In 2011 Bernstein, Lange and Peters proposed the ball-collision algorithm [31], where they keep the partitioning of the information set but they reintroduce errors in the zero window, in fact they partition the zero window into two sets and

ask for w errors in both and hence for $t-2v-2w$ errors outside. The ball-collision algorithm was recently generalized to an arbitrary finite field $\mathbb{F}_q$, in [87]. In 2016, Hirose [81] generalized the nearest neighbor algorithm over $\mathbb{F}_q$ and applied it to the generalized Stern algorithm.

The second direction is following Dumer's splitting approach [60], which is asking for v errors in $k+\ell$ bits, which are containing an information set, and $t-v$ in the remaining $n-k-\ell$ bits. The second direction has resulted in many improvements, for example in 2009 Finiasz and Sendrier [69] have built two intersecting subsets of the $k+\ell$ bits, which contain an information set, and ask for v disjoint errors in both sets and $t-2v$ in the remaining $n-k-\ell$ bits. Niebuhr, Persichetti, Cayrel, Bulygin and Buchmann [127] in 2010 improved the performance of ISD algorithms over $\mathbb{F}_q$ based on the idea of Finiasz and Sendrier [69]. In 2011 May, Meurer and Thomae [111] proposed an improvement using the representation technique introduced by Howgrave-Graham and Joux [86]. To this algorithm Becker, Joux, May and Meurer [22] (BJMM) in 2012 introduced further improvements. In the same year Meurer in his dissertation [118] proposed a new generalized ISD algorithm based on these two papers. In 2015, May and Ozerov [112] used the nearest neighbor algorithm to improve the BJMM version of ISD. Later in 2017, the nearest neighbor algorithm over $\mathbb{F}_q$ was applied to generalized BJMM algorithm by Gueye, Klamti and Hirose [75].

It is important to remark (see [118]) that the BJMM algorithm, even if having the smallest complexity, comes with a different cost: memory. In order to achieve a complexity of 128 bits, BJMM needs about 10^9 terabytes of memory. In fact, Meurer observed, that if one restricts the memory to 2^{40}, BJMM and the ball-collision algorithm are performing almost the same.

Apart from improvements regarding the success probability, one can also improve the cost of one iteration: Canteaut and Chabaud [40] have provided a speed up for finding information sets. They show that the information set should not be taken at random after one unsuccessful iteration, but rather a part of the previous information set should be reused and therefore a part of the Gaussian elimination step is already performed. In the following we describe Stern's ISD algorithm, a modification of which we will be using to discuss the security of one of the proposed cryptosystems in this thesis.

Algorithm 2 Stern's ISD algorithm over $\mathbb{F}_q$

Input: a vector $x \in \mathbb{F}_q^n$, a generator matrix G of an $[n, k]$ linear code $\mathcal{C}$, a positive integer w. For simplicity we assume k is even.
Output: $e \in \mathbb{F}_q^n$ such that $x + e \in \mathcal{C}$ and $\mathrm{wt}(e) = w$.

1: Choose an information set I and a uniform random partition of I into disjoint sets X and Y, each of size $k/2$.
2: Choose a random subset $Z \subseteq \{1, \ldots, n\} \setminus I$ of size ℓ.
3: Compute $x' = x - x_I G_I^{-1} G$.
4: For each size v subset $U = \{u_1, \ldots, u_v\} \subset X$, compute the set

$$S_U = \left\{ \left(s := x' - \sum_{i=1}^{v} y_i g_{u_i}, s_Z \right) : (y_1, \ldots, y_v) \in (\mathbb{F}_q^*)^v \right\}$$

5: For each size v subset $W = \{w_1, \ldots, w_v\} \subset Y$, compute the set

$$T_W = \left\{ \left(t := \sum_{i=1}^{v} y_i g_{w_i}, t_Z \right) : (y_1, \ldots, y_v) \in (\mathbb{F}_q^*)^v \right\}$$

6: **for all** pairs (U, W) **do**
7: **for** $((s, y), (t, y)) \in S_U \times T_W$ **do**
8: **if** $\mathrm{wt}(s - t) = w$ **then**
9: output $e = s - t$
10: **else**
11: go to Step 1.

Stern's ISD Algorithm: Stern's modification uses two parameters v and ℓ. It allows a fixed number of errors in the information set I. Stern's algorithm partitions the information set I into two equal-sized subsets X and Y, and chooses uniformly at random a subset Z of size ℓ outside of I. Then it looks for vectors having exactly weight v among the columns indexed by X, exactly weight v among the columns indexed by Y, and exactly weight 0 in columns indexed by Z and the missing weight $t - 2v$ in the remaining indices. See Algorithm 2 for details.

Additional notations used in Algorithm 2: For an information set I, let g_u denote the unique row of $G_I^{-1} G$ having 1 at the u-th position.

2.3 McEliece Variant Based on Expanded GRS Codes

In this section, we present our first variant of the McEliece cryptosystem which uses an expanded GRS code as the hidden private code. The expanded GRS codes have

a lot of algebraic structure that can be exploited if used directly as an replacement of Goppa codes. In this proposal, we first destroy the algebraic structure present in the expanded GRS codes and then use it in the McEliece-type cryptosystem.

2.3.1 Protocol

We will present the proposed cryptosystem in the Niederreiter version.

In a nutshell, we consider a GRS code over $\mathbb{F}_{q^m}$ and expand it over $\mathbb{F}_q$. Recall from Lemma 2.10 that a parity-check matrix of the expanded code can be viewed as n blocks, where each block consist of m columns. In order to destroy the algebraic structure of the expanded code, we shorten the code, i.e., we delete some number of randomly chosen columns from each block. We then hide the shortened code by multiplying it with an invertible matrix which preserves the weight of a vector over the extension field $\mathbb{F}_{q^m}$.

The full description of the cryptosystem is as follows:

- **Key generation:** Let q be a prime power, $2 \leq \lambda < m$ be positive integers and $k < n \leq q^m$ be positive integers, satisfying $R := k/n > (1 - \lambda/m)$. Consider a GRS code $\mathcal{C} = \mathrm{GRS}_{n,k}(\alpha, \beta)$ of dimension k and length n over the finite field $\mathbb{F}_{q^m}$ and choose a parity-check matrix H of $\mathcal{C}$. Let t be the error correction capacity of $\mathcal{C}$, i.e., $t = \lfloor \frac{n-k}{2} \rfloor$.

  Let $\widehat{H}$ be the expanded parity-check matrix of the expanded code $\widehat{\mathcal{C}}$ of $\mathcal{C}$ with respect to a primitive element $\gamma \in \mathbb{F}_{q^m}$. We use Lemma 2.10 to obtain $\widehat{H}$, which is an $m(n-k) \times mn$ matrix over $\mathbb{F}_q$. We destroy the algebraic structure of $\widehat{H}$ using the following two steps:

  1. Shortening $\widehat{\mathcal{C}}$
     - For each $1 \leq i \leq n$, let S_i be a randomly chosen subset of $\{(i-1)m+1, (i-1)m+2, \ldots, im\}$ of size $m-\lambda$ and define $S = \bigcup_{i=1}^{n} S_i$.
     - We puncture $\widehat{H}$ on columns indexed by S. Let $\widehat{H}_S$ be the resulting $m(n-k) \times \lambda n$ parity-check matrix and let $\widehat{\mathcal{C}}_S$ be the shortened code.
  2. Hiding $\widehat{\mathcal{C}}_S$
     - Choose n random $\lambda \times \lambda$ invertible matrices $T_1, T_2, \ldots, T_n$ over $\mathbb{F}_q$. Define T to be the block diagonal matrix having $T_1, T_2, \ldots, T_n$ as diagonal blocks.

$$\begin{pmatrix} T_1 & 0 & 0 & 0 \\ 0 & T_2 & 0 & 0 \\ 0 & 0 & T_3 & 0 \\ 0 & 0 & 0 & T_4 \end{pmatrix} \qquad \begin{pmatrix} 0 & \mathbf{1}_\lambda & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1}_\lambda \\ \mathbf{1}_\lambda & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1}_\lambda & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & T_1 & 0 & 0 \\ 0 & 0 & 0 & T_2 \\ T_3 & 0 & 0 & 0 \\ 0 & 0 & T_4 & 0 \end{pmatrix}$$

(A) Matrix T (B) Matrix P_σ (C) Matrix $Q = TP_\sigma$

FIGURE 2.1: Illustration of matrices involved in the key generation process (an example with $n = 4$, where $\mathbf{1}_\lambda$ is the identity matrix of size λ).

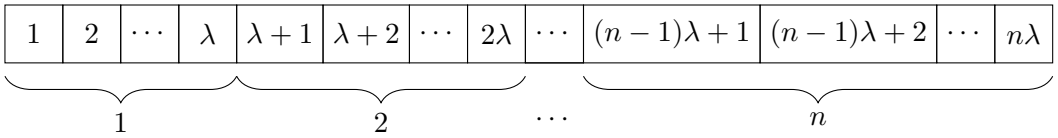

FIGURE 2.2: Illustration of error vectors involved in the encryption step. Support of an error vector lies inside randomly chosen t out of the n blocks.

- Now choose a random permutation σ of length n and define P_σ to be the block permutation matrix of size $\lambda n \times \lambda n$. It can also be seen as Kronecker product of the $n \times n$ permutation matrix corresponding to σ and the identity matrix of size λ.
- Define $Q := TP_\sigma$ and compute $H' = \widehat{H}_S Q$. See Figure 2.1 for an illustration of the matrices T, P_σ and Q.

The private key is then (H, Q, γ) and the public key is (H', t, λ).

- **Encryption:** Let $y \in \mathbb{F}_q^{\lambda n}$ be a message having support in t sub-vectors each of length λ, in particular

$$\begin{aligned} \operatorname{support}(y) \subseteq \{&\lambda(i_1 - 1) + 1, \lambda(i_1 - 1) + 2, \ldots, \lambda(i_1), \\ &\lambda(i_2 - 1) + 1, \lambda(i_2 - 1) + 2, \ldots, \lambda(i_2), \\ &\ldots, \lambda(i_t - 1) + 1, \lambda(i_t - 1) + 2, \ldots, \lambda(i_t)\}, \end{aligned} \tag{2.1}$$

for some distinct $i_1, i_2, \ldots, i_t \in \{1, 2, \ldots, n\}$. See Figure 2.2 for an illustration of an error vector. Then compute the cipher text

$$c = H' y^\intercal.$$

- **Decryption:** For the decryption we apply ϕ_{n-k}^{-1} on c, i.e.,

$$\phi_{n-k}^{-1}(c) \quad = \quad \phi_{n-k}^{-1}\left(\widehat{H}_S Q y^\intercal\right).$$

This is a vector in $\mathbb{F}_{q^m}^{n-k}$, which corresponds to the syndrome of $Qy^\intercal$ with respect to the parent GRS code $\mathcal{C}$. We syndrome decode $\phi_{n-k}^{-1}(c)$ and delete the coordinates in S to obtain $Qy^\intercal$. Finally, we multiply Q^{-1} and recover the message y. Proposition 2.20 proves the correctness of the decryption process.

Proposition 2.20. *The decryption process is correct.*

Proof. Observe that $\widehat{H}_S Q y^\intercal = \widehat{H}\bar{y}^\intercal$, where $\bar{y}$ is the embedding of $yQ^\intercal$ in to $\mathbb{F}_q^{mn}$, by introducing zeros on the positions indexed by S.
From Proposition 2.11 we get

$$\phi_{n-k}^{-1}\left(\widehat{H}\bar{y}^\intercal\right) \quad = \quad H\left(\phi_n^{-1}(\bar{y})\right)^\intercal.$$

Due to the block structure of the matrix Q, the vector of $Qy^\intercal$ has support in t sub-vectors each of length λ, thus $\bar{y}$ has support in t sub-vectors each of length m. Henceforth $\mathrm{wt}(\phi_n^{-1}(\bar{y})) \leq t$, and we can decode $\phi_{n-k}^{-1}(c)$ to get $\phi_n^{-1}(\bar{y})$.

By applying ϕ_n we get $\bar{y}$ and by projecting on positions not indexed by S, we get $Qy^\intercal$ and thereafter multiplying by Q^{-1}, we recover the message y. □

Remark 2.21. For low key sizes it is desirable to use a small degree of extension m and small λ. In the case of quadratic extension and in the case of $\lambda = 1$, puncturing all but one column from each block results in an alternant code (subfield subcode of a GRS code). Alternant codes are known to be vulnerable to square code attacks [51, 66]. Hence, we do not propose to use quadratic extensions or $\lambda = 1$. We therefore propose to use $m = 3$ and $m = 4$ with $\lambda = 2$.

2.3.2 Security Agianst Known Attacks

In this section we discuss the security of the proposed cryptosystem. We first focus on the two main structural attacks on cryptosystems based on GRS codes, namely the Sidelnikov–Shestakov attack and the distinguisher attack based on the Schur product of the public code. Later we discuss a non-structural (or plaintext) attack, which is an adaptation of Stern's ISD algorithm to our cryptosystem.

Sidelnikov and Shestakov attack

Directly using GRS codes as secret codes makes the cryptosystem vulnerable against the attack by Sidelnikov and Shestakov in [153]. The attack uses the fact that the public matrix is permutation equivalent to a generator matrix of the secret GRS code. This helps the attack in recovering the evaluation points of the public matrix in polynomial time.

In the proposed cryptosystem, the secret GRS parity-check matrix H over $\mathbb{F}_{q^m}$ is hidden in two ways: first by puncturing its expanded parity-check matrix $\widehat{H}$ over $\mathbb{F}_q$ and then by scrambling the columns of the punctured matrix $\widehat{H}_S$. Due to multiplying $\widehat{H}_S$ with a block diagonal matrix it is clear that the resulting code is no more equivalent to an evaluation code (or an expanded evaluation code). Hence evaluations (or expanded evaluation column vectors) can not be exploited using the Sidelnikov–Shestakov attack.

Distinguisher Attack Based on the Schur Product

Various McEliece cryptosystems based on modifications of GRS codes have been proved to be insecure [49, 52, 73]. This is because the dimension of the square code of GRS codes is very low compared to a random linear code of the same dimension. The class of such attacks, based on the low dimensional square code of the public code (or of the shortened public code), is known as distinguisher attacks.

In the following, based on experimental observations, we infer that the public code of the proposed cryptosystem cannot be distinguished using square code techniques. We also provide theoretical arguments on the behavior of the square code dimension of the public code.

Let $\widehat{\mathcal{C}}_S$ be the public code of the proposed cryptosystem. Note that $\widehat{\mathcal{C}}_S$ is a shortening of an expanded GRS code $\widehat{\mathcal{C}}$.

1. **Squares of expanded GRS codes:** Like in the case of Reed–Solomon codes and their subfield subcodes, the expanded GRS codes also have low square code dimension. To see this, we visualize expanded GRS codes as subfield subcodes of GRS-like codes. Let $\mathcal{C}$ be a GRS code of length n and dimension k over

$\mathbb{F}_{q^m}$ having the following parity-check matrix

$$H = V_r(x, y) := \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1x_1 & y_2x_2 & \cdots & y_nx_n \\ \vdots & \vdots & \ddots & \vdots \\ y_1x_1^{r-1} & y_2x_2^{r-1} & \cdots & y_nx_n^{r-1} \end{pmatrix},$$

where $x = (x_1, \ldots, x_n)$ is a vector of distinct elements in $\mathbb{F}_{q^m}$, $y = (y_1, \ldots, y_n)$ is a vector over $\mathbb{F}_{q^m}^*$ and $r := n - k$. Let γ be a primitive element in $\mathbb{F}_{q^m}$. We define a new code $\mathcal{B}$ of length mn over $\mathbb{F}_{q^m}$ given by the kernel of the following parity-check matrix

$$H' = \begin{pmatrix} V_r(x, y) & | & V_r(x, \gamma y) & | & \cdots & | & V_r(x, \gamma^{m-1} y) \end{pmatrix}.$$

Using Lemma 2.10, it is easy to observe, that the expanded code $\widehat{\mathcal{C}}$ of $\mathcal{C}$ with respect to γ is permutation equivalent to the $\mathbb{F}_q$-kernel of H'. In other words, $\widehat{\mathcal{C}}$ is permutation equivalent to the subfield subcode of $\mathcal{B}$ over $\mathbb{F}_q$. Observe that a generator matrix G' of $\mathcal{B}$ is given by

$$\left(\begin{array}{ccccc} V_k(x, y') & 0 & \ldots & 0 & 0 \\ 0 & V_k(x, \gamma^{-1}y') & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & V_k(x, \gamma^{-(m-2)}y') & 0 \\ 0 & 0 & \ldots & 0 & V_k(x, \gamma^{-(m-1)}y') \\ \hline V_r(x, y'') & 0 & \ldots & 0 & -V_r(x, \gamma^{-(m-1)}y'') \\ 0 & V_r(x, \gamma^{-1}y'') & \ldots & 0 & -V_r(x, \gamma^{1-(m-1)}y'') \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & V_r(x, \gamma^{-(m-2)}y'') & -V_r(x, \gamma^{(m-2)-(m-1)}y'') \end{array}\right),$$

where y' is such that $V_k(x, y')V_r(x, y)^\intercal = 0$, and $y'' = (x_1^k, x_2^k, \ldots, x_n^k) \star y'$. One can verify that $G'(H')^\intercal = 0$. Observe that a generator matrix of $\widehat{\mathcal{C}}$ is

permutation equivalent to

$$\widehat{G} = \left(\begin{array}{cccc} G_1 & 0 & \dots & 0 \\ 0 & G_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & G_m \\ \hline & & G_{gv} & \end{array}\right),$$

where G_i is a generator matrix of the subfield subcode of $V_k(x, \gamma^{-(i-1)}y')$ over $\mathbb{F}_q$, and G_{gv} is a generator matrix of the $\mathbb{F}_q$-subfield subcode of the bottom $(m-1)r$ rows of G'. The matrix G_{gv} is also known as the glue-vector generator matrix, as in [158]. Due to the block structure of $\widehat{G}$ the Schur matrix of $\widehat{G}$ will have many zero rows. As a result, the dimension of the square code is not full, given large enough n. This may lead to vulnerabilities when using expanded GRS codes directly in the cryptosystem.

2. **Effect of Shortening:** Consider the parity-check matrix $\widehat{H}$ of an expanded GRS code as shown in Lemma 2.10, i.e.,

$$\begin{aligned}\widehat{H} := [&\phi_{n-k}(h_1)^\intercal, \phi_{n-k}(\gamma h_1)^\intercal, \dots, \phi_{n-k}(\gamma^{m-1}h_1)^\intercal \mid \phi_{n-k}(h_2)^\intercal, \phi_{n-k}(\gamma h_2)^\intercal, \\ &\dots, \phi_{n-k}(\gamma^{m-1}h_2)^\intercal \mid \dots \mid \phi_{n-k}(h_n)^\intercal, \phi_{n-k}(\gamma h_n)^\intercal, \dots, \phi_{n-k}(\gamma^{m-1}h_n)^\intercal].\end{aligned}$$

We partition the columns of $\widehat{H}$ into n blocks, each of size m, as shown above. By the definition of $\widehat{H}$, each of these blocks corresponds to a unique column vector of the parity-check matrix of the parent GRS code. In order words, the first block of m columns corresponds to the column $h_1^\intercal$, the second block of m columns correspond to the column $h_2^\intercal$, and so on.

In order to weaken this correspondence, we puncture (randomly chosen) $m-\lambda$ of the columns from each block of $\widehat{H}$. As a result the correspondence of each block to the parent column vector is inconsistent. Note that the correspondence still exists but the way i^{th} block corresponds to $h_i^\intercal$ is now different from the way j^{th} block corresponds to $h_j^\intercal$.

In addition, we multiply the punctured parity-check matrix by an invertible block diagonal matrix T. This further destroys the algebraic structure inherited from the parent GRS code. This was evident in our computations of the

square code dimension of such shortened codes. Even in the case of $m = 3$ we observed that puncturing one column from each block of $\widehat{H}$ results in a full square code dimension.

Information Set Decoding

Information set decoding (ISD) algorithms are best known algorithms for decoding a general linear code. Hence, they are the best known ciphertext attacks for McEliece-like cryptosystems. We modify one of the ISD algorithms according to the error pattern we use in our cryptosystem.

ISD for the Proposed Cryptosystem: In the proposed cryptosystem we introduce a burst pattern in the error vector, in particular the error vector has support in t sub-vectors each of length λ. Henceforth, we modify Stern's ISD algorithm to incorporate such pattern in the error vector.

We first recall Stern's algorithm. The algorithm partitions the information set I into two equal-sized subsets X and Y, and chooses uniformly at random a subset Z of size ℓ outside of I. Then it looks for vectors having exactly weight v among the columns indexed by X, exactly weight v among the columns indexed by Y, and exactly weight 0 in columns indexed by Z and the missing weight $t - 2v$ in the remaining indices. See Algorithm 2 for a detailed description of the Stern's ISD algorithms over an arbitrary finite field.

In the proposed cryptosystem we have been given a public code $\widehat{\mathcal{C}}_S$ of length λn and dimension $k' := mk - (m - \lambda)n$ over $\mathbb{F}_q$. We also know that the error vector (the plaintext y in (2.1)) has support in t sub-vectors of length λ. Hence we use Stern's algorithm on the blocks of size λ. We consider the information set I to have $\lfloor k'/\lambda \rfloor$ blocks. We partition I into two equal-sized subsets X and Y, and choose uniformly at random a subset Z of ℓ blocks outside of I. Then we look for vectors having support in exactly v blocks in X, exactly v blocks in Y, exactly 0 blocks in Z, and the remaining $t - 2v$ blocks outside $I \cup Z$. For calculation of cost of this modified ISD algorithm, we follow the same approach as in [136].

In the next section, we compute the key sizes of the proposed cryptosystem having 128-bit and 256-bit security against this modified ISD algorithm.

2.3.3 Parameters

In this section we find the best set of parameters that minimizes the public key size of the proposed cryptosystem, fixing 128-bit and 256-bit security against the modified ISD algorithm discussed in previous section. Later, in Section 2.5, we compare these key sizes with the key sizes of the classical McEliece cryptosystem and some other variants.

In the proposed cryptosystem, the public key is a parity-check matrix of a linear code over $\mathbb{F}_q$ having length λn and dimension $mk-(m-\lambda)n$. Hence the public key size is

$$(\lambda n - m(n-k)) \cdot m(n-k) \cdot \log_2(q)$$

bits. For a degree of extension m, let $\mathcal{C}_m$ be the public code.

In Table 2.1 and Table 2.2, we provide the key sizes for different rates of the public code $\mathcal{C}_3$ achieving a 128-bit and 256-bit security level, respectively, against the modified ISD algorithm discussed in Section 2.3.2. Observe that the smallest key size is achieved at rate 0.80 and 0.82, respectively.

Rate	q	n	k	t	Key Size (bits)
0.60	9	639	383	128	1241596
0.65	9	587	381	103	1089212
0.70	9	557	389	84	974562
0.75	9	557	417	70	923970
0.80	9	577	461	58	889125
0.85	9	635	539	48	896506
0.90	11	755	679	38	1011178

TABLE 2.1: Comparing key sizes of the proposed cryptosystem with $m = 3$ and $\lambda = 2$ reaching a 128-bit security level against the modified ISD algorithm.

In Table 2.3 and Table 2.4, we provide the key sizes for different rates of the public code $\mathcal{C}_4$ achieving a 128-bit and 256-bit security level, respectively, against the modified ISD algorithm discussed in Section 2.3.2. In this case the smallest key size is achieved at rate 0.87 and 0.89, respectively.

Rate	q	n	k	t	Key Size (bits)
0.60	13	1382	829	277	6783627
0.65	13	1270	825	223	5952804
0.70	13	1207	844	182	5339456
0.75	13	1192	894	149	4929077
0.80	13	1230	984	123	4702652
0.82	13	1258	1031	114	4624198
0.85	13	1340	1139	101	4634545
0.87	13	1420	1235	93	4692805
0.90	13	1602	1441	81	4863276

TABLE 2.2: Comparing key sizes of the proposed cryptosystem with $m = 3$ and $\lambda = 2$ reaching a 256-bit security level against the modified ISD algorithm.

Rate	q	n	k	t	Key Size (bits)
0.60	7	1489	893	298	3975484
0.65	7	1082	703	189	2757856
0.70	7	892	624	134	2142753
0.75	7	798	598	100	1787724
0.80	7	766	612	77	1584067
0.85	7	794	674	60	1498454
0.87	7	824	716	54	1474737
0.90	7	911	819	46	1502137

TABLE 2.3: Comparing key sizes of the proposed cryptosystem with $m = 4$ and $\lambda = 2$ reaching a 128-bit security level against the modified ISD algorithm.

Rate	q	n	k	t	Key Size (bits)
0.65	7	2360	1534	413	13134108
0.70	7	1945	1361	292	10191102
0.75	7	1738	1303	218	8480009
0.80	7	1662	1329	167	7448878
0.85	7	1700	1445	128	6815134
0.87	7	1770	1539	116	6785893
0.89	7	1872	1666	103	6754721
0.91	7	2024	1841	92	6814326

TABLE 2.4: Comparing key sizes of the proposed cryptosystem with $m = 4$ and $\lambda = 2$ reaching a 256-bit security level against the modified ISD algorithm.

2.4 McEliece Variant Based on Weight Two Masking of GRS Codes in Conjunction with List Decoding

In this section, we present our second variant of the McEliece cryptosystem which uses a weight two masking on GRS codes. In addition, we use list decoding to increase on number of errors we can correct and as a consequence improve on the key sizes. As per the security point of view, we hide the algebraic structure of the GRS code by masking it with a constant row and column weight two matrix. We will see in Section 2.4.3 how this masking affects the dimension of the square code.

2.4.1 Protocol

In the following cryptosystem we use the Guruswami–Sudan (GS) list decoding algorithm for decryption with an aim to reduce the size of the keys. Although the running time of the GS list decoding algorithm is high, the trade-off between the running time and the key size can easily be achieved. In the following proposed cryptosystem we use the interpolation multiplicity $m = \lfloor n^{1/2} \rfloor$.

In this section we will present the proposed cryptosystem in the Niederreiter version.

- **Key generation:** Consider a GRS code $\mathcal{C} = \mathrm{GRS}_{n,k}(\alpha, \beta)$ of dimension k and length n over the finite field $\mathbb{F}_q$ and choose a parity-check matrix H of $\mathcal{C}$.

  Choose a random $(n-k) \times (n-k)$ invertible matrix S and an invertible $n \times n$ matrix Q of constant row weight two, both over $\mathbb{F}_q$. Then we compute

  $$H' = SHQ.$$

  Let $R = \frac{k}{n}$ be the rate of the code $\mathcal{C}$ and m be the interpolation multiplicity (refer Section 2.2.1). The amount of errors which we can correct for the GRS code using the Guruswami–Sudan list decoding algorithm is then given by

  $$t = \left\lfloor \frac{t_m}{2} \right\rfloor = \left\lfloor \frac{n}{2} \left(1 - \sqrt{R \left(\frac{m+1}{m} \right)} \right) \right\rfloor.$$

  The Guruswami–Sudan algorithm gives us a list of possible messages, to recover the sent message we also send hash of the message in the cipher. Let $\mathcal{H}$ be a fixed hash function, globally known, with output size of h bits. The

value of h depends on the list size ℓ_m in such a way that we do not encounter second pre-images in the list of hash values of possible messages.

The private key is given by (S, H, Q) and the public key is given by (H', t).

- **Encryption:** Let $y \in \mathbb{F}_q^n$ be a message having Hamming weight $\mathrm{wt}(y) \leq t$. Then compute
$$c = H'y^\intercal.$$
The cipher text is then given by $(c, \mathcal{H}(y))$.

- **Decryption:** For the decryption we first multiple the ciphertext by S^{-1}, i.e.,
$$c' := S^{-1}c = HQy^\intercal.$$
Since $\mathrm{wt}(yQ^\intercal) \leq 2t \leq t_m$, we list decode c' to get a list $\mathcal{L}_m$ of size ℓ_m of possible messages, say
$$\mathcal{L}_m = \{z_1, \ldots, z_{\ell_m}\}.$$
In order to recover the original message y from the list, we compute $\mathcal{H}(z_i(Q^\intercal)^{-1})$ for all $i \in \{1, \ldots, \ell_m\}$ and compare it with $\mathcal{H}(y)$. The sent message y is given by the $z_j(Q^\intercal)^{-1}$, which is such that $\mathcal{H}(z_j(Q^\intercal)^{-1}) = \mathcal{H}(y)$, for some $j \in \{1, \ldots, \ell_m\}$.

The output size h of the hash function should be chosen in such a way that the probability of finding a second pre-image of $\mathcal{H}(y)$ in the list $\{\mathcal{H}(z(Q^\intercal)^{-1}) | z \in \mathcal{L}_m\}$ is negligible. Let $z \in \mathcal{L}_m$ with $z \neq y$. With an ideal hash function, the probability that $\mathcal{H}(z(Q^\intercal)^{-1}) = \mathcal{H}(y)$ is 2^{-h}. Hence the probability of finding a second pre-image of $\mathcal{H}(y)$ is $1 - \left(1 - 2^{-h}\right)^{(\ell_m - 1)}$. From Section 2.2.1 we know that $\ell_m = \mathcal{O}(n^{1/2})$. In particular, $\ell_m \leq 2\lfloor n^{1/2} \rfloor + 1$, assuming that the rate $R > 1/4$. In practice, if $n = 2^{10}$, then $h = 20$ should be sufficient. In this case, the probability of finding a second pre-image is less than 10^{-4}.

Since we are taking $m = \lfloor n^{1/2} \rfloor$, we get the decryption complexity to be $\mathcal{O}(n^4)$ field operations.

Remark 2.22. The Guruswami–Sudan error correction capacity bound can be improved, for example with the Parvaresh–Vardy [130] or the Guruswami–Rudra algorithm [76], when using folded Reed–Solomon codes. A folded Reed–Solomon code is a Reed–Solomon code viewed over an extension field. We observed, that the folded

Reed–Solomon code cannot be used directly in the key generation, since it is a non-linear code. Nevertheless, one can use a Reed–Solomon code during encryption and fold the received cipher with a folding parameter m. To get a better error correction bound, one needs to bundle the error positions in the encryption step, and in order not to destroy this bundling, one should also use a weight two matrix of block diagonal form. We noted, that the public key is then vulnerable to ISD attack on the smaller subcodes.

2.4.2 Security Against Known Attacks

In this section we will discuss the security of the proposed cryptosystem. Similar to the security analysis of our first proposal, this cryptosystem is potentially vulnerable to the following two structural attacks: Sidelnikov–Sheshtakov attack [153] and the distinguisher attack.

Clearly the attack of Sidelnikov and Shestakov can not be applied, since the public code is not permutation equivalent to the secret GRS code.

The security of the weight two masking is already discussed in [15], a scheme of which the weight two masking is a special case of. The only vulnerability to the scheme of [15] are the attacks based on the Schur product.

2.4.3 Distinguisher Attack Based on the Schur Product

For the definitions and notations of the Schur product and square codes we refer the reader to Section 2.2.1.

In [15], Baldi et al. proposed the BBCRS scheme which uses GRS codes as secret codes and as scrambling matrix the sum $T + R$, where T is a matrix of average row weight m and R is a matrix of rank z, i.e., the public key is

$$SH(T + R),$$

where H is a parity-check matrix of the secret GRS code, and S is an $(n-k)\times(n-k)$ invertible matrix.

In [73], Gauthier-Umaña et al. were able to attack this proposal for $m = 1$, $z = 1$ and $k < \frac{n-2}{2}$ or $k > \frac{n+2}{2}$. This attack is based on the fact that the square code of a GRS code has small dimension. Even after the scrambling with $T + R$, the

square code dimension is still low, whereas for a random secret code, the dimension is with high probability maximal (see [42], [66], [134]). With this they can construct a subcode of the public code, which is also a subcode of a permutation equivalent GRS code to the secret code.

In [52] Couvreur et al. were able to extend this attack for $m \leq 1 + k/n < 2$. In this extended attack it is observed that in the Niederreiter version of the BBCRS scheme puncturing the public code gives a small square code dimension. This helps to detect the weights of the rows of T and reduce to the case $z = 1$ and $m = 1$.

Altough these attacks are only for certain parameters of the BBCRS scheme, it is not excluded that the whole scheme is vulnerable to the Schur product attacks. The purpose of the weight two masking is to be a countermeasure to these attacks. More precisely, we claim that raising m to 2 is enough for the Schur product attacks to fail, which aims in proving that under the weight two masking the square code of the public code has maximal dimension and thus it behaves like a random code. We provide experimental results, which give evidence that this is indeed the case with high probability.

The security of the proposed cryptosystem against the attack based on the Schur product relies on the following: for a parity-check matrix H of any GRS code, and a random matrix Q of constant row weight two, the Schur matrix of HQ has with high probability maximal rank. Moreover, if an attacker tries to puncture, like in [52], the parity-check matrix of the public code, then the shortened code again corresponds to a weight two masked GRS code. As a result, even after puncturing the attacker will be left with a code having maximal square code dimension.

In the experiments, for sufficiently large n the Schur matrix of HQ always had maximal rank. As a consequence, we conjecture the following statement.

Conjecture 2.23. *Let H be a parity-check matrix of a random GRS code of length n and dimension k over a finite field $\mathbb{F}_q$. Let Q represent a weight two matrix having variables $x_1, \ldots, x_n, y_1, \ldots, y_n$ as the nonzero entries. Then, with probability close to 1, the Schur matrix $S(HQ) \in \mathbb{F}_q[x_1, \ldots, x_n, y_1, \ldots, y_n]^{s(n-k)\times n}$ has maximal rank, i.e., there exists a nontrivial $u \times u$ minor of $S(HQ)$, where $u = \min\{s(n-k), n\}$.*

Note that each entry in the i^{th} column of $S(HQ)$ is a homogeneous polynomial of degree 2 in the variables x_i and y_i. Since the variables $y_1, \ldots, y_n$ are representing

nonzero elements of $\mathbb{F}_q$, we can normalize y_i in each column. Hence we can assume that $S(HQ) \in \mathbb{F}_q[x_1, \ldots, x_n]^{s(n-k)\times n}$.

If Conjecture 2.23 holds, we can assume that the nontrivial $u \times u$ minor is the leading $u \times u$ minor, let $p(x_1, \ldots, x_u)$ be this nontrivial $u \times u$ minor. The total degree of p is at most $2u$ and each individual degree $\deg_{x_i}(p)$ is at most 2. We use the Schwartz–Zippel lemma to get a bound on the number of points in $\left(\mathbb{F}_q^\times\right)^u$ where p is non-zero.

Theorem 2.24 (Schwartz–Zippel lemma [143, 165])**.** *Let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ be a nontrivial polynomial of total degree d over a finite field $\mathbb{F}_q$. Let S be a subset of $\mathbb{F}_q$. Then f is nonzero on at least a fraction $\left(1 - \frac{d}{|S|}\right)$ of points in S.*

We apply the Schwartz–Zippel lemma iteratively on each variable of p with $S = \mathbb{F}_q^\times$, to get the following corollary.

Corollary 2.25. *Let $p(x_1, \ldots, x_u)$ be the nontrivial $u \times u$ minor of $S(HQ)$. Then p is nonzero on at least a fraction $\left(1 - \frac{2}{q-1}\right)^u$ of points in $\left(\mathbb{F}_q^\times\right)^u$.*

We performed several experiments for small values of n on different field sizes, and observed that the exact number of weight two matrices giving maximal $S(HQ)$ rank is invariant of the choice of the GRS code. Let $P(q, n)$ denote the fraction of weight two matrices giving maximal $S(HQ)$ rank. For example, let H be a parity-check matrix of a random GRS code of length $n = 8$ and dimension 4 over the field $\mathbb{F}_9$. Then the Corollary 2.25 says that $P(9, 8) \geq (1 - 2/8)^8 = 0.1001$. However we computed the exact value of $P(9, 8) \approx 0.988$, which is much higher than the bound given by Corollary 2.25.

In Section 2.4.4, we see that for fixed field size q and length of the code n, the smallest key size is achieved at the rate $1/2$. Thus for any $n \geq 8$, we have $u = \min\{s(n-k), n\} = n$. The lower bound on $P(q, n)$ is then $(1 - 2/(q-1))^n$. This implies that for a fixed n, the lower bound tends to 1 as q increases. For fixed $n = 8$ and $n = 9$ respectively, we performed Monte-Carlo experiments to get an estimate on the fraction $P(q, n)$ for increasing q. These tests were made with Sage [155] taking 10^7 random constant row weight two matrices Q. In Figure 2.3 and Figure 2.4, corresponding to $n = 8$ and $n = 9$ respectively, we observe that the estimated value of $P(q, n)$ tends to 1 much faster than the Schwartz-Zippel lower bound.

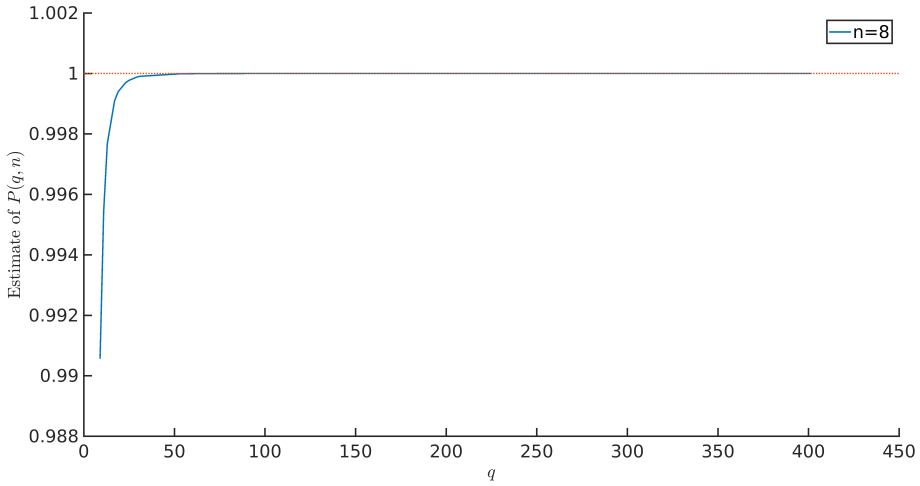

FIGURE 2.3: Estimate of $P(q, 8)$ obtained from Monte-Carlo tests on 10^7 weight two matrices

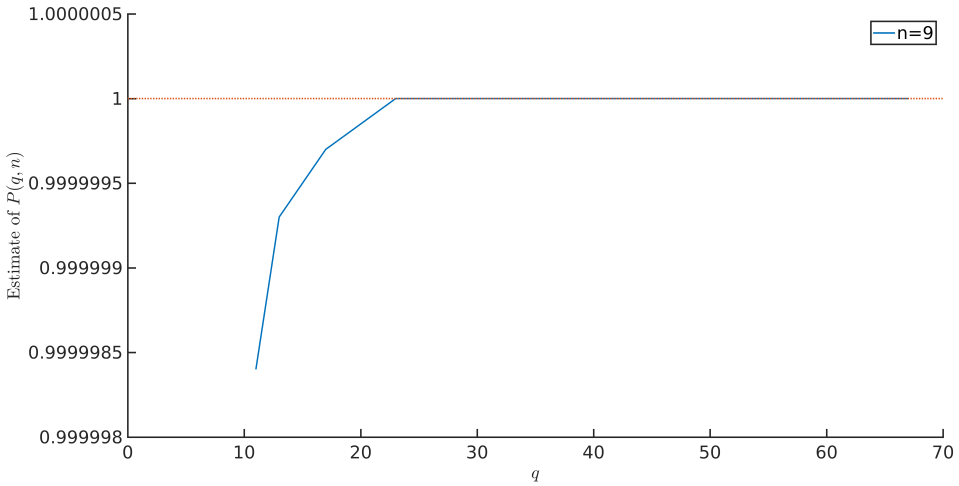

FIGURE 2.4: Estimate of $P(q, 9)$ obtained from Monte-Carlo tests on 10^7 weight two matrices

In further experiments for $n \geq 12$, we noticed the rank of the Schur matrix $S(HQ)$ for a randomly chosen weight two matrix Q is always maximal. Experimental and therotical ananlysis on the rank of Schur matrix is also presented in detail by Weger in [159]. As a conclusion, these experiments tend to imply that our cryptosystem is not vulnerable to the attacks based on Schur product of the public matrix.

2.4.4 Parameters

In this section we find the best set of parameters that minimizes the public key size of the proposed cryptosystem with or without using list decoding, for fixed security against ISD attacks. In particular, we compute the parameters following the complexity of the generalized ball-collision ISD algorithm presented in [87]. The ISD attack takes as input q, n, k, t, where t is the weight of the error vector. In the case of the weight two masking with list decoding we introduce the rate $R = \frac{k}{n}$ and the interpolation multiplicity $m = \lfloor n^{1/2} \rfloor$ and we have

$$t = \left\lfloor \frac{n}{2} \left(1 - \sqrt{R \left(\frac{m+1}{m} \right)} \right) \right\rfloor .$$

In the case of the weight two masking without list decoding we have

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor /2.$$

In both the cases, the public key is a parity-check matrix of a linear code over $\mathbb{F}_q$ having length n and dimension k. Hence the public key size is

$$k(n-k)\log_2(q) \text{ bits.}$$

In Table 2.5, we provide the key sizes for different rates of the public code of the proposed cryptosystem with list decoding, achieving a 128-bit security level against the ISD algorithm. Observe that the smallest key size is achieved at rate 0.5. In Table 2.6, we do the same for the proposed cryptosystem without using list decoding. In this case, $t = \lfloor \frac{n-k}{2} \rfloor /2$ and the smallest key size is achieved at rate 0.7.

In Table 2.7, we provide the key sizes for different rates of the public code of the proposed cryptosystem with list decoding, achieving a 256-bit security level against the ISD algorithm. Observe that the smallest key size is achieved at rate 0.6. In Table 2.8, we do the same for the proposed cryptosystem without using list decoding. In this case, $t = \lfloor \frac{n-k}{2} \rfloor /2$ and the smallest key size is achieved at rate 0.75.

In the next section, we compare these optimized key sizes with different cryptosystems.

Rate	q	n	k	t	Key Size (bits)
0.30	821	818	245	181	1359101
0.35	769	765	267	152	1274724
0.40	733	732	292	130	1222830
0.45	709	708	318	112	1174425
0.50	709	702	351	98	1166660
0.55	709	708	389	86	1175097
0.60	727	726	435	76	1203293
0.65	751	750	487	67	1223515
0.70	797	796	557	59	1283098

TABLE 2.5: Comparing key sizes of the proposed cryptosystem using list decoding for different rates having 128-bit security against ISD attack

Rate	q	n	k	t	Key Size (bits)
0.30	1061	1056	316	185	2350375
0.40	877	875	350	131	1796420
0.50	797	791	395	99	1507644
0.60	769	759	455	76	1326052
0.65	769	767	498	67	1284272
0.70	787	785	549	59	1246434
0.75	839	829	621	52	1254548
0.80	919	916	732	46	1325858
0.85	1039	1034	878	39	1372554

TABLE 2.6: Comparing key sizes of the proposed cryptosystem without using list decoding for different rates having 128-bit security against ISD attack

Rate	q	n	k	t	Key Size (bits)
0.30	1801	1800	540	401	7358242
0.35	1693	1680	588	336	6886719
0.40	1601	1600	640	287	6540139
0.45	1553	1550	697	248	6302635
0.50	1523	1516	760	215	6074693
0.55	1523	1520	836	189	6045724
0.60	1543	1541	924	166	6038312
0.65	1601	1595	1036	146	6164635
0.70	1693	1685	1179	129	6398475

TABLE 2.7: Comparing key sizes of the proposed cryptosystem using list decoding for different rates having 256-bit security against ISD attack

Rate	q	n	k	t	Key Size (bits)
0.30	2467	2359	707	413	13161251
0.40	1949	1948	779	292	9952066
0.50	1747	1744	872	218	8189841
0.60	1669	1668	1000	167	7150785
0.65	1693	1678	1090	147	6874102
0.70	1721	1717	1201	129	6661347
0.75	1811	1805	1353	113	6618608
0.80	1973	1957	1565	98	6715260
0.85	2237	2234	1898	84	7096222

TABLE 2.8: Comparing key sizes of the proposed cryptosystem without using list decoding for different rates having 256-bit security against ISD attack

2.5 Comparison

In this section we compare the two cryptosystem proposed in this chapter with two other McEliece based cryptosystems. The first one is the classical McEliece cryptosystem, which is one of the most promising candidates in the ongoing competition of post-quantum cryptosystems organized by NIST. The second one is the BBCRS cryptosystem [15, 16].

The BBCRS cryptosystem is also a variant of McEliece cryptosystem, where the authors proposed to hide the structure of the secret GRS code using as transformation matrix the sum of a rank z matrix and a weight w matrix. The proposed parameters in [15, 16] with $z = 1$ and $w \leq 1 + R$ were broken by the square code attack [49, 52], where R denotes the rate of the code. Two countermeasures were recently proposed in [18, 93]. In order to hide the structure of the Reed–Solomon code the authors of [18] use $w > 1 + R$ and $z = 1$ or $w < 1 + R$ and $z > 1$.

In Table 2.9 and Table 2.10 we do the comparison for fixed 128-bit and 256-bit security level, respectively. For the proposed variant based on expanded GRS codes, we provide two sets of parameter, namely Type I and Type II. For the proposed variant based on weight two masking of GRS codes, we provide two kinds: with list decoding and without list decoding.

Compared to the classical McEliece cryptosystem, the proposal based on expanded GRS codes with Type I set of parameters reduces the key size by 42.17% for 128-bit security level and by 44.8% for 256-bit security level. On the other hand, weight two masking with list decoding improves the key size by 24.1% for 128-bit

	q	m	n	k	Key Size (in bits)
Expanded GRS Type I	9	3	577	461	889125
Expanded GRS Type II	7	4	824	716	1474737
Weight-two masking with list decoding	709	1	702	351	1166669
Weight-two masking without list decoding	787	1	785	549	1246434
classical McEliece	2	12	2960	2288	1537536
BBCRS [18] ($w = 1.7$ and $z = 1$)	653	1	652	357	990900
BBCRS [18] ($w = 1.2$ and $z = 10$)	563	1	562	438	548512

TABLE 2.9: Comparing the key sizes of different McEliece-based cryptosystems having 128-bit security.

	q	m	n	k	Key Size (in bits)
Expanded GRS Type I	13	3	1258	1031	4624198
Expanded GRS Type II	7	4	1872	1666	6754721
Weight-two masking with list decoding	1543	1	1541	924	6038312
Weight-two masking without list decoding	1811	1	1805	1353	6618608
classical McEliece	2	13	6960	5413	8373911
BBCRS [18] ($w = 1.708$ and $z = 1$)	1423	1	1422	786	5251176
BBCRS [18] ($w = 1.2$ and $z = 10$)	1163	1	1162	928	2330748

TABLE 2.10: Comparing the key sizes of different McEliece-based cryptosystems having 256-bit security.

security level and by 27.9% for 256-bit security level.

2.6 Conclusion

In this chapter we presented two code-based cryptosystem, using two different ways of disguising a Reed–Solomon codes.

In the first cryptosystem, we used shortened expanded Reed–Solomon codes as the secret codes. We observed that shortening an expanded Reed–Solomon on random indices destroys the algebraic structure present in expanded Reed–Solomon codes. We allowed errors in burst pattern, this increases the error-correction capacity of the secret code. As a consequence, we achieved better key sizes than the classical McEliece cryptosystem. In particular, for 128-bit security level against modified ISD attack we improved the key sizes by 42% compared to the classical McEliece cryptosystem. Also notice that, the classical McEliece cryptosystem can be thought of as a special case of this construction: binary Goppa codes are subfield subcodes of a GRS code and hence a shortening of an expanded GRS code with $\lambda = 1$. This leads us to ask a question about an optimum trade-off between algebraic security and key size.

The second cryptosystem uses a Reed–Solomon code as the secret code and an invertible matrix of constant row weight two for masking. This masking appears to be hiding the algebraic structure of the private Reed–Solomon code against all known attacks. In particular, we analyzed the effect of the weight two masking on the security against the attack based on the Schur product, which has become an enormous threat to code-based cryptosystems. Furthermore, with a view to reduce the key size, we used the Guruswami–Sudan list decoding algorithm in the decryption step. We recovered the original message from the list by marking the message using its hash value. List decoding allowed us to correct more errors compared to unique decoding and hence results in smaller key sizes. For example, for 128-bit security level against ISD attack, the key size of the proposed cryptosystem is 1166669 bits, which is 24% less than the key size of the standard McEliece cryptosystem proposed by Bernstein et al. in [30]. On mathematical side, an open problem would be to prove Conjecture 2.23, which states that weight-two masking of Reed–Solomon codes have full square code dimension with high probability.

Chapter 3

Cryptanalysis of Noncommutative Cryptographic Protocols

In this chapter, we shift our focus to group based cryptography. It is the area of cryptology, where the cryptographic protocols are based on algebraic structures like semigroups, groups and rings, mostly noncommutative.

This chapter is based on the following paper:

- Karan Khathuria, Giacomo Micheli, and Violetta Weger. "On the Algebraic Structure of $E_p^{(m)}$ and Applications to Cryptography". In: *Applicable Algebra in Engineering, Communication and Computing* (2019). ISSN: 1432-0622. DOI: https://doi.org/10.1007/s00200-019-00410-1
  The paper presents a polynomial time attack on the protocol based on the Diffie–Hellman decomposition problem and the ElGamal decomposition problem over the noncommutative ring $E_p^{(m)}$.

In this thesis, using the techniques presented in the above paper, we also break the protocol based on the semigroup action problem (SAP) over $E_p^{(m)}$ in cubic time. Moreover, we present an algorithm to solve a linear system over the ring $E_p^{(m)}$. These two results, presented in Section 3.5 and 3.6, are original and do not appear in any research articles.

3.1 Introduction

Public-key cryptosystems are often based on number theoretical problems, such as integer factorization as in RSA [140] or the discrete logarithm problem over finite fields or over elliptic curves. The latter is the base for well known protocols,

such as the ElGamal protocol [61] or the Diffie–Hellman key exchange protocol [56]. Increasing computing powers threaten these classical cryptographic schemes and new ambient spaces are demanded, for example involving noncommutative structures (see [6, 96, 97, 142, 151]).

In this chapter we will deal with cryptographic schemes that are based on the following two problems over nonabelian groups: the semigroup action problem (SAP), and the decomposition problem (DP). For an overview see Section 3.2.2.

Based on these two problems, J.J. Climent and J.A. López-Ramos proposed three protocols in [47] over a special ring of matrices, called $E_p^{(m)}$. It involves operations modulo different powers of the same prime. Similar cryptosystems can be found in [107, Example 4.3.c]. The ring $E_p^{(m)}$ is a generalization of the ring E_p, that Climent, Navarro and Tartosa introduced in [46]. The first cryptographic scheme based on E_p [45], was broken in [90]. This attack can be prevented by admitting only few invertible elements, as it is the case in the ring $E_p^{(m)}$ [44, Corollary 1]. In addition, another nice property of such rings is that they do not admit embeddings into matrix rings over a field (see [24]). This is often the main problem of cryptographic schemes over matrix rings (see for example [119]) and it prevents a reduction to small extensions of finite fields as in [117].

The first protocol proposed in [47] by Climent and López-Ramos is based on the semigroup action problem over the ring $E_p^{(m)}$. It was broken by Micheli and Weger in [120] using a solution sieve argument. The remaining two protocols proposed in [47] are based on the decomposition problem over $E_p^{(m)}$ and hence are equivalent with respect to security. They will be referred to as the Diffie–Hellman Decomposition Problem (DHDP) and the ElGamal Decomposition Problem (EGDP), respectively. A cryptanalysis of these two protocols was considered by Zhang in [164], where the Cayley–Hamilton Theorem is used to derive a linear system over $E_p^{(m)}$. However, even though the main idea is correct, the system over $E_p^{(m)}$ is then directly considered over $\mathbb{Z}/p^m\mathbb{Z}$, where the system does not necessarily admits a solution, as we will show in an example in Section 3.7.1. The running time of the claimed attack is $\mathcal{O}(m^7)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations.

In this chapter, we introduce a new approach for solving linear systems over $E_p^{(m)}$, where we consider an auxilary $\mathbb{Z}/p^m\mathbb{Z}$-module that is isomorphic to $E_p^{(m)}$. As an application, we efficiently break all the protocols proposed in [47]. In particular, this new approach solves the semigroup action problem in $\mathcal{O}(m^3)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations,

and the decomposition problem in $\mathcal{O}(m^6)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations.

3.2 Preliminaries

In the first part of this section, we recall some notions of noncommutative rings and modules that we will be using in this chapter. Later in the second part, we define some generic problems based on semigroups that have applications in the construction of different cryptographic protocols.

3.2.1 Semigroups, Rings and Modules

A *semigroup* G is a set equipped with an associative binary operation $\cdot : (x, y) \mapsto x \cdot y$. Thus, semigroups can be considered as generalizations of groups, by dropping the existence of an identity element and inverses. Similarly, we can generalize group actions to define semigroup actions: let G be a semigroup and S be a set. Then we say G *acts on* S if there exists a map $\phi : G \times S \to S$, such that for all $x, y \in G$ and $s \in S$, $\phi(x \cdot y, s) = \phi(x, \phi(y, s))$.

Let R be a (possibly noncommutative) ring, and let T be a subset of R. We define the *centralizer* of T as the set of elements in R that commutes with the elements of T, i.e.,

$$\mathrm{Cen}(T) = \{r \in R \mid rt = tr \ \forall \ t \in T\}.$$

Notice that $\mathrm{Cen}(T)$ is a subring of R. When $T = R$, then $\mathrm{Cen}(R)$ is said to be the *center* of R and will be denoted by $Z(R)$.

Let $\mathbb{N}$ denote the natural numbers, i.e., $\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For any commutative ring R, and any two positive integers $k, m \in \mathbb{N}$ we will denote by $\mathrm{Mat}_{k\times m}(R)$ the set of $k \times m$ matrices with coefficients in R.

If M is an abelian group and R is a ring acting on M, we denote by $\mathrm{End}_R(M)$ the set of endomorphisms of M as an R-module. Notice that $\mathrm{End}_R(M)$ has a natural ring structure, which contains R as a subring. Let $\phi \in \mathrm{End}_R(M)$, we denote by $R[\phi]$ the smallest subring of $\mathrm{End}_R(M)$ which contains R and ϕ.

One of the main result that we will be using in our cryptanalysis is the Cayley–Hamilton theorem over a ring R.

Theorem 3.1. *[9, Proposition 2.4] Let R be a ring, let M be a finitely generated R-module, let $\phi : M \to M$ be a module morphism and let $I \subset R$ be an ideal of R, such that $\phi(M) \subseteq IM$. Let $n \in \mathbb{N}$ be the number of elements needed to generate M. Then there exist $a_{n-1}, \ldots, a_0 \in I$, such that*

$$\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 = 0.$$

Proof. Let $\{x_1, \ldots, x_n\}$ be a set of generators of M. Since $\phi(M) \subseteq IM$, for each $1 \leq i \leq n$ we have

$$\phi(x_i) = \sum_{j=1}^{n} a_{i,j} x_j$$

for some $a_{i,j} \in I$. This implies

$$\sum_{j=1}^{n} (\delta_{i,j}\phi - a_{i,j}) x_j = 0,$$

where $\delta_{i,j}$ is the Kronecker delta. Now, by left multiplication with the adjoint of the matrix $[\delta_{i,j}\phi - a_{i,j}]_{i,j}$, we deduce that $\det([\delta_{i,j}\phi - a_{i,j}]_{i,j}) \cdot x_k = 0$ for each $1 \leq k \leq n$. But since $\det([\delta_{i,j}\phi - a_{i,j}]_{i,j})$ is a degree n monic polynomial in ϕ with coefficients in I, we have the desired form. □

3.2.2 The Semigroup Action Problem and the Decomposition Problem

Many cryptographic protocols are based on nonabelian algebraic structures, such as groups, semigroups and rings. A subclass of such protocols are based on the difficulty of solving the following two problems:

Definition 3.2 (Semigroup Action Problem (SAP))**.** Let G be a finite semigroup acting on a set S. Given $a, b \in S$ such that $b = g \cdot a$ for some $g \in G$, find $g' \in G$ such that $b = g' \cdot a$.

Definition 3.3 (Decomposition Problem (DP))**.** Let G be a semigroup, $A, B \subseteq G$ be two subsemigroups such that $a \cdot b = b \cdot a$ for every $a \in A$ and $b \in B$. Given two elements $a_1 \cdot x \cdot a_2$ and $b_1 \cdot x \cdot b_2$, with $x \in G$, $a_1, a_2 \in A$ and $b_1, b_2 \in B$, find the element $a_1 \cdot b_1 \cdot x \cdot b_2 \cdot a_2$.

Cryptographic Protocols Based on SAP: In [113], Maze et al. introduced the SAP and generalized the Diffie–Hellman key exchange protocol and the ElGamal protocol.

Protocol 3.4 (Diffie–Hellman protocol using semigroup action)**.** *Let G be a semigroup acting on a set S via ϕ. Let G, S and $s \in S$ be publicly known.*

1. *Alice chooses $x \in G$, computes $x \cdot s$ and sends it to Bob.*
2. *Bob chooses $y \in G$, computes $y \cdot s$ and sends it to Alice.*
3. *The exchanged key is then*

$$x \cdot (y \cdot s) = (xy) \cdot s = (yx) \cdot s = y \cdot (x \cdot s).$$

Note that $x, y \in G$ are chosen, such that they commute with each other. In practice, this is achieved by choosing x, y from a publicly known subsemigroup $H \leq G$, where the elements commute with each other.

Protocol 3.5 (ElGamal protocol using semigroup action)**.** *Let G be a semigroup acting on a set S via ϕ. Let G, S and $s \in S$ be publicly known. Let $m \in S$ be the message that Bob wants to send to Alice.*

1. *Alice chooses $x \in G$, computes $t = x \cdot s$. She publishes y and keeps x private.*
2. *Bob chooses randomly $y \in G$, and computes*

$$c_1 = y \cdot s, c_2 = m + y \cdot t$$

3. *Bob sends (c_1, c_2) to Alice.*
4. *Alice recovers the message m by computing*

$$c_2 - x \cdot c_1 = m + y \cdot (x \cdot s) - x \cdot (y \cdot s) = m$$

Note that $x, y \in G$ are chosen, such that they commute with each other. Similar to Protocol 3.4 this is achieved by choosing x, y from a publicly known subsemigroup $H \leq G$, where the elements commute with each other.

Cryptographic Protocols Based on DP: In [149], Shpilrain–Zapata presented the Commuting Action Key Exchange (CAKE) protocol based on the decomposition problem over a semigroup G.

Protocol 3.6 (CAKE protocol)**.** *Let G be a semigroup, $A, B \subseteq G$ be two subsemigroups such that $a \cdot b = b \cdot a$ for every $a \in A$ and $b \in B$ and assume that $x \in G$. Here G, A, B and x are publicly known.*

1. *Alice chooses $a_1, a_2 \in A$ and sends $a_1 \cdot x \cdot a_2$ to Bob.*
2. *Bob chooses $b_1, b_2 \in B$ and sends $b_1 \cdot x \cdot b_2$ to Alice.*
3. *The exchanged key is then*

$$a_1 \cdot b_1 \cdot x \cdot b_2 \cdot a_2 = a_1 \cdot (b_1 \cdot x \cdot b_2) \cdot a_2 = b_1 \cdot (a_1 \cdot x \cdot a_2) \cdot b_2.$$

3.3 The Ring $E_p^{(m)}$

In this section we introduce the ring $E_p^{(m)}$ and discuss some properties of it. Let p be a prime integer and m be a positive integer, then the definition of the matrix ring $E_p^{(m)}$ is as follows:

Definition 3.7. Let $E_p^{(m)}$ be the following set of matrices.

$$E_p^{(m)} = \left\{ (a_{i,j})_{i,j\in\{1,\dots,m\}} \;\middle|\; a_{i,j} \in \mathbb{Z}/p^i\mathbb{Z} \text{ if } i \le j, \text{ and } a_{i,j} \in p^{i-j}\mathbb{Z}/p^i\mathbb{Z} \text{ if } i > j \right\}.$$

See Figure 3.1 for an illustration of the structure of a matrix in $E_p^{(m)}$. To shorten the notation we will write $[a_{i,j}] = (a_{i,j})_{i,j\in\{1,\dots,m\}}$. This set forms a ring with the addition and multiplication defined, respectively, as follows

$$\begin{aligned} [a_{i,j}] + [b_{i,j}] &= \left[(a_{i,j} + b_{i,j}) \bmod p^i \right], \\ [a_{i,j}] \cdot [b_{i,j}] &= \left[\left(\sum_{k=1}^{m} a_{ik} b_{kj} \right) \bmod p^i \right]. \end{aligned}$$

We clearly see that $E_p^{(m)}$ cannot be embedded in the matrix ring over any commutative ring. However, if one considers $V = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$ as a $\mathbb{Z}$-module, then $E_p^{(m)}$ is isomorphic to $\mathrm{End}_{\mathbb{Z}}(V)$ as rings. The case of $m = 2$ was proved in [46, Theorem 3], which can be directly generalized to any m.

$$\begin{pmatrix} \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} & \cdots & \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} & \cdots & \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} \\ \vdots & & \ddots & & \vdots \\ p^{m-2}\mathbb{Z}/p^{m-1}\mathbb{Z} & p^{m-3}\mathbb{Z}/p^{m-1}\mathbb{Z} & \cdots & \mathbb{Z}/p^{m-1}\mathbb{Z} & \mathbb{Z}/p^{m-1}\mathbb{Z} \\ p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p\mathbb{Z}/p^m\mathbb{Z} & \mathbb{Z}/p^m\mathbb{Z} \end{pmatrix}$$

FIGURE 3.1: Illustration of the structure of a matrix in $E_p^{(m)}$.

The cardinality of the ring $E_p^{(m)}$ is $p^{(2m^3+3m^2+m)/6}$, which can be proved using induction on m (see [44, Theorem 2]). The invertible elements in $E_p^{(m)}$ can be characterized as follows:

Theorem 3.8. *[44, Theorem 3, Corollary 1] Let $A = [a_{i,j}] \in E_p^{(m)}$. Then A is invertible if and only if $a_{i,i} \mod p \neq 0$ for all $i \in \{1, \ldots, m\}$. The number of invertible elements in $E_p^{(m)}$ is $p^{(2m^3+3m^2-5m)/6}$.*

This shows that the fraction of invertible elements in $E_p^{(m)}$ is $\left(\frac{p-1}{p}\right)^m$. With security point of view, having a low number of invertible elements is a desirable feature of the cryptographic protocols presented in [44, 47].

Theorem 3.9. *[47, Theorem 2] The center of $E_p^{(m)}$ is given by the set*

$$Z\left(E_p^{(m)}\right) = \left\{ [a_{i,j}] \in E_p^{(m)} \;\middle|\; a_{i,i} = \sum_{j=0}^{i-1} p^j u_j \text{ with } u_j \in \mathbb{Z}_p, \text{ and } a_{i,j} = 0 \text{ if } i \neq j \right\}.$$

As a corollary of this theorem we see that $Z\left(E_p^{(m)}\right)$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$ as rings.

Corollary 3.10. *The center of the ring $E_p^{(m)}$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$ as rings.*

Proof. It is easy to see that the following map is a ring isomorphism

$$\begin{aligned} \psi : \mathbb{Z}/p^m\mathbb{Z} &\to Z(E_p^{(m)}), \\ z &\mapsto [a_{i,j}], \end{aligned}$$

where $a_{i,i} = z \mod p^i$ and $a_{i,j} = 0$ for $i \neq j$. □

For $M \in E_p^{(m)}$, let us denote by $\mathrm{Cen}(M)$ the centralizer of M, i.e., the set of elements $X \in E_p^{(m)}$, such that $XM = MX$. It is not easy to characterize all the elements in $\mathrm{Cen}(M)$, but using the center of $E_p^{(m)}$ we obtain the following subring of $\mathrm{Cen}(M)$,

$$H(M) = \left\{ \sum_{i=0}^{k} C_i M^i \;\middle|\; C_i \in Z(E_p^{(m)}), k \in \mathbb{N} \right\}.$$

Using the fact that $E_p^{(m)}$ is isomorphic to the ring $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z})$, and the Cayley–Hamilton Theorem (see Theorem 3.1), we can prove that the subring generated by a matrix in $E_p^{(m)}$ is a finite dimensional $\mathbb{Z}$-module.

Lemma 3.11. *For every $A \in E_p^{(m)}$, there exists $a_0, \ldots, a_{m-1} \in \mathbb{Z}$, such that*

$$A^m = a_0 + a_1 A + \cdots a_{m-1} A^{m-1}.$$

Proof. In Theorem 3.1, set $I = R = \mathbb{Z}$ and $M = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$, hence $n = m$ and ϕ is a matrix in $E_p^{(m)}$. It follows now immediately that $\mathbb{Z}[\phi]$ has dimension less than or equal to m (as a $\mathbb{Z}$-module). □

Remark 3.12. Notice that in the statement and the proof of Lemma 3.11, $\mathbb{Z}$ could as well be replaced by $\mathbb{Z}/p^m\mathbb{Z}$ since any element in $p^m\mathbb{Z}$ acts as the zero morphism over M.

Proposition 3.13. *Let $M \in E_p^{(m)}$. Then the map $\psi : (\mathbb{Z}/p^m\mathbb{Z})[x] \to H(M)$ given by $\psi(f(x)) = f(M)$ is a surjective $\mathbb{Z}/p^m\mathbb{Z}$-algebra homomorphism.*

Proof. First, using Corollary 3.10 one can identify the center of $E_p^{(m)}$ with $\mathbb{Z}/p^m\mathbb{Z}$, from which follows that the map is well defined. It is easy to check that ψ is a $\mathbb{Z}/p^m\mathbb{Z}$-algebra homomorphism.

Finally, the map ψ is surjective because $H(M) \cong (\mathbb{Z}/p^m\mathbb{Z})[M]$: in fact, using Corollary 3.10, for $\sum_{i=0}^{k} C_i M^i \in H(M)$ there exist $u_0, \ldots, u_k \in \mathbb{Z}/p^m\mathbb{Z}$ such that each C_i is the diagonal matrix with entries $(u_i \mod p, u_i \mod p^2, \ldots, u_i \mod p^m)$. □

3.4 Cryptographic Protocols from the Ring $E_p^{(m)}$

In [47], Climent and López-Ramos proposed three protocols over the ring $E_p^{(m)}$. The first one is a public-key cryptosystem based on the semigroup action problem over

$E_p^{(m)}$. The other two are based on the decomposition problem over $E_p^{(m)}$, a Diffie–Hellman key exchange protocol and an ElGamal protocol, both analogous to the Diffie–Hellman key exchange [56] and the ElGamal cryptosystem [61], respectively.

3.4.1 A Public-Key Cryptosystem Based on the Semigroup Action Problem

The first protocol, a public-key cryptosystem, is based on the action of $E_p^{(m)}$ over the set $V = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$, given by the usual matrix-vector multiplication.

Protocol 3.14 (SAP protocol)**.** *Let $M \in E_p^{(m)}$ be a publicly known, and $S \in V$ be a message that Bob wants to send to Alice.*

1. *Alice chooses $F \in \mathrm{Cen}(M)$ and $R \in V$, and computes $T = F \cdot R$.*
2. *Alice publishes (R, T) and keeps private F.*
3. *Bob chooses randomly $G \in H(M)$, and computes*

$$H = G \cdot R, \quad D = S + G \cdot T.$$

4. *Bob send (H, D) to Alice.*
5. *Alice recovers the message S by computing*

$$D - F \cdot H = S + G \cdot F \cdot R - F \cdot G \cdot R = S.$$

Note that as $F, G \in \mathrm{Cen}(M)$, they commute with each other.

The basis for the security of the protocol is the difficulty of solving the SAP for the action of $E_p^{(m)}$ over the set V, i.e., given $R \in V$ and $T = F \cdot R \in V$, find $X \in E_p^{(m)}$ such that $T = X \cdot R$. Note that in Protocol 3.14 we are also given that $F \in \mathrm{Cen}(M)$ and M is publicly known. Hence this reduces to solving the following system of linear equations

$$\begin{aligned} X \cdot M &= M \cdot X, \\ X \cdot R &= T, \end{aligned} \tag{3.1}$$

where $X, M \in E_p^{(m)}$ and $R, T \in V$. The system (3.1) breaks down to solving m systems of linear congruences moduli p^i for each $i \in \{1, 2, \ldots, m\}$. In [120], Micheli

and Weger used this observation to break the SAP protocol using $\mathcal{O}(m^9)$ $\mathbb{Z}/p^m\mathbb{Z}$ operations. The main idea in [120] is to iteratively compute the solution space of the system of linear congruences modulo p^i and adjoining them with the system of linear congruences modulo p^{i-1}.

Synopsis of the Micheli–Weger Attack on the SAP Protocol

To attack the SAP protocol we are looking for $X \in E_p^{(m)}$ that satisfies (3.1). Let the entries of $X = [x_{i,j}]$ be the unknowns, represented by the vector $x = (x_{i,j})$. Then (3.1) breaks down into m systems of linear congruences modulo p^i for each $i \in \{1, 2, \ldots, m\}$. Let these system be represented by the equations

$$A^{(i)}x = b_i \mod p^i, \tag{3.2}$$

for all $i \in \{1, \ldots, m\}$, for some $A^{(i)} \in \mathrm{Mat}_{(2m-i+1)\times m^2}(\mathbb{Z})$ and $b_i \in \mathbb{Z}^{2m-i+1}$. The equations in the system (3.2) are constructed in the following way: for each $i \in \{1, \ldots, m\}$, the i-th row of $XM = MX$ gives rise to m equations modulo p^i, the i-th entry of $XR = T$ gives one additional equation, and the remaining $m-i$ equations are coming from the condition $x_{s+i,s} \equiv 0 \mod p^i$ for each $s \in \{1, \ldots, m-i\}$.

A common solution to the congruence systems in (3.2) is obtained by solving them iteratively in backward direction. So, we start by solving the m-th system, i.e., $A^{(m)}x = b_m \mod p^m$, to obtain the solution space V_m. Now, in the next step, while solving the $(m-1)$-th system, we impose the condition on x to lie in the previous step's solution space V_m. As a result we obtain a solution space V_{m-1}, which solves both the systems m and $m-1$. We carry on in the similar way until we obtain a common solution to all the m systems. For more details we refer the reader to [120, Proposition 15].

The i-th step of this attack involves solving a system of linear equations in m^2 unknowns over $\mathbb{Z}/p^{m-i}\mathbb{Z}$. In [120, Lemma 13], Micheli and Weger provide a method to solve such a system by computing the Smith normal form of the corresponding rectangular matrix over $\mathbb{Z}/p^{m-i}\mathbb{Z}$, which has a complexity of $\mathcal{O}((m^2)^4)$ $\mathbb{Z}/p^{m-i}\mathbb{Z}$ operations. Hence, the overall complexity of the attack is $\mathcal{O}(m^9)$ $\mathbb{Z}/p^m\mathbb{Z}$ operations.

3.4.2 A Key-Exchange and a Public-Key Cryptosystem Based on the Decomposition Problem

In the same paper of the SAP protocol, Climen and López-Ramos presented two more protocols based on the decomposition problem over $E_p^{(m)}$. The first one is a key exchange protocol based on the idea of Commuting Action Key Exchange (CAKE) from [149]. The second one is a public-key protocol analogues to the ElGamal cryptosystem [61].

Protocol 3.15 (DHDP protocol)**.** *Alice and Bob agree on two public elements $M, X \in E_p^{(m)}$, such that $M \notin \mathrm{Cen}(X)$.*

1. *Alice chooses $A_1, A_2 \in H(M)$ and sends $G_A = A_1 X A_2$ to Bob.*
2. *Bob chooses $B_1, B_2 \in \mathrm{Cen}(M)$ such that $B_1 X \neq X B_2$ and sends $G_B = B_1 X B_2$ to Alice.*
3. *Alice computes $A_1 G_B A_2$.*
4. *Bob computes $B_1 G_A B_2$.*

Since A_i and B_i commute for all $i \in \{1, 2\}$, it is clear that Alice and Bob share a common value.

The basis for the security of the DHDP protocol is the difficulty of solving the decomposition problem (DP) for the ring $E_p^{(m)}$ and subrings $\mathrm{Cen}(M)$ and $H(M)$, i.e., given $A_1 X A_2$ and $B_1 X B_2 \in E_p^{(m)}$ for some $X \in E_p^{(m)}$, $A_1, A_2 \in H(M)$ and $B_1, B_2 \in \mathrm{Cen}(M)$, find $A_1 B_1 X B_2 A_2$ or $B_1 A_1 X A_2 B_2$.

Protocol 3.16 (EGDP protocol)**.** *Alice and Bob agree on a public element $M \in E_p^{(m)}$. Let $S \in E_p^{(m)}$ be the secret that Bob wants to send Alice.*

1. *Alice chooses $N \in E_p^{(m)}$, such that $NM \neq MN$ and two elements $A_1, A_2 \in H(M)$ and publishes her public key $(N, A_1 N A_2)$.*
2. *Bob chooses randomly two elements $B_1, B_2 \in \mathrm{Cen}(M)$ and sends $(F, D) = (B_1 N B_2, S + B_1 A_1 N A_2 B_2)$ to Alice.*
3. *Alice recovers S by computing $D - A_1 F A_2$.*

Since A_i and B_i commute for all $i \in \{1, 2\}$, we have that

$$D - A_1 F A_2 = S + B_1 A_1 N A_2 B_2 - A_1 B_1 N B_2 A_2 = S.$$

The security of the EGDP protocol also relies on the DP problem over $E_p^{(m)}$.

Proposition 3.17. *[47, Theorem 4] Breaking the EGDP protocol is equivalent to solving the decompostion problem (DP).*

Proof. Consider M, N, B_1, B_2, A_1, A_2 as given in the EGDP protocol. Let the ciphertext be given by

$$(F, D) = (B_1 N B_2, S + B_1 A_1 N A_2 B_2),$$

where S is the message that an attacker wants to recover. Assume that the attacker can solve the DP. The attacker knows the public key $A_1 N A_2$ and the first part of the ciphertext $F = B_1 N B_2$, hence by solving the DP with these inputs she computes $B_1 A_1 N A_2 B_2$. By simply subtracting this from D, she recovers the sent message S.

Now assume the attacker can break the EGDP protocol, and given $B_1 N B_2$, $A_1 N A_2$ she wants to compute $B_1 A_1 N A_2 B_2$. She intercepts a random ciphertext (F, D) of the EGDP protocol. Then she attacks the protocol to obtain the plaintext S and subtracts it from D to obtain $B_1 A_1 N A_2 B_2$. □

3.5 Solving a System of Linear Equations over $E_p^{(m)}$

As observed by Micheli and Weger in [120], a crucial step in cryptanalyzing the protocols based on $E_p^{(m)}$ is solving a system of linear congruences over different moduli. In particular, solving the system (3.1) efficiently would break the SAP protocol. Moreover, in Section 3.7 we will see that the decomposition problem also reduces to solving a system of linear congruences over different moduli.

In this section, we provide a new way of solving a linear system over $E_p^{(m)}$, without going through different moduli. To do this, we define a $\mathbb{Z}/p^m\mathbb{Z}$-submodule of the matrix ring $\mathrm{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$, which will be used to translate the equations over $E_p^{(m)}$ to equations over this new $\mathbb{Z}/p^m\mathbb{Z}$-module.

Definition 3.18. Let $F_p^{(m)} \subseteq \mathrm{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$ be the following set of matrices.

$$F_p^{(m)} = \left\{ (a_{i,j})_{i,j\in\{1,\dots,m\}} \mid a_{i,j} \in p^\ell \mathbb{Z}/p^m\mathbb{Z} \text{ where } \ell = \max(m-i, m-j) \right\}.$$

$$\begin{pmatrix} \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} & \cdots & \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ p\mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} & \cdots & \mathbb{Z}/p^2\mathbb{Z} & \mathbb{Z}/p^2\mathbb{Z} \\ \vdots & & \ddots & & \vdots \\ p^{m-2}\mathbb{Z}/p^{m-1}\mathbb{Z} & p^{m-3}\mathbb{Z}/p^{m-1}\mathbb{Z} & \cdots & \mathbb{Z}/p^{m-1}\mathbb{Z} & \mathbb{Z}/p^{m-1}\mathbb{Z} \\ p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p\mathbb{Z}/p^m\mathbb{Z} & \mathbb{Z}/p^m\mathbb{Z} \end{pmatrix}$$

(A) Structure of a matrix in $E_p^{(m)}$

$$\begin{pmatrix} p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-1}\mathbb{Z}/p^m\mathbb{Z} \\ p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} \\ \vdots & & \ddots & & \vdots \\ p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p\mathbb{Z}/p^m\mathbb{Z} & p\mathbb{Z}/p^m\mathbb{Z} \\ p^{m-1}\mathbb{Z}/p^m\mathbb{Z} & p^{m-2}\mathbb{Z}/p^m\mathbb{Z} & \cdots & p\mathbb{Z}/p^m\mathbb{Z} & \mathbb{Z}/p^m\mathbb{Z} \end{pmatrix}$$

(B) Structure of a matrix in $F_p^{(m)}$

FIGURE 3.2: Illustration of the structure of a matrix in $E_p^{(m)}$ and $F_p^{(m)}$.

It is easy to check that $F_p^{(m)}$ is a $\mathbb{Z}/p^m\mathbb{Z}$-submodule of $\mathrm{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$. Moreover the following proposition shows that $F_p^{(m)}$ is isomorphic to $E_p^{(m)}$ as $\mathbb{Z}/p^m\mathbb{Z}$-modules, where the scalar multiplication in $E_p^{(m)}$ is as follows: for $r \in \mathbb{Z}/p^m\mathbb{Z}$ and $[a_{i,j}] \in E_p^{(m)}$ we have that

$$r[a_{i,j}] = [ra_{i,j}] = \left(ra_{i,j} \mod p^i\right)_{i,j\in\{1,\dots,m\}}.$$

Proposition 3.19. *$E_p^{(m)}$ is isomorphic to $F_p^{(m)}$ as $\mathbb{Z}/p^m\mathbb{Z}$-modules.*

Proof. One can easily check that the following map is an isomorphism between $E_p^{(m)}$ and $F_p^{(m)}$

$$\begin{aligned} \delta: \quad & E_p^{(m)} \to F_p^{(m)}, \\ & (a_{i,j})_{i,j\in\{1,\dots,m\}} \mapsto \left(a_{i,j}p^{m-i}\right)_{i,j\in\{1,\dots,m\}}. \end{aligned} \tag{3.3}$$

□

Solving a Linear System over $E_p^{(m)}$: Let $A \in E_p^{(m)}$ and $B \in V = \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$, and we want to find $X \in V$, such that

$$A \cdot X = B. \tag{3.4}$$

The system (3.4) can be seen as an action of $E_p^{(m)}$ on V, i.e.,

$$\begin{aligned} \phi : E_p^{(m)} \times V &\to V, \\ (A, X) &\mapsto A \cdot X. \end{aligned} \tag{3.5}$$

The main idea is to translate the system (3.4) to a system of linear equation over $F_p^{(m)}$. In order to do that, we first obtain the natural action of $F_p^{(m)}$ on $(\mathbb{Z}/p^m\mathbb{Z})^m$, i.e.,

$$\begin{aligned} \psi : F_p^{(m)} \times (\mathbb{Z}/p^m\mathbb{Z})^m &\longrightarrow (\mathbb{Z}/p^m\mathbb{Z})^m, \\ (M, Y) &\longmapsto M \cdot Y. \end{aligned} \tag{3.6}$$

Let $W = p^{m-1}\mathbb{Z}/p^m\mathbb{Z} \times p^{m-2}\mathbb{Z}/p^m\mathbb{Z} \times \cdots \times \mathbb{Z}/p^m\mathbb{Z}$. Then, we observe that the image of ψ is contained in W. Also, we have the following $\mathbb{Z}/p^m\mathbb{Z}$-linear isomorphism between V and W

$$\begin{aligned} \chi : V &\to W, \\ (a_i)_{i\in\{1,\ldots,m\}} &\mapsto (p^{m-i}a_i)_{i\in\{1,\ldots,m\}}. \end{aligned} \tag{3.7}$$

In this chapter, we use the notation $(x_i)_{i\in\{1,\ldots,n\}}$ to denote the vector $(x_1, \ldots, x_n)$.

Proposition 3.20. *Let δ, ϕ, ψ and χ as in* (3.3), (3.5), (3.6) *and* (3.7), *respectively. Then the following diagram of $\mathbb{Z}/p^m\mathbb{Z}$-linear and $\mathbb{Z}/p^m\mathbb{Z}$-bilinear maps commutes*

$$\begin{array}{ccc} E_p^{(m)} \times V & \xrightarrow{\quad\phi\quad} & V \\ {\scriptstyle \delta\times\eta}\downarrow & & \downarrow{\scriptstyle \chi} \\ F_p^{(m)} \times (\mathbb{Z}/p^m\mathbb{Z})^m & \xrightarrow{\quad\psi\quad} & (\mathbb{Z}/p^m\mathbb{Z})^m \end{array} \tag{3.8}$$

where $\eta : V \to (\mathbb{Z}/p^m\mathbb{Z})^m$ is an arbitrary lift.

Proof. Let $A = [a_{i,j}]_{i,j\in\{1,\dots,m\}} \in E_p^{(m)}$ and $X = (x_i)_{i\in\{1,\dots,m\}} \in V$. Then

$$\begin{aligned}
\chi\left(\phi(A,X)\right) &= \chi\left(\left(\sum_j a_{i,j}x_j \mod p^i\right)_{i\in\{1,\dots,m\}}\right) \\
&= \left(p^{m-i}\sum_j a_{i,j}x_j\right)_{i\in\{1,\dots,m\}} \\
&= \left(\sum_j p^{m-i}a_{i,j}x_j\right)_{i\in\{1,\dots,m\}} \\
&= \delta(A)\cdot\eta(X) \\
&= \psi\left((\delta\times\eta)(A,X)\right).
\end{aligned}$$

□

Remark 3.21. The ring $E_p^{(m)}$ and the ring $F_p^{(m)}$ are not isomorphic as rings. They are only isomorphic as $\mathbb{Z}/p^m\mathbb{Z}$-module via the map δ in (3.3). Hence the horizontal maps ϕ and ψ in (3.8) cannot be treated as semigroup actions, but rather as $\mathbb{Z}/p^m\mathbb{Z}$-bilinear maps. Eventually, this is enough to satisfy our purpose of solving a linear system over $E_p^{(m)}$ via $F_p^{(m)}$.

Finally, the following theorem gives a way to solve the system (3.4).

Theorem 3.22. *Let $A \in E_p^{(m)}$ and $B \in V$. Then $X_0 \in V$ is a solution of $A\cdot X = B$ if and only if $\eta(X_0)$ is a solution of $\delta(A)\cdot Y = \chi(B)$, where $\eta : V \to (\mathbb{Z}/p^m\mathbb{Z})^m$ is an arbitrary lift.*

Proof. Using the commutativity of (3.8), we clearly see that if $A\cdot X_0 = B$, then $\delta(A)\eta(X_0) = \chi(A\cdot X_0) = \chi(B)$.

Conversely, let $Y \in (\mathbb{Z}/p^m\mathbb{Z})^m$ be a solution of $\delta(A)\cdot Y = \chi(B)$, and let $\epsilon : (\mathbb{Z}/p^m\mathbb{Z})^m \to V$ be the natural surjection. Then for $X_0 = \epsilon(Y_0)$, we have that $\eta(X_0) = Y_0$. Moreover, the commutativity of (3.8) implies that

$$\begin{aligned}
\chi(A\cdot X_0) &= \psi\left((\delta\times\eta)(A,X_0)\right) \\
&= \delta(A)\cdot Y_0 \\
&= \chi(B).
\end{aligned}$$

Now since χ is injective, we have $A\cdot X_0 = B$. □

As a direct application of this result, we obtain an algorithm to solve a linear system over $E_p^{(m)}$, see Algorithm 3. The most expensive step in Algorithm 3 is solving a system of m linear equations over $\mathbb{Z}/p^m\mathbb{Z}$. Thus the running time of the algorithm is $\mathcal{O}(m^3)\mathbb{Z}/p^m\mathbb{Z}$ operations or $\mathcal{O}(m^5 \log(p)^2)$ bit operations.

Algorithm 3 Solving a linear system over $E_p^{(m)}$

Input: $A \in E_p^{(m)}, B \in V$, such that there exists $X \in V$ such that $A \cdot X = B$.
Output: $X_0 \in V$, such that $A \cdot X_0 = B$.

1: Compute $\delta(A) \in F_p^{(m)}$ using (3.5).
2: Compute $\chi(B) \in (\mathbb{Z}/p^m\mathbb{Z})^m$ using (3.7).
3: Solve the system $\delta(A) \cdot Y = \chi(B)$ for Y over $\mathbb{Z}/p^m\mathbb{Z}$. By Theorem 3.22, such a solution exists.
4: Return $\epsilon(Y)$, where $\epsilon : (\mathbb{Z}/p^m\mathbb{Z})^m \to V$ denotes the natural surjection.

In the next two sections, we will use the correspondence between $E_p^{(m)}$ and $F_p^{(m)}$ to efficiently solve the semigroup action problem and the decomposition problem over $E_p^{(m)}$. As a consequence, we break all three cryptographic protocols defined in Section 3.4.

3.6 Solving the Semigroup Action Problem over $E_p^{(m)}$

In this section, we shift our focus on breaking the Protocol 3.14 that is based on solving the following semigroup action problem. Given $H, R \in V$ and $M \in E_p^{(m)}$, find $G \in H(M)$ such that $H = G \cdot R$.

First, we recall from Proposition 3.13 that $H(M) \cong \mathbb{Z}/p^m\mathbb{Z}[M]$. Hence,

$$G = \sum_{i=0}^{m-1} a_i M^i,$$

for some $a_0, a_1, \ldots, a_{m-1} \in \mathbb{Z}/p^m\mathbb{Z}$. Thus, $H = G \cdot R$ gives us a linear system over $E_p^{(m)}$ with unknowns $a_0, \ldots, a_{m-1}$.

Again, the idea is to translate the system $H = G \cdot R$ to $F_p^{(m)}$. Using Proposition 3.20, we obtain $\chi(H) = \delta(G) \cdot \eta(R)$, where χ, δ and η are maps used in (3.8). Since δ is a $\mathbb{Z}/p^m\mathbb{Z}$-linear map (see Proposition 3.19),

$$\delta(G) = \sum_{i=0}^{m-1} a_i \delta(M^i).$$

Hence, the system is now over $\mathbb{Z}/p^m\mathbb{Z}$ and can easily be solved using $\mathcal{O}(m^3)\mathbb{Z}/p^m\mathbb{Z}$ operations. See Algorithm 4 for details. Notice that this attack is 6 orders faster than the previous attack by Micheli and Weger in [120].

Algorithm 4 Break protocol based on SAP over $E_p^{(m)}$

Input: $M \in E_p^{(m)}, H, R \in V$, such that $H = G \cdot R$ for some $G \in H(M)$.
Output: $G_0 \in H(M)$, such that $H = G_0 \cdot R$.

1: Compute $\delta(M^i) \in F_p^{(m)}$ for each $i \in \{0, \dots, m-1\}$, using (3.3)
2: Compute $\chi(H), \eta(R) \in (\mathbb{Z}/p^m\mathbb{Z})^m$, where χ is defined in (3.7) and η is an arbitrary lift.
3: Solve the system of m linear equations in m unknowns $a_0, a_1, \dots, a_{m-1} \in (\mathbb{Z}/p^m\mathbb{Z})^m$ arising from

$$\left(\sum_{i=0}^{m-1} a_i \delta(M^i)\right) \cdot \eta(R) = \chi(H).$$

4: Return $\sum_{i=0}^{m-1} a_i M^i \in H(M)$.

3.6.1 Toy Example

We use a toy example to illustrate Algorithm 4. Let $m = 2$ and $p = 3$. The attacker sees

$$M = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}, R = \begin{pmatrix} 1 \\ 5 \end{pmatrix}, H = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

and wants to find $G \in H(M)$, such that $G \cdot R = H$.
In Step 1 of Algorithm 4, the attacker computes

$$\delta(M^0) = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \delta(M) = \begin{pmatrix} 3 & 3 \\ 3 & 4 \end{pmatrix} \in F_p^{(m)}.$$

In the second step the attackers compute

$$\chi(H) = \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \eta(R) = \begin{pmatrix} 1 \\ 5 \end{pmatrix}.$$

From $a_0\delta(M^0)\eta(R)+a_1\delta(M)\eta(R) = \chi(H)$, the attacker obtains the following system of m linear equations in m unknowns $a_0, \ldots, a_{m-1}$:

$$3a_0 + 0a_1 = 3,$$
$$5a_0 + 5a_1 = 1.$$

The solution of this system over $\mathbb{Z}/p^m\mathbb{Z}$ is $(a_0, a_1) = (1, 1)$. Finally, the attacker computes

$$G = \sum_{i=0}^{m=1} a_i M^i = M^0 + M = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix}.$$

One can directly check that $G \cdot R = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = H.$

3.7 Solving the Decomposition Problem over $E_p^{(m)}$

In this section we provide an algorithm to solve the decomposition problem over $E_p^{(m)}$ and therefore to break the DHDP and EGDP protocols.

It is worth mentioning that in [164] the author claims to have an attack on DHDP and EGDP protocols, which runs with $\mathcal{O}(m^7)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations. Even though the main idea of the attack is correct (i.e., reducing the problem to solving a system of linear equations over $E_p^{(m)}$), it presents an issue when building the actual linear equations. In fact, the equations have different moduli, depending on which row is considered, so the claim that it is enough to solve the system over $\mathbb{Z}/p^m\mathbb{Z}$ is incorrect (we provide an explicit example where the attack fails in Subsection 3.7.1). Moreover, the aforementioned attack would run in $\mathcal{O}(m^7)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations, instead our attack runs in $\mathcal{O}(m^6)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations, reducing the complexity of the DHDP.

As mentioned in Protocol 3.15 and Protocol 3.16, the two subgroups used are $H(M)$ and $\mathrm{Cen}(M)$ for a publicly known $M \in E_p^{(m)}$. Then the decomposition problem is as follows: given $G_A = A_1XA_2, G_BB_1XB_2 \in E_p^{(m)}$ for some $X \in E_p^{(m)}$, $A_1, A_2 \in H(M)$ and $B_1, B_2 \in \mathrm{Cen}(M)$, find $A_1B_1XB_2A_2$.

Our strategy is to first obtain a system of linear equations over $E_p^{(m)}$ that solves the decomposition problem, and then translates it over $F_p^{(m)}$ and solve over $\mathbb{Z}/p^m\mathbb{Z}$.

In the first step, the crucial point is to use the Cayley-Hamilton theorem, as shown in the following proposition.

Proposition 3.23. *Let $M, X \in E_p^{(m)}$ and $G_A = A_1 X A_2$ for some $A_1, A_2 \in H(M)$. Then there exists $\lambda_{1,1}, \lambda_{1,2}, \ldots, \lambda_{m,m} \in \mathbb{Z}/p^m\mathbb{Z}$ such that $G_A = \sum_{i,j=0}^{m-1} \lambda_{i,j} M^i X M^j$.*

Proof. Combining Lemma 3.11 and Proposition 3.13, we can write $A_1 = \sum_{i=0}^{m-1} u_i M^i$ and $A_2 = \sum_{i=0}^{m-1} v_i M^i$, for some $u_0, \ldots, u_{m-1}, v_0, \ldots, v_{m-1} \in \mathbb{Z}/p^m\mathbb{Z}$. Then

$$\begin{aligned} G_A &= A_1 X A_2 \\ &= \left(\sum_{i=0}^{m-1} u_i M^i\right) X \left(\sum_{j=0}^{m-1} v_j M^j\right) \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} u_i v_j M^i X M^j \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \lambda_{i,j} M^i X M^j, \end{aligned}$$

for $\lambda_{i,j} = u_i v_j$. □

Now, we translate our problem to $F_p^{(m)}$ by using Proposition 3.19.

Lemma 3.24. *Let $M_1, M_2, \ldots, M_k, G \in E_p^{(m)}$. Then $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in (\mathbb{Z}/p^m\mathbb{Z})^k$ is a solution for $\sum_{i=1}^k \lambda_i M_i = G$ if and only if $\sum_{i=1}^k \lambda_i \delta(M_i) = \delta(G)$.*

Proof. The proof follows directly by applying the isomorphism δ, defined in (3.3), to both sides of the equation $\sum_{i=1}^k \lambda_i M_i = G$. □

Now we are ready for the main result.

Theorem 3.25. *The decomposition problem over $E_p^{(m)}$ can be solved in polynomial time.*

Proof. Let $M, X \in E_p^{(m)}$ such that $MX \neq XM$, and let $A_1, A_2 \in H(M)$ and $B_1, B_2 \in \mathrm{Cen}(M)$. Given $M, X, G_A = A_1 X A_2$ and $G_B = B_1 X B_2$, we want to find $A_1 G_B A_2$.

Using Proposition 3.23, we know that there exist $\lambda_{1,1}, \ldots, \lambda_{m,m} \in \mathbb{Z}/p^m\mathbb{Z}$, such that $G_A = \sum_{i,j=0}^{m-1} \lambda_{i,j} M^i X M^j$. We use Lemma 3.24 to solve this system of linear

equations for $\lambda_{1,1}, \lambda_{1,2} \ldots, \lambda_{m,m}$. Then the exchanged secret is given by

$$\begin{aligned}
\sum_{i,j=0}^{m-1} \lambda_{i,j} M^i G_B M^j &= \sum_{i,j=0}^{m-1} \lambda_{i,j} M^i B_1 X B_2 M^j \\
&= \sum_{i,j=0}^{m-1} \lambda_{i,j} B_1 M^i X M^j B_2 \\
&= B_1 \left(\sum_{i,j=0}^{m-1} \lambda_{i,j} M^i X M^j \right) B_2 \\
&= B_1 G_A B_2 = A_1 G_B A_2.
\end{aligned}$$

Algorithm 5 provides a formal way to solve the DHDP protocol over $E_p^{(m)}$.

□

Algorithm 5 Break protocol based on DHDP over $E_p^{(m)}$ using pseudo-$E_p^{(m)}$

Input: $M, X, G_A, G_B \in E_p^{(m)}$.
Output: the exchanged secret $A_1 G_B A_2 \in E_p^{(m)}$.

1: Construct the matrix of linear equations arising from $A_1 X A_2 = G_A$ using Proposition 3.23, given by

$$G_A = \sum_{i,j=0}^{m-1} \lambda_{i,j} M^i X M^j,$$

where $\lambda_{i,j}$'s are unknown.
2: Apply the $\mathbb{Z}/p^m\mathbb{Z}$-module isomorphism δ mentioned in Lemma 3.19 to the above equation

$$\delta(G_A) = \sum_{i,j=0}^{m-1} \lambda_{i,j} \delta(M^i X M^j).$$

3: Solve the system of m^2 linear equations in m^2 unknowns over $\mathbb{Z}/p^m\mathbb{Z}$, generated by equating entries of the above matrix equality. By Proposition 3.23 and Lemma 3.24, such a solution exists.
4: Return $\sum_{i,j=0}^{m-1} \lambda_{i,j} M^i G_B M^j$.

Running time. The running time of Algorithm 5 is given by solving m^2 linear equations in m^2 unkowns over $\mathbb{Z}/p^m\mathbb{Z}$, which costs $\mathcal{O}((m^2)^3)$ $\mathbb{Z}/p^m\mathbb{Z}$-operations, or $\mathcal{O}(m^8 \log(p)^2)$ bit operations. In [44], Climent et. al. proposed to use the DHDP protocol and the EGDP protocol for the parameters $p = 2$ and $m = 128$. In our implementation, Algorithm 5 took 23.1 days to break these parameters. The results

were obtained by a MAGMA [38] implementation using a personal computer with processor Intel Core 6C i7-8700K at 3.7 GHz and 64 GB RAM (see www.math.uzh.ch/aa/uploads/media/attack_CLR.txt).

3.7.1 Toy Example

In the following we provide an example, which serves two purposes, first it shows the Algorithm 5 in practice and second it provides an example where the claimed attack in [164] does not work.

Let $m = 2, p = 5$ and let $M = \begin{pmatrix} 4 & 3 \\ 15 & 20 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 4 \\ 15 & 4 \end{pmatrix}$ be public elements.

Alice chooses

$$A_1 = \begin{pmatrix} 1 & 3 \\ 15 & 17 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 3 \\ 15 & 11 \end{pmatrix}$$

and publishes $G_A = \begin{pmatrix} 0 & 1 \\ 20 & 23 \end{pmatrix}$. Bob chooses

$$B_1 = \begin{pmatrix} 3 & 3 \\ 15 & 9 \end{pmatrix} \quad B_2 = \begin{pmatrix} 3 & 0 \\ 0 & 18 \end{pmatrix}$$

and publishes $G_B = \begin{pmatrix} 0 & 2 \\ 5 & 3 \end{pmatrix}$. The shared secret is then

$$A_1 G_B A_2 = B_1 G_A B_2 = \begin{pmatrix} 0 & 1 \\ 15 & 21 \end{pmatrix}.$$

The attacker sees only M, X, G_A, G_B and wants to find $A_1 G_B A_2 \in E_5^{(2)}$.
In Step 1 of Algorithm 5, the attacker constructs

$$\begin{aligned} G_A &= \sum_{i,j=0}^{2-1} \lambda_{i,j} M^i X M^j \\ &= \lambda_{00} \begin{pmatrix} 0 & 4 \\ 15 & 4 \end{pmatrix} + \lambda_{01} \begin{pmatrix} 10 & 5 \\ 20 & 0 \end{pmatrix} + \lambda_{10} \begin{pmatrix} 20 & 3 \\ 0 & 15 \end{pmatrix} + \lambda_{11} \begin{pmatrix} 0 & 20 \\ 0 & 0 \end{pmatrix}. \end{aligned} \tag{3.9}$$

In the second step the attacker applies δ getting

$$\delta(G_A) = \begin{pmatrix} 0 & 5 \\ 20 & 23 \end{pmatrix} = \lambda_{0,0} \begin{pmatrix} 0 & 20 \\ 15 & 4 \end{pmatrix} + \lambda_{0,1} \begin{pmatrix} 0 & 0 \\ 20 & 0 \end{pmatrix} + \lambda_{1,0} \begin{pmatrix} 0 & 15 \\ 0 & 15 \end{pmatrix} + \lambda_{1,1} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

From this we get the system of 2^2 linear equations in 2^2 unknowns $\lambda_{i,j}$, but since we applied δ these are now equations over $\mathbb{Z}/5^2\mathbb{Z}$:

$$\begin{aligned} 0\lambda_{0,0} + 0\lambda_{0,1} + 0\lambda_{1,0} + 0\lambda_{1,1} &= 0, \\ 20\lambda_{0,0} + 0\lambda_{0,1} + 15\lambda_{1,0} + 0\lambda_{1,1} &= 5, \\ 15\lambda_{0,0} + 20\lambda_{0,1} + 0\lambda_{1,0} + 0\lambda_{1,1} &= 20, \\ 4\lambda_{0,0} + 0\lambda_{0,1} + 15\lambda_{1,0} + 0\lambda_{1,1} &= 23. \end{aligned}$$

One particular solution of this system over $\mathbb{Z}/5^2\mathbb{Z}$ is given by

$$(\lambda_{0,0}, \lambda_{0,1}, \lambda_{1,0}, \lambda_{1,1}) = (2, 22, 1, 0)\,.$$

The attacker now computes

$$\begin{aligned} \sum_{i,j=0}^{m-1} \lambda_{i,j} M^i G_B M^j &= 2G_B + 22G_B M + 1MG_B + 0MG_B M \\ &= \begin{pmatrix} 0 & 1 \\ 15 & 21 \end{pmatrix} = A_1 G_B A_2. \end{aligned}$$

Compared to our attack, the approach presented in [164] does not make use of Corollary 3.10, Proposition 3.13 and Lemma 3.24. Instead the elements of $Z(E_5^{(2)})$ are seen as diagonal matrices having entries

$$(a_0, a_0 + pa_1, \ldots, a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}),$$

where $0 \leq a_0, a_1, \ldots, a_{m-1} \leq p - 1$. Using this representation and the Cayley-Hamilton theorem results in a linear system over $E_p^{(m)}$ of m^2 equations in m^3 unknowns, as mentioned in Theorem 2 of [164]. One should observe that this system does not necessarily admit a solution over $\mathbb{Z}/p^m\mathbb{Z}$, which is the approach used in [164]. The above mentioned example provides an instance where this approach fails.

Using the approach in [164], the analogue of equation (3.9) is

$$G_A = \sum_{i,j=0}^{m-1} W_{i,j} M^i X M^j,$$

where $W_{i,j} = \begin{pmatrix} a_0^{i,j} & 0 \\ 0 & a_0^{i,j} + 5a_1^{i,j} \end{pmatrix} \in Z(E_5^{(2)})$. This results in the following system of linear equations:

$$\begin{aligned}
0a_0^{00} + 0a_1^{00} + 0a_0^{01} + 0a_1^{01} + 0a_0^{10} + 0a_1^{10} + 0a_0^{11} + 0a_1^{11} &= 0 \mod 5, \\
4a_0^{00} + 0a_1^{00} + 0a_0^{01} + 0a_1^{01} + 15a_0^{10} + 0a_1^{10} + 0a_0^{11} + 0a_1^{11} &= 5 \mod 5, \\
15a_0^{00} + 0a_1^{00} + 20a_0^{01} + 0a_1^{01} + 0a_0^{10} + 0a_1^{10} + 0a_0^{11} + 0a_1^{11} &= 20 \mod 25, \\
4a_0^{00} + 20a_1^{00} + 0a_0^{01} + 0a_1^{01} + 15a_0^{10} + 5a_1^{10} + 0a_0^{11} + 0a_1^{11} &= 23 \mod 25.
\end{aligned}$$

In Section 4 of [164], the author claims that it is enough to consider this system over $\mathbb{Z}/25\mathbb{Z}$. However in this example the claim does not hold and shows that the approach used in [164] to solve a linear system over $E_p^{(m)}$ is incorrect.

Chapter 4

Rank Analysis of Cubic Multivariate Schemes

In this chapter, we deal with multivariate cryptography. It is the area of cryptology where the cryptographic protocols are based on the hardness of solving a system of multivariate polynomial equations over a finite field.

This chapter is based on the following paper:

- John Baena, Daniel Cabarcas, Daniel Escudero, Karan Khathuria, and Javier Verbel. "Rank Analysis of Cubic Multivariate Cryptosystems". In: *Post-Quantum Cryptography. PQCrypto 2018*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 355–374. DOI: 10.1007/978-3-319-79063-3_17
  The paper analyzes the security of cubic multivariate cryptosystems with respect to rank weakness. It provides a framework for the study of the rank of multivariate cubic polynomials.

4.1 Introduction

Given k $m \times n$ matrices and a target rank r, the MinRank problem (MR) is to determine whether there exists a linear combination of the matrices of rank less or equal to r. Although NP-complete in its general setting, there are efficient algorithms to solve it for certain parameters. Indeed, Kipnis and Shamir [95] modeled an attack on the hidden field equation (HFE) system as an MR problem and were able to break it. Since then, other multivariate public-key schemes (MPK) have been subject to similar attacks. Rank defects also lead to other weakness such as a fixed degree of regularity in the algebraic attack on HFE [57].

The importance of the rank itself, and the prevalence of MR as an attack technique in MPK suggest a more central role as the underlying problem that supports security. For example, we can think of HFE as a way to construct low rank quadratic polynomials, where rank of a quadratic polynomial is given by the rank of the symmetric matrix representing its homogeneous quadratic part. Their low rank allows inversion, but it is insecure because the same low rank is preserved as a linear combination of the public key which can be efficiently solved through the Kipnis–Shamir modeling (KS) of MR.

Although the MR problem is stated for two-dimensional matrices, it can be naturally extended to d-dimensional matrices. It is particularly interesting to analyze it for three-dimensional matrices, since rank problems become much harder there. For example, simply determining the rank of a matrix is difficult for three-dimensional matrices, and it is not even known the maximum possible rank a matrix may have (see e.g. [80]).

Three-dimensional matrices lead to cubic polynomials. They are less common than quadratic polynomials in MPKs for two reasons. First, they are larger thus less efficient than quadratics. But more important, if f is cubic, its differential $Df_{\mathbf{a}}(\mathbf{x}) := f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a})$ is a quadratic map that preserves some of the properties of f. Thus, it is possible to extend rank analysis techniques from quadratics to cubics targeting the differential, c.f. [126]. Yet one important question remains open: Is this a general property of any cubic map that dooms any such construction? In this chapter we address this question, by taking a general perspective not focused on a particular construction.

In order to close the knowledge gap, we gather the appropriate literature to frame the discussion of the rank of cubic polynomials. We use the language of tensors that allows for very natural extensions of key concepts from two to d-dimensional matrices.

We extend the MR problem to three-dimensional matrices and we propose two ways to solve it, which naturally extend the KS modeling. Interestingly, if the rank is small, the complexity is even lower than for the quadratic case. However, the rank of a cubic polynomial in n variables can be larger than n, and in this case the attack is very inefficient.

We also discuss the relevance of two other typical lines of attack for MPK in the context of cubic low rank polynomials, namely the algebraic and differential attacks.

We show that the rank of the differential is not necessarily much smaller than the rank of the cubic polynomial, rendering this line of attack inefficient if the rank is large enough. Similarly, the algebraic attack is exponential in the rank, thus useless for high rank.

Although our approach is general, we provide a detailed example. We show how to efficiently construct cubic polynomials over a finite field from a weight three polynomial over a field extension, extending the so called big field idea. And then, we show that the rank is preserved by this construction in the sense that, a low rank core polynomial leads to a set of cubic polynomials with a low rank linear combination.

4.2 Preliminaries

This section is divided in three parts. In the first part, we extend the notion of rank to three-dimensional matrices and trilinear forms. In the second part, we describe the general construction of multivariate cryptosystems based on the big fields idea. In the third part, we introduce the MinRank attack, one of the most famous attack on quadratic multivariate schemes.

Notation

Given a natural number n, the set $\{1, \ldots, n\}$ is denoted by $[n]$. Let $\mathbb{F}$ be a finite field of order q which, unless explicitly stated, has characteristic different from 2 or 3.

Vectors are denoted by bold letters, e.g. $\mathbf{u}, \mathbf{v}$, and they are treated as column vectors by default unless stated otherwise. The vector $\mathbf{e}_i$ denotes the i-th canonical vector, i.e. the vector whose only non-zero entry is the i-th one, which is equal to 1. The i-th entry of a vector $\mathbf{u}$ is denoted by $\mathbf{u}[i]$, but sometimes we also use the non-bold version of the corresponding letter with subscript i: u_i.

The space of all $n \times m$ matrices is denoted by $\mathbb{F}^{n \times m}$. The entry of a matrix A indexed by (i, j) is denoted by $A[i, j]$. We use the notation $A[i, \cdot]$ to refer to the i-th row of a matrix A (as a row vector), and $A[\cdot, j]$ to refer to the j-th column of A (as a column vector).

A three dimensional matrix of dimensions $n \times m \times \ell$ is an array of elements in $\mathbb{F}$ indexed by tuples (i, j, k), where $1 \leq i \leq n$, $1 \leq j \leq m$ and $1 \leq k \leq \ell$. The

vector space of these three-dimensional matrices is denoted by $\mathbb{F}^{n\times m\times \ell}$, and the entry indexed by (i,j,k) in a matrix $A \in \mathbb{F}^{n\times m\times \ell}$ will be denoted by $A[i,j,k]$. We denote by $A[i,\cdot,\cdot]$ the two-dimensional matrix whose entry (j,k) is given by $A[i,j,k]$, and similarly for $A[\cdot,j,\cdot]$ and $A[\cdot,\cdot,k]$.

For $\mathbf{u} \in \mathbb{F}^n$ and $\mathbf{v} \in \mathbb{F}^m$, $\mathbf{u} \otimes \mathbf{v}$ denotes the Kronecker product which we usually see as the matrix $\mathbf{u}\mathbf{v}^\intercal$.

4.2.1 Rank and Trilinear Forms

Let n, m, ℓ be positive integers and let U, V and W be the vector spaces $\mathbb{F}^n$, $\mathbb{F}^m$ and $\mathbb{F}^l$, respectively. The rank of a matrix $A \in \mathbb{F}^{n\times m}$ can be defined as the minimum number of summands r required to write A as

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i,$$

where $\mathbf{u}_i \in U$ and $\mathbf{v}_i \in V$ for all $i = 1, \ldots, r$. This definition of rank is more flexible than other definitions as it is independent of the number of dimensions so it can be extended to three-dimensional matrices as follows.

Definition 4.1. Let $A \in \mathbb{F}^{n\times m\times \ell}$ be a three-dimensional matrix, we define the *rank* of A as the minimum number of summands r required to write A as

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i \otimes \mathbf{w}_i,$$

where $\mathbf{u}_i \in U$, $\mathbf{v}_i \in V$ and $\mathbf{w}_i \in W$ for all $i = 1, \ldots, r$. We denote this number by $\mathsf{Rank}(A)$.

Let $A \in \mathbb{F}^{n\times m\times \ell}$ be a three-dimensional matrix. Then clearly, $\mathsf{Rank}(A) = 0$ if and only if A is zero (empty sum). For an arbitrary $A \in \mathbb{F}^{n\times n\times n}$, the maximal value that $\mathsf{Rank}(A)$ can attain is unknown. To our knowledge, the best known upper bound for the maximal value of $\mathsf{Rank}(A)$ is $\lceil (3/4)n^2 \rceil$ (see [85, Theorem 7]).

A *bilinear map* $\mathcal{B} : U \times U \to \mathbb{F}$ is a map that is linear in each argument, so it can be written as

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) = \mathbf{x}^\intercal A \mathbf{y} \tag{4.1}$$

where $A \in \mathbb{F}^{n\times n}$ is the matrix such that $A[i,j] = \mathcal{B}(\mathbf{e}_i, \mathbf{e}_j)$.

A bilinear map $\mathcal{B}$ is *symmetric* if for all $\mathbf{a}, \mathbf{b} \in U$ it holds that $\mathcal{B}(\mathbf{a}, \mathbf{b}) = \mathcal{B}(\mathbf{b}, \mathbf{a})$, which is equivalent to A being symmetric.

Given a bilinear map $\mathcal{B}$ we can obtain a quadratic homogeneous polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ by defining $f(\mathbf{x}) := \mathcal{B}(\mathbf{x}, \mathbf{x})$. Different bilinear maps can yield the same quadratic polynomial. However, symmetric bilinear maps are in bijection with the set of quadratic homogeneous polynomials. Given a quadratic homogeneous polynomial f, its corresponding symmetric bilinear map can be computed as

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) := \frac{1}{2}\left(f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})\right)$$

.

Similarly, a *trilinear map* $\mathcal{T} : U \times U \times U \to \mathbb{F}$ is a map that is linear in each argument. It can be written as

$$\mathcal{T}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \sum_{i,j,k \in [n]} x_i y_j z_k \cdot \alpha_{i,j,k}$$

where $\alpha_{i,j,k} := \mathcal{T}(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k)$. Let $A \in \mathbb{F}^{n \times n \times n}$ be such that $A[i,j,k] = \alpha_{i,j,k}$. We say that $\mathcal{T}$ is *symmetric* if for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in U$, it is invariant under any permutation of the indices, i.e.

$$\mathcal{T}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \mathcal{T}(\mathbf{a}, \mathbf{c}, \mathbf{b}) = \mathcal{T}(\mathbf{b}, \mathbf{a}, \mathbf{c}) = \mathcal{T}(\mathbf{c}, \mathbf{a}, \mathbf{b}) = \mathcal{T}(\mathbf{b}, \mathbf{c}, \mathbf{a}) = \mathcal{T}(\mathbf{c}, \mathbf{b}, \mathbf{a}),$$

or equivalently, the three-dimensional matrix A is symmetric. Given a trilinear form $\mathcal{T}$ (symmetric or not) we can obtain the homogeneous cubic polynomial $f(\mathbf{x}) \in \mathbb{F}[\mathbf{x}]$ defined as $f(\mathbf{x}) := \mathcal{T}(\mathbf{x}, \mathbf{x}, \mathbf{x})$, and given a homogeneous polynomial f of degree 3 we can obtain the corresponding symmetric trilinear form as

$$\mathcal{T}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \frac{1}{3!}(f(\mathbf{x}+\mathbf{y}+\mathbf{z}) - f(\mathbf{y}+\mathbf{z}) - f(\mathbf{x}+\mathbf{z}) \\ - f(\mathbf{x}+\mathbf{y}) + f(\mathbf{x}) + f(\mathbf{y}) + f(\mathbf{z})). \quad (4.2)$$

For a cubic homogeneous polynomial $f \in \mathbb{F}[\mathbf{x}]$, we define its *rank*, denoted by $\mathsf{Rank}(f)$, as the rank of the corresponding three-dimensional symmetric matrix.

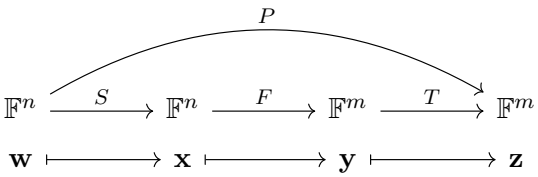

FIGURE 4.1: Outline of a general multivariate cryptosystem

4.2.2 Multivariate Cryptosystems Using Big Field Idea

Multivariate cryptography is the study of public-key cryptosystems based on difficulty of solving a system of multivariate polynomials over a finite field. In multivariate public-key cryptosystems (MPKC) the private and public keys are multivariate polynomials over a finite field $\mathbb{F}_q$. The generic structure of a multivariate scheme is as follows:

- **Key generation:** The private key consists of two random invertible affine transformations $S : \mathbb{F}^n \to \mathbb{F}^n, T : \mathbb{F}^m \to \mathbb{F}^m$, and an easy to invert system of multivariate polynomials $F : \mathbb{F}^n \to \mathbb{F}^m$, called the *central map*. The public key is the composition $P = T \circ F \circ S$, see Figure 4.1.
- **Encryption:** Given a message $\mathbf{w} \in \mathbb{F}^n$, to encrypt one simply computes the ciphertext $\mathbf{z} = P(\mathbf{w})$.
- **Decryption:** To decrypt, one computes $\mathbf{y} = T^{-1}(\mathbf{z})$, $\mathbf{x} = F^{-1}(\mathbf{y})$ and $\mathbf{w} = S^{-1}(\mathbf{x})$ in turn.

Since 1980's, many multivariate cryptosystems have been proposed and cryptanalysed. Most famous among them are Matsumoto–Imai (MI) cryptosystem [110], Hidden Field Equations (HFE) [132], Unbalanced Oil and Vinegar (UOV) signature scheme [133, 94], Rainbow signature scheme [59]. About the current state of research in multivariate cryptography, various multivariate cryptosystems are included in the ongoing process of standardization of post-quantum cryptography by NIST. Namely, GeMSS (Great Multivariate Signature Scheme), LUOV (Lifted Unbalanced Oil and Vinegar) signature scheme [34], Rainbow signature scheme [59, 137] and Gui signature scheme [138].

The cryptosystems MI, HFE, GeMSS and Gui are based on the so called "Big Field" construction, where the central map F is constructed by a univariate polynomial over an extension field (Big Field). Let $g(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_1 y + a_0$ be

an irreducible polynomial of degree n over $\mathbb{F}$. Consider the degree n field extension $\mathbb{K} = \mathbb{F}[y]/(g(y))$. Notice that $\mathbb{K}$ can be seen as a vector space over $\mathbb{F}$ of dimension n, so $\mathbb{K} \cong \mathbb{F}^n$ through the usual vector space isomorphism $\phi : \mathbb{K} \to \mathbb{F}^n$ given by

$$\phi(u_1 + u_2 y + \cdots + u_n y^{n-1}) = (u_1, u_2, \ldots, u_n).$$

Let Δ be the matrix given by

$$\Delta := \begin{pmatrix} y^0 & y^1 & \cdots & y^{n-1} \\ (y^0)^q & (y^1)^q & \cdots & (y^{n-1})^q \\ \vdots & \vdots & \ddots & \vdots \\ (y^0)^{q^{n-1}} & (y^1)^{q^{n-1}} & \cdots & (y^{n-1})^{q^{n-1}} \end{pmatrix}. \tag{4.3}$$

The matrix Δ, whose transpose is known as a *Moore matrix*, is invertible because $\{y^0, y^1, \ldots, y^{n-1}\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}$ [105, Page 109].

For $\beta \in \mathbb{K}$ let $\mathsf{Fr}(\beta)$ denote the vector $(\beta, \beta^{q^1}, \ldots, \beta^{q^{n-1}}) \in \mathbb{K}^n$. If $\alpha \in \mathbb{K}$, then it is easy to see that $\mathsf{Fr}(\alpha) = \Delta \cdot \phi(\alpha)$.

We refer to a polynomial in $\mathbb{K}[X]$ of the form

$$\mathcal{F}(X) = \sum_{0 \le i_1 \le \cdots \le i_d \le n-1} \alpha_{i_1,\ldots,i_d} X^{q^{i_1} + \cdots + q^{i_d}}, \tag{4.4}$$

where $\alpha_{i_1,\ldots,i_d} \in \mathbb{K}$, as a *homogeneous weight d polynomial*. Notice that a homogeneous weight 0 polynomial is simply a constant polynomial, i.e. an element of $\mathbb{K}$. A *weight d polynomial* $\mathcal{F} \in \mathbb{K}[X]$ is a polynomial that can be written as $\mathcal{F} = \mathcal{F}_0 + \cdots + \mathcal{F}_d$ where each $\mathcal{F}_j \in \mathbb{K}[X]$ is a homogeneous weight j polynomial.

The main property of this type of polynomials is that if $\mathcal{F} \in \mathbb{K}[X]$ is homogeneous of weight d then the map $F = \phi \circ \mathcal{F} \circ \phi^{-1} : \mathbb{F}^n \to \mathbb{F}^n$ can be represented as evaluation of n homogeneous multivariate polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of degree d. We state this formally in the following theorem.

Theorem 4.2. *Let $\mathcal{F} \in \mathbb{K}[X]$ be a homogeneous weight d polynomial. There exist homogeneous degree d polynomials $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that for all $\mathbf{a} \in \mathbb{F}^n$ it holds that $F(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_n(\mathbf{a}))^\intercal$ where F is the composition $\phi \circ \mathcal{F} \circ \phi^{-1}$.*

Proof. Note that it is enough to prove the theorem for monomial functions, i.e. we may assume that $\mathcal{F}(X) = \alpha X^{q^{a_1} + \cdots + q^{a_d}}$ for some $\alpha \in \mathbb{K}$ and non-negative integers $a_1, \ldots, a_d$. Now, we prove it by applying induction on d.

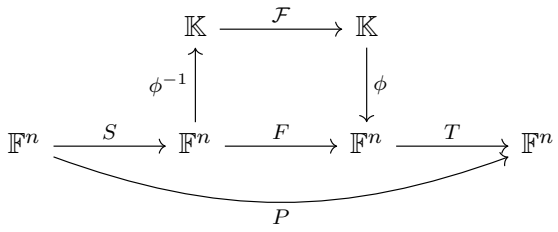

FIGURE 4.2: Outline of a Big Field Construction

Base case $d = 1$: Since $\mathcal{F} : X \mapsto \alpha X^{q^a}$ is an $\mathbb{F}$-linear map over $\mathbb{K}$, it follows that $F = \phi \circ \mathcal{F} \circ \phi^{-1}$ is also an $\mathbb{F}$-linear map and hence each component of F is a degree 1 multivariate polynomial over $\mathbb{F}$.

Now let $d > 1$ and assume that the theorem holds for $d-1$. We write $\mathcal{F}(X) = \alpha X^{q^{a_1}+\cdots+q^{a_d}} = \mathcal{G}(X)\mathcal{H}(X)$ with $\mathcal{G}(X) = \alpha X^{q^{a_1}+\cdots+q^{a_{d-1}}}$ and $\mathcal{H}(X) = X^{q^{a_d}}$. By induction hypothesis, there exist homogeneous degree $d-1$ polynomials $g_1, \ldots, g_n \in \mathbb{F}[x_1, \ldots, x_n]$ and homogeneous degree 1 polynomials $h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that $G = \phi \circ \mathcal{G} \circ \phi^{-1}$ and $H = \phi \circ \mathcal{H} \circ \phi^{-1}$ where $G = (g_1, \ldots, g_n)^\intercal$ and $H = (h_1, \ldots, h_n)^\intercal$. Thus

$$\begin{aligned}
\mathcal{F}\left(\phi^{-1}(\mathbf{x})\right) &= \mathcal{G}\left(\phi^{-1}(\mathbf{x})\right) \cdot \mathcal{H}\left(\phi^{-1}(\mathbf{x})\right) \\
&= \phi^{-1}\left(G(\mathbf{x})\right) \cdot \phi^{-1}\left(H(\mathbf{x})\right) \\
&= \left(g_1(\mathbf{x}) + g_2(\mathbf{x})y + \cdots + g_n(\mathbf{x})y^{n-1}\right)\left(h_1(\mathbf{x}) + h_2(\mathbf{x})y + \cdots + h_n(\mathbf{x})y^{n-1}\right) \\
&= f_1(\mathbf{x}) + f_2(\mathbf{x})y + \cdots + f_n(\mathbf{x})y^{n-1},
\end{aligned}$$

where $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_n]$ such that each f_i is a linear combination of the terms $g_j h_k$. Hence each f_i is a homogeneous polynomial of degree d. □

The previous property has been used extensively in order to construct the central map F of a multivariate scheme. This construction can be observed in Figure 4.2.

In the MI cryptosystem, we have $\mathcal{F}(X) = X^{1+q^i} =: Y$, for some $i \geq 1$. MI was broken by Patarin [131] using the relation $XY^{q^i} = X^{q^{2i}}Y$. On the other hand, the HFE cryptosystem is a generalization of MI, where $\mathcal{F}(X)$ is a weight 2 polynomial as in (4.4) with indices i_1, i_2 bounded above by a parameter r, i.e.

$$\mathcal{F}(X) = \sum_{0 \leq i_1 \leq i_2 < r} \alpha_{i_1,i_2} X^{q^{i_1}+q^{i_2}} + \sum_{0 \leq i_1 < r} \beta_{i_1} X^{q^{i_1}} + \gamma. \tag{4.5}$$

Notice that the degree of the homogeneous quadratic part is bounded by $D = 2q^r$. To invert $\mathcal{F}$ one uses the Berlekamp algorithm [27] which has complexity $\mathcal{O}(D^3 + nD^2 \log q)$. HFE with a high degree D is unbroken, although it can be really slow to decrypt/invert. Whereas small value of D (or r) leads to vulnerabilities like MinRank attacks, discussed in Section 4.2.3. Hence, it is difficult to obtain a good trade-off between efficiency and security in HFE cryptosystem.

An important remark is that the polynomials representing the map F can be efficiently computed from the coefficients of the polynomial $\mathcal{F}$. The construction for $d = 2$ can be found in [62, Section 6.3]. We will show the construction for $d = 3$ in Section 4.4.

4.2.3 Two-Dimensional MinRank Attack

Buss et al. [39] introduced the MinRank problem (MR) in the context of linear algebra and proved its NP-completeness.

Definition 4.3 (MinRank Problem)**.** Given positive integers m, n, r, k, and matrices $M_0, \ldots, M_k \in \mathbb{F}^{m \times n}$, determine whether there exist $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$ such that the rank of $\sum_{i=1}^{k} \lambda_i M_i - M_0$ is less or equal to r.

MinRank Attack on the HFE Cryptosystem

In the context of cryptography, MR first appeared as part of an attack against the HFE cryptosystem by Kipnis and Shamir [95]. Kipnis and Shamir showed that an attack on HFE can be reduced to an instance of MR with a small rank r. In particular, if $M_1, \ldots, M_n \in \mathbb{F}^{n \times n}$ are the symmetric matrices representing public polynomials, then there exists a linear combination $\sum_{i=1}^{n} \lambda_i M_i$ having rank at most the rank of $\mathcal{F}$. Moreover, these coefficients can be used to construct an equivalent secret key. Since we generalize this attack to the cubic case in Section 4.4.1, it is worth to describe the main idea here.

Let $\mathcal{F}$ be the central map of the HFE cryptosystem, which is a weight two polynomial as in (4.5). Since it is enough to consider only the homogeneous weight two part of $\mathcal{F}$, we assume that $\mathcal{F}$ is homogeneous of weight two, i.e.

$$\mathcal{F}(X) = \sum_{1 \leq i,j \leq r} \alpha_{i,j} X^{q^{i-1}+q^{j-1}}.$$

Hence we can write $\mathcal{F}$ as

$$\mathcal{F}(X) = \begin{pmatrix} X^{q^0} & X^{q^1} & \cdots & X^{q^{n-1}} \end{pmatrix} \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} X^{q^0} \\ X^{q^1} \\ \vdots \\ X^{q^{n-1}} \end{pmatrix},$$

where the $r \times r$ square on the top left is non-zero. We represent the map $\mathcal{F}$ as $\mathcal{F}(X) = \mathcal{B}_{\mathcal{F}}(\mathbf{X}, \mathbf{X})$ where $\mathbf{X} = (X^{q^0}, \ldots, X^{q^{n-1}})^\intercal$ and $\mathcal{B}_{\mathcal{F}} : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ is the bilinear form given by

$$\mathcal{B}_{\mathcal{F}}(\boldsymbol{\beta}, \boldsymbol{\gamma}) = \sum_{1 \le i,j \le n} \alpha_{i,j} \cdot \beta_i \gamma_j,$$

where $\alpha_{i,j} = 0$ when $i > r$ or $j > r$. Now, we lift also the linear maps $S, T : \mathbb{F}^n \to \mathbb{F}^n$ to the extension field $\mathbb{K}$ using the following proposition:

Proposition 4.4. *Let $A : \mathbb{F}^n \to \mathbb{F}^n$ be a linear map. Then there exists a homogeneous weight one polynomial $\mathcal{A} \in \mathbb{K}[X]$ such that $\phi \circ \mathcal{A} \circ \phi^{-1} = A$, where $\phi : \mathbb{K} \to \mathbb{F}^n$ is an $\mathbb{F}$-linear isomorphism.*

Proof. Using Theorem 4.2, we know that for every homogeneous weight one polynomial $\mathcal{A}$ there exists a linear transformation $A : \mathbb{F}^n \to \mathbb{F}^n$ such that $\phi \circ \mathcal{A} \circ \phi^{-1} = A$. Now, by using counting argument, it is easy to see that the converse also holds. The number of linear maps A is equal to the number of $n \times n$ matrices over $\mathbb{F}$, which is q^{n^2}. And, the number of homogeneous weight one polynomials in $\mathbb{K}[X]$ is also equal to $(q^n)^n = q^{n^2}$. □

Let $\mathcal{S}, \mathcal{T} : \mathbb{K} \to \mathbb{K}$ be the univariate homogeneous weight one polynomials obtained by lifting S and T, respectively.

Recall that the public key is given by $P = T \circ F \circ S$. Let $\mathcal{P} : \mathbb{K} \to \mathbb{K}$ be the lift of the system of public polynomials P, note that $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ and we represent $\mathcal{P}$ as $\mathcal{P}(X) = \mathcal{B}_{\mathcal{P}}(\mathbf{X}, \mathbf{X})$ for some bilinear map $\mathcal{B}_{\mathcal{P}} : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ given by

$$\mathcal{B}_{\mathcal{P}}(\boldsymbol{\beta}, \boldsymbol{\gamma}) = \sum_{1 \le i,j \le n} \delta_{i,j} \cdot \beta_i \gamma_j.$$

In order to show that there exists low rank linear combination of some bilinear maps corresponding to the public known $\mathcal{B}_{\mathcal{P}}$, we compute the bilinear representations of the composite maps $\mathcal{F} \circ \mathcal{S}$ and $\mathcal{T}^{-1} \circ \mathcal{P}$, which are the equal maps.

First we compute the bilinear representation of $\mathcal{F} \circ \mathcal{S}$. Let $\beta \in \mathbb{K}$ and let $\gamma = \phi^{-1}(S(\phi(\beta)))$, then recall from (4.3) that $\mathsf{Fr}(\gamma) = \Delta \cdot \phi(\gamma) = \Delta S \cdot \phi(\beta)$. Thus

$$\begin{aligned}(\mathcal{F} \circ \mathcal{S})(\beta) = \mathcal{F}(\gamma) &= \mathcal{B}_{\mathcal{F}}(\mathsf{Fr}(\gamma), \mathsf{Fr}(\gamma)) \\ &= \mathcal{B}_{\mathcal{F}}(\Delta S \cdot \phi(\beta), \Delta S \cdot \phi(\beta)) \\ &= \mathcal{B}'_{\mathcal{F}}(\mathsf{Fr}(\beta), \mathsf{Fr}(\beta)),\end{aligned}$$

where $\mathcal{B}'_{\mathcal{F}} : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ is the bilinear map given by

$$\mathcal{B}'_{\mathcal{F}}(\boldsymbol{\beta}, \boldsymbol{\gamma}) = \mathcal{B}_{\mathcal{F}}(\Delta S \Delta^{-1} \cdot \boldsymbol{\beta}, \Delta S \Delta^{-1} \cdot \boldsymbol{\gamma}).$$

Notice that $\Delta S \Delta^{-1}$ represents the change of basis on $\mathbb{K}^n$ and hence $\mathsf{Rank}(\mathcal{B}'_{\mathcal{F}}) = \mathsf{Rank}(\mathcal{B}_{\mathcal{F}}) = r$.

Now, we can compute the bilinear representation of $\mathcal{T}^{-1} \circ \mathcal{P}$. Let $\mathcal{T}^{-1}$ be given by $\mathcal{T}^{-1}(X) = \sum_{i=1}^{n} \tau_i X^{q^{i-1}}$. Then

$$\begin{aligned}(\mathcal{T}^{-1} \circ \mathcal{P})(\beta) &= \mathcal{T}^{-1}\left(\mathcal{B}_{\mathcal{P}}(\mathsf{Fr}(\beta), \mathsf{Fr}(\beta))\right) \\ &= \mathcal{T}^{-1}\left(\sum_{1 \le i,j \le n} \delta_{i,j} \cdot \beta^{q^{i-1}+q^{j-1}}\right) \\ &= \sum_{k=1}^{n} \tau_k \left(\sum_{1 \le i,j \le n} \delta_{i,j}^{q^{k-1}} \cdot \beta^{q^{i-1+k-1}+q^{j-1+k-1}}\right) \\ &= \sum_{k=1}^{n} \tau_k \; \mathcal{B}_{\mathcal{P}}^{(k)}(\mathsf{Fr}(\beta), \mathsf{Fr}(\beta)),\end{aligned}$$

where $\mathcal{B}_{\mathcal{P}}^{(k)} : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ is the bilinear map given by

$$\mathcal{B}_{\mathcal{P}}^{(k)}(\boldsymbol{\beta}, \boldsymbol{\gamma}) = \sum_{1 \le i,j \le n} \delta_{i_k, j_k}^{q^{k-1}} \cdot \beta_i \gamma_j,$$

here i_k denotes $i - k \mod n$ and j_k denotes $j - k \mod n$.

Since $\mathcal{F} \circ \mathcal{S} = \mathcal{T}^{-1} \circ \mathcal{P}$, we obtain the following relation

$$\mathcal{B}'_{\mathcal{F}} = \sum_{k=1}^{n} \tau_k \mathcal{B}^{(k)}_{\mathcal{P}}.$$

And since $\mathsf{Rank}(\mathcal{B}'_{\mathcal{F}}) = \mathsf{Rank}(\mathcal{B}_{\mathcal{F}}) = r$, we obtain an instance of the MinRank problem.

Next we discuss some of the most common approaches to solve the MinRank problem.

Solving the Two-Dimensional MinRank Problem

Kipnis–Shamir Modeling: Kipnis and Shamir [95] attacked the HFE scheme by reducing to an instance of the MinRank problem having small rank r. In the same paper, they described the following approach to solve the MinRank problem.

Let $A = \sum_{i=1}^{k} t_i M_i - M_0$ be the matrix with entries in the polynomial ring $\mathbb{F}[t_1, \ldots, t_k]$. The Kipnis–Shamir modeling is based on the following characterization of the rank of a matrix:

Theorem 4.5 (Rank-Nullity Theorem)**.** *The rank of a matrix $A \in \mathbb{F}^{n \times n}$ equals r if and only if the dimension of its kernel is $n - r$.*

Therefore, the matrix A has rank at most r if and only if the dimension of its right kernel is at least $n-r$. Hence, we construct $(n-r)$ linearly independent vectors in the right kernel of A. Notice that with high probability there exists kernel vectors of the following form:

$$A \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ v_{1,1} & v_{1,2} & \cdots & v_{1,n-r} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n-r} \\ \vdots & & \ddots & \vdots \\ v_{r,1} & v_{r,2} & \cdots & v_{r,n-r} \end{pmatrix} = 0_{n \times (n-r)}. \tag{4.6}$$

This relation produces a system of $n(n-r)$ bi-homogeneous polynomials in $\mathbb{F}[t_1, \ldots, t_k, v_{1,1}, \ldots, v_{r,n-r}]$ of bi-degree (1,1) in $k + r(n-r)$ variables. Clearly, if

$(t_1, \ldots, t_k, v_{1,1}, \ldots, v_{r,n-r})$ is a solution of the system, then the evaluation of the matrix A at the point $(t_1, \ldots, t_k)$ has rank at most r.

Unfortunately, this again reduces to solve a system of multivariate quadratic equations. However, in this case we obtain an overdefined system of about n^2 homogeneous bilinear equations in about nr variables. Moreover, if $r \ll n$, then one could use linearlization or relinearization techniques to solve the system without using Gröbner basis techniques.

Guessing Kernel Vectors: As with any system of equations, it is possible to guess some variables in (4.6) and solve for the others. Because of the structure of this system, it is particularly appealing to guess kernel vectors (i.e. the $v_{i,j}$ variables) and solve the resulting linear system in the t_i variables, as proposed in [74] (in fact, if the linear system is very overdetermined, it is enough to guess k/n kernel vectors). The complexity of such attack is dominated by the guessing part and depends on the probability of a correct guess. A tight bound on this probability can be significantly improved by understanding the structure of the solution space, e.g. by exploiting the interlinked kernel structure [163] or by using the subspace differential invariant structure [124].

Minors Modeling: In [67], Faugère et al. introduced the minors approach to solve the MinRank problem and in [33] they improved the MinRank attack on HFE using this modeling.

Let $A = \sum_{i=1}^{k} t_i M_i$ be the matrix with entries in the polynomial ring $\mathbb{F}[t_1, \ldots, t_k]$. The minors modeling is based on the following characterization of the rank:

Theorem 4.6. *The rank of a matrix $A \in \mathbb{F}^{n \times n}$ is at most r if and only if every minor of A of size $r+1$ is zero.*

Let I be the ideal in $\mathbb{F}[t_1, \ldots, t_k]$ generated by all the $(r+1) \times (r+1)$ minors of A. Let $V(I)$ be the zero locus of I.

If $(\lambda_1, \ldots, \lambda_k) \in V(I) \cap \mathbb{F}^k$, then all the $(r+1) \times (r+1)$ minors of the matrix A evaluated at $(\lambda_1, \ldots, \lambda_k)$ are zero. As a result the rank of the matrix A evaluated at $(\lambda_1, \ldots, \lambda_k)$ is at most r.

Each $(r+1)$-minor is a homogeneous polynomial in $\mathbb{F}[t_1, \ldots, t_k]$ of degree $r+1$, and the number of $(r+1)$-minors in A is $\binom{n}{r+1}^2$.

Support Minors Modeling: Recently, in [19], Bardet et al. introduced a new modeling of MR with an aim to solve rank syndrome decoding problem as an application of MR. This modeling is based on the following simple characterization of the rank:

Theorem 4.7. *Let M be a $m \times n$ matrix over $\mathbb{F}$ having rank at least r. Then there exist two matrices $S \in \mathbb{F}^{m\times r}$ and $C \in \mathbb{F}^{r\times n}$ such that $SC = M$.*

Let $A = \sum_{i=1}^{k} t_i M_i$ be the matrix with entries in the polynomial ring $\mathbb{F}[t_1, \ldots, t_k]$. Using the above theorem, there exist two matrices $S \in \mathbb{F}^{m\times r}$ and $C \in \mathbb{F}^{r\times n}$ such that

$$SC = \sum_{i=1}^{k} t_i M_i. \tag{4.7}$$

Define m matrices $C_1, \ldots, C_m$ by stacking a row of A on top of C, i.e.

$$C_j = \begin{pmatrix} \mathbf{r}_j \\ C \end{pmatrix},$$

where $\mathbf{r}_j$ is the j-th row of A. Since each row of A is in the span of the rows of C, it follows that the row rank of C_j is at most r. Hence each $(r+1)\times(r+1)$ minor of C_j is zero, which is referred to as the *support minors modeling*. The $m\binom{n}{r+1}$ equations arising from the minors of C_j, can be seen as bilinear equations in variables t_i and the $r \times r$ minors of C. As a result, the system can be expected to be solved by linearization technique whenever

$$m\binom{n}{r+1} \geq k\binom{n}{r} - 1.$$

4.3 Rank Analysis of Cubic Polynomials

Despite the disadvantages in terms of efficiency of considering cubic polynomials, one possible advantage would be avoiding the MinRank attack on the quadratic case. This might be expected since the MinRank attack relies on the fact that the degree is 2. For instance, this allows us to represent the polynomials as $\mathbf{x}^\intercal A\mathbf{x}$, which is crucial as the attack performs matrix operations and properties of such. Therefore, a natural question is whether or not the MinRank attack applies in a cubic setting. Let us start by defining the MinRank problem in this context.

Definition 4.8 (Cubic MinRank Problem)**.** Given positive integers $\ell, m, n,\ r, k$, and three-dimensional matrices $M_0, \ldots, M_k \in \mathbb{F}^{n\times m\times \ell}$, determine whether there exist $\lambda_1, \ldots, \lambda_k \in \mathbb{F}$ such that the rank of $\sum_{i=1}^{k} \lambda_i M_i - M_0$ is less or equal to r.

In this section we show that if there is a low-rank linear combination of the cubic polynomials of the public key then the resulting instance of the MinRank problem can be solved with an extension of the Kipnis–Shamir modeling. This is by itself a weakness on the scheme as it allows an adversary to distinguish between a public key and a random polynomial system of equivalent size. Thereafter, we discuss other consequences of the low-rank for the differentials and for the direct algebraic attack.

4.3.1 Solving the Three-Dimensional MinRank Problem

The following characterization of rank for cubic matrices leads to a generalization of the Kipnis–Shamir modeling for the MinRank problem.

Theorem 4.9. *Given a three-dimensional matrix $A \in \mathbb{F}^{n\times m\times \ell}$, the rank of A is the minimal number r of rank one matrices $S_1, \ldots, S_r \in \mathbb{F}^{m\times \ell}$, such that, for all slices $A[i,\cdot,\cdot]$ of A, $A[i,\cdot,\cdot] \in \mathrm{Span}(S_1, \ldots, S_r)$.*

Proof. Suppose $A = \sum_{j=1}^{r} \mathbf{u}_j \otimes \mathbf{v}_j \otimes \mathbf{w}_j$. Then

$$A[i,\cdot,\cdot] = \sum_{j=1}^{r} u_j[i] \cdot (\mathbf{v}_j \otimes \mathbf{w}_j).$$

Hence, for $S_j := \mathbf{v}_j \otimes \mathbf{w}_j$, $A[i,\cdot,\cdot] \in \mathrm{Span}(S_1, \ldots, S_r)$.

Conversely, let $A[i,\cdot,\cdot] \in \mathrm{Span}(S_1, \ldots, S_r)$ for some rank one matrices $S_1, \ldots, S_r \in \mathbb{F}^{m\times \ell}$, i.e. $A[i,\cdot,\cdot] = \sum_{j=1}^{r} u_{i,j} S_j$. Then for $\mathbf{u}_j := (u_{1,j}, \ldots, u_{n,j})$, $A = \sum_{j=1}^{r} \mathbf{u}_j \otimes S_j$. □

Let $M_0, \ldots, M_k \in \mathbb{F}^{n\times n\times n}$. Then, $A = \sum_{i=1}^{k} \lambda_i M_i - M_0$ is of rank r, if and only if, there exist rank one matrices $S_1, \ldots, S_r \in \mathbb{F}^{n\times n}$, such that, for $i = 1, \ldots, n$, $A[i,\cdot,\cdot] \in \mathrm{Span}(S_1, \ldots, S_r)$. Since each S_i matrix is of rank one, we can write it as $S_i = \mathbf{u}_i \mathbf{v}_i^T$ for some vectors $\mathbf{u}_i, \mathbf{v}_i \in \mathbb{F}^n$. Considering the entries of the $\mathbf{u}_i$'s, $\mathbf{v}_i$'s, and the linear combination coefficients as variables, we obtain a system of n^3 cubic polynomials in $3rn + k$ $(= r(2n) + rn + k)$ variables

$$\sum_{j=1}^{r} \alpha_{ij} \mathbf{u}_j \mathbf{v}_j^T = A[i,\cdot,\cdot], \text{ for } i = 1, \ldots, n. \tag{4.8}$$

If $r \ll n$ we can do much better. In that case, for most such rank r matrices A, the first r slices $A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot]$ are linearly independent. In this case, $\mathrm{Span}(S_1,\ldots,S_r) = \mathrm{Span}(A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot])$. Then, for $i = r+1,\ldots,n$, $A[i,\cdot,\cdot] \in \mathrm{Span}(A[1,\cdot,\cdot],\ldots,A[r,\cdot,\cdot])$. Considering the coefficients of the linear combinations as variables yields a system of $n^2(n-r)$ quadratic equations in $(n-r)r+k$ variables

$$\sum_{j=1}^{r} \alpha_{ij} A[j,\cdot,\cdot] = A[i,\cdot,\cdot], \text{ for } i = r+1,\ldots,n. \tag{4.9}$$

Notice that the converse is not necessarily true. A solution to the system in (4.9) does not necessarily implies the existence of the rank one S_i matrices, neither that A has rank r. However, this is a very overdetermined system, hence a solution is very unlikely, unless indeed A has rank r.

Another approach in the $r < n$ case is to take differentials (or slices) and reduce the problem to a two-dimensional MR problem. If $A \in \mathbb{F}^{n\times n\times n}$ has rank r, the corresponding symmetric trilinear map is likely to have rank r as well. Then, the differentials of this map will have rank less or equal to r. Since the differential operator is lineal, we have an MR problem among the differentials of the symmetric trilinear maps corresponding to $M_0,\ldots,M_k$. In the next section we discuss the relation between the rank of a cubic and its differential in more detail.

To the best of our knowledge, the complexity of solving a system such as (4.8) has not been studied. It can be seen as a multi-homogeneous system of multi-degree $(1,1,1,1)$, i.e. a tetra-linear system, and assuming some notion of tetra-regularity, analyze it using the techniques in [65]. It should be noticed that the techniques in [65] do not address the semi-regularity inherent to such an overdetermined system. Alternatively, the techniques in [20] could be used to establish the asymptotic behavior of an upper bound of the degree of regularity based on the semi-regularity assumption. Although a complete asymptotic analysis is outside the scope of this thesis, Table 4.1 shows the growth of such bound for selected parameters.

In the case $r \ll n$, the system in (4.9) has $\mathcal{O}(n^3)$ quadratic equations in $\mathcal{O}(n)$ variables. Since the number of degree two monomials is $\mathcal{O}(n^2)$ the system can be solved by relinearization at degree 2, which reduces to solving a $\mathcal{O}(n^2)$ square matrix. Notice that this is much faster than the KS approach in the two-dimensional case.

n	r	$vars$	# equations	d-reg	complexity
10	10	310	1000	67	699
11	11	374	1331	74	798
12	12	444	1728	81	899
13	13	520	2197	89	1010
14	14	602	2744	97	1123
15	15	690	3375	105	1240

TABLE 4.1: Complexity of MR by KS modeling for cubic system. For different values of n, KS yields a cubic system of n^3 equations in $(3r+1)n$ variables (assuming $k=n$). The d-reg column gives the degree of regularity for such a semi-regular system without field equations. The $vars$ column gives the number of variables. The complexity column, gives the log base 2 of $\binom{vars+d-1}{d}^{2.8}$.

4.3.2 Differentials

Given an instance of the cubic MinRank problem, one can always obtain a quadratic instance by taking the differential (defined below) of the associated polynomials. For example, it is known ([79]) that computing the differential of the public polynomials of a cubic HFE instance yields an instance of the quadratic HFE scheme, and therefore we can perform a quadratic MinRank attack. In this section we explore the relation between the rank of a cubic polynomial and the rank of its differential. More precisely, given a random homogeneous cubic polynomial $f \in \mathbb{F}[\mathbf{x}]$ of rank r, we want to estimate the rank of the quadratic part of its *differential* $D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a})$, with respect to some fixed $\mathbf{a} \in \mathbb{F}^n$.

The first and principal problem that we face in our analysis is: given an integer r, how can we generate random homogeneous cubic polynomials of rank r? Or equivalently, how can we generate random symmetric three-dimensional matrices of rank r? To address these questions, we introduce the concept of symmetric rank. We then choose random polynomials and use Kruskal's theorem to guarantee that those polynomials have certain symmetric rank.

Definition 4.10. Let $S \in \mathbb{F}^{n\times n\times n}$ be a three-dimensional symmetric matrix. We define the *symmetric rank* of S as the minimum number of summands s required to write S as

$$S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i,$$

where $\mathbf{u}_i \in \mathbb{F}^n$, $t_i \in \mathbb{F}$. If such decomposition does not exist, this number is defined to be ∞. We denote this number by $\mathsf{SRank}(S)$.

The following proposition gives us a sufficient condition over $\mathbb{F}$ to guarantee that for all matrices in $\mathbb{F}^{n\times n\times n}$ the symmetric rank is finite. A more general result is shown in [145, Proposition 7.2].

Proposition 4.11. *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| \geq 3$. Then each three-dimensional symmetric matrix $S \in \mathbb{F}^{n\times n\times n}$ can be written as $S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$, where $\mathbf{u}_i \in \mathbb{F}^n$ and $t_i \in \mathbb{F}$.*

By the previous proposition, if $|\mathbb{F}| \geq 3$, any homogeneous cubic polynomial f can be written as $\sum_{i=1}^{k} t_i u_i(\mathbf{x}) u_i(\mathbf{x}) u_i(\mathbf{x})$, where each $u_i(\mathbf{x})$ is a homogeneous linear polynomial and k depends on f. Furthermore, the symmetric rank of a homogeneous cubic $f \in \mathbb{F}[\mathbf{x}]$, denoted by $\mathsf{SRank}(f)$ and defined as the symmetric rank of its symmetric matrix representation, does exist.

The symmetric rank is a good parameter to consider because it is a bound of the rank of the differential.

Proposition 4.12. *Let $f \in \mathbb{F}[\mathbf{x}]$ be a homogeneous cubic polynomial. If g is the quadratic homogeneous part of $Df_{\mathbf{a}}(\mathbf{x})$, then $\mathsf{Rank}(g) \leq \mathsf{SRank}(f)$.*

Proof. If f can be written as $f(\mathbf{x}) = \sum_{i=1}^{r} t_i u_i(\mathbf{x}) u_i(\mathbf{x}) u_i(\mathbf{x})$, then for any $\mathbf{a} \in \mathbb{F}^n$ the quadratic part of $Df_{\mathbf{a}}(\mathbf{x})$ is $\sum_{i=1}^{r} 3 t_i u_i(\mathbf{a}) u_i(\mathbf{x}) u_i(\mathbf{x})$.

□

Let $U = \mathbb{F}^n$. Clearly, each symmetric matrix $A \in \mathbb{F}^{n\times n\times n}$ with symmetric rank r can be written as a sum of exactly r terms of the form $t\mathbf{u}\otimes\mathbf{u}\otimes\mathbf{u}$, where $t \in \mathbb{F} - \{0\}$ and $\mathbf{u} \in U$.

Let $\mathcal{S}_r$ be the function which outputs $A = \sum_{i=1}^{r} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$, for $t_i \in \mathbb{F} - \{0\}$ and $\mathbf{u}_i \in U$. By Proposition 4.11, if $|\mathbb{F}| \geq 3$, then each symmetric matrix $A \in \mathbb{F}^{n\times n\times n}$ with symmetric rank equal to r is in the codomain of $\mathcal{S}_r$. But some symmetric matrices having symmetric rank less than r can also be there.

The following theorem is a particular case of the known Kruskal's theorem [100, 144]. We use it to argue that if $t_i \in \mathbb{F} - \{0\}$ and $\mathbf{u}_i \in U$ are chosen uniformly at random, then with high probability the corresponding output A of $\mathcal{S}_r$ has symmetric rank equal to r. Moreover, by Kruskal's theorem with high probability $\mathsf{Rank}(A) = \mathsf{SRank}(A)$. The Kruskal rank of a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_m$, denoted by $\mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_m)$, is defined as the maximum integer k such that any subset of $\{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$ of size k is linearly independent.

Theorem 4.13. *Let* $\mathbb{F}$ *be a finite field,* $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ *and* $t_1, \ldots, t_r \in \mathbb{F}$. *Suppose that* $A = \sum_{i=1}^{r} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i$ *and that* $2r + 2 \leq \mathsf{KRank}(t_1\mathbf{u}_1, \ldots, t_r\mathbf{u}_r) + 2 \cdot \mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_r)$. *Then* $\mathsf{Rank}(A) = r$.

Suppose $2 \leq r \leq n$. If $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ are taken uniformly at random, then with high probability a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_r$ has full rank. If a matrix with columns $\mathbf{u}_1, \ldots, \mathbf{u}_r \in U$ is full rank, then $\mathsf{KRank}(\mathbf{u}_1, \ldots, \mathbf{u}_r) = r$ and $\mathsf{KRank}(t_1\mathbf{u}_1, \ldots, t_r\mathbf{u}_r) = r$, for any $t_1, \ldots, t_r \in \mathbb{F} - \{0\}$. In this case, by Theorem 4.13 the corresponding output A of $\mathcal{S}_r$ is such that $\mathsf{Rank}(A) = \mathsf{SRank}(A) = r$.

We experimentally analyze the behavior of the rank of the differential of a polynomial that is the output of $\mathcal{S}_{r^2}$. The experimental results are shown in Figure 4.3, where each curve represents the percentage of times that a rank is obtained, over 100,000 iterations.

4.3.3 Direct Algebraic Attack

The direct algebraic attack, or simply the direct attack, refers to the case when an attacker aims to find the plaintext associated with a ciphertext $(c_1, \ldots, c_n)$ directly from the public multivariate equations $p_1 = c_1, \ldots, p_n = c_n$, without the knowledge of any other information of the system. In almost all the cases, the most efficient way to perform this attack is to compute a Gröbner basis of the ideal I generated by the multivariate polynomials $p_1 - c_1, \ldots, p_n - c_n$.

Gröbner bases have played an important role not only in multivariate cryptography, but also in coding theory and lattices [21, 4]. There is a general consensus that when computing a Gröbner basis over a finite field, one of the most efficient ways to do it is to use the F_4 or F_5 algorithms [63, 64]. In a recent work [108], the authors used their M4GB algorithm to solve some of Fukuoka's MQ challenges within 11 days. The complexity of all these algorithms depends on the *degree of regularity* of the system. Since the degree of regularity is hard to determine, it is usually approximated by its *first fall degree*, defined as the first degree at which non-trivial relations between the polynomials $p_1, \ldots, p_n$ occur.

Let p be a linear combination of the polynomials $p_1, \ldots, p_n$. We now want to derive an upper bound for the first fall degree $D_{\mathrm{ff}}(p_1, \ldots, p_n)$ of the system that depends on $\mathsf{Rank}(p)$. Before we do that, we need the following definition.

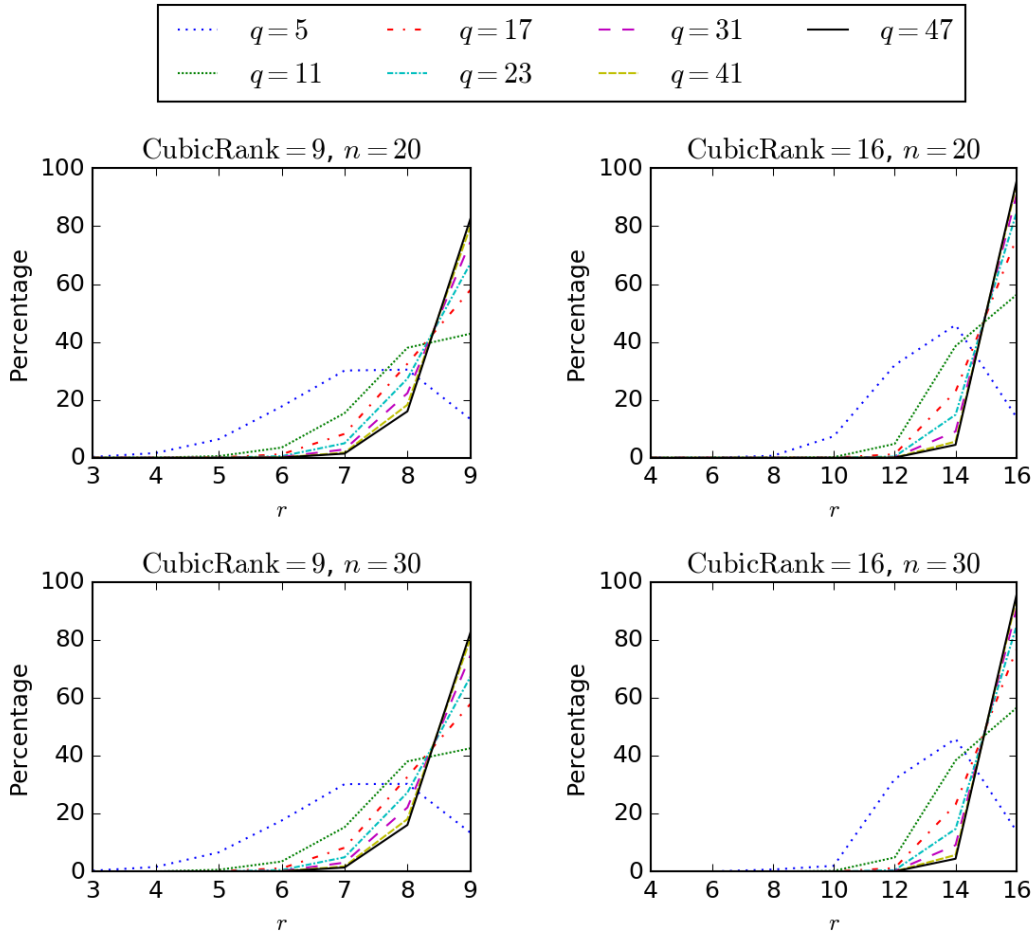

FIGURE 4.3: For different values of q, CubicRank, and n a polynomial f is chosen according $\mathcal{S}_{\text{CubicRank}}$, the $\mathsf{Rank}(Df_{\mathbf{a}})$ is computed for a random $\mathbf{a} \in U$. Each graph represents the percentage of times that a particular value $\mathsf{Rank}(Df_{\mathbf{a}})$ is obtained over 100,000 iterations.

Definition 4.14. The LRank of a homogeneous $\lambda \in \mathbb{F}[x_1, \ldots, x_n]$ is the smallest integer s such that there exist linear homogeneous $\mu_1, \ldots, \mu_s \in \mathbb{F}[x_1, \ldots, x_n]$ with λ contained in the algebra $\mathbb{F}[\mu_1, \ldots, \mu_s]$.

Hodges et al. [82] proved that $D_{\text{ff}}(p_1, \ldots, p_n)$ is bounded by

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq D_{\text{ff}}(p) \leq \frac{\mathsf{LRank}(p)(q-1)+5}{2}.$$

Also, since $\mathsf{LRank}(p) \leq 3 \cdot \mathsf{Rank}(p)$ then

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{3 \cdot \mathsf{Rank}(p)(q-1)+5}{2}. \tag{4.10}$$

On the other hand, the complexity of finding a Gröbner basis $\mathcal{G}$ for the ideal I is bounded by

$$\mathcal{O}\left(\binom{n+D_{\text{ff}}}{D_{\text{ff}}}^{\omega}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant. When n grows to infinity, the complexity [1] becomes $\mathcal{O}\left(n^{\omega D_{\text{ff}}}\right)$. Therefore, according to the bound in (4.10), the complexity of finding $\mathcal{G}$ is bounded by

$$\mathcal{O}\left(n^{\omega \frac{3\cdot \mathsf{Rank}(p)(q-1)+5}{2}}\right).$$

Thus, if q and $\mathsf{Rank}(p)$ are constant, then the complexity of finding $\mathcal{G}$ is polynomial in the number of variables n. We also observe that the complexity is exponential in $\mathsf{Rank}(p)$.

4.3.4 Previous Related Work

In [126] and [125], Moody, Perlner, and Smith-Tone do a rank analysis of the cubic ABC scheme [58]. They expose a subspace differential invariant extending the ideas used in the quadratic case [124]. They show that the MR attack used in [124] can be adapted to this cubic case.

Their work avoids discussing the rank of cubic polynomials by focusing on the differentials. This is rewarding in the ABC case because of the band structure of the scheme. There are linear combinations of the public polynomials with a band structure (they show it for the second differential) whose rank is bounded (possibly by a factor of s^2). The rank of some of their slices (or the second differential evaluated at some vectors as they show) drops by a square root factor to $2s$. This allows an attack on cubic ABC even more efficient than on its quadratic counterpart.

For a good reason, they approach the MR problem by guessing kernel vectors instead of using the Kipnis-Shamir or minors modeling (see Section 4.2.3 for a discussion of these techniques). The subspace differential invariant allows a tight analysis of the efficiency of this approach.

[1] Notice that we are using an upper bound to estimate the complexity. This is a customary usage for this kind of attacks. In practice, it has been observed [154] that, on average, this bound is not too far from the actual complexity.

4.4 Rank Analysis for Cubic Big Field Constructions

As we pointed out in Section 4.2.2, the big field idea has been a basis to propose quadratic multivariate encryption schemes for decades. Nevertheless, Theorem 4.2 is not restricted to any particular degree, which means that this approach works to generate polynomials of any degree, in particular degree 3. In this section we show that if the central map is a low rank cubic polynomial, then, as in the quadratic case, there must exists a low-rank linear combination of the polynomials of the public key. In particular, we obtain an instance of the cubic MinRank problem which can be solved using the techniques presented in Section 4.3. Thereafter, we discuss the direct algebraic attack on cubic big field schemes having low rank central map.

4.4.1 Big Field Idea for Cubic Polynomials

Let $\mathcal{F} \in \mathbb{K}[X]$ be a homogeneous weight 3 polynomial given by

$$\mathcal{F}(X) = \sum_{1 \leq i,j,k \leq n} \alpha_{i,j,k} X^{q^{i-1}+q^{j-1}+q^{k-1}}$$

and $S, T \in \mathbb{F}^{n \times n}$ invertible matrices. Our first goal is to give an explicit expression for the multivariate cubic polynomials of the composition $T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$. We begin by representing the map $\mathcal{F}$ as $\mathcal{F}(X) = \mathcal{T}(\mathbf{X}, \mathbf{X}, \mathbf{X})$ where $\mathbf{X} = (X^{q^0}, \ldots, X^{q^{n-1}})^\intercal$ and $\mathcal{T} : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ is the trilinear form given by

$$\mathcal{T}(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1 \leq i,j,k \leq n} \alpha_{i,j,k} \cdot (\beta_i \delta_j \gamma_k).$$

Let A be the three-dimensional matrix whose entry (i, j, k) is given by $\alpha_{i,j,k}$, and assume without loss of generality that the matrix A is symmetric (otherwise we can take the matrix whose (i, j, k) entry is given by $\frac{1}{3!} \cdot (A[i, j, k] + A[i, k, j] + A[j, i, k] + A[j, k, i] + A[k, i, j] + A[k, j, i])$, which represents the same trilinear form $\mathcal{T}$).

Let $\mathcal{T}' : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ be the trilinear form given by $\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \mathcal{T}(\Delta S\boldsymbol{\beta}, \Delta S\boldsymbol{\delta}, \Delta S\boldsymbol{\gamma})$, we can write this trilinear form as

$$\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1 \leq i,j,k \leq n} \alpha'_{i,j,k} \cdot (\beta_i \delta_j \gamma_k)$$

where $\alpha'_{i,j,k} = \mathcal{T}'(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) = \mathcal{T}(\Delta S\mathbf{e}_i, \Delta S\mathbf{e}_j, \Delta S\mathbf{e}_k)$.

Let A' be the three-dimensional matrix whose entry (i,j,k) is given by $\alpha'_{i,j,k}$. Notice that this is the cubic version of the matrix $(\Delta S)^{\intercal} A(\Delta S)$ from Section 4.2.2. It is easy to see that the matrix A' is symmetric since the matrix A is.

Let $\mathbf{a} \in \mathbb{F}^n$ and let $\alpha = \phi^{-1}(S\mathbf{a})$, we know that $\mathsf{Fr}(\alpha) = \Delta \cdot \phi(\alpha) = \Delta S \cdot \mathbf{a}$ and therefore

$$\begin{aligned}\mathcal{F} \circ \phi^{-1}(S\mathbf{a}) = \mathcal{F}(\alpha) = \mathcal{T}(\mathsf{Fr}(\alpha), \mathsf{Fr}(\alpha), \mathsf{Fr}(\alpha)) = \mathcal{T}(\Delta S \cdot \mathbf{a}, \Delta S \cdot \mathbf{a}, \Delta S \cdot \mathbf{a}) \\ = \mathcal{T}'(\mathbf{a}, \mathbf{a}, \mathbf{a}) = \sum_{1 \le i,j,k \le n} \alpha'_{i,j,k} \cdot (a_i a_j a_k).\end{aligned}$$

Let $R_1, \ldots, R_n \in \mathbb{F}^{n \times n \times n}$ be three-dimensional symmetric matrices such that $A' = y^0 \cdot R_1 + y^1 \cdot R_2 + \cdots + y^{n-1} \cdot R_n$, where $y^0, y^1 \ldots y^{n-1}$ is the basis of $\mathbb{K}$ over $\mathbb{F}$, as explained in Section 4.2.2. Then

$$\begin{aligned}\mathcal{F} \circ \phi^{-1} \circ S(\mathbf{a}) &= \sum_{1 \le i,j,k \le n} \alpha'_{i,j,k} \cdot (a_i a_j a_k) \\ &= \sum_{1 \le i,j,k \le n} \left(\sum_{\ell=1}^{n} y^{\ell-1} R_\ell[i,j,k] \right) \cdot (a_i a_j a_k) \\ &= \sum_{\ell=1}^{n} y^{\ell-1} \underbrace{\left(\sum_{1 \le i,j,k \le n} R_\ell[i,j,k] \cdot (a_i a_j a_k) \right)}_{t_\ell}.\end{aligned}$$

Since $t_\ell \in \mathbb{F}$, we obtain that $\phi \circ \mathcal{F} \circ \phi^{-1} \circ S(\mathbf{a}) = (t_1, \ldots, t_\ell)^{\intercal}$, therefore, each cubic polynomial in the composition $\phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ is given by $f_\ell(\mathbf{x}) = \sum_{1 \le i,j,k \le n} R_\ell[i,j,k] \cdot (x_i x_j x_k)$. Finally, when we apply the transformation T we obtain that each cubic polynomial in the composition $P = T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ is given by

$$p_\ell(\mathbf{x}) = \sum_{1 \le i,j,k \le n} \left(\sum_{t=1}^{n} T[\ell, t] \cdot R_t[i,j,k] \right) \cdot (x_i x_j x_k).$$

As a conclusion, if we let A_ℓ be the matrix whose entry (i,j,k) is given by $\sum_{t=1}^{n} T[\ell,t] \cdot R_t[i,j,k]$ then we obtain that this is the symmetric matrix corresponding to the ℓ-th polynomial in P. In particular, this shows we can compute efficiently the composition $T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ from S, T and $\mathcal{F}$.

4.4.2 Existence of Low Rank Linear Combination

Let us continue with the same setting as before, and let r be the rank of A, which in particular means that A can be written as $\sum_{\ell=1}^{r} \mathbf{u}_\ell \otimes \mathbf{v}_\ell \otimes \mathbf{w}_\ell$. Suppose that r is small. In this section we prove that there exists a low-rank linear combination of the three-dimensional matrices representing the composition P, and in Section 4.3.1 we showed how to find such combination.

Recall that the matrix A' was defined as $A'[i,j,k] = \mathcal{T}(\Delta S\mathbf{e}_i, \Delta S\mathbf{e}_j, \Delta S\mathbf{e}_k)$, we claim that the rank of this matrix is at most the rank of A. We show this by exhibiting vectors $\mathbf{u}'_\ell, \mathbf{v}'_\ell, \mathbf{w}'_\ell \in \mathbb{K}^n$ such that $A' = \sum_{\ell=1}^{r} \mathbf{u}'_\ell \otimes \mathbf{v}'_\ell \otimes \mathbf{w}'_\ell$. Let M be the matrix ΔS, we define $\mathbf{u}'_\ell = \sum_{i=1}^{n} \mathbf{u}_\ell[i] \cdot M[i,\cdot]$, $\mathbf{v}'_\ell = \sum_{i=1}^{n} \mathbf{v}_\ell[i] \cdot M[i,\cdot]$ and $\mathbf{w}'_\ell = \sum_{i=1}^{n} \mathbf{w}_\ell[i] \cdot M[i,\cdot]$, then

$$
\begin{aligned}
&A'[i',j',k'] \\
&\quad = \mathcal{T}'(M\mathbf{e}_{i'}, M\mathbf{e}_{j'}, M\mathbf{e}_{k'}) \\
&\quad = \sum_{1\le i,j,k\le n} A[i,j,k] \cdot \big((M\mathbf{e}_{i'})[i] \cdot (M\mathbf{e}_{j'})[j] \cdot (M\mathbf{e}_{k'})[k]\big) \\
&\quad = \sum_{1\le i,j,k\le n} \left(\sum_{\ell=1}^{r} \mathbf{u}_\ell[i] \cdot \mathbf{v}_\ell[j] \cdot \mathbf{w}_\ell[k]\right) \big((M[i,\cdot]\mathbf{e}_{i'}) \cdot (M[j,\cdot]\mathbf{e}_{j'}) \cdot (M[k,\cdot]\mathbf{e}_{k'})\big) \\
&\quad = \sum_{\ell=1}^{r} \sum_{1\le i,j,k\le n} \big(\mathbf{u}_\ell[i]M[i,\cdot]\mathbf{e}_{i'}\big)\big(\mathbf{v}_\ell[j]M[j,\cdot]\mathbf{e}_{j'}\big)\big(\mathbf{w}_\ell[k]M[k,\cdot]\mathbf{e}_{k'}\big) \\
&\quad = \sum_{\ell=1}^{r} \left(\sum_{i=1}^{n} \mathbf{u}_\ell[i]M[i,\cdot]\mathbf{e}_{i'}\right)\left(\sum_{j=1}^{n} \mathbf{v}_\ell[j]M[j,\cdot]\mathbf{e}_{j'}\right)\left(\sum_{k=1}^{n} \mathbf{w}_\ell[k]M[k,\cdot]\mathbf{e}_{k'}\right) \\
&\quad = \sum_{\ell=1}^{r} \left[\left(\mathbf{u}'_\ell\right)\mathbf{e}_{i'}\right]\left[\left(\mathbf{v}'_\ell\right)\mathbf{e}_{j'}\right]\left[\left(\mathbf{w}'_\ell\right)\mathbf{e}_{k'}\right] \\
&\quad = \sum_{\ell=1}^{r} \mathbf{u}'_\ell[i'] \cdot \mathbf{v}'_\ell[j'] \cdot \mathbf{w}'_\ell[k'].
\end{aligned}
$$

From this we conclude that $A' = \sum_{\ell=1}^{r} \mathbf{u}'_\ell \otimes \mathbf{v}'_\ell \otimes \mathbf{w}'_\ell$ and hence $\mathsf{Rank}(A') \le r$.

Now let $(\lambda_1, \ldots, \lambda_n) = (y^0, \ldots, y^{n-1}) \cdot T^{-1}$, then

$$
\sum_{i=1}^{n} \lambda_i A_i = \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{n} T[i,j] \cdot R_j\right) = \sum_{j=1}^{n} R_j \sum_{i=1}^{n} T[i,j] \cdot \lambda_i = \sum_{j=1}^{n} R_j \cdot y^{j-1} = A'.
$$

This shows that there is a linear combination of the matrices representing the public key whose result is a low rank three-dimensional matrix. This yields directly

an instance of the cubic MinRank problem which can be solved with the extension of the Kipnis–Shamir modeling presented in Section 4.3. As we mentioned before, this is by itself a weakness of the scheme, as it allows distinguishing public keys from random polynomial systems and also have implications on the degree of regularity of the system, as stated in Section 4.3.3. Moreover, the coefficients we have obtained here carry the same information about the secret key as those in the original (quadratic) MinRank attack, and this can be used in a similar way to construct equivalent keys.

4.4.3 Algebraic Attack for Cubic Big Field Constructions

As a complement of Section 4.3.3, we now consider the case when the polynomials $p_1, \ldots, p_n$ are constructed using the big field idea for cubic polynomials. Hodges et al. [82] proved that for a scheme with core polynomial of weight 3, its first fall degree $D_{\text{ff}}(p_1, \ldots, p_n)$ is bounded by

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{\mathsf{LRank}(P_0)(q-1)+5}{2}.$$

Here P_0 is the homogeneous part of highest degree of the core polynomial $\mathcal{F}$ seen as an element of the graded algebra $\mathbb{K}[X_0, \ldots, X_{n-1}]/\left(X_0^q, \ldots, X_{n-1}^q\right)$, where X_i corresponds to X^{q^i}, for $i = 0, \ldots, n-1$. In our case

$$P_0 = \sum_{1 \leq i,j,k \leq n} \alpha_{i,j,k} X_{i-1} X_{j-1} X_{k-1}.$$

If we take α_{ijk} uniformly at random, then with high probability $\mathsf{LRank}(P_0) \leq \mathsf{Rank}(P_0)$, so

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{\mathsf{Rank}(\mathcal{F})(q-1)+5}{2}, \tag{4.11}$$

since $\mathsf{Rank}(P_0) = \mathsf{Rank}(\mathcal{F})$.

In [82] the authors show that if $\deg \mathcal{F} = D$, then $\mathsf{LRank}(\mathcal{F}) \leq \lfloor \log_q(D-2) \rfloor + 1$, and hence

$$D_{\text{ff}}(p_1, \ldots, p_n) \leq \frac{(q-1)\lfloor \log_q(D-2) \rfloor + 4 + q}{2}. \tag{4.12}$$

We now want to experimentally study the tightness of the bound (4.12), as they

q	t	n	B	D_{ff}
5	3	8	8	8
5	3	9	8	8
5	3	10	8	8
5	4	8	10	9
5	4	9	10	9
5	4	10	10	10
5	5	8	12	9
5	5	9	12	9
5	5	10	12	10

q	t	n	B	D_{ff}
7	3	8	11	10
7	3	9	11	10
7	3	10	11	10
7	4	8	14	10
7	4	9	14	11
7	4	10	14	12
7	5	8	17	10
7	5	9	17	11
7	5	10	17	12

q	t	n	B	D_{ff}
11	3	8	17	13
11	3	9	17	14
11	3	10	17	15
11	4	8	22	13
11	4	9	22	14
11	4	10	22	15
11	5	8	27	13
11	5	9	27	14
11	5	10	27	15

q	t	n	B	D_{ff}
17	3	8	26	17
17	3	9	26	18
17	3	10	26	18
17	4	8	34	17
17	4	9	34	18
17	4	10	34	18
17	5	8	42	17
17	5	9	42	18
17	5	10	42	18

TABLE 4.2: Experimental results to study the tightness of the bound for D_{ff} given by (4.12), for different choices of the parameters q, t and n. The value of D_{ff} is read from Magma's verbose output.

did in [82] for different parameters[2]. In Table 4.2 we present some of the results obtained for different values of the parameters q, n and t, where t is the smallest integer such that $D \leq q^t - 1$. The value B corresponds to the bound given by equation (4.12), and D_{ff} is the first fall degree of the system for each choice of the parameters, which is read from Magma's verbose output. All the polynomials used in the attack were built as explained in Section 4.4.1, and for all cases we have included the field equations, i.e., $x_i^q - x_i$ for $i = 1, \ldots, n$.

We notice that the bound given by (4.12) is very tight for small values of q and t, and that it starts to widen considerably as q increases, and with a smaller pace as t increases. We also observe that for fixed q and t, the bound gets tighter as n increases. It is very clear that the bound needs to be improved for larger values of q.

4.5 Conclusions and Future Work

The minimum rank of a linear combination of the public polynomials is an important property of multivariate schemes. We have shown that this is still true for cubic schemes. The rank for cubic maps can be directly studied and exploited.

Many attacks have shown that it is hard to escape a low-rank when constructing quadratic encryption schemes. A high rank defect is necessary to allow decryption, leaving a low rank map exposed. Our rank analysis of cubic cryptosystems shows that low, fixed rank constructions have no chance of being secure. On the other

[2]Table 1 in [82] do not include the values for the parameters we are interested in, so we constructed our own version of it.

hand, we are convinced that cubic polynomials allow more versatile constructions than quadratic, where a rank defect can help decryption but leave a rank large enough so that it does not necessarily represent a weakness.

This work is preliminary in the sense that it opens new questions. Can we construct cubic maps with a rank defect that allows decryption but leave a rank large enough for security? Other algorithms to solve the cubic-MinRank problem are likely, for example based on the minors modeling or on guessing kernel vectors. The complexity of each of these approaches needs to be studied more carefully (even in the quadratic case). These attacks could also be extendable to the cases where the field has characteristic 2 or 3. Finally, the hardness of rank problems for three-dimensional matrices can be further harvest as a security assumption.

Bibliography

[1] Carlos Aguilar, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. "Efficient Encryption From Random Quasi-Cyclic Codes". In: *IEEE Transactions on Information Theory* 64.5 (2018), pp. 3927–3943. ISSN: 0018-9448. DOI: 10.1109/TIT.2018.2804444.

[2] Gorjan Alagic, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. US Department of Commerce, National Institute of Standards and Technology, 2019.

[3] Martin Albrecht, Carlos Cid, Kenneth G. Paterson, Cen Jung Tjhai, and Martin Tomlinson. *NTS-KEM*. 2018.

[4] Malihe Aliasgari, Mohammad-Reza Sadeghi, and Daniel Panario. "Gröbner Bases for Lattices and an Algebraic Decoding Algorithm". In: *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. 2011, pp. 1414–1415. DOI: 10.1109/Allerton.2011.6120333.

[5] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. "Post-Quantum Key Exchange – a New Hope". In: *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 2016, pp. 327–343.

[6] Iris Anshel, Michael Anshel, and Dorian Goldfeld. "An algebraic method for public-key cryptography". In: *Mathematical Research Letters* 6 (1999), pp. 287–292.

[7] Nicolas Aragon, Paulo S.L.M. Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, and Gilles Zémor. *Bike: Bit flipping key encapsulation*. 2017.

[8] Nicolas Aragon, Olivier Blazy, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. "Durandal: a rank metric based signature scheme". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2019, pp. 728–758.

[9] Michael Atiyah and Ian G. MacDonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Avalon Publishing, 1994.

[10] Daniel Augot, Matthieu Finiasz, and Nicolas Sendrier. "A family of fast syndrome based cryptographic hash functions". In: *International Conference on Cryptology in Malaysia*. Springer. 2005, pp. 64–83.

[11] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation". In: *NIST PQC Round* 2 (2017), p. 4.

[12] Hayo Baan, Sauvik Bhattacharya, Scott Fluhrer, Oscar Garcia-Morchon, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. "Round5: Compact and Fast Post-Quantum Public-Key Encryption". In: *International Conference on Post-Quantum Cryptography*. Springer. 2019, pp. 83–102.

[13] John Baena, Daniel Cabarcas, Daniel Escudero, Karan Khathuria, and Javier Verbel. "Rank Analysis of Cubic Multivariate Cryptosystems". In: *Post-Quantum Cryptography. PQCrypto 2018*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 355–374. DOI: 10.1007/978-3-319-79063-3_17.

[14] Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, and Paolo Santini. "LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes". In: *International Conference on Post-Quantum Cryptography*. Springer. 2018, pp. 3–24.

[15] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani. "A Variant of the McEliece Cryptosystem with Increased Public Key Security." In: *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC2011)*. 2011, pp. 173 –182.

[16] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani. *Method and Apparatus for Public-Key Cryptography Based on Error Correcting Codes*. US Patent 9,191,199. 2015.

[17] Marco Baldi, Marco Bodrato, and Franco Chiaraluce. "A new analysis of the McEliece cryptosystem based on QC-LDPC codes". In: *International Conference on Security and Cryptography for Networks*. Springer Berlin Heidelberg. 2008, pp. 246–262.

[18] Marco Baldi, Franco Chiaraluce, Joachim Rosenthal, Paolo Santini, and Davide Schipani. "On the Security of Generalized Reed-Solomon Code-Based Cryptosystems". In: *IET Information Security* (2019).

[19] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. "Algebraic attacks for solving the Rank Decoding and MinRank problems without Gröbner basis". In: *arXiv preprint arXiv:2002.08322* (2020).

[20] Magali Bardet, Jean-Charles Faugère, Bruno Salvy, and Bo-Yin Yang. "Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems". In: *MEGA 2005. Eighth International Symposium on Effective Methods in Algebraic Geometry*. 2005, pp. 1–14.

[21] Ismara Álvarez Barrientos, Mijail Borges-Quintana, Miguel Angel Borges-Trenard, and Daniel Panario. "Computing Gröbner Bases Associated with Lattices." In: *Adv. in Math. of Comm.* 10.4 (2016), pp. 851–860.

[22] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. "Decoding random binary linear codes in 2n/20: How 1+ 1= 0 improves information set decoding". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2012, pp. 520–536.

[23] Thierry P. Berger and Pierre Loidreau. "How to mask the structure of codes for a cryptographic use". In: *Designs, Codes and Cryptography* 35.1 (2005), pp. 63–79. ISSN: 0925-1022. DOI: 10.1007/s10623-003-6151-2.

[24] George M. Bergman. "Some Examples in PI Ring Theory". In: *Israel Journal of Mathematics* 18.3 (1974), pp. 257–277. ISSN: 1565-8511. DOI: 10.1007/BF02757282.

[25] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. "On the inherent intractability of certain coding problems (corresp.)" In: *IEEE Transactions on Information Theory* 24.3 (1978), pp. 384–386.

[26] Elwyn R. Berlekamp. *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[27] Elwyn R Berlekamp. "Factoring polynomials over finite fields". In: *Bell Labs Technical Journal* 46.8 (1967), pp. 1853–1859.

[28] Daniel J Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. "NTRU Prime: Reducing Attack Surface at Low Cost". In: *International Conference on Selected Areas in Cryptography*. Springer. 2017, pp. 235–260.

[29] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. "The SPHINCS+ Signature Framework". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019, pp. 2129–2146.

[30] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. "Attacking and defending the McEliece cryptosystem". In: *Post-Quantum Cryptography* (2008), pp. 31–46.

[31] Daniel J Bernstein, Tanja Lange, and Christiane Peters. "Smaller decoding exponents: ball-collision decoding". In: *Annual Cryptology Conference*. Springer. 2011, pp. 743–760.

[32] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. "Wild McEliece". In: *International Workshop on Selected Areas in Cryptography*. Springer. 2010, pp. 143–158.

[33] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. "Cryptanalysis of HFE, multi-HFE and Variants for Odd and Even Characteristic". In: *Designs, Codes and Cryptography* 69.1 (2013), pp. 1–52.

[34] Ward Beullens and Bart Preneel. "Field Lifting for Smaller UOV Public Keys". In: *Progress in Cryptology – INDOCRYPT 2017*. Ed. by Arpita Patra and Nigel P. Smart. Cham: Springer International Publishing, 2017, pp. 227–246.

[35] Nina Bindel, Sedat Akleylek, Erdem Alkim, PSLM Barreto, Johannes Buchmann, Edward Eaton, Gus Gutoski, Juliane Kramer, Patrick Longa, Harun Polat, et al. *Submission to NIST's Post-Quantum Project: Lattice-Based Digital Signature Scheme qTESLA*. 2018.

[36] Jessalyn Bolkema, Heide Gluesing-Luerssen, Christine A. Kelley, Kristin Lauter, Beth Malmskog, and Joachim Rosenthal. "Variations of the McEliece Cryptosystem". In: *Algebraic Geometry for Coding Theory and Cryptography*. Springer, 2017, pp. 129–150.

[37] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 2016, pp. 1006–1018.

[38] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125.

[39] Jonathan F. Buss, Gudmund S. Frandsen, and Jeffrey O. Shallit. "The Computational Complexity of Some Problems of Linear Algebra". In: *Journal of Computer and System Sciences* 58.3 (1999), pp. 572 –596.

[40] Anne Canteaut and Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511". In: *IEEE Transactions on Information Theory* 44.1 (1998), pp. 367–378.

[41] Antoine Casanova, Jean-Charles Faugere, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. "Gemss: A Great Multivariate Short Signature". In: *Submission to NIST* (2017).

[42] Ignacio Cascudo, Ronald Cramer, Diedo Mirandola, and Giles Zémor. "Squares of random linear codes". In: *IEEE Transactions on Information Theory* 61.3 (2015), pp. 1159–1173.

[43] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. "MQDSS specifications". In: *NIST PQC Round* 2 (2018), p. 13.

[44] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. "An Extension of the Noncommutative Bergman's Ring with a large Number of Noninvertible Elements". In: *Applicable Algebra in Engineering, Communication and Computing* 25.5 (2014), pp. 347–361.

[45] Joan-Josep Climent, Pedro R Navarro, and Leandro Tortosa. "Key exchange protocols over noncommutative rings. The case of End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$)". In: *International Journal of Computer Mathematics* 89.13-14 (2012), pp. 1753–1763.

[46] Joan-Josep Climent, Pedro R. Navarro, and Leandro Tortosa. "On the Arithmetic of the Endomorphisms ring End ($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$)". In: *Applicable Algebra in Engineering, Communication and Computing* 22.2 (2011), pp. 91–108.

[47] Joan-Josep Climent and Juan Antonio López Ramos. "Public Key Protocols over the Ring $E_p^{(m)}$". In: *Advances in Mathematics of Communications* 10.4 (2016), pp. 861–870.

[48] Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier. "How to Achieve a McEliece-Based Digital Signature Scheme". In: *Advances in Cryptology — ASIACRYPT 2001*. Ed. by Colin Boyd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 157–174. ISBN: 978-3-540-45682-7.

[49] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. "Distinguisher-Based Attacks on Public-Key Cryptosystems using Reed-Solomon Codes". In: *Designs, Codes and Cryptography* 73.2 (2014), pp. 641–666.

[50] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. "Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes". In: *IEEE Transactions on Information Theory* 63.8 (2017), pp. 5404–5418. ISSN: 0018-9448. DOI: 10.1109/TIT.2017.2712636.

[51] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. "Polynomial time attack on wild McEliece over quadratic extensions". In: *IEEE Transactions on Information Theory* 63.1 (2017), pp. 404–427.

[52] Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich, and Valérie Gauthier-Umaña. "A Polynomial-Time Attack on the BBCRS Scheme". In: *Public-key cryptography—PKC 2015*. Lecture Notes in Comput. Sci. 9020 (2015), pp. 175–193. DOI: 10.1007/978-3-662-46447-2_8.

[53] Ronald Cramer and Victor Shoup. "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack". In: *Advances in Cryptology — CRYPTO '98*. Ed. by Hugo Krawczyk. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 13–25. ISBN: 978-3-540-68462-6.

[54] Luca De Feo, David Jao, and Jérôme Plût. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247.

[55] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. "Wave: A new family of trapdoor one-way preimage sampleable functions based on codes". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2019, pp. 21–51.

[56] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.

[57] Jintai Ding and Timothy J. Hodges. "Inverting HFE Systems is Quasi-Polynomial for All Fields". In: *Advances in Cryptology – CRYPTO 2011*. Ed. by Phillip Rogaway. Vol. 6841. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, pp. 724–742. ISBN: 978-3-642-22791-2. DOI: 10.1007/978-3-642-22792-9_41.

[58] Jintai Ding, Albrecht Petzoldt, and Lih-chung Wang. "The Cubic Simple Matrix Encryption Scheme". In: *Post-Quantum Cryptography*. Ed. by Michele Mosca. Cham: Springer International Publishing, 2014, pp. 76–87.

[59] Jintai Ding and Dieter Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". In: *Applied Cryptography and Network Security*. Ed. by John Ioannidis, Angelos Keromytis, and Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 164–175. ISBN: 978-3-540-31542-1.

[60] Il'ya Isaakovich Dumer. "Two decoding algorithms for linear codes". In: *Problemy Peredachi Informatsii* 25.1 (1989), pp. 24–32.

[61] Taher ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In: *IEEE transactions on information theory* 31.4 (1985), pp. 469–472.

[62] Daniel Escudero. "Groebner Bases and Applications to the Security of Multivariate Public Key Cryptosystems". Accessed: 2017-11-25. Medellín, Colombia: National University of Colombia, 2016.

[63] Jean-Charles Faugère. "A New Efficient Algorithm for Computing Gröbner Bases (F_4)". In: *J. Pure Appl. Algebra* 139.1-3 (1999). Effective methods in algebraic geometry (Saint-Malo, 1998), pp. 61–88. ISSN: 0022-4049.

[64] Jean Charles Faugère. "A New Efficient Algorithm for Computing Gröbner Bases Without Reduction to Zero (F5)". In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ISSAC '02. Lille, France: ACM, 2002, pp. 75–83. ISBN: 1-58113-484-3. DOI: 10.1145/780506.780516.

[65] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. "Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1,1): Algorithms and complexity". In: *Journal of Symbolic Computation* 46.4 (2011), pp. 406 –437. ISSN: 0747-7171.

[66] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. "A Distinguisher for High-Rate McEliece Cryptosystems". In: *IEEE Transactions on Information Theory* 59.10 (2013), pp. 6830–6844.

[67] Jean-Charles Faugère, Françoise Levy-dit Vehel, and Ludovic Perret. "Cryptanalysis of MinRank". In: *Advances in Cryptology – CRYPTO 2008*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 280–296. ISBN: 978-3-540-85174-5.

[68] Gui-Liang Feng and Kenneth K. Tzeng. "A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis with Appl. to Decoding Cyclic Codes". In: *IEEE Transactions on Information Theory* IT-37.5 (1991), pp. 1274–1287.

[69] Matthieu Finiasz and Nicolas Sendrier. "Security bounds for the design of code-based cryptosystems". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2009, pp. 88–105.

[70] Jean-Bernard Fischer and Jacques Stern. "An efficient pseudo-random generator provably as secure as syndrome decoding". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 1996, pp. 245–255.

[71] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. "Falcon: Fast-Fourier Lattice-Based Compact Signatures over NTRU". In: *Submission to the NIST's post-quantum cryptography standardization process* (2018).

[72] Philippe Gaborit, Cedric Laudaroux, Nicolas Sendrier, et al. "Synd: a very fast code-based cipher stream with a security reduction". In: *IEEE Conference, ISIT*. Vol. 7. 2007, pp. 186–190.

[73] Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. "A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes". In: *arXiv preprint arXiv:1204.6459* (2012).

[74] Louis Goubin and Nicolas T. Courtois. "Cryptanalysis of the TTM Cryptosystem". In: *Advances in Cryptology — ASIACRYPT 2000: 6th International Conference on the Theory and Application of Cryptology and Information Security Kyoto, Japan, December 3–7, 2000 Proceedings*. Ed. by Tatsuaki Okamoto. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 44–57.

[75] Cheikh Thiécoumba Gueye, Jean Belo Klamti, and Shoichi Hirose. "Generalization of BJMM-ISD Using May-Ozerov Nearest Neighbor Algorithm over an Arbitrary Finite Field $\mathbb{F}_q$". In: *Codes, Cryptology and Information Security*. Ed. by Said El Hajji, Abderrahmane Nitaj, and El Mamoun Souidi. Cham: Springer International Publishing, 2017, pp. 96–109.

[76] Venkatesan Guruswami and Atri Rudra. "Explicit Codes achieving List Decoding Capacity: Error-Correction With Optimal Redundancy". In: *IEEE Transactions on Information Theory* 54.1 (2008), pp. 135–150. ISSN: 0018-9448. DOI: 10.1109/TIT.2007.911222.

[77] Venkatesan Guruswami and Madhu Sudan. "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes". In: *IEEE Transactions on Information Theory* 45.6 (1999), pp. 1757–1767. DOI: 10.1109/18.782097.

[78] Mike Hamburg. "Post-Quantum Cryptography Proposal: ThreeBears". In: *NIST PQC Round* 2 (2019), p. 4.

[79] Yasufumi Hashimoto. "Multivariate Public Key Cryptosystems". In: *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*. Ed. by Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, and Dung Hoang Duong. Singapore: Springer Singapore, 2018, pp. 17–42.

[80] Christopher J. Hillar and Lek-Heng Lim. "Most Tensor Problems Are NP-Hard". In: *J. ACM* 60.6 (Nov. 2013), 45:1–45:39. ISSN: 0004-5411.

[81] Shoichi Hirose. "May-Ozerov Algorithm for Nearest-Neighbor Problem over $\mathbb{F}_q$ and Its Application to Information Set Decoding". In: *International Conference for Information Technology and Communications*. Springer. 2016, pp. 115–126.

[82] Timothy J. Hodges, Christophe Petit, and Jacob Schlather. "First Fall Degree and Weil Descent". In: *Finite Fields Appl.* 30 (Nov. 2014), pp. 155–177. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2014.07.001.

[83] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". In: *International Algorithmic Number Theory Symposium*. Springer. 1998, pp. 267–288.

[84] Anna-Lena Horlemann-Trautmann and Violetta Weger. "Information Set Decoding in the Lee Metric with Applications to Cryptography". In: *arXiv preprint arXiv:1903.07692* (2019).

[85] Thomas D. Howell. "Global Properties of Tensor Rank". In: *Linear Algebra and its Applications* 22.Supplement C (1978), pp. 9 –23. ISSN: 0024-3795.

[86] Nick Howgrave-Graham and Antoine Joux. "New generic algorithms for hard knapsacks". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2010, pp. 235–256.

[87] Carmelo Interlando, Karan Khathuria, Nicole Rohrer, Joachim Rosenthal, and Violetta Weger. "Generalization of the ball-collision algorithm". In: *Journal of Algebra Combinatorics Discrete Structures and Applications* 7 (2020), pp. 195 –207. DOI: 10.13069/jacodesmath.729477.

[88] Heeralal Janwa and Oscar Moreno. "McEliece public key cryptosystems using algebraic-geometric codes". In: *Designs, Codes and Cryptography* 8.3 (1996), pp. 293–307.

[89] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, et al. "Supersingular Isogeny Key Encapsulation". In: *NIST Round* 1 (2017).

[90] Abdel Alim Kamal and Amr M. Youssef. "Cryptanalysis of a Key Exchange Protocol based on the Endomorphisms ring End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$". In: *Applicable Algebra in Engineering, Communication and Computing* 23.3 (2012), pp. 143–149. ISSN: 1432-0622. DOI: 10.1007/s00200-012-0170-z.

[91] Karan Khathuria, Giacomo Micheli, and Violetta Weger. "On the Algebraic Structure of $E_p^{(m)}$ and Applications to Cryptography". In: *Applicable Algebra in Engineering, Communication and Computing* (2019). ISSN: 1432-0622. DOI: https://doi.org/10.1007/s00200-019-00410-1.

[92] Karan Khathuria, Joachim Rosenthal, and Violetta Weger. "Encryption Scheme Based on Expanded Reed-Solomon Codes". In: *Advances in Mathematics of Communications* (2019). ISSN: 1930-5346. DOI: 10.3934/amc.2020053.

[93] Karan Khathuria, Joachim Rosenthal, and Violetta Weger. "Weight Two Masking of the Reed-Solomon Structure in Conjugation with List Decoding". In: Proceedings of the 23rd International Symposium on Mathematical Theory of Networks and Systems – MTNS. 2018. DOI: 10.5167/uzh-168132.

[94] Aviad Kipnis, Jacques Patarin, and Louis Goubin. "Unbalanced Oil and Vinegar Signature Schemes". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 206–222.

[95] Aviad Kipnis and Adi Shamir. "Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization". In: *Advances in Cryptology — CRYPTO' 99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings*. Ed. by Michael Wiener. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 19–30.

[96] Ki Hyoung Ko, Jang Won Lee, and Tony Thomas. "Towards generating secure keys for braid cryptography". In: *Designs, Codes and Cryptography* 45.3 (2007), pp. 317–333.

[97] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. "New public-key cryptosystem using braid groups". In: *Annual International Cryptology Conference*. Springer. 2000, pp. 166–183.

[98] Kazukuni Kobara and Hideki Imai. "Semantically Secure McEliece Public-Key Cryptosystems -Conversions for McEliece PKC -". In: *Public Key Cryptography*. Ed. by Kwangjo Kim. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 19–35. ISBN: 978-3-540-44586-9.

[99] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209.

[100] Joseph B. Kruskal. "Three-way Arrays: Rank and Uniqueness of Trilinear Decompositions, with Application to Arithmetic Complexity and Statistics". In: *Linear Algebra and its Applications* 18.2 (1977), pp. 95 –138. ISSN: 0024-3795. DOI: https://doi.org/10.1016/0024-3795(77)90069-6.

[101] Grégory Landais and Jean-Pierre Tillich. "An efficient attack of a McEliece cryptosystem variant based on convolutional codes". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2013, pp. 102–117.

[102] Pil Joong Lee and Ernest F. Brickell. "An observation on the security of McEliece2019s public-key cryptosystem". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1988, pp. 275–280.

[103] Jeffrey S. Leon. "A probabilistic algorithm for computing minimum weights of large error-correcting codes". In: *IEEE Transactions on Information Theory* 34.5 (1988), pp. 1354–1359.

[104] Yuan Xing Li, Robert H. Deng, and Xin Mei Wang. "On the Equivalence of McEliece's and Niederreiter's Public-Key Cryptosystems". In: *IEEE Transactions on Information Theory* 40.1 (1994), pp. 271–273.

[105] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Second. Vol. 20. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn. Cambridge: Cambridge University Press, 1997, pp. xiv+755. ISBN: 0-521-39231-4.

[106] Carl Löndahl and Thomas Johansson. "A new version of McEliece PKC based on convolutional codes". In: *International Conference on Information and Communications Security*. Springer. 2012, pp. 461–470.

[107] Juan Antonio López-Ramos, Joachim Rosenthal, Davide Schipani, and Reto Schnyder. "Group Key Management based on Semigroup Actions". In: *Journal of Algebra and Its Applications* 16.8 (2017). DOI: 10.1142/S0219498817501481.

[108] Rusydi H. Makarim and Marc Stevens. "M4GB: An Efficient Gröbner-Basis Algorithm". In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. ISSAC '17. Kaiserslautern, Germany: ACM, 2017, pp. 293–300. ISBN: 978-1-4503-5064-8. DOI: 10.1145/3087604.3087638.

[109] James L. Massey. "Shift-Register Synthesis and BCH Decoding". In: *IEEE Transactions on Information Theory* IT-15 (1969), pp. 122–127.

[110] Tsutomu Matsumoto and Hideki Imai. "Public Quadratic Polynominal-Tuples for Efficient Signature-Verification and Message-Encryption." In: *Eurocrypt*. Vol. 88. Springer. 1988, pp. 419–453.

[111] Alexander May, Alexander Meurer, and Enrico Thomae. "Decoding Random Linear Codes in $\mathcal{O}(2^{0.054n})$". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2011, pp. 107–124.

[112] Alexander May and Ilya Ozerov. "On computing nearest neighbors with applications to decoding of binary linear codes". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2015, pp. 203–228.

[113] Gérard Maze, Chris Monico, and Joachim Rosenthal. "Public Key Cryptography based on Semigroup Actions". In: *Advances in Mathematics of Communications* 1.4 (2007), pp. 489–507.

[114] Robert J. McEliece. *A Public-Key Cryptosystem Based on Algebraic Coding Theory*. Tech. rep. Jet Propulsion Laboratory, Pasadena: DSN Progress report, 1978, pp. 114–116.

[115] Robert J. McEliece. "The Guruswami–Sudan Decoding Algorithm for Reed–Solomon Codes". In: *Interplanetary Network Progress Report* 153 (2003), pp. 1–60.

[116] Carlos Aguilar Melchor, Nicolas Aragon, Magali Bardet, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Ayoub Otmani, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. "ROLLO-Rank-Ouroboros, LAKE & LOCKER". In: (2018).

[117] Alfred J. Menezes and Yi-Hong Wu. "The discrete logarithm problem in GL(n, q)". In: *Ars Combinatoria* 47 (1997), pp. 23–32.

[118] Alexander Meurer. "A coding-theoretic approach to cryptanalysis". PhD thesis. Bochum-Ruhr University, 2012.

[119] Giacomo Micheli. "Cryptanalysis of a non-commutative Key Exchange Protocol". In: *Advances in Mathematics of Communications* 9.2 (2015), pp. 247–253.

[120] Giacomo Micheli and Violetta Weger. "Cryptanalysis of the CLR-cryptosystem". In: *Designs, Codes and Cryptography* 87.5 (2019), pp. 1069–1086.

[121] Victor S Miller. "Use of elliptic curves in cryptography". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426.

[122] Lorenz Minder and Amin Shokrollahi. "Cryptanalysis of the Sidelnikov cryptosystem". In: *Advances in cryptology—EUROCRYPT 2007*. Vol. 4515. Lecture Notes in Comput. Sci. Springer, Berlin, 2007, pp. 347–360. DOI: 10.1007/978-3-540-72540-4_20.

[123] Rafael Misoczki, Jean-Piere Tillich, Nicolas Sendrier, and Paulo S.L.M. Barreto. "MDPC-McEliece: New McEliece variants from moderate density parity-check codes". In: (2013), pp. 2069–2073.

[124] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. "An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme". In: *Post-Quantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*. Ed. by Michele Mosca. Cham: Springer International Publishing, 2014, pp. 180–196.

[125] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. "Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme". In: *Post-Quantum Cryptography*. Ed. by Tanja Lange and Tsuyoshi Takagi. Cham: Springer International Publishing, 2017, pp. 255–271.

[126] Dustin Moody, Ray Perlner, and Daniel Smith-Tone. "Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme". In: *Selected Areas in Cryptography – SAC 2016*. Ed. by Roberto Avanzi and Howard Heys. Cham: Springer International Publishing, 2017, pp. 543–558.

[127] Robert Niebuhr, Edoardo Persichetti, Pierre-Louis Cayrel, Stanislav Bulygin, and Johannes Buchmann. "On Lower Bounds for Information Set Decoding over $\mathbb{F}_q$ and on the Effect of Partial Knowledge". In: *Int. J. Inf. Coding Theory* 4.1 (Jan. 2017), pp. 47–78. ISSN: 1753-7703. DOI: 10.1504/IJICOT.2017.081458.

[128] Harald Niederreiter. "Knapsack-Type Cryptosystems and Algebraic Coding Theory". In: *Problems of Control and Information Theory 15* 1.6 (1986), pp. 159–166.

[129] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot. "Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes". In: *Mathematics in Computer Science* 3.2 (2010), pp. 129–140.

[130] Farzad Parvaresh and Alex Vardy. "Correcting Errors Beyond the Guruswami-Sudan Radius in Polynomial Time". In: *Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on* (2005), pp. 285–294. DOI: 10.1109/SFCS.2005.29.

[131] Jacques Patarin. "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88". In: *Des. Codes Cryptogr.* 20.2 (2000), pp. 175–209.

[132] Jacques Patarin. "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms". In: *Advances in Cryptology — EUROCRYPT '96*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 33–48. ISBN: 978-3-540-68339-1.

[133] Jacques Patarin. "The Oil and Vinegar Signature Scheme". In: *Dagstuhl Workshop on Cryptography1997*. 1997.

[134] Ruud Pellikaan and Irene Márquez-Corbella. "Error-Correcting Pairs for a Public-Key Cryptosystem". In: *Journal of Physics: Conference Series*. Vol. 855. 1. IOP Publishing. 2017, p. 012032.

[135] Christiane Peters. "Information-set decoding for linear codes over $\mathbb{F}_q$". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2010, pp. 81–94.

[136] Christiane Peters. "Information-Set Decoding for Linear Codes over $\mathbb{F}_q$." In: *PQCrypto* 2010 (2010). http://christianepeters.wordpress.com/publications/tools/, pp. 81–94.

[137] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. "Selecting Parameters for the Rainbow Signature Scheme". In: *Post-Quantum Cryptography*. Ed. by Nicolas Sendrier. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 218–240.

[138] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. "Design Principles for HFEv- Based Multivariate Signature Schemes". In: *Advances in Cryptology – ASIACRYPT 2015*. Ed. by Tetsu Iwata and Jung Hee Cheon. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 311–334.

[139] Eugene Prange. "The use of information sets in decoding cyclic codes". In: *IRE Transactions on Information Theory* 8.5 (1962), pp. 5–9.

[140] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.

[141] Ronny M. Roth and G. Ruckenstein. "Efficient Decoding of Reed-Solomon Codes Beyond Half the Minimum Distance". In: *IEEE Transactions on Information Theory* 46.1 (2000), pp. 246–257. ISSN: 0018-9448. DOI: 10.1109/18.817522.

[142] Eligijus Sakalauskas and Tomas Burba. "Basic semigroup primitive for cryptographic session key exchange protocol (SKEP)". In: *Information Technology and Control* 3 (2003), p. 28.

[143] James T. Schwartz. "Fast Probabilistic Algorithms for Verification of Polynomial Identities". In: *Journal of the ACM (JACM)* 27.4 (1980), pp. 701–717.

[144] Friedland Shmuel. "Remarks on the Symmetric Rank of Symmetric Tensors". In: *arxiv.org/pdf/1505.00860* (Jan. 2016).

[145] Friedland Shmuel and Mał gorzata Stawiska. "Best Approximation on Semi-Algebraic Sets and k-border Rank Approximation of Symmetric Tensors". In: *arxiv.org/pdf/1311.1561* (Nov. 2013).

[146] Peter W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*. Los Alamitos, CA: IEEE Comput. Soc. Press, 1994, pp. 124–134.

[147] Peter W Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM review* 41.2 (1999), pp. 303–332.

[148] Vladimir Shpilrain and Alexander Ushakov. "Thompson's group and public key cryptography". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2005, pp. 151–163.

[149] Vladimir Shpilrain and Gabriel Zapata. "Combinatorial group theory and public key cryptography". In: *Applicable Algebra in Engineering, Communication and Computing* 17.3-4 (2006), pp. 291–302.

[150] Vladimir M. Sidelnikov. "A public key cryptosystem based on Reed-Muller binary codes". In: *Discrete Math. Appl.* 4.3 (1994), pp. 191–207.

[151] Vladimir M. Sidelnikov, Mikhail A. Cherepnev, and Valerii V. Yashchenko. "Systems of open distribution of keys on the basis of noncommutative semigroups". In: *Russian Academy of Sciences-Doklady Mathematics*. Vol. 48. 2. 1994, pp. 384–386.

[152] Vladimir M. Sidelnikov and Sergey O. Shestakov. "On an encoding system constructed on the basis of generalized Reed-Solomon codes". In: *Diskret. Mat.* 4.3 (1992), pp. 57–63. ISSN: 0234-0860.

[153] Vladimir M. Sidelnikov and Sergey O. Shestakov. "On Insecurity of Cryptosystems Based on Generalized Reed-Solomon Codes". In: *Discrete Mathematics and Applications* 2.4 (1992), pp. 439–444.

[154] Pierre-Jean Spaenlehauer. "Solving multi-homogeneous and determinantal systems. Algorithms - Complexity - Applications." PhD thesis. PhD thesis, Université Paris 6, 2012. URL: http://www-polsys.lip6.fr/~spaenleh/data/these_spaenlehauer.pdf.

[155] William Stein et al. *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team. 2014. URL: http://www.sagemath.org.

[156] Jacques Stern. "A new identification scheme based on syndrome decoding". In: *Annual International Cryptology Conference*. Springer. 1993, pp. 13–21.

[157] Jean-Pierre Tillich and Gilles Zémor. "Hashing with SL 2". In: *Annual International Cryptology Conference*. Springer. 1994, pp. 40–49.

[158] Alexander Vardy and Yair Be′ery. "Bit-level soft-decision decoding of Reed-Solomon codes". In: *IEEE Transactions on Communications* 39.3 (1991), pp. 440–444.

[159] Violetta Weger. "A Code-Based Cryptosystem using GRS Codes". Master Thesis at the University of Zürich (Switzerland). 2016.

[160] Violetta Weger, Massimo Battaglioni, Paolo Santini, Franco Chiaraluce, Marco Baldi, and Edoardo Persichetti. "Information set decoding of Lee-metric codes over finite rings". In: *arXiv preprint arXiv:2001.08425* (2020).

[161] Violetta Weger, Massimo Battaglioni, Paolo Santini, Anna-Lena Horlemann-Trautmann, and Edoardo Persichetti. "On the Hardness of the Lee Syndrome Decoding Problem". In: (2020). arXiv: 2002.12785 [cs.IT].

[162] Christian Wieschebrink. "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2010, pp. 61–72.

[163] Bo-Yin Yang and Jiun-Ming Chen. "Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS". In: *Information Security and Privacy*. Ed. by Colin Boyd and Juan Manuel González Nieto. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 518–531.

[164] Yang Zhang. "Cryptanalysis of a key exchange protocol based on the ring $E_p^{(m)}$". In: *Applicable Algebra in Engineering, Communication and Computing* 29.2 (2018), pp. 103–112.

[165] Richard Zippel. "Probabilistic Algorithms for Sparse Polynomials". In: *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*. EUROSAM '79. London, UK, UK: Springer-Verlag, 1979, pp. 216–226. ISBN: 3-540-09519-5. URL: http://dl.acm.org/citation.cfm?id=646670.698972.