

A Survey on Code-based Cryptography

Violetta Weger¹, Niklas Gassner², and Joachim Rosenthal²

¹Department of Electrical and Computer Engineering, Technical University of Munich, Theresienstrasse 90, 80333 Munich, Germany, violetta.weger@tum.de

²Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich, Switzerland, {niklas.gassner, rosenthal}@math.uzh.ch

February 2, 2024

Abstract

The improvements on quantum technology are threatening our daily cybersecurity, as a capable quantum computer can break all currently employed asymmetric cryptosystems. In preparation for the quantum-era the National Institute of Standards and Technology (NIST) has initiated in 2016 a standardization process for public-key encryption (PKE) schemes, key-encapsulation mechanisms (KEM) and digital signature schemes. In 2023, NIST made an additional call for post-quantum signatures. With this chapter we aim at providing a survey on code-based cryptography, focusing on PKEs and signature schemes. We cover the main frameworks introduced in code-based cryptography and analyze their security assumptions. We provide the mathematical background in a lecture notes style, with the intention of reaching a wider audience.

Contents

1	Introduction	4
1.1	Organization of the Chapter	5
2	Preliminaries	6
2.1	Notation	6
2.2	Algebraic Coding Theory	6
2.2.1	Basics on Hamming-Metric Codes	6
2.2.2	Matrix Codes	11
2.2.3	Generalized Reed-Solomon Codes	13
2.2.4	Goppa Codes	14
2.2.5	Cyclic Codes	15
2.2.6	LDPC Codes	17
2.2.7	Reed-Muller Codes	18
2.2.8	Concatenated Codes	19
2.2.9	$(U, U + V)$ -Codes	19
2.2.10	Product Codes	19
2.2.11	Rank-Metric Codes	20
2.2.12	Gabidulin Code	23
2.2.13	LRPC Codes	25
2.2.14	Code Equivalence	25
2.2.15	Lee Metric Codes	27
2.2.16	Restricted Errors	29
2.3	Cryptography	30
2.3.1	Public-Key Encryption	31
2.3.2	Key-Encapsulation Mechanisms	32
2.3.3	Digital Signature Schemes	34
2.3.4	Zero-Knowledge Protocols	35
2.3.5	Fiat-Shamir Transform	38
2.3.6	Multi-Party-Computations-in-the-Head	39
3	Code-Based Public-Key Encryption Frameworks	43
3.1	McEliece Framework	44
3.2	Niederreiter Framework	48
3.3	Alekhnovich's Cryptosystems	50
3.3.1	The First Variant	50
3.3.2	The Second Variant	52
3.4	Quasi-Cyclic Scheme	53
3.5	Augot-Finiasz Cryptosystem	57
3.6	GPT Cryptosystem	59
4	Code-based Signature Schemes	62
4.1	Hash-and-Sign	62
4.1.1	CFS Scheme	62
4.1.2	RankSign	66
4.2	Code-Based ZK Protocols	67
5	Security Analysis	73

5.1	Problems from Coding Theory	73
5.2	NP-completeness	76
5.2.1	Decoding Problem	78
5.2.2	Code Equivalence Problems	82
5.2.3	Rank SDP	84
5.2.4	Lee SDP	86
5.2.5	Restricted SDP	86
5.3	Information Set Decoding	89
5.3.1	General Algorithm	90
5.3.2	Overview Algorithms	90
5.3.3	Techniques	93
5.3.4	Prange’s Algorithm	96
5.3.5	Stern’s Algorithm	98
5.3.6	BJMM Algorithm	102
5.3.7	Generalized Birthday Decoding Algorithms	106
5.3.8	Asymptotic Cost	108
5.3.9	Rank-metric ISD Algorithms	109
5.3.10	Attacks on other Code-Based Problems	114
5.4	Algebraic Attacks	115
5.5	Other Attacks	118
6	Historical Overview	121
7	Submissions to NIST	124
7.1	Round 4 Candidates: Classic McEliece, BIKE and HQC	127
7.1.1	Classic McEliece	127
7.1.2	Proposed Parameters for Classic McEliece	128
7.1.3	BIKE	128
7.1.4	Proposed Parameters for BIKE	130
7.1.5	HQC	130
7.1.6	Proposed Parameters for HQC	131
7.2	Code-Based Signature Schemes	132
7.2.1	Hash-and-sign schemes	133
7.2.2	ZK Protocols and Fiat-Shamir Transform	136
7.2.3	ZK Protocols and MPCitH	140
8	Conclusion	148

1 Introduction

Current public-key cryptosystems are based on integer factorization or the discrete logarithm problem over an elliptic curve or over a finite field. While there are no algorithms known for classical computers to solve these problems efficiently, Shor’s algorithm allows a quantum computer to solve these problems in polynomial time [241]. As research on quantum computers advances, the cryptographic community is searching for cryptosystems that will survive attacks on quantum computers. This area of research is called *post-quantum cryptography*.

In 2016, the National Institute of Standards and Technology (NIST) has initiated a standardization process for post-quantum cryptosystems. Such cryptosystems can be based on any hard problem, which cannot be solved by a capable quantum computer in polynomial time. Preferably, these are NP-complete problems, i.e., at least as hard as the hardest problems in NP.

The main candidates for post-quantum cryptography are:

- **Code-based cryptography (CBC):** CBC is using hard problems from algebraic coding theory. Usually, this is the NP-complete problem of decoding a random linear code.
- **Lattice-based cryptography:** Lattice-based cryptography is based on hard problems over lattices, such as the NP-complete problems of finding the shortest vector, respectively the closest vector to a given vector in a lattice. For an overview see [210].
- **Multivariate cryptography:** Multivariate cryptography is based on the NP-complete problem of solving multivariate (quadratic) equations defined over some finite field. For an overview see [113].
- **Isogeny-based cryptography:** Isogeny-based cryptography is based on finding the isogeny map between two supersingular elliptic curves [161].
- **Hash-based cryptography:** These cryptosystems base their security on the security of hash functions.

This survey only covers code-based cryptography, thus, we refer an interested reader to [69], for an overview on post-quantum cryptography in general.

Code-based cryptography denotes any cryptographic system, which bases its security on hard problems from algebraic coding theory. Classically, this problem is the decoding of a random linear code. This problem was shown to be NP-complete in 1978, by Berlekamp, McEliece and Van Tilborg in [67]. In the same year, McEliece proposed the first code-based cryptosystem [193], in which one picks a code with underlying algebraic structure that allows efficient decoding and then disguises this code as a seemingly random linear code. A message gets encrypted as corrupted codeword. With the knowledge of the secret code, one can recover the initial message, but an adversary faces the challenge of decoding a random linear code.

In 2022, NIST selected 4 cryptographic systems to get standardized, namely the lattice-based encryption scheme KYBER [235], the lattice-based signature schemes DILITHIUM [115] and FALCON [124] and the hash-based signature scheme SPHINCS⁺ [34]. However, the standardization process of 2016 is not over yet, as three code-based schemes have moved to the fourth and final round, namely Classical McEliece [14], HQC [5] and BIKE [20].

The research in this area is, however, far from complete. In fact, in 2023, NIST has reopened the standardization call for signature schemes. Within this new call, we can find many code-based schemes and many new and interesting problems.

In this chapter we give an extensive survey on code-based cryptography, explaining the mathematical background of such systems and the difficulties of proposing secure and at the same time practical schemes. We cover the main proposals in the standardization call and the approaches to break such systems. With the reopened standardization process for digital signature schemes, we hope to reach different research communities to tackle this new challenge together.

1.1 Organization of the Chapter

This chapter is organized as follows. In Section 2, we introduce some basics of algebraic coding theory as well as the basics of asymmetric cryptography, such as public-key encryption schemes and signature schemes. In particular, we aim at introducing all used coding-theoretic objects in Section 2.2 and to describe on a high-level the considered cryptographic schemes in 2.3. This includes public-key encryption (PKE), key-encapsulation mechanism (KEM) and signature schemes. In particular, we show how to construct a signature scheme via the Fiat-Shamir transform on a Zero-Knowledge (ZK) protocol. We also cover the new methods, such as protocols with helpers and Multi-Party Computations (MPC).

The main focus of this chapter will lay on Section 3 where we introduce the public-key encryption frameworks by McEliece, Niederreiter, Alekhnovich as well as the quasi-cyclic scheme, the GPT cryptosystem and the Faure-Loidreau cryptosystem.

In Section 4, we discuss some code-based signatures, starting with the first construction method, namely hash-and-sign in Section 4.1, then moving to some classic code-based ZK protocols in Section 4.2 and describe some new techniques, such as MPC-in-the-head.

In Section 5, we analyze the security of these systems, where we first focus on the decoding problem of a random linear code: we present the proofs of NP-completeness in Section 5.2 and the best-known solvers for the underlying problems in Section 5.3. In the second part of the security analysis, namely Section 5.4 we also present some algebraic attacks, which clearly depend on the chosen secret code. For this section, we focus on two of the most preferred codes, one being Reed-Solomon codes and the other being their rank metric analog, Gabidulin codes. Finally, we end the security analysis by shortly reporting on some other ways of attacking code-based systems, such as side-channel attacks, in Section 5.5.

In Section 6, we provide a historical overview on the main code-based PKE and signature scheme proposals, stating their differences, in the notion of the given frameworks, and whether they are broken.

In Section 7, we shortly cover the submissions to the NIST standardization process with a focus on the finalists in Section 7.1: Classic McEliece, BIKE and HQC.

In Section 7.2, we present the 11 code-based signature schemes submitted to the reopened standardization call and compare their performance in terms of signature and public key size and their running times.

2 Preliminaries

In order to make this chapter as self-contained as possible, we present here a rather long preliminary section, which hopefully makes this survey also accessible to non-experts. We start with the notation used throughout this chapter, followed by the basics of algebraic coding theory and defining all concepts and codes that will be used or mentioned and finally presenting the basics of the considered schemes on a very high-level and with specific examples.

2.1 Notation

We denote by \mathbb{F}_q the finite field with q elements, where q is a prime power and denote by \mathbb{F}_q^\star its multiplicative group, i.e., $\mathbb{F}_q \setminus \{0\}$. Throughout this chapter, we denote by bold upper case or lower case letters matrices, respectively vectors, e.g. $\mathbf{x} \in \mathbb{F}_q^n$ and $\mathbf{A} \in \mathbb{F}_q^{k \times n}$. The identity matrix of size k is denoted by Id_k . Sets are denoted by upper case letters and for a set S , we denote by $|S|$ its cardinality. By $\text{GL}_n(\mathbb{F}_q)$ we denote the $n \times n$ invertible matrices over \mathbb{F}_q . Notation specific to only one part of this chapter will be defined right before they are used.

2.2 Algebraic Coding Theory

This section is designed to recall and/or introduce all definitions and coding theoretic objects required in this chapter. Most proofs will be omitted or left as an exercise. For interested readers that are completely new to algebraic coding theory we recommend the following books [229, 66, 254, 188]. We also leave away the references to standard definitions and results, which can be found in any book on coding theory. For more specific results, we will give a proper reference.

2.2.1 Basics on Hamming-Metric Codes

In classical coding theory one considers the finite field \mathbb{F}_q of q elements, where q is a prime power.

Definition 1 (Linear Code). Let $1 \leq k \leq n$ be integers. Then, an $[n, k]$ *linear code* \mathcal{C} over \mathbb{F}_q is a k -dimensional linear subspace of \mathbb{F}_q^n .

Note that we emphasize the linearity, as a *code* is simply any subset $\mathcal{C} \subseteq \mathbb{F}_q^n$.

The parameter n is called the *length* of the code, the elements in the code are called *codewords* and $R = k/n$ is called the *rate* of the code. In order to measure how far apart two vectors are, we endow \mathbb{F}_q with a metric. Usually, this is the *Hamming metric*.

Definition 2 (Hamming Metric). Let n be a positive integer. For $\mathbf{x} \in \mathbb{F}_q^n$, the *Hamming weight* of \mathbf{x} is given by the size of its support, i.e.,

$$\text{wt}_H(\mathbf{x}) = |\{i \in \{1, \dots, n\} \mid x_i \neq 0\}|.$$

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, the *Hamming distance* between \mathbf{x} and \mathbf{y} is given by the number of positions in which they differ, i.e.,

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}|.$$

Note that the Hamming distance is induced from the Hamming weight, that is $d_H(\mathbf{x}, \mathbf{y}) = \text{wt}_H(\mathbf{x} - \mathbf{y})$. Having defined a metric, one can also consider the minimum distance of a code, i.e., the smallest distance achieved by its distinct codewords.

Definition 3 (Minimum Distance). Let \mathcal{C} be a code over \mathbb{F}_q . The *minimum Hamming distance* of \mathcal{C} is denoted by $d_H(\mathcal{C})$ and given by

$$d_H(\mathcal{C}) = \min\{d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}.$$

Exercise 4. Show that for a linear code \mathcal{C} , we have

$$d_H(\mathcal{C}) = \min\{\text{wt}_H(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{0}\}.$$

Exercise 5. Give an example, where

$$d_H(\mathcal{C}) \neq \min\{\text{wt}_H(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{0}\}.$$

We denote by $d_H(\mathbf{x}, \mathcal{C})$ the minimal distance between $\mathbf{x} \in \mathbb{F}_q^n$ and a codeword in \mathcal{C} .

Let r be a positive integer. We define the Hamming ball as all the vectors which have at most Hamming weight r , i.e.,

$$B_H(r, n, q) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \text{wt}_H(\mathbf{x}) \leq r\}.$$

Exercise 6. Show that

$$|B_H(r, n, q)| = \sum_{i=0}^r \binom{n}{i} (q-1)^i.$$

The minimum distance of a code is an important parameter, since it is connected to the error correction capability of the code.

We say that a code can *correct* up to t errors, if for all $\mathbf{x} \in \mathbb{F}_q^n$ with $d_H(\mathbf{x}, \mathcal{C}) \leq t$, there exists exactly one $\mathbf{y} \in \mathcal{C}$, such that $d_H(\mathbf{x}, \mathbf{y}) \leq t$. A *decoding algorithm* \mathcal{D} is an algorithm that is given such a word $\mathbf{x} \in \mathbb{F}_q^n$ and returns the closest codeword, $\mathbf{y} \in \mathcal{C}$, such that $d_H(\mathbf{x}, \mathbf{y}) \leq t$. The most interesting codes for applications are codes with an efficient decoding algorithm, which clearly not every code possesses.

Exercise 7. Let \mathcal{C} be a linear code over \mathbb{F}_q of length n and of minimum distance d_H . Show that the code can correct up to $t := \left\lfloor \frac{d_H-1}{2} \right\rfloor$ errors.

One of the most important bounds in coding theory is the Singleton bound, which provides an upper bound on the minimum distance of a code.

Theorem 8 (Singleton Bound [246]). Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Then,

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

Exercise 9. Prove the Singleton Bound by showing that deleting $d_H - 1$ of the positions is an injective map.

A code that achieves the Singleton bound is called a *maximum distance separable* (MDS) code. MDS codes are of immense interest, since they can correct the maximal amount of errors for fixed code parameters.

Linear codes allow for an easy representation through their generator matrices, which have the code as an image.

Definition 10 (Generator Matrix). Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Then, a matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ is called a *generator matrix* of \mathcal{C} if

$$\mathcal{C} = \{\mathbf{xG} \mid \mathbf{x} \in \mathbb{F}_q^k\},$$

that is, the rows of \mathbf{G} form a basis of \mathcal{C} .

We will often write $\langle \mathbf{G} \rangle$ to denote the code generated by \mathbf{G} .

One can also represent the code through a matrix \mathbf{H} , which has the code as kernel.

Definition 11 (Parity-Check Matrix). Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Then, a matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ is called a *parity-check matrix* of \mathcal{C} , if

$$\mathcal{C} = \left\{ \mathbf{y} \in \mathbb{F}_q^n \mid \mathbf{H}\mathbf{y}^\top = \mathbf{0} \right\}.$$

For any $\mathbf{x} \in \mathbb{F}_q^n$, we call $\mathbf{x}\mathbf{H}^\top$ a *syndrome*.

Exercise 12. Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Let \mathbf{H} be a parity-check matrix of \mathcal{C} . Show that \mathcal{C} has minimum distance d_H if and only if every $d_H - 1$ columns of \mathbf{H} are linearly independent and there exist d_H columns, which are linearly dependent.

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ let us denote by $\langle \mathbf{x}, \mathbf{y} \rangle$ the standard inner product, i.e.,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i y_i.$$

Then, we can define the dual of an $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q as the orthogonal space of \mathcal{C} .

Definition 13 (Dual Code). Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . The *dual code* \mathcal{C}^\perp is an $[n, n - k]$ linear code over \mathbb{F}_q , defined as

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \ \forall \ \mathbf{y} \in \mathcal{C} \}.$$

Exercise 14. Show that a parity-check matrix of \mathcal{C} is in fact a generator matrix of \mathcal{C}^\perp .

Exercise 15. Show that the dual of an MDS code is an MDS code.

For $\mathbf{x} \in \mathbb{F}_q^n$ and $S \subseteq \{1, \dots, n\}$ we denote by \mathbf{x}_S the vector consisting of the entries of \mathbf{x} indexed by S . While for $\mathbf{A} \in \mathbb{F}_q^{k \times n}$, we denote by \mathbf{A}_S the matrix consisting of the columns of \mathbf{A} indexed by S . Similarly, we denote by \mathcal{C}_S the code consisting of the codewords \mathbf{c}_S .

Observe that an $[n, k]$ linear code can be completely defined by certain sets of k positions. The following concept characterizes such defining sets.

Definition 16 (Information Set). Let $k \leq n$ be positive integers and let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Then, a set $I \subset \{1, \dots, n\}$ of size k is called an *information set* of \mathcal{C} if

$$|\mathcal{C}| = |\mathcal{C}_I|.$$

Exercise 17. How many information sets can an $[n, k]$ linear code have at most?

Exercise 18. Let \mathcal{C} be an $[n, k]$ linear code, I an information set and let \mathbf{G} be a generator matrix and \mathbf{H} a parity-check matrix. Show that \mathbf{G}_I is an invertible matrix of size k . If $I^C := \{1, \dots, n\} \setminus I$ is the complement set of I , then, \mathbf{H}_{I^C} is an invertible matrix of size $n - k$.

Exercise 19. Let \mathcal{C} be the code generated by $\mathbf{G} \in \mathbb{F}_5^{2 \times 4}$, given as

$$\mathbf{G} = \begin{pmatrix} 1 & 3 & 2 & 3 \\ 0 & 4 & 4 & 3 \end{pmatrix}.$$

Determine all information sets of this code.

Definition 20 (Systematic Form). Let $k \leq n$ be positive integers and \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . Then, there exist some permutation matrix \mathbf{P} and some invertible matrix \mathbf{U} that bring \mathbf{G} in *systematic form*, i.e.,

$$\mathbf{UGP} = (\text{Id}_k \quad \mathbf{A}),$$

where $\mathbf{A} \in \mathbb{F}_q^{k \times (n-k)}$. Similarly, there exist some permutation matrix \mathbf{P}' and some invertible matrix \mathbf{U}' , that bring \mathbf{H} into systematic form as

$$\mathbf{U}'\mathbf{HP}' = (\mathbf{B} \quad \text{Id}_{n-k}),$$

where $\mathbf{B} \in \mathbb{F}_q^{(n-k) \times k}$.

Let us denote by $V_H(r, n, q)$ the volume of a ball in the Hamming metric, i.e.,

$$V_H(r, n, q) = |B_H(r, n, q)|.$$

The Gilbert-Varshamov bound [139, 257, 231] is one of the most prominent bounds in coding theory and widely used in code-based cryptography since it provides a sufficient condition for the existence of linear codes.

Theorem 21 (Gilbert-Varshamov bound). *Let q be a prime power and let $k \leq n$ and d_H be positive integers, such that*

$$V_H(d_H - 2, n - 1, q) < q^{n-k}.$$

Then, there exists a $[n, k]$ linear code over \mathbb{F}_q with minimum Hamming distance at least d_H .

The better known Gilbert-Varshamov bound is a statement on the maximal size of a code, that is: let us denote by $A_H(n, d, q)$ the maximal size of a code in \mathbb{F}_q^n having minimum Hamming distance d .

Theorem 22 (Gilbert-Varshamov Bound). *Let q be a prime power and n, d be positive integers. Then,*

$$A_H(n, d, q) \geq \frac{q^n}{V_H(d - 1, n, q)}.$$

It turns out that random codes attain the asymptotic Gilbert-Varshamov bound with high probability. This will be an important result for the asymptotic analysis of some algorithms. Let us first give some notation: let $0 \leq \delta \leq 1$ denote the relative minimum distance, i.e., $\delta = d/n$ and let us denote by

$$\overline{R}(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log_q A_H(n, \delta n, q)$$

the asymptotic information rate.

Definition 23 (Entropy Function). For a positive integer $q \geq 2$ the q -ary entropy function is defined as follows:

$$\begin{aligned} h_q : [0, 1] &\rightarrow \mathbb{R}, \\ x &\rightarrow x \log_q(q - 1) - x \log_q(x) - (1 - x) \log_q(1 - x). \end{aligned}$$

Exercise 24. Show that for $s \in [0, 1 - 1/q]$ we have that

1. $V_H(sn, n, q) \leq q^{h_q(s)n}$,
2. $V_H(sn, n, q) \geq q^{h_q(s)n - o(n)}$,

using Stirling's formula.

Theorem 25 (The Asymptotic Gilbert-Varshamov Bound). *For every prime power q and $\delta \in [0, 1 - 1/q]$ there exists an infinite family \mathcal{C} of codes with rate*

$$\overline{R}(\delta) \geq 1 - h_q(\delta).$$

Recall that in complexity theory we write $f(n) = \Omega(g(n))$, if

$$\limsup_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| > 0.$$

For example, $f(n) = \Omega(n)$ means that $f(n)$ grows at least polynomially in n .

Theorem 26. *For every prime power q , $\delta \in [0, 1 - 1/q]$ and $0 < \varepsilon < 1 - h_q(s)$ and sufficiently large positive integer n . The following holds for*

$$k = \lceil (1 - h_q(\delta) - \varepsilon)n \rceil.$$

If $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ is chosen uniformly at random, the linear code \mathcal{C} generated by \mathbf{G} has rate at least $1 - h_q(\delta) - \varepsilon$ and relative minimum distance at least δ with probability at least $1 - e^{-\Omega(n)}$.

Exercise 27. Prove Theorem 26 following these steps:

1. What is the probability for \mathbf{G} to have full rank?
2. For each non-zero $\mathbf{x} \in \mathbb{F}_q^k$ show that \mathbf{xG} is a uniformly random element.
3. Show that the probability that $\text{wt}_H(\mathbf{xG}) \leq \delta n$ is at most $q^{(h_q(\delta) - 1)n}$.
4. Use the union bound over all non-zero \mathbf{x} and the choice of k to get the claim.

This was first proven in [55, 215] and shows that for a random code with large length, we know what minimum Hamming distance to expect.

These results hold also more generally over any finite chain ring and for any additive weight, see [80].

We also want to introduce the following two methods to get a new code from an old code: puncturing and shortening. When we puncture a code we essentially delete all coordinates indexed by a certain set in all codewords, while shortening can be regarded as the puncturing of a special subcode.

Definition 28. Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q and let $S \subseteq \{1, \dots, n\}$ be a set of size s . Then, we define the *punctured code* \mathcal{C}^S in S as follows

$$\mathcal{C}^S = \{(c_i)_{i \notin S} \mid c \in \mathcal{C}\}.$$

Let us define $\mathcal{C}(S)$ to be the subcode containing all codewords which are 0 in S , that is

$$\mathcal{C}(S) = \{c \in \mathcal{C} \mid c_i = 0 \ \forall i \in S\}.$$

Then, we define the *shortened code* \mathcal{C}_S in S to be

$$\mathcal{C}_S = \mathcal{C}(S)^S.$$

Clearly, the punctured code \mathcal{C}^S has now length $n - s$. What happens to its dimension?

Exercise 29. Show that if $s < d$, the minimum distance of \mathcal{C} , then \mathcal{C}^S has dimension k .

Shortening and puncturing of a code are heavily connected through the dual code:

Theorem 30. Let \mathcal{C} be a linear $[n, k]$ code over \mathbb{F}_q with dual code \mathcal{C}^\perp . Let $S \subseteq \{1, \dots, n\}$ be a set of size s . Then

1. $(\mathcal{C}^\perp)_S = (\mathcal{C}^S)^\perp$,
2. $(\mathcal{C}^\perp)^S = (\mathcal{C}_S)^\perp$.

Example 31. Let us consider the binary code generated by

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and $S = \{4, 5\}$. Then, the punctured code \mathcal{C}^S has generator matrix

$$\mathbf{G}^S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Note that $\mathcal{C}(S) = \{(1, 0, 1, 0, 0, 1), (0, 0, 0, 0, 0, 0)\}$, thus the generator matrix of \mathcal{C}_S is given by

$$\mathbf{G}_S = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}.$$

Exercise 32. Show that Theorem 30 holds for this example.

2.2.2 Matrix Codes

Let us denote by $\mathbb{F}_q^{n \times m}$ the $n \times m$ matrices over \mathbb{F}_q .

Instead of considering subspaces in \mathbb{F}_q^n , we can also consider subspaces in $\mathbb{F}_q^{m \times n}$, referred to as *matrix codes*.

Definition 33 (Matrix Codes). An \mathbb{F}_q -linear subspace of $\mathbb{F}_q^{n \times m}$ is called a *matrix code*.

Thus, instead of a $k \times n$ generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, we generate the code with k generating matrices $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$, then every codeword is of the form

$$\mathbf{C} = \lambda_1 \mathbf{G}_1 + \dots + \lambda_k \mathbf{G}_k,$$

for some $\lambda_i \in \mathbb{F}_q$. Since these codes are only linear over \mathbb{F}_q , they are also called \mathbb{F}_q -linear codes.

One can define the Hamming metric on such matrices, by either considering the number of non-zero columns or the number of non-zero entries.

For a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ let us denote by $\mathbf{c}_i \in \mathbb{F}_q^m$ its columns for $i \in \{1, \dots, n\}$, by $\mathbf{r}_j \in \mathbb{F}_q^n$ its rows for $j \in \{1, \dots, m\}$ and finally by $a_{i,j}$ its entries for $(i, j) \in \{1, \dots, n\} \times \{1, \dots, m\}$. Given $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ we define

$$\begin{aligned} \text{wt}_{H,c}(\mathbf{A}) &= |\{i \in \{1, \dots, n\} \mid \mathbf{c}_i \neq \mathbf{0}\}|, \\ \text{wt}_{H,v}(\mathbf{A}) &= |\{(i, j) \in \{1, \dots, n\} \times \{1, \dots, m\} \mid a_{i,j} \neq 0\}|. \end{aligned}$$

We will specify which notion of Hamming metric we are using, whenever we use matrix codes.

Definition 34. Given a matrix $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ with rows $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{F}_q^n$ we define the *vectorization* of \mathbf{A} to be $\text{vec}(\mathbf{A}) = (\mathbf{a}_1, \dots, \mathbf{a}_m) \in \mathbb{F}_q^{mn}$.

The Hamming weight of $\text{vec}(\mathbf{A})$ coincides with the second notion of Hamming metric of matrices, i.e.,

$$\text{wt}_H(\text{vec}(\mathbf{A})) = \text{wt}_{H,v}(\mathbf{A}).$$

Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . That is, we can write every element $a \in \mathbb{F}_{q^m}$ as

$$a = \sum_{i=1}^m a_i \gamma_i,$$

with $a_i \in \mathbb{F}_q$.

Definition 35. Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Then, we can define the *extension map*

$$\begin{aligned} \Gamma : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q^m \\ a = \sum_{i=1}^m a_i \gamma_i &\mapsto (a_1, \dots, a_m). \end{aligned}$$

By abuse of notation we will also use Γ to denote the extension map $\Gamma : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_q^{m \times n}$, where each entry is extended to a column.

The Hamming weight of the vector $\Gamma^{-1}(\mathbf{A}) = \mathbf{a} \in \mathbb{F}_{q^m}^n$ coincides with the first notion of Hamming weight for matrices, i.e.,

$$\text{wt}_H(\Gamma^{-1}(\mathbf{A})) = \text{wt}_{H,c}(\mathbf{A}). \quad (2.1)$$

Exercise 36. Show that Equation (2.1) is independent of the choice of basis Γ .

The extension map can also be applied to a code itself, that is:

Definition 37. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code and let Γ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . The *code associated with* Γ is given by

$$\Gamma(\mathcal{C}) = \{\Gamma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\}.$$

Note that since $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ was \mathbb{F}_{q^m} -linear, we get that $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$ is \mathbb{F}_q -linear.

The dual code of a matrix code, requires a new inner product, which extends the previous standard inner product. For this, recall that the *trace* of a matrix is the sum of the entries on its diagonal.

Definition 38. Let $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{m \times n}$, then we define their trace product as

$$\text{Tr}(\mathbf{AB}^\top).$$

Definition 39. Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be a linear matrix code, then its *dual code* is given by

$$\mathcal{C}^\perp = \{\mathbf{A} \in \mathbb{F}_q^{m \times n} \mid \text{Tr}(\mathbf{AB}^\top) = 0 \text{ for all } \mathbf{B} \in \mathcal{C}\}.$$

This product is compatible with the standard inner product on $\mathbb{F}_q^{m \times n}$. For this we need the following definition.

Definition 40. Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}, \Gamma' = \{\gamma'_1, \dots, \gamma'_m\}$ be bases of \mathbb{F}_{q^m} over \mathbb{F}_q . We say that Γ and Γ' are orthogonal if

$$\text{Tr}_{\mathbb{F}_q}(\gamma_i \gamma'_j) = \delta_{i,j},$$

where $\delta_{i,j}$ denotes the Kronecker delta function, i.e., it outputs 0 if $i \neq j$ and 1 if $i = j$, and $\text{Tr}_{\mathbb{F}_q}$ denotes the field trace, i.e.,

$$\begin{aligned} \text{Tr} : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q \\ a &\mapsto \sum_{i=0}^{m-1} a^{q^i}. \end{aligned}$$

Proposition 41. Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code. Let Γ, Γ' be orthogonal bases of \mathbb{F}_{q^m} over \mathbb{F}_q , then

$$\Gamma(\mathcal{C})^\perp = \Gamma'(\mathcal{C}^\perp).$$

Exercise 42. Show that Proposition 41 holds for the example

$$\mathcal{C} = \langle 1, \alpha \rangle \subseteq \mathbb{F}_8^2,$$

where $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ and $\alpha^3 = \alpha + 1$, $\Gamma = \{1, \alpha, \alpha^2\}, \Gamma' = \{1, \alpha^2, \alpha\}$.

The new inner product is in fact also compatible with the vectorization:

Proposition 43. Let $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{m \times n}$, then

$$\text{Tr}(\mathbf{A}^\top \mathbf{B}) = \langle \text{vec}(\mathbf{A}), \text{vec}(\mathbf{B}) \rangle.$$

2.2.3 Generalized Reed-Solomon Codes

In order to give a self-contained chapter, we also want to introduce some of the most prominent codes that are used in code-based cryptography. For this we start with Generalized Reed-Solomon codes (GRS), [221].

Definition 44 (Generalized Reed-Solomon Code). Let $k \leq n \leq q$ be positive integers. Let $\alpha \in \mathbb{F}_q^n$ be an n -tuple of distinct elements, i.e., $\alpha = (\alpha_1, \dots, \alpha_n)$ with $\alpha_i \neq \alpha_j$, for all $i \neq j \in \{1, \dots, n\}$. Let $\beta \in \mathbb{F}_q^n$ be an n -tuple of nonzero elements, i.e., $\beta = (\beta_1, \dots, \beta_n)$, with $\beta_i \neq 0$ for all $i \in \{1, \dots, n\}$. The *Generalized Reed-Solomon code* of length n and dimension k , denoted by $\text{GRS}_{n,k}(\alpha, \beta)$ is defined as

$$\text{GRS}_{n,k}(\alpha, \beta) = \{(\beta_1 f(\alpha_1), \dots, \beta_n f(\alpha_n)) \mid f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

In the case where $\beta = (1, \dots, 1)$, we call the code $\text{GRS}_{n,k}(\alpha, \beta)$ a *Reed-Solomon* (RS) code and denote it by $\text{RS}_{n,k}(\alpha)$.

Exercise 45. Show that the Vandermonde matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & & \vdots \\ \alpha_1^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

is a generator matrix of a RS code. Similarly, build a generator matrix of the $\text{GRS}_{n,k}(\alpha, \beta)$ code.

Exercise 46. Show that GRS codes are MDS codes, i.e.,

$$d_H(\text{GRS}_{n,k}(\alpha, \beta)) = n - k + 1.$$

Observe that the dual code of a GRS code is again a GRS code.

Proposition 47. *Let $k \leq n \leq q$ be positive integers. Then*

$$\text{GRS}_{n,k}(\alpha, \beta)^\perp = \text{GRS}_{n,n-k}(\alpha, \gamma),$$

where

$$\gamma_i = \beta_i^{-1} \prod_{\substack{j=1 \\ j \neq i}}^n (\alpha_i - \alpha_j)^{-1}.$$

2.2.4 Goppa Codes

Another important family of codes in code-based cryptography is the family of classical q -ary Goppa codes [142, 143, 144].

Let m be a positive integer, $n = q^m$ and \mathbb{F}_{q^m} be a finite field. Let $G \in \mathbb{F}_{q^m}[x]$. Then define the quotient ring

$$S_m = \mathbb{F}_{q^m}[x] / \langle G \rangle.$$

Lemma 48. *Let $\alpha \in \mathbb{F}_q$ be such that $G(\alpha) \neq 0$. Then $(x - \alpha)$ is invertible in S_m and*

$$(x - \alpha)^{-1} = -\frac{1}{G(\alpha)} \frac{G(x) - G(\alpha)}{x - \alpha}.$$

Definition 49 (Classical Goppa Code). Let $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_{q^m}^n$, be such that $\alpha_i \neq \alpha_j$ for all $i \neq j \in \{1, \dots, n\}$, and $G(\alpha_i) \neq 0$ for all $i \in \{1, \dots, n\}$. Then we can define the classical q -ary Goppa code as

$$\Gamma(\alpha, G) = \left\{ c \in \mathbb{F}_q^n \mid \sum_{i=1}^n \frac{c_i}{x - \alpha_i} = 0 \text{ in } S_m \right\}.$$

Proposition 50. *The Goppa code $\Gamma(\alpha, G)$ has minimum Hamming distance $d_H(\Gamma(\alpha, G)) \geq \deg(G) + 1$ and dimension $k \geq n - m \deg(G)$.*

In order to construct a parity-check matrix of a classical Goppa code, let us define $\beta = (G(\alpha_1)^{-1}, \dots, G(\alpha_n)^{-1})$. The parity-check matrix of $\Gamma(\alpha, G)$ is then given by the weighted Vandermonde matrix

$$\mathbf{H} = \begin{pmatrix} \beta_1 & \cdots & \beta_n \\ \beta_1 \alpha_1 & \cdots & \beta_n \alpha_n \\ \vdots & & \vdots \\ \beta_1 \alpha_1^{r-1} & \cdots & \beta_n \alpha_n^{r-1} \end{pmatrix}.$$

Note that $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, but the code $\Gamma(\alpha, G)$ is the \mathbb{F}_q -kernel of \mathbf{H} .

From this construction, we can already see that strong connection between classical Goppa codes and GRS codes. For this we define subfield subcodes and alternant codes in the following.

Definition 51 (Subfield Subcode). Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_{q^m} . The *subfield subcode* of \mathcal{C} over \mathbb{F}_q is then defined as

$$\mathcal{C}_{\mathbb{F}_q} = \mathcal{C} \cap \mathbb{F}_q^n.$$

Proposition 52. Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_{q^m} with minimum distance d . Then $\mathcal{C}_{\mathbb{F}_q}$ has dimension $\geq n - m(n - k)$ and minimum distance $\geq d$.

Exercise 53. Prove Proposition 52 using the map

$$\begin{aligned} \phi : \mathbb{F}_{q^m}^n &\rightarrow \mathbb{F}_{q^m}^n, \\ (x_1, \dots, x_n) &\mapsto (x_1^q - x_1, \dots, x_n^q - x_n). \end{aligned}$$

A special case of subfield subcodes are the alternant codes, where one takes subfield subcodes of GRS codes.

Definition 54 (Alternant Code). Let $\alpha \in \mathbb{F}_{q^m}^n$ be pairwise distinct and $\beta \in (\mathbb{F}_{q^m}^*)^n$. Then the *alternant code* $\mathcal{A}_{m,n,k}(\alpha, \beta)$ is defined as

$$\mathcal{A}_{m,n,k}(\alpha, \beta) = \text{GRS}_{m,n,k}(\alpha, \beta) \cap \mathbb{F}_q^n.$$

Proposition 55. The alternant code $\mathcal{A}_{m,n,k}(\alpha, \beta)$ has dimension $\geq n - m(n - k)$ and minimum distance $\geq n - k + 1$.

Exercise 56. Prove Proposition 55.

Thus, classical Goppa codes are alternant codes, i.e., subfield subcodes of particular GRS codes, where the weights β_i are the inverses of the evaluations $g(\alpha_i)$, for a polynomial g .

2.2.5 Cyclic Codes

Another important family of codes is that of cyclic codes. They can be represented through only one vector. Let $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$, then we denote by $\sigma(c)$ its *cyclic shift*, i.e.,

$$\sigma(c_1, \dots, c_n) = (c_n, c_1, \dots, c_{n-1}).$$

We call a code cyclic, if the cyclic shift of any codeword is also a codeword.

Definition 57 (Cyclic Code). Let \mathcal{C} be an $[n, k]$ linear code over \mathbb{F}_q . We say that \mathcal{C} is *cyclic* if $\sigma(\mathcal{C}) = \mathcal{C}$.

Proposition 58. Let $k \leq n = q - 1$ be positive integers and let $\alpha \in \mathbb{F}_q^n$ be such that $\alpha_i = \gamma^{i-1}$, for $i \in \{1, \dots, n\}$ and γ a primitive element in \mathbb{F}_q . Then $RS_{n,k}(\alpha)$ is a cyclic code.

Exercise 59. Prove Proposition 58.

Note that any polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]$ of degree (at most) $n - 1$ corresponds naturally to a vector $c = (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$.

Proposition 60. Cyclic codes over \mathbb{F}_q of length n correspond to ideals of $\mathbb{F}_q[x]/(x^n - 1)$.

Exercise 61. Prove Proposition 60 using the map

$$\begin{aligned} \varphi : \mathbb{F}_q[x]/(x^n - 1) &\rightarrow \mathbb{F}_q^n, \\ c(x) &\mapsto (c_0, \dots, c_{n-1}). \end{aligned}$$

In particular, what is $\varphi(x \cdot c(x))$?

Since we can see cyclic codes as ideals in $\mathbb{F}_q[x]/(x^n - 1)$, we can also consider the generator polynomial of a cyclic code.

Definition 62 (Generator Polynomial). The *generator polynomial* of a cyclic code $\mathcal{C} \subset \mathbb{F}_q^n$ is the unique monic generator of minimal degree of the corresponding ideal in $\mathbb{F}_q[x]/(x^n - 1)$.

Proposition 63. Let \mathcal{C} be a cyclic code over \mathbb{F}_q of length n with generator polynomial $g(x) = \sum_{i=0}^r g_i x^i$, where r is the degree of g . Then

1. $g(x) \mid x^n - 1$.
2. \mathcal{C} has dimension $n - r$.
3. A generator matrix $G \in \mathbb{F}_q^{(n-r) \times n}$ of \mathcal{C} is given by

$$G = \begin{pmatrix} g_0 & \cdots & g_r & & \\ & \ddots & & \ddots & \\ & & g_0 & \cdots & g_r \end{pmatrix}.$$

4. Let $h(x)$ be such that $g(x)h(x) = x^n - 1$, then $\langle g(x) \rangle^\perp = \langle h(x) \rangle$.

Exercise 64. Prove Proposition 63.

Exercise 65. How many cyclic codes over \mathbb{F}_3 of length 4 exist?

Note that the generator matrix in Proposition 63 is in a special form, such a matrix is called a *circulant matrix*.

Exercise 66. Give the generator polynomial of $\text{RS}_{n,k}(\alpha)$.

Exercise 67. Let us consider the code \mathcal{C} over \mathbb{F}_3 generated by

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

1. Show that \mathcal{C} is cyclic.
2. Find the generator polynomial of \mathcal{C} .
3. Find the generator polynomial of \mathcal{C}^\perp .

Finally, since we know how to compute the polynomial product $u(x) \cdot v(x) \in \mathbb{F}_q[x]/(x^n - 1)$, we can define a new vector multiplication in \mathbb{F}_q^n .

Definition 68 (Rotation Matrix). Let $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$ and define the *rotation matrix* as

$$\text{rot}(\mathbf{u}) = \begin{pmatrix} \mathbf{u} \\ \sigma(\mathbf{u}) \\ \vdots \\ \sigma^{n-1}(\mathbf{u}) \end{pmatrix}.$$

Let us denote by $\mathbf{uv} = \mathbf{u} \text{rot}(\mathbf{v})$.

Exercise 69. 1. Show that $\varphi(\mathbf{uv}) = u(x)v(x)$.

2. Show that $\mathbf{uv} = \mathbf{vu}$.

Finally, we introduce quasi-cyclic codes. For $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ and some $\ell \in \{1, \dots, n\}$ we denote by $\sigma_\ell(x)$ its ℓ -cyclic shift, i.e.,

$$\sigma_\ell(\mathbf{x}) = (x_{1+\ell}, \dots, x_{n+\ell}),$$

where the indices $i + \ell$ should be considered modulo n .

Definition 70. An $[n, k]$ linear code \mathcal{C} is a *quasi-cyclic* (QC) code, if there exists $\ell \in \mathbb{N}$, such that $\sigma_\ell(\mathcal{C}) = \mathcal{C}$.

In addition, if $n = \ell a$, for some $a \in \mathbb{N}$, then it is convenient to write the generator matrix composed into $a \times a$ circulant matrices.

2.2.6 LDPC Codes

Another interesting family of codes for cryptography are the *low-density parity-check* (LDPC) codes introduced by Gallager [134]. The idea of LDPC codes is to have a parity-check matrix that is sparse. These codes are usually defined over the binary, although they can be generalized to arbitrary finite fields [107], for the applications in cryptography the binary LDPC codes suffice. In order to define LDPC codes we introduce the notation of *row-weight*, respectively *column-weight* of a matrix, which refers to the Hamming weight of each row, respectively of each column. Thus, a matrix having row-weight w , asks for each row to have Hamming weight w . Classically LDPC codes are defined as follows.

Definition 71. Let $\lambda, \rho \in \mathbb{N}$. An $[n, k]$ linear code \mathcal{C} over \mathbb{F}_2 is called a (λ, ρ) -regular LDPC code, if there exists a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ of \mathcal{C} which has column-weight λ and row-weight ρ .

A more common definition for cryptographic applications reads as follows.

Definition 72. Let $w \in \mathbb{N}$ be a constant. An $[n, k]$ linear code \mathcal{C} over \mathbb{F}_2 is called a *w-low-density parity-check code*, if there exists a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ of \mathcal{C} having row-weight w .

Exercise 73. Show that the rate of an (λ, ρ) -regular LDPC code is given by $1 - \lambda/\rho$.

For a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ and a received vector $\mathbf{x} \in \mathbb{F}_2^n$ we call the $(n - k)$ equations derived from $\mathbf{H}\mathbf{x}^\top$ *parity-checks*, i.e.,

$$\sum_{j=1}^n h_{ij}x_j$$

for all $i \in \{1, \dots, n - k\}$. We say that a parity-check is *satisfied* if

$$\sum_{j=1}^n h_{ij}x_j = 0,$$

and else call it *unsatisfied*.

LDPC codes are interesting from a coding-theoretic point of view, as they (essentially) achieve Shannon capacity in a practical way. From a cryptographic stand point, these codes are interesting as they have no algebraic structure, which might be detected by an attacker, but nevertheless have an efficient decoding algorithm.

One decoding algorithm dates back to Gallager [134] and is called Bit-Flipping algorithm. There have been many improvements (e.g. [260, 165, 189]). The algorithm is iterative and its error correction capability increases with the code length. The idea of the Bit-Flipping algorithm is that at each iteration the number of unsatisfied parity-check equations associated to each bit of the received vector is computed. Each bit which has more than $b \in \mathbb{N}$ (some threshold parameter) unsatisfied parity-check equations is flipped and the syndrome is updated accordingly. This process is repeated until either the syndrome becomes $\mathbf{0}$, or until a maximal number of iteration $M \in \mathbb{N}$ is reached. In the later case we have a *decoding failure*. The complexity of this algorithm is thus given by $\mathcal{O}(nwN)$, where w is the row-weight of the parity-check matrix and N is the average number of iterations.

One can also relax the condition on the row-weight of LDPC codes, to get moderate-density parity-check (MDPC) codes [208].

Definition 74. An $[n, k]$ linear code \mathcal{C} over \mathbb{F}_2 is called a *moderate-density parity-check code*, if there exists a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ having row-weight $\mathcal{O}(\sqrt{n \log(n)})$.

Thus, the only difference to LDPC codes is that we allow a larger row-weight in the parity-check matrix (for LDPC codes w was chosen constant in n). This might however lead to an increase of iterations within the Bit-Flipping algorithm and decoding failures become increasingly likely.

2.2.7 Reed-Muller Codes

Next, we introduce a class of codes, the Reed-Muller codes, introduced in [201] in 1954. They are, similarly to Reed-Solomon codes, constructed as the evaluation of polynomials. While Reed-Solomon codes only consider polynomials in one variable, Reed-Muller codes use multivariate polynomials. For this part we follow [150].

Let p be a prime, $q = p^n$ and m, r be positive integers. Denote with $\mathbb{F}_q[x_1, \dots, x_m]_{\leq r}$ the \mathbb{F}_q -vector space of polynomials in m variables of degree at most r and fix an order $\{\alpha_1, \alpha_2, \dots, \alpha_{q^m}\}$ of \mathbb{F}_q^m .

Definition 75. The *Reed-Muller code* $\text{RM}_q(m, r)$ over \mathbb{F}_q is defined as the image of the evaluation map

$$\begin{aligned} \text{ev} : \mathbb{F}_q[x_1, \dots, x_m]_{\leq r} &\rightarrow \mathbb{F}_q^{q^m}, \\ f &\mapsto (f(\alpha_1), f(\alpha_2), \dots, f(\alpha_{q^m})). \end{aligned}$$

We will note that there exist efficient decoding algorithms for Reed-Muller codes, the first efficient decoding algorithm was published in [220].

For the case $q = 2$, we can compute dimension and minimum distance of $\text{RM}_q(m, r)$.

Proposition 76. Let $r \leq m$. Then $\dim_{\mathbb{F}_2}(\text{RM}_2(m, r)) = \sum_{i=0}^r \binom{m}{i}$.

Proposition 77. Let $r \leq m$. The minimum distance of $\text{RM}_2(m, r)$ is 2^{m-r} .

2.2.8 Concatenated Codes

Concatenated codes were first introduced by Forney [123], and use the basic idea of a double encoding process through two codes.

Definition 78. Let \mathcal{C}_1 be an $[n_1, k_1]$ linear code of minimum distance d_1 over \mathbb{F}_q , called *inner code* and \mathcal{C}_2 be an $[n_2, k_2]$ linear code of minimum distance d_2 over $\mathbb{F}_{q^{k_1}}$, called *outer code*. Then, the *concatenated code* $\mathcal{C} = \mathcal{C}_2 \circ \mathcal{C}_1$ is an $[n_1 n_2, k_1 k_2]$ linear code over \mathbb{F}_q of minimum distance at least $d_1 d_2$.

The codewords of \mathcal{C} are built as follows: for any $\mathbf{u} \in \mathbb{F}_{q^{k_1}}^{k_2}$, encode \mathbf{u} using a generator matrix \mathbf{G}_2 of \mathcal{C}_2 , receiving the codeword $((\mathbf{u}\mathbf{G}_2)_1, \dots, (\mathbf{u}\mathbf{G}_2)_{n_2})$. Let us denote for $a \in \mathbb{F}_{q^{k_1}}$ by \bar{a} the corresponding vector in $\mathbb{F}_q^{k_1}$ having fixed a basis. As a next step we represent the entries of each codeword as a vector in $\mathbb{F}_q^{k_1}$ and encode them using a generator matrix \mathbf{G}_1 of \mathcal{C}_1 . Then, the codewords of \mathcal{C} are of the form

$$((\overline{\mathbf{u}\mathbf{G}_2})_1 \mathbf{G}_1, \dots, (\overline{\mathbf{u}\mathbf{G}_2})_{n_2} \mathbf{G}_1).$$

2.2.9 $(U, U + V)$ -Codes

Given two codes \mathcal{C}_1 and $\mathcal{C}_2 \subseteq \mathbb{F}_q^n$, we can also construct new codes, for example using the $(U, U + V)$ -construction.

Definition 79. Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ with dimension k_1 , respectively k_2 . Then, the $(U, U + V)$ -code of $\mathcal{C}_1, \mathcal{C}_2$ is given by

$$\mathcal{C} = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}) \mid \mathbf{u} \in \mathcal{C}_1, \mathbf{v} \in \mathcal{C}_2\}.$$

Proposition 80. Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ with dimension k_1 , respectively k_2 and minimum Hamming distance d_1 , respectively d_2 . Then, the $(U, U + V)$ -code $\mathcal{C} \subseteq \mathbb{F}_q^{2n}$ has dimension $k = k_1 + k_2$ and minimum Hamming distance $d = \min\{2d_1, d_2\}$.

Exercise 81. Prove Proposition 80. *Hint:* Show first that if $\mathbf{G}_1, \mathbf{G}_2$ are generator matrices of \mathcal{C}_1 , respectively \mathcal{C}_2 , then $\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{G}_1 \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix}$ is a generator matrix of \mathcal{C} .

The encoding of a message $(\mathbf{m}_1, \mathbf{m}_2)$ gives then the codeword $(\mathbf{m}_1 \mathbf{G}_1, \mathbf{m}_1 \mathbf{G}_1 + \mathbf{m}_2 \mathbf{G}_2)$ and a received word can be assumed of the form $(\mathbf{r}_1, \mathbf{r}_2) = (\mathbf{m}_1 \mathbf{G}_1 + \mathbf{e}_1, \mathbf{m}_1 \mathbf{G}_1 + \mathbf{m}_2 \mathbf{G}_2 + \mathbf{e}_2)$ for some error vector $(\mathbf{e}_1, \mathbf{e}_2)$. Note that a decoder for \mathcal{C} would first decode \mathbf{r}_1 using the decoder of \mathcal{C}_1 to get \mathbf{m}_1 . One can then take $\mathbf{m}_1 \mathbf{G}_1$ away from \mathbf{r}_2 and then use the decoder of \mathcal{C}_2 , to recover \mathbf{m}_2 .

Exercise 82. Show that the Reed-Muller code $\text{RM}_2(m, r)$ is a $(U, U + V)$ -code for the code \mathcal{C}_1 being a $\text{RM}_2(m - 1, r)$ and \mathcal{C}_2 a $\text{RM}_2(m - 1, r - 1)$ code.

2.2.10 Product Codes

Similar to concatenation of codes and the $(U, U + V)$ -construction, we can also build the tensor product of two codes $\mathcal{C}_1, \mathcal{C}_2$. For a matrix $\mathbf{C} \in \mathbb{F}_q^{k \times n}$ let us denote by $\mathbf{c}_i \in \mathbb{F}_q^k$ for $i \in \{1, \dots, n\}$ the columns of \mathbf{C} , and similarly by $\mathbf{r}_i \in \mathbb{F}_q^n$ for $i \in \{1, \dots, k\}$ the rows of \mathbf{C} .

Definition 83. Let $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$. Then, the *product code* of $\mathcal{C}_1, \mathcal{C}_2$ is defined as

$$\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2 = \{\mathbf{C} \in \mathbb{F}_q^{n_1 \times n_2} \mid \mathbf{c}_i \in \mathcal{C}_1, \mathbf{r}_j \in \mathcal{C}_2, i \in \{1, \dots, n_2\}, j \in \{1, \dots, n_1\}\}.$$

Let us define the Hamming weight of a matrix \mathbf{A} to be the number of non-zero entries in \mathbf{A} .

Proposition 84. *Let $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$ of dimension k_1 , respectively k_2 and minimum Hamming distance d_1 , respectively d_2 . Then, the tensor product code $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$ has dimension $k_1 k_2$ and minimum Hamming distance $d_1 d_2$.*

Exercise 85. Show that every codeword of $\mathcal{C}_1 \otimes \mathcal{C}_2$ is given by

$$\mathbf{G}_1^\top \mathbf{A} \mathbf{G}_2,$$

for $\mathbf{G}_1 \in \mathbb{F}_q^{k_1 \times n_1}$ a generator matrix of \mathcal{C}_1 , $\mathbf{G}_2 \in \mathbb{F}_q^{k_2 \times n_2}$ a generator matrix of \mathcal{C}_2 and a matrix $\mathbf{A} \in \mathbb{F}_q^{k_1 \times k_2}$.

Exercise 86. Prove Proposition 84.

Note that this is very similar to the definition of concatenated codes, where the resulting code also had length $n_1 n_2$ and dimension $k_1 k_2$. However, for concatenated codes we only know that $d \geq d_1 d_2$, while for tensor product codes, we know that their minimum distance is exactly $d_1 d_2$.

2.2.11 Rank-Metric Codes

Until now, we have considered classical coding theory, where the finite field is endowed with the Hamming metric. However, there exist many more metrics, for example the rank metric (introduced in [111, 228, 125]). In the following we introduce *rank-metric codes*, for which we follow the notation of [145].

Definition 87 (Rank Metric). Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^m}^n$. The *rank weight* of \mathbf{x} is defined as the dimension of the \mathbb{F}_q -vector space generated by its entries, i.e.,

$$\text{wt}_R(\mathbf{x}) = \dim_{\mathbb{F}_q} (\langle x_1, \dots, x_n \rangle_{\mathbb{F}_q})$$

and the *rank distance* between \mathbf{x} and \mathbf{y} is given by

$$d_R(\mathbf{x}, \mathbf{y}) = \text{wt}_R(\mathbf{x} - \mathbf{y}).$$

Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code, then its *minimum rank distance* is given by

$$d_R(\mathcal{C}) = \min\{\text{wt}_R(\mathbf{c}) \mid \mathbf{c} \neq \mathbf{0}, \mathbf{c} \in \mathcal{C}\}.$$

The rank support of a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ is often given by

$$\text{supp}(\mathbf{x}) = \langle x_1, \dots, x_n \rangle_{\mathbb{F}_q} \subset \mathbb{F}_{q^m}.$$

We will later see also two different notions of rank support.

Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Using the extension map, i.e.,

$$\begin{aligned} \Gamma : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q^{m \times n} \\ \mathbf{a} &\mapsto \Gamma(\mathbf{a}), \end{aligned}$$

we can see that

$$\text{wt}_R(\mathbf{a}) = \text{rk}(\Gamma(\mathbf{a})). \quad (2.2)$$

Exercise 88. Show that Equation (2.2) is independent of the choice of basis Γ .

Thus, the extension map is a \mathbb{F}_q -linear isometry.

In fact, we can also endow $\mathbb{F}_q^{m \times n}$ with the rank metric.

Definition 89 (Rank Metric). Let $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{n \times m}$. The *rank weight* of \mathbf{A} is given by the rank of \mathbf{A} , denoted by $\text{rk}(\mathbf{A})$ and the rank distance between \mathbf{A} and \mathbf{B} is given by

$$d_R(\mathbf{A}, \mathbf{B}) = \text{rk}(\mathbf{A} - \mathbf{B}).$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be a linear matrix code, then its *minimum rank distance* is given by

$$d_R(\mathcal{C}) = \min\{\text{rk}(\mathbf{C}) \mid \mathbf{C} \neq \mathbf{0}, \mathbf{C} \in \mathcal{C}\}.$$

Recall, that for $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ we defined the matrix code associated to Γ as

$$\Gamma(\mathcal{C}) = \{\Gamma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}\} \subseteq \mathbb{F}_q^{m \times n}.$$

Proposition 90. Let Γ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code of dimension k and minimum rank distance d_R , then the associated matrix code $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$ is a matrix code of dimension km and minimum rank distance d_R .

Thus, using the extension map any \mathbb{F}_{q^m} -linear code can also be seen as \mathbb{F}_q -linear code, however, the opposite is not true.

Example 91. Let us consider $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ and $\alpha^2 = \alpha + 1$, and $\Gamma = \{1, \alpha\}$. The code $\mathcal{C} = \langle (1, \alpha) \rangle \subseteq \mathbb{F}_4^2$ has dimension 1 and minimum rank distance 2. Then

$$\mathcal{C} = \{(0, 0), (1, \alpha), (\alpha, \alpha + 1)\}$$

and

$$\Gamma(\mathcal{C}) = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

The code $\Gamma(\mathcal{C}) \subseteq \mathbb{F}_2^{2 \times 2}$ has dimension 2 and minimum rank distance 2. However, consider $\mathcal{C}' = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \subseteq \mathbb{F}_2^{2 \times 2}$ has dimension 2 and minimum rank distance 1. We have

$$\mathcal{C}' = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right\}$$

and

$$\Gamma^{-1}(\mathcal{C}') = \{(0, 0), (1 + \alpha, \alpha), (\alpha, \alpha + 1), (1, 1)\} \subseteq \mathbb{F}_4^2.$$

This subset of vectors is not a \mathbb{F}_4 -linear code as for example $\alpha(1, 1) = (\alpha, \alpha) \notin \Gamma^{-1}(\mathcal{C}')$.

Definition 92. The *rank-metric ball* of radius r is defined as

$$B_R(r, n, m, q) = \{\mathbf{x} \in \mathbb{F}_{q^m}^n \mid \text{wt}_R(\mathbf{x}) \leq r\}.$$

Proposition 93. The size of the rank-metric ball is approximately

$$|B_R(r, n, m, q)| \sim q^{r(n+m-r+1)},$$

for large n, m .

Given a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ of rank weight t , we can split the vector into

$$\mathbf{x} = \mathbf{c}\mathbf{R},$$

for $\mathbf{c} \in \mathbb{F}_{q^m}^t$ and the entries c_i are \mathbb{F}_q -linearly independent, and $\mathbf{R} \in \mathbb{F}_q^{t \times n}$ of rank t .

Definition 94. The *column support* of a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ of rank weight t , with splitting $\mathbf{c}\mathbf{R}$, is given by

$$\text{supp}_C(\mathbf{x}) = \langle \Gamma(\mathbf{c})^\top \rangle \subseteq \mathbb{F}_q^m$$

and has dimension t .

The *row support* of a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ of rank weight t and splitting $\mathbf{c}\mathbf{R}$ is given by

$$\text{supp}_R(\mathbf{x}) = \langle \mathbf{R} \rangle \subseteq \mathbb{F}_q^n$$

and has dimension t .

Exercise 95. Show that the definition of row and column support are independent of the choice of splitting.

Recall that in the Hamming metric the support of $x \in \mathbb{F}_{q^m}^n$ is defined as the indices of non-zero entries of \mathbf{x} , i.e.,

$$\text{supp}_H(\mathbf{x}) = \{i \in \{1, \dots, n\} \mid x_i \neq 0\},$$

and the Hamming weight coincides with its size, i.e.,

$$\text{wt}_H(\mathbf{x}) = |\text{supp}_H(\mathbf{x})|.$$

For the rank metric, whether we choose the row or column support, the rank weight of \mathbf{x} coincides with the dimension of the support, i.e.,

$$\text{wt}_R(\mathbf{x}) = \dim(\text{supp}_R(\mathbf{x})) = \dim(\text{supp}_C(\mathbf{x})).$$

For a vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ of Hamming weight t there are $\binom{n}{t}$ many possible Hamming supports of \mathbf{x} , whereas if the rank weight is t , there are $\begin{bmatrix} n \\ t \end{bmatrix}_q$, respectively $\begin{bmatrix} m \\ t \end{bmatrix}_q$ many possible row supports, respectively column supports.

With the minimum rank distance we can also state a Singleton bound [111]:

Theorem 96 (\mathbb{F}_q -linear Rank-Metric Singleton Bound). *Let $\mathcal{C} \subset \mathbb{F}_q^{n \times m}$ be a matrix code of dimension k with minimum rank distance $d_R(\mathcal{C})$. Then*

$$k \leq \max\{n, m\}(\min\{n, m\} - d_R(\mathcal{C}) + 1).$$

Theorem 97 (\mathbb{F}_{q^m} -linear Rank-Metric Singleton Bound). *Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be a linear code of dimension k with minimum rank distance $d_R(\mathcal{C})$. Then*

$$k \leq n - d_R(\mathcal{C}) + 1.$$

Codes achieving these bounds are called Maximum Rank Distance (MRD) codes.

Note that MDS codes have density 1 for q going to infinity, and density 0 for n going to infinity. Similar results hold also for the rank metric: \mathbb{F}_{q^m} -linear MRD codes are dense for q going to infinity by [202] and since $d_R(\mathcal{C})$ is bounded by m , have density 0 for n going to

infinity. It was shown in [148] that \mathbb{F}_q -linear MRD codes are sparse for all parameter sets as the field grows, with only very few exceptions. Unlike in the Hamming metric, we know that \mathbb{F}_{q^m} -linear MRD codes exist for any set of parameters (with $n \leq m$), by the seminal work of Delsarte [111] and Gabidulin [125].

We also have a rank-analogue of the Gilbert-Varshamov bound, [133]. Let us denote by $A_R(n, d, m, q)$ the maximal size of a code in $\mathbb{F}_{q^m}^n$ having minimum rank distance d .

Theorem 98 (Gilbert-Varshamov Bound in the Rank Metric). *Let q be a prime power and m, n, d be positive integers. Then,*

$$A_R(n, d, m, q) \geq \frac{q^{mn}}{|B_R(d-1, n, m, q)|}.$$

We can also give the asymptotic version of this bound, for which we first define the *relative minimum rank distance* to be $\delta = d_R(\mathcal{C})/n$ and when considering the extension degree m as function in n , we can define $M = \lim_{n \rightarrow \infty} m(n)/n$. Then, the rank-metric Gilbert-Varshamov bound states, that

$$\overline{R}(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log_{q^m} A_R(n, \delta n, m, q) \geq (1 - \delta)(1 - M).$$

As in the Hamming metric, we know by [184] that random codes attain the Gilbert-Varshamov bound with high probability.

Proposition 99. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a random linear code of dimension k . For n large enough, we have that \mathcal{C} has the relative minimum distance*

$$\delta = d_R/n = M/2 + 1/2 - \sqrt{RM + (M-1)^2/4}$$

with high probability.

Interestingly, this bound does not depend on the field size q , which is in contrast to its Hamming-metric counterpart. In particular, if $M = 1$, which will often be the case for applications, we get $\delta = 1 - \sqrt{R}$.

2.2.12 Gabidulin Code

In order to introduce the classical Gabidulin codes let us first recall the basics of q -polynomials.

A q -polynomial or linearized polynomial f of q -degree d over \mathbb{F}_{q^m} is a polynomial of the form

$$f(x) = \sum_{i=0}^d f_i x^{q^i}.$$

Let us denote by P_ℓ the q -polynomials of q -degree up to ℓ over \mathbb{F}_{q^m} .

The classical Gabidulin code can now be defined in a similar fashion as the Reed-Solomon code, i.e., as evaluation code.

Definition 100 (Classical Gabidulin Code). Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over \mathbb{F}_q and let $k \leq n \leq m$. The classical Gabidulin code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ of dimension k is defined as

$$\mathcal{C} = \{(f(g_1), \dots, f(g_n)) \mid f \in P_{k-1}\}.$$

Exercise 101. Show that classical Gabidulin codes are \mathbb{F}_{q^m} -linear MRD codes, by taking a non-zero codeword $c = (f(g_1), \dots, f(g_n))$ and considering the \mathbb{F}_q -dimension of the kernel of the q -polynomial f .

In order to introduce the generalized Gabidulin codes, we first have to define the rank analog of the Vandermonde matrix, i.e., the Moore matrix [200].

Definition 102 (Moore Matrix). Let $(v_1, \dots, v_n) \in \mathbb{F}_{q^m}^n$ and v_i are \mathbb{F}_q -linearly independent. We denote by

$$M_{s,k}(v_1, \dots, v_n) \in \mathbb{F}_{q^m}^{k \times n}$$

the s -Moore matrix:

$$M_{s,k}(v_1, \dots, v_n) = \begin{pmatrix} v_1 & \cdots & v_n \\ v_1^{[s]} & \cdots & v_n^{[s]} \\ \vdots & & \vdots \\ v_1^{[s(k-1)]} & \cdots & v_n^{[s(k-1)]} \end{pmatrix},$$

where $[i] = q^i$.

The definition of Gabidulin codes can also be generalized, e.g. [171]:

Definition 103 (Generalized Gabidulin Code). Let $g_1, \dots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over \mathbb{F}_q and let s be coprime to m . The generalized Gabidulin code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ of dimension k is defined as the rowspan of $M_{s,k}(g_1, \dots, g_s)$.

For $s = 1$, we can see that this coincides with the classical Gabidulin codes, which have the generator matrix

$$M_{1,k}(g_1, \dots, g_n) = \begin{pmatrix} g_1 & \cdots & g_n \\ g_1^q & \cdots & g_n^q \\ \vdots & & \vdots \\ g_1^{q^{k-1}} & \cdots & g_n^{q^{k-1}} \end{pmatrix}.$$

Since the Moore matrix can be seen as a rank analog of a Vandermonde matrix, a generalized Gabidulin code can be seen as a rank analog of a generalized Reed-Solomon code.

Theorem 104. *The generalized Gabidulin code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ of dimension k is a \mathbb{F}_{q^m} -linear MRD code.*

In addition, as in the Hamming metric we have nice duality results.

Proposition 105. *Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be a k dimensional generalized Gabidulin code, then $\mathcal{C}^\perp \subset \mathbb{F}_{q^m}^n$ is a $n - k$ dimensional generalized Gabidulin code.*

This duality result holds (as in the Hamming metric) also more in general; for all \mathbb{F}_{q^m} -linear MRD codes.

Proposition 106. *Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ be a k -dimensional \mathbb{F}_{q^m} -linear MRD code, then $\mathcal{C}^\perp \subset \mathbb{F}_{q^m}^n$ is a $(n - k)$ -dimensional \mathbb{F}_{q^m} -linear MRD code.*

The classical Gabidulin code has been the first rank-metric code introduced into code-based cryptography in [126], which is known as the GPT system.

2.2.13 LRPC Codes

Other classes of rank-metric codes that are used in code-based cryptography are the rank analogues of LDPC and MDPC codes, first defined in [128]. Instead of asking for a low (respectively moderate) number of non-zero entries within each row of the parity-check matrix, one now has to consider the \mathbb{F}_q -subspace generated by the coefficients of the parity-check matrix.

Definition 107 (Low Rank Parity-Check Code (LRPC)). Let $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ be a full rank matrix, such that its coefficients $h_{i,j}$ generate an \mathbb{F}_q -subspace F of small dimension d ,

$$F = \langle (h_{i,j})_{i,j} \rangle_{\mathbb{F}_q}.$$

The code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ having parity-check matrix \mathbf{H} is called a *Low Rank Parity-Check* (LRPC) code of dual weight d and support F .

2.2.14 Code Equivalence

For the newer problems used in code-based cryptography, we will also need the notion of code equivalence.

Definition 108 (Isometry). Let us consider the space V endowed with the distance d . A linear map $\varphi : V \rightarrow V$ is called *isometry* if it keeps the distance invariant. That is, for all $\mathbf{x}, \mathbf{y} \in V$ we have $d(\mathbf{x}, \mathbf{y}) = d(\varphi(\mathbf{x}), \varphi(\mathbf{y}))$.

Let us denote the set of all isometries for a fixed distance d by I_d .

Proposition 109. *The linear isometries of the Hamming metric in $V = \mathbb{F}_q^n$ consist of monomial transformations and automorphisms on \mathbb{F}_q .*

For cryptography, we mainly focus on a subset of the Hamming-metric isometries, namely the monomial transformations $M_{n,q} = S_n \rtimes (\mathbb{F}_q^*)^n$. Any map $\varphi \in M_{n,q}$ can be seen as a matrix $\mathbf{M} = \mathbf{P}\mathbf{D}$, where \mathbf{P} is a $n \times n$ permutation matrix and $\mathbf{D} = \text{diag}(\mathbf{v})$ for $\mathbf{v} \in (\mathbb{F}_q^*)^n$ is a diagonal matrix.

Proposition 110. *The linear isometries of the rank metric in $V = \mathbb{F}_q^{m \times n}$ for $m \leq n$, are given by $GL_m(q) \rtimes GL_n(q)$ and automorphisms of \mathbb{F}_q .*

For applications in cryptography, we again only focus on $\varphi \in GL_m(q) \rtimes GL_n(q)$.

Definition 111 (Code Equivalence). Let us consider V endowed with the distance d . Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq V$ be linear codes. We say \mathcal{C}_1 is equivalent to \mathcal{C}_2 , if there exists $\varphi \in I_d$ such that $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Since $I_H = S_n \rtimes (\mathbb{F}_q^*)^n \rtimes \text{Aut}(\mathbb{F}_q)$, we get two subclasses of code equivalence in the Hamming metric.

In the lightest version, we have the *permutation equivalence*.

Definition 112 (Permutation Equivalence). We say that two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ are *permutation equivalent*, if there exists a permutation of indices, which transforms \mathcal{C}_1 into \mathcal{C}_2 , that is there exists $\sigma \in S_n$, such that $\sigma(\mathcal{C}_1) = \mathcal{C}_2$.

When considering any monomial transformation, we get the *linear equivalence*.

Definition 113 (Linear Equivalence). We say that two codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ are *linear equivalent*, if there exists a map $\varphi \in S_n \rtimes (\mathbb{F}_q^*)^n$, such that $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

Clearly, permutation equivalent codes are also linear equivalent codes.

Exercise 114. Consider the code $\mathcal{C}_1 \subseteq \mathbb{F}_3^3$ generated by $\mathbf{G}_1 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$ and the code $\mathcal{C}_2 \subseteq \mathbb{F}_3^3$ generated by $\mathbf{G}_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Are the two codes linear equivalent, permutation equivalent or not equivalent?

Proposition 115. If $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ are permutation equivalent codes, then for any generator matrix \mathbf{G}_1 of \mathcal{C}_1 and \mathbf{G}_2 of \mathcal{C}_2 , there exists a $n \times n$ permutation matrix \mathbf{P} such that

$$\mathbf{G}_1 \mathbf{P} = \mathbf{G}_2.$$

If $\mathcal{C}_1, \mathcal{C}_2$ are linear equivalent codes, then for any generator matrix \mathbf{G}_1 of \mathcal{C}_1 and \mathbf{G}_2 of \mathcal{C}_2 , there exists a $n \times n$ permutation matrix \mathbf{P} and a diagonal matrix $\text{diag}(\mathbf{v})$ for $\mathbf{v} \in (\mathbb{F}_q^*)^n$ such that

$$\mathbf{G}_1 \mathbf{P} \text{diag}(\mathbf{v}) = \mathbf{G}_2.$$

Exercise 116. Let $\mathcal{C}_1, \mathcal{C}_2$ be linear equivalent codes. Show that \mathcal{C}_1^\perp is linear equivalent to \mathcal{C}_2^\perp . *Hint:* Use the fact that $\mathbf{G}_1 \mathbf{H}_1^\top = \mathbf{0}$ and $\mathbf{G}_1 \mathbf{P} \text{diag}(\mathbf{v}) = \mathbf{G}_2$.

Note that linear equivalent codes have the same minimum distance. Even more is true.

Definition 117 (Weight Enumerator). Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code. For any $w \in \{1, \dots, n\}$, let us denote by $A_w(\mathcal{C}) = |\{\mathbf{c} \in \mathcal{C} \mid \text{wt}_H(\mathbf{c}) = w\}|$ the *weight enumerator* of \mathcal{C} .

Proposition 118. Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ be linear equivalent codes, then for all $w \in \{1, \dots, n\}$ we have that

$$A_w(\mathcal{C}_1) = A_w(\mathcal{C}_2).$$

Definition 119 (Automorphism Group). Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code. The *automorphism group* of \mathcal{C} is given by the linear isometries that map \mathcal{C} to \mathcal{C} .

Exercise 120. Give the automorphism group of $\mathcal{C} = \langle (1, 0, 0), (0, 1, 1) \rangle \subseteq \mathbb{F}_2^3$.

Exercise 121. Let $\varphi \in \text{Aut}(\mathcal{C})$. Show that $\varphi \in \text{Aut}(\mathcal{C}^\perp)$.

Definition 122 (Hull). Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code. Then the *hull* of \mathcal{C} is given by

$$\mathcal{C} \cap \mathcal{C}^\perp.$$

In [122] it was shown, that the hull of a random code is with high probability trivial, i.e., $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$.

Exercise 123. Let $\varphi \in \text{Aut}(\mathcal{C})$. Show that $\varphi \in \text{Aut}(\mathcal{C} \cap \mathcal{C}^\perp)$.

Definition 124 (Rank-metric Equivalence). Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{m \times n}$. We say that \mathcal{C}_1 is equivalent to \mathcal{C}_2 if there exists $\varphi \in \text{GL}_m(q) \rtimes \text{GL}_n(q)$ such that $\varphi(\mathcal{C}_1) = \mathcal{C}_2$.

2.2.15 Lee Metric Codes

Let us consider \mathbb{F}_p , for $p > 3$ a prime. Then we can define a different metric, called *Lee metric*.

Definition 125 (Lee Metric). Let $x \in \mathbb{F}_p$, and represent $x \in \{0, \dots, p-1\}$. The *Lee weight* of x is given by

$$\text{wt}_L(x) = \min\{x, |p-x|\}.$$

The largest possible Lee weight is thus $M = (p-1)/2$. Let $\mathbf{x} \in \mathbb{F}_p^n$. The Lee weight is then extended additively on the entries, that is

$$\text{wt}_L(\mathbf{x}) = \sum_{i=1}^n \text{wt}_L(x_i).$$

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_p^n$. Their *Lee distance* is induced by the Lee weight, that is

$$d_L(\mathbf{x}, \mathbf{y}) = \text{wt}(\mathbf{x} - \mathbf{y}).$$

Let $\mathcal{C} \subseteq \mathbb{F}_p^n$ be a linear code. The *minimum Lee distance* of \mathcal{C} is given by

$$d_L(\mathcal{C}) = \min\{\text{wt}_L(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0\}.$$

Note that the Lee metric can be defined over any integer residue ring $\mathbb{Z}/m\mathbb{Z}$, for any integer m . However, for the cryptographic purposes it is enough to consider prime fields. Since the Lee metric coincides with the Hamming metric in \mathbb{F}_2 and \mathbb{F}_3 , we only focus on primes $p > 3$.

Note that, $\text{wt}_H(\mathbf{v}) \leq \text{wt}_L(\mathbf{v}) \leq M\text{wt}_H(\mathbf{v})$ and the average Lee weight of the vectors in \mathbb{F}_p^n is given by $(M/2)n$. We, thus, also get that linear code $\mathcal{C} \subseteq \mathbb{F}_p^n$ can correct more errors in the Lee metric as in the Hamming metric, i.e.,

$$d_H(\mathcal{C}) \leq d_L(\mathcal{C}).$$

Using the other bound, i.e., $d_L(\mathcal{C}) \leq Md_H(\mathcal{C})$, we can easily adapt the Singleton bound [240].

Theorem 126. *Let $\mathcal{C} \subseteq \mathbb{F}_p^n$ be a linear code of dimension k . Then,*

$$d_L(\mathcal{C}) \leq M(n - k + 1).$$

Unfortunately, this bound is only tight in $p = 5, n = 2$, as shown in [81].

Exercise 127. Consider the symmetric representation $\{-(p-1)/2, \dots, (p-1)/2\}$. Show that $\text{wt}_L(x) = |x|$.

We denote by δ the *relative minimum Lee distance*, that is

$$\delta = \frac{d_L(\mathcal{C})}{nM}.$$

Let us denote by $V_L(p, n, r)$ the *Lee sphere* of radius t

$$V_L(p, n, t) := \{\mathbf{m}x \in \mathbb{F}_p^n \mid \text{wt}_L(\mathbf{m}x) = t\},$$

and by

$$F_L(p, T) = \lim_{n \rightarrow \infty} \frac{1}{n} \log_p(|V_L(p, n, TnM)|)$$

its asymptotic size. The exact formulas for the size of $V_L(p, n, t)$ and $F_L(p, T)$ can be found in [263, 136].

Let us denote by $A_L(n, d, p)$ the maximal size of a code in \mathbb{F}_p^n of minimum Lee distance d and by

$$R(\delta) = \limsup_{n \rightarrow \infty} \frac{1}{n} \log_p(A(n, d/(Mn), p)).$$

We can then state the Gilbert-Varshamov bound in the Lee-metric [31].

Theorem 128. *Let p be a prime and n, d positive integers. Then,*

$$R(\delta) \geq 1 - F_L(p, \delta).$$

In [80], it was shown that random Lee-metric codes attain with high probability the Lee-metric GV bound, i.e., a random code has with high probability a relative minimum Lee distance δ such that $R(\delta) = 1 - F_L(p, \delta)$.

We define a function $\text{sgn}(x)$, that gives us the sign of an element in \mathbb{F}_p .

Definition 129 (Signum). For $x \in \mathbb{F}_p = \left\{-\frac{p-1}{2}, \dots, 0, \dots, \frac{p-1}{2}\right\}$ let

$$\text{sgn}(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x > 0, \\ -1 & \text{if } x < 0. \end{cases}$$

For the symmetric representation of \mathbb{F}_p , this corresponds to the common signum function.

Let us also define a matching function $\text{mt}(\mathbf{x}, \mathbf{y})$ that compares \mathbf{x} and \mathbf{y} and counts the number of symbols that hold the same sign.

Definition 130 (Sign Matches). Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_p^n$ and consider the number of matches in their sign such that

$$\text{mt}(\mathbf{x}, \mathbf{y}) = |\{i \in \{1, \dots, n\} \mid \text{sgn}(x_i) = \text{sgn}(y_i), x_i \neq 0, y_i \neq 0\}|.$$

Finally, we introduce a function calculating the probability that a vector and a uniformly random hash digest (in $\{\pm 1\}^n$) have μ sign matches.

Definition 131 (Logarithmic Matching Probability (LMP)). For a fixed $\mathbf{v} \in \mathbb{F}_p^n$ and a randomly chosen $\mathbf{y} \in \{\pm 1\}^n$, the probability of \mathbf{y} to have μ sign matches with \mathbf{v} is

$$B(\mu, \text{wt}_H(\mathbf{v}), 1/2),$$

where $B(k, n, q)$ is the binomial distribution defined as

$$B(k, n, q) = \binom{n}{k} q^k (1-q)^{n-k}.$$

To ease notation, we write $\text{LMP}(\mathbf{v}, \mathbf{y}) = -\log_2(B(\mu, \text{wt}_H(\mathbf{v}), 1/2))$.

In [58], the authors computed the marginal distribution of entries where vectors are uniformly distributed in $V_L(p, n, w)$. Let E denote a random variable corresponding to the realization of an entry of $\mathbf{x} \in \mathbb{F}_p^n$. As n tends to infinity, we have the following result on the distribution of the elements in $\mathbf{x} \in \mathbb{F}_p^n$.

Lemma 132 ([58, Lemma 1]). *For any $x \in \mathbb{F}_p$, the probability that one entry of \mathbf{x} is equal to x is given by*

$$p_w(x) = \frac{1}{Z(\beta)} \exp(-\beta \text{wt}_L(x)),$$

where $Z(\beta) = \sum_{i=0}^{p-1} \exp(-\beta \text{wt}_L(i))$ denotes the normalization constant and β is the unique solution to $w = \sum_{i=0}^{p-1} \text{wt}_L(i) p_w(i)$.

Definition 133 (Typical Lee Set). For a fixed weight w , let $p_w(x)$ be the probability from Lemma 132 of the element $x \in \mathbb{F}_p$. Then, we define the typical Lee set as

$$T(p, n, w) = \{\mathbf{x} \in \mathbb{F}_p^n \mid \mathbf{x}_i = x \text{ for } p_w(x)n \text{ coordinates } i \in \{1, \dots, n\}\}$$

That is the set of vectors, for which the element x occurs $p_w(x)n$ times.

2.2.16 Restricted Errors

Instead of considering a different metric on the vectors in \mathbb{F}_p^n , we can also restrict their entries.

Definition 134 (Restriction). Let us consider $g \in \mathbb{F}_p^*$ of prime order z and the subgroup $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$. We say E is a *restriction*.

Let us denote by \star the component-wise multiplication of vectors.

Proposition 135. (\mathbb{E}^n, \star) is a commutative, transitive group isomorphic to $(\mathbb{F}_z^n, +)$.

The isomorphism is given by

$$\begin{aligned} \ell : \mathbb{E}^n &\rightarrow \mathbb{F}_z^n, \\ \mathbf{x} = (g^{\ell_1}, \dots, g^{\ell_n}) &\mapsto \ell(\mathbf{x}) = (\ell_1, \dots, \ell_n). \end{aligned}$$

This representation of vectors in \mathbb{E}^n as vectors in \mathbb{F}_z^n is helpful to shorten the sizes of objects. For the opposite direction of the isomorphism, we use the following abuse of notation

$$\mathbf{a} = g^{\ell(\mathbf{a})} = (g^{\ell(\mathbf{a})_1}, \dots, g^{\ell(\mathbf{a})_n}),$$

for some $\ell(\mathbf{a}) = (\ell(\mathbf{a})_1, \dots, \ell(\mathbf{a})_n) \in \mathbb{F}_z^n$.

Proposition 136. Any linear map $\varphi : \mathbb{E}^n \rightarrow \mathbb{E}^n$ which acts transitively on \mathbb{E}^n is simply given by component-wise multiplication, i.e., $\varphi(\mathbf{b}) = \mathbf{a} \star \mathbf{b}$, for some $\mathbf{a} \in \mathbb{E}^n$.

Exercise 137. Prove Proposition 136

Let the map φ be the component-wise multiplication with $\mathbf{a} \in \mathbb{E}^n$. Then we can compactly represent φ through the vector $\ell(\mathbf{a}) \in \mathbb{F}_z^n$. Additionally, the computation $\varphi(\mathbf{b}) = \mathbf{a} \star \mathbf{b}$ is given by an addition in \mathbb{F}_z^n ; namely $\ell(\mathbf{a}) + \ell(\mathbf{b})$.

Instead of the restriction \mathbb{E} , we can also consider a *restricted subgroup*.

Definition 138 (Restricted Subgroup). Let $(G, \star) \leq (\mathbb{E}^n, \star)$ with

$$G = \langle \mathbf{a}_1, \dots, \mathbf{a}_m \rangle = \{ \star_{i=1}^m \mathbf{a}_i^{u_i} \mid u_i \in \{1, \dots, z\} \},$$

for some $m < n$. Then, we call G a *restricted subgroup* of \mathbb{E} .

To construct elements $\mathbf{e} \in G$, we can collect all the exponents of the generators \mathbf{a}_i into a matrix. That is, we define the matrix $\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$ as

$$\mathbf{M}_G = \begin{pmatrix} \ell(\mathbf{a}_1)_1 & \cdots & \ell(\mathbf{a}_1)_n \\ \vdots & & \vdots \\ \ell(\mathbf{a}_m)_1 & \cdots & \ell(\mathbf{a}_m)_n \end{pmatrix} = \begin{pmatrix} \ell(\mathbf{a}_1) \\ \vdots \\ \ell(\mathbf{a}_m) \end{pmatrix}.$$

To check whether $|G| = z^m$, it is enough to verify $\text{rank}(\mathbf{M}_G) = m$. For the remainder, we assume that this is the case. Hence, we can think of $\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$ as a generator matrix of a m -dimensional code in \mathbb{F}_z^n . Thus, each codeword $\mathbf{c} \in \langle \mathbf{M}_G \rangle$ can be represented using an information vector $\mathbf{u} \in \mathbb{F}_z^m$, that is

$$\mathbf{c} = \mathbf{u} \mathbf{M}_G.$$

The corresponding $\mathbf{e} \in G$ has then the exponents $\ell(\mathbf{c})$.

Proposition 139. *Let G be a restricted subgroup, where \mathbf{M}_G has full rank m . Then, ℓ_G is a group homomorphism, where*

$$\begin{aligned} \ell_G : G &\rightarrow \mathbb{F}_z^m, \\ \mathbf{e} = \mathbf{a}_1^{u_1} \star \cdots \star \mathbf{a}_m^{u_m} &\mapsto \ell_G(\mathbf{e}) = (u_1, \dots, u_m). \end{aligned}$$

Proposition 140. *The linear maps $\varphi : G \rightarrow G$, which act transitively on G , are still given by component-wise multiplication with another element in G , i.e., for $\mathbf{e} \in G$, $\varphi(\mathbf{e}) = \mathbf{e}' \star \mathbf{e}$.*

2.3 Cryptography

As coding theory is the art of *reliable* communication, this goes hand in hand with cryptography, the art of *secure* communication. In cryptography we differ between two main branches, symmetric cryptography and asymmetric cryptography.

In *symmetric* cryptography there are the two parties that want to communicate with each other and prior to communication have exchanged some key, that will enable them a secure communication. Such secret key exchange might be performed using protocols such as the Diffie-Hellman key exchange [112], which itself lies in the realm of asymmetric cryptography.

More mathematically involved is the branch of *asymmetric* cryptography, where the two parties do not share the same key. In this survey we will focus on two main subjects of asymmetric cryptography, that were also promoted by the NIST standardization call [92], namely public-key encryption (PKE) schemes and digital signature schemes.

Many of these cryptographic schemes seem very abstract when discussed in generality. To get a grasp of the many definitions and concepts, we will also provide some easy examples. First of all, let us recall the definition of a hash function. A *hash function* is a function that compresses the input value to a fixed length. In addition, we want that it is computationally hard to reverse a hash function and also to find a different input giving the same hash value. In this chapter, we denote a publicly known hash function by **Hash**.

2.3.1 Public-Key Encryption

Let us start with public-key encryption (PKE) schemes. A PKE consists of three steps:

1. key generation,
2. encryption,
3. decryption.

The main idea is that one party, usually called Alice, constructs a *secret key* \mathcal{S} and a connected *public key* \mathcal{P} . The public key, as the name suggests, is made publicly known, while the secret key is kept private.

This allows another party, usually called Bob, to use the public key to encrypt a *message* m by applying the public key, gaining the so called *cipher* c .

The cipher is now sent through the insecure channel to Alice, who can use her secret key \mathcal{S} to decrypt the cipher and recover the message m .

An adversary, usually called Eve, can only see the cipher c and the public key \mathcal{P} . In order for a public-key encryption scheme to be considered secure, it should be infeasible for Eve to recover from c and \mathcal{P} the message m . This also implies that the public key should not reveal the secret key.

Table 1: Public-Key Encryption

ALICE	BOB
KEY GENERATION	
Construct a secret key \mathcal{S}	
Construct a connected public key \mathcal{P}	
$\xrightarrow{\mathcal{P}}$	
	ENCRYPTION
	Choose a message m
	Encrypt the message $c = \mathcal{P}(m)$
	\xleftarrow{c}
DECRYPTION	
Decrypt the cipher $m = \mathcal{S}(c)$	

What exactly does infeasible mean, however? This is the topic of *security*. For a cryptographic scheme, we define its *security level* to be the average number of binary operations needed for an adversary to break the cryptosystem, that means either to recover the message (called *message recovery*) or the secret key (called *key recovery*).

Usual security levels are 2^{80} , 2^{128} , 2^{256} or even 2^{512} , meaning for example that an adversary is expected to need at least 2^{80} binary operations in order to reveal the message. These are referred to as 80 bit, 128 bit, 256 bit, or 512 bit security levels.

Apart from the security of a PKE, one is also interested in the performance, including how fast the PKE can be executed and how much storage the keys require. Important parameters of a public-key encryption are

- the public key size,
- the secret key size,
- the ciphertext size,
- the decryption time.

These values are considered to be the *performance* of the public-key encryption. With 'size' we intend the bits that have to be sent or stored for this key, respectively for the cipher. Clearly, one prefers small sizes and a fast decryption.

As an example for a PKE, we can choose one of the most currently used schemes, namely RSA [227].

Example 141 (RSA). 1. Key Generation: Alice chooses two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. She chooses a natural number $e < \varphi(n)$, which is coprime to $\varphi(n)$. The public key is $\mathcal{P} = (n, e)$ and the secret key is $\mathcal{S} = (p, q)$.

2. Encryption: Bob chooses a message m and encrypts it by computing

$$c = m^e \mod n.$$

3. Decryption: Alice can decrypt the cipher by first computing d and b such that

$$de + b\varphi(n) = 1.$$

Since

$$c^d = (m^e)^d = m^{1-b\varphi(n)} = m \left(m^{\varphi(n)} \right)^{-b} = m 1^{-b} = m,$$

she can recover the message m .

Eve sees n but there is no feasible algorithm to compute p and q .

Exercise 142. Assume that Alice has chosen p and q to have 100 digits. How large is the public key size?

Exercise 143. Assume that the fastest known algorithm to factor n into p and q costs \sqrt{n} binary operations. In order to reach a security level of 2^{80} binary operations, how large should Alice choose p and q ?

Exercise 144. To give you also a feeling for cryptanalysis; why should we always choose two distinct primes? Or in other words; how can you attack RSA if $p = q$?

2.3.2 Key-Encapsulation Mechanisms

A *key-encapsulation mechanism* (KEM) is a way to transmit a key for symmetric cryptography using an asymmetric cryptosystem.

Public-key systems are often not optimal to transmit longer messages. Instead, the two parties use a public-key system to share a random m , usually a number or vector. Then both parties use an agreed-on function, called *key derivation function*, to calculate a key M from m .

Table 2: Key-Encapsulation Scheme

ALICE	BOB
KEY GENERATION	
Generate a secret key \mathcal{S}	
Construct a connected public key \mathcal{P}	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
Choose a random message m	
Generate a key $M = \text{Hash}(m)$	
Use the public key \mathcal{P} to encrypt m as cipher c	
\xleftarrow{c}	
DECRYPTION	
Using the secret key \mathcal{S} , decrypt c to get m	
compute $\text{Hash}(m) = M$	
COMMUNICATION	
The parties may now communicate with each other since they both possess a key to encrypt and decrypt messages	

The function is usually chosen to be a one-way function, meaning that computing back m with only the knowledge of the function and M is not computationally feasible. With this key, the parties can then encrypt their message.

Most KEM schemes are based on Shoup's idea [242]. In Table 2 we give an outline, in which we assume that a public-key system is given. For this, let Hash denote a hash function.

As mentioned before, it is often the case that instead of directly encrypting the key M , a random m is encrypted. From this m , both parties can generate a key using the agreed-on key derivation function.

Example 145. For an example of a KEM we again consider RSA.

1. Key generation: Alice choose two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. Alice also chooses a positive integer $e < \varphi(n)$, which is coprime to $\varphi(n)$. The public key is given by $\mathcal{P} = (n, e)$ and the private key is given by (p, q) .
2. Encryption: Bob chooses a random message m and computes its hash $M = \text{Hash}(m)$. He then performs the usual steps of RSA, that is: he encrypts $c = m^e \bmod n$ and sends this to Alice.
3. Decryption: Alice can compute $d = e^{-1} \bmod \varphi(n)$ and computes $c^d = m \bmod n$. Also Alice can now compute the shared key $M = \text{Hash}(m)$.

2.3.3 Digital Signature Schemes

Digital Signature schemes aim at giving a guarantee of the legitimate origin of an object, such as a digital message, exactly as signing a letter to prove that the sender of this letter is really you.

In this process we speak of *authentication*, meaning that a receiver of the message can (with some probability) be sure that the sender is legit, and of *integrity*, meaning that the message has not been altered.

A digital signature scheme again consists of three steps:

1. key generation,
2. signing,
3. verification.

In digital signature schemes we consider two parties, one is the *prover*, that has to prove his identity to the second party called *verifier*, that in turn, verifies the identity of the prover.

As a first step, the prover constructs a secret key \mathcal{S} , which he keeps private and a public key \mathcal{P} , which is made public. The prover then chooses a message m , and creates a signature s using his secret key \mathcal{S} and the message m , getting a signed message (m, s) .

The verifier can easily read the message m , but wants to be sure that the sender really is the prover. Thus, he uses the public key \mathcal{P} and the knowledge of the message m on the signature s to get authentication.

Table 3: Digital Signature Scheme

PROVER	VERIFIER
KEY GENERATION	
Construct a secret key \mathcal{S}	
Construct a connected public key \mathcal{P}	
$\xrightarrow{\mathcal{P}}$	
SIGNING	
Choose a message m	
Construct a signature s from \mathcal{S} and m	
$\xrightarrow{m,s}$	
VERIFICATION	
Verify the signature s using \mathcal{P} and m	

The security of a digital signature scheme introduces a new person, the *impersonator*. An impersonator, tries to cheat the verifier and acts as a prover, however without the knowledge of the secret key \mathcal{S} . An impersonator wins if a verifier has verified a forged signature. This comes with a certain probability, called *cheating probability* or *soundness error*. In order to ensure integrity a digital signature should always involve a secret key as well as the message itself.

Clearly, the secret key should still be infeasible to recover from the publicly known private key, thus one still has the usual adversary, called Eve, and a security level, as in a public-key encryption scheme.

The performance of a digital signature scheme consists of

- the *communication cost*, that is the total number of bits, that have been exchanged within the process,
- the *signature size*,
- the public key size,
- the secret key size,
- the verification time.

An easy example for a signature scheme is given by turning the RSA public-key encryption protocol into a signature scheme.

Example 146 (RSA Signature Scheme). 1. Key Generation: Alice chooses two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. She chooses a natural number $e < \varphi(n)$, which is coprime to $\varphi(n)$. She computes d and b such that

$$de + b\varphi(n) = 1.$$

The public key is $\mathcal{P} = (n, e)$ and the secret key is $\mathcal{S} = (p, q, d)$.

2. Signing: Alice chooses a message m and signs it by computing

$$s = m^d \mod n.$$

She then sends m, s to Bob.

3. Verification: Bob can verify the signature s by checking if

$$s^e = m \mod n.$$

Exercise 147. How would an impersonator forge a signature provided that the impersonator does not care about the content of the message m ?

2.3.4 Zero-Knowledge Protocols

Since digital signature schemes can be constructed using the Fiat-Shamir transform [121] on *Zero-Knowledge* (ZK) protocols, we will also introduce the concept of ZK protocols and then of the transform itself.

The process and notation for a ZK protocols are similar to that of a digital signature scheme. We have two parties, a prover and a verifier. Different to a digital signature scheme, the prover does not want to prove his identity to the verifier, but rather convince the verifier of his knowledge of a secret object, without revealing said object.

A ZK protocol consists of two stages: key generation and verification. The verification process can consist of several communication steps between the verifier and the prover, in particular, we are interested in the following scheme:

1. The prover prepares two *commitments* c_0, c_1 , and sends them to the verifier.
2. The verifier randomly picks a *challenge* $b \in \{0, 1\}$, and sends it to the prover.
3. The prover provides a *response* r_b that only allows to verify c_b .
4. The verifier checks the validity of c_b , usually by recovering c_b using r_b and the public key.

Table 4: ZK Protocol

PROVER	VERIFIER
KEY GENERATION	
Construct a secret key \mathcal{S}	
Construct a connected public key \mathcal{P}	
$\xrightarrow{\mathcal{P}}$	
VERIFICATION	
Construct commitments c_0, c_1	
$\xrightarrow{c_0, c_1}$	
	Choose $b \in \{0, 1\}$
\xleftarrow{b}	
Construct response r_b	
$\xrightarrow{r_b}$	
	Verify c_b using r_b

A ZK protocol has three important attributes:

1. *Zero-knowledge*: this means that no information about the secret is revealed during the process.
2. *Completeness*: meaning that an honest prover will always get accepted.
3. *Soundness*: for this, we want that an impersonator has only a small cheating probability to get accepted.

Again, for the performance of the protocol, we have

- the communication cost,
- the secret key,
- the public key size,
- the verification time.

In order to achieve an acceptable cheating probability, the protocols are often repeated several times (called *rounds*) and only if each instance was verified will the prover be accepted. Thus, if the ZK protocol previously had cheating probability α , after N such rounds we have a cheating probability of α^N .

There exist several techniques in order to compress the communication cost within N rounds, for example the *compression technique*, first introduced in [3]. Let us explain this method in detail.

Before the first round, the prover generates the commitments for all the N rounds, that is c_b^i for $i \in \{1, \dots, N\}$ and $b \in \{0, 1\}$. The prover then sends the hash value

$$c = \text{Hash}(c_0^1, c_1^1, \dots, c_0^N, c_1^N)$$

to the verifier.

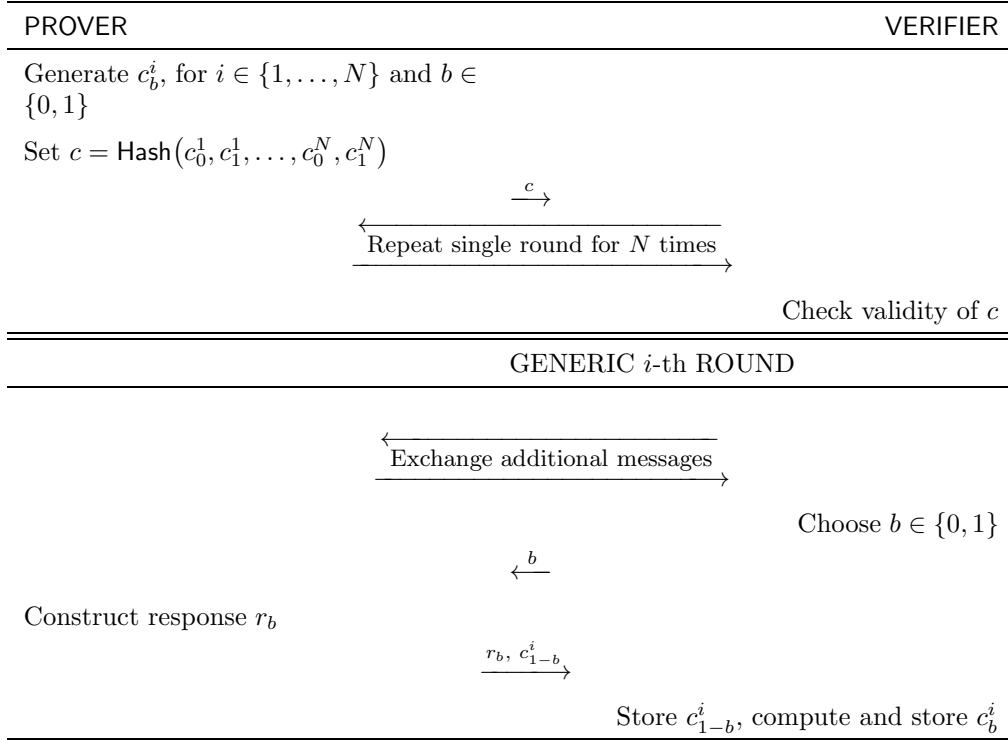
In the i -th round, after receiving the challenge b , the prover sets their response r_b such that the verifier can compute c_b^i , and additionally includes c_{1-b}^i .

At the end of each round, the verifier uses r_b to compute c_b^i , and stores it together with c_{1-b}^i .

After the final round N , the verifier is able to check validity of the initial commitment c , by computing the hash of all the stored c_b^i .

This way, one hash is sent at the beginning of the protocol, and only one hash (instead of two) is transmitted in each round and thus, the number of exchanged hash values reduces from $2N$ to $N + 1$.

Figure 1: Compression Technique for N Rounds



An easy example is again provided using the hardness of integer factorization, namely the Feige-Fiat-Shamir protocol [120].

Example 148 (Feige-Fiat-Shamir). 1. Key generation: The prover chooses two distinct primes p, q and computes $n = pq$ and some positive integer k . The prover chooses s_1, \dots, s_k coprime to n . The prover now computes

$$v_i \equiv s_i^{-2} \pmod{n}.$$

The public key is given by $\mathcal{P} = (n, v_1, \dots, v_k)$. The secret key is given by $\mathcal{S} = (p, q, s_1, \dots, s_k)$.

2. Verification: The prover chooses a random integer c and a random sign $\sigma \in \{-1, 1\}$ and computes

$$x \equiv \sigma c^2 \pmod{n}$$

and sends this to the verifier. The verifier chooses the challenge $b = (b_1, \dots, b_k) \in \mathbb{F}_2^k$ and sends b to the prover. The prover then computes the response

$$r \equiv c \prod_{b_j=1} s_j \pmod{n}$$

and sends r to the verifier. The verifier can now check whether

$$x \equiv \pm r^2 \prod_{b_j=1} v_j \pmod{n}.$$

Eve, the impersonator, can see the public v_i but she does not know the s_i . She can pick a random r and $b = (b_1, \dots, b_k) \in \mathbb{F}_2^k$. She then computes

$$x \equiv r^2 \prod_{b_j=1} v_j \pmod{n}$$

and sends x to the verifier. The verifier will then challenge her with his b' , but Eve simply returns her r . If Eve has correctly chosen $b = b'$, she will be verified.

Exercise 149. What is the cheating probability of this scheme? If you repeat this process t times before accepting the prover, what is now your cheating probability?

Exercise 150. Let us assume that $k = 10$. How many times should you repeat this process in order to reach a cheating probability of at least 2^{128} ?

2.3.5 Fiat-Shamir Transform

The *Fiat-Shamir transform* allows us to build a signature scheme from a ZK protocol. To avoid the communication with the verifier that randomly picks a challenge, the challenge is replaced with the seemingly random hash of the commitment and message.

The following table follows the general description of the Fiat-Shamir transform from [121]. We assume that we are given a zero-knowledge identification scheme and a public hash function **Hash**.

Using the Fiat-Shamir transform we can turn the Feige-Fiat-Shamir ZK protocol into a signature scheme.

Example 151 (Fiat-Shamir digital signature scheme). 1. Key Generation: Let **Hash** be a publicly known hash function. The prover chooses a positive integer k and two distinct primes p, q and computes $n = pq$. The prover chooses s_1, \dots, s_k integers coprime to n and computes $v_i \equiv s_i^{-2} \pmod{n}$ for all $i \in \{1, \dots, k\}$. The secret key is given by $\mathcal{S} = (p, q, s_1, \dots, s_k)$ and the public key is given by (n, v_1, \dots, v_k) .

Table 5: Fiat-Shamir Transform

PROVER	VERIFIER
KEY GENERATION	
Given the public key \mathcal{P} and the secret key \mathcal{S} of some ZK protocol and a message m	
Choose a commitment c	
Compute $a = \text{Hash}(m, c)$	
Compute a response r to the challenge a	
The signature is the pair $s = (a, r)$	
$\xrightarrow{m, s}$	
VERIFICATION	
Use the response r and the public key \mathcal{P} to construct the commitment c	
Check if $\text{Hash}(m, c) = a$	

2. Verification: the prover chooses randomly $c_1, \dots, c_t < n$ and computes $x_i \equiv c_i^2 \pmod n$ for all $i \in \{1, \dots, t\}$. In order to bypass the communication with the verifier from before, the prover computes the first kt bits of

$$\text{Hash}(m, x_1, \dots, x_t) = (a_{1,1}, \dots, a_{t,k}) = a.$$

The prover now computes $r_i \equiv c_i \prod_{a_{ij}=1} s_j \pmod n$ for all $i \in \{1, \dots, t\}$ and sends (m, a, r_1, \dots, r_t) to the verifier. The verifier computes

$$z_i \equiv r_i^2 \prod_{a_{i,j}=1} v_j \pmod n$$

for all $i \in \{1, \dots, t\}$ and checks if

$$\text{Hash}(m, z_1, \dots, z_t) = a.$$

2.3.6 Multi-Party-Computations-in-the-Head

Recall that any ZK protocol can be turned into a signature scheme via the Fiat-Shamir transform. Assume that the used ZK protocol has a cheating probability of α and recall that this probability might be quite large. In order to get a resulting signature scheme attaining the security level 2^λ , we require N rounds of the ZK protocol, such that $\alpha^N < 2^{-\lambda}$.

Since the final signature is given by the communication cost within all N rounds, such signature schemes usually suffer from large signature sizes.

One very prominent technique in order to reduce the signature size was introduced in [158] and uses the idea of Multi-Party-Computations (MPC).

In an MPC we have N parties, called p_1, \dots, p_N , each party is secretly provided a share s_i . The parties wish to collectively compute a certain function of their shares, say $f(s_1, \dots, s_N)$, in such a way that the shares s_i remain only known to the party p_i and an such that all shares are required.

We say that an MPC protocol is

- correct, if the parties can correctly compute $f(s_1, \dots, s_N)$,
- t -private, if any t shares (or less) do not reveal any information on $f(s_1, \dots, s_N)$,
- secure, if $f(s_1, \dots, s_N)$ does not reveal any information on s_i .

An easy way to achieve an MPC protocol is to use Secret Sharing (SS) schemes. The whole theory of MPC and SS schemes is highly involved and we refer the interested reader to [86].

In a SS scheme, we have a *dealer*, who wants to share a secret message with the parties, p_1, \dots, p_N and again each party p_i is provided with a share s_i . We introduce two parameters; $k \leq n$ the decoding threshold and $z < k$ the confidentiality threshold. These parameters take care of the following two constraint:

1. A group of $k \leq n$ parties can decode the secret message using their shares.
2. A group of $z < k$ parties do not gain any information about the secret from their shares.

The security goal for such a scheme is thus *confidentiality*, that is: no information about the secret should be leaked from any z shares.

Important for this survey, will be additive sharing schemes. Let us, thus, start with a toy example.

Example 152. Let us consider $n = 4, k = 2, z = k - 1 = 1$ and $q = 5$. The secret message is some $m \in \mathbb{F}_5$, we choose a random value $r \in \mathbb{F}_q$ and we use an *encoding polynomial* $p(x) = m + rx$. The secret shares are then given by $s_i = p(i) = m + ir$.

Exercise 153. Consider the SS scheme in Example 152.

1. Show that the SS scheme attains privacy, i.e., an individual party with share s_i does not gain information about m .
2. Show that the SS scheme is decodable, i.e., any two parties can recover m .

The more general construction, is called *Shamir's secret sharing scheme* [238]. Given the integers $z = k - 1, k \leq n < q$ and a polynomial $p(x) \in \mathbb{F}_q[x]$ of degree z , given by

$$p(x) = m + \sum_{i=1}^z r_i x^i,$$

where r_i are chosen uniform at random from \mathbb{F}_q . The secret shares are then given by $s_i = p(i)$.

Exercise 154. Show that Shamir's SS scheme is attains privacy and is decodable.

One can also construct a SS scheme with $z < k - 1$, e.g. using McEliece-Sarwate's construction [194]. Given the integers $z < k \leq n < q$ and a polynomial $p(x) \in \mathbb{F}_q[x]$ of degree $k - 1$, given by

$$p(x) = \sum_{i=1}^z r_i x^i + \sum_{i=1}^{k-z} m_i x^{z-1+i},$$

where r_i are chosen uniform at random from \mathbb{F}_q . The secret shares are then given by $s_i = p(i)$.

Exercise 155. Show that McEliece-Sarwate's SS scheme is attains privacy and is decodable.
Hint: Use the property of a $k \times n$ Vandermonde matrix, that each $k \times k$ submatrix is invertible.

For a more sophisticated SS scheme, we assume that the secret is given by $\mathbf{s} \in \mathbb{F}_q^n$ and all N parties are provided with random $\mathbf{s}_i \in \mathbb{F}_q^n$, such that $\sum_{i=1}^N \mathbf{s}_i = \mathbf{s}$. Clearly, only if all N parties open their shares, they can compute collectively

$$f(\mathbf{s}_1, \dots, \mathbf{s}_N) = \sum_{i=1}^N \mathbf{s}_i = \mathbf{s},$$

while any $k < N$ parties cannot compute \mathbf{s} .

For a secret s , we will use the notation $[[s]]$ to denote a possible splitting into N additive shares

$$[[s]] = (s_1, \dots, s_N).$$

The idea of MPC-in-the-head (MPCitH), introduced in [158] is to use MPC protocols to build ZK protocols.

For this, assume we are given an MPC protocol in which N parties P_1, \dots, P_N securely and correctly evaluate a function f on a secret input s . Additionally, we require

- the secret s has a sharing $[[s]] = (s_1, \dots, s_N)$ and each party P_i gets the input s_i ,
- for some functions φ_i , the party P_i computes the broadcast $\alpha_i = \varphi(s_i)$,
- the function f , such that $f(\alpha_1, \dots, \alpha_N) = 1$, and anything else evaluates to 0,
- if $N - 1$ parties reveal their shares s_i , or their broadcasts α_i , they do not reveal anything on the secret s .

The resulting ZK protocol, requires a trapdoor function F , which is easy to compute and hard to invert. In code-based cryptography, this is usually the syndrome decoding problem. Namely,

$$F : B_H(t, n, q) \rightarrow \mathbb{F}_q^{n-k},$$

$$\mathbf{e} \mapsto \mathbf{e}\mathbf{H}^\top.$$

That is, we send vectors of Hamming weight at most t , to their syndromes for a fixed parity-check matrix \mathbf{H} . While this is easy to compute given \mathbf{H} and \mathbf{e} , it is hard to invert, that is: given \mathbf{H}, \mathbf{s} find \mathbf{e} . We say that the trapdoor function F has *target* y if, for the sought solution x we have $F(x) = y$.

In the previous example of syndrome decoding, the target would be the syndrome of the sought-after solution \mathbf{e} and F is completely determined by \mathbf{H} .

Assuming such a trapdoor function F and an MPC protocol, the resulting ZK protocol works as follows. The main idea of the ZK protocol using MPCitH, is to run a MPC protocol in the prover's head, i.e., the prover simulates locally all the parties of the MPC protocol and sends commitments to each party's share. To check that the MPC protocol runs correctly, the prover also sends the broadcasts α_i .

The main benefit of MPCitH lies in the cheating probability. Since the MPC protocol is $N - 1$ -private, an impersonator not knowing the secret s , can guess any $N - 1$ many shares and compute broadcasts and commitments to those. However, the last share s_f is chosen

Table 6: ZK Protocol from MPC

PROVER	VERIFIER
KEY GENERATION	
Given MPC with secret s and function f and φ_i	
Given trapdoor function F with target y .	
Secret key $\mathcal{S} = s$	
Public key $\mathcal{P} = \{f, F, y\}$	
$\xrightarrow{\mathcal{P}}$	
VERIFICATION	
For $i \in \{1, \dots, N\}$:	
Compute $\alpha_i = \varphi_i(s_i)$	
Compute $c_i = \text{Hash}(s_i, \rho_i)$	
for some random ρ_i .	
$\xrightarrow{c_1, \dots, c_N}$	
Check if $f(\alpha_1, \dots, \alpha_N) = 1$	$\xrightarrow{\alpha_1, \dots, \alpha_N}$
	Choose $b \in \{1, \dots, N\}$
\xleftarrow{b}	
Response $r_b = \{(s_i, \rho_i) \mid i \neq b\}$	
$\xrightarrow{r_b}$	
	For all $i \neq b$:
	Check $c_i = \text{Hash}(s_i, \rho_i)$
	Check $\alpha_i = \varphi_i(s_i)$
	Check $F(\alpha_1, \dots, \alpha_N) = y$.

at random, and is not such that $\sum_{i=1}^N s_i = s$. In fact, finding the last s_f would require the impersonator to invert the trapdoor function.

The verifier accepts the impersonator, only if the verifier challenges exactly the random s_f , i.e., $b = f$. In any other case, the impersonator is required to send s_f in the response and the verifier can check that the target y is not reached.

Thus, the new cheating probability is $\frac{1}{N}$. This allows us to reduce the number of rounds required to achieve a certain security level and thus, in turn, the signature size. However, the broadcast computation has to be performed in each such round N times, by the prover and the verifier.

3 Code-Based Public-Key Encryption Frameworks

Code-based cryptography and in particular code-based PKEs first came up with the seminal work of Robert J. McEliece in 1978 [193]. The main idea of code-based cryptography is to base the security of the cryptosystem on the hardness of decoding a random linear code. Since this problem is NP-hard, code-based cryptography is considered to be one of the most promising candidates for post-quantum cryptography.

In a nutshell, McEliece’s idea as follows: the private key is given by a linear code \mathcal{C} , which can efficiently correct t errors. The public key is \mathcal{C}' a disguised version of the linear code, which should not reveal the secret code, in fact, should behave randomly.

While anyone with \mathcal{C}' , the publicly known code, can encode their message and possibly add some intentional errors, an attacker would only see a random code and in order to recover the message would need to decode it.

The constructor of the secret code however, can transform the encoded message to a codeword of \mathcal{C} , which is efficiently decodable.

The first code-based cryptosystem by McEliece uses the generator matrix \mathbf{G} as a representation of the secret code and in order to disguise the generator matrix, one computes $\mathbf{G}' = \mathbf{SGP}$, where \mathbf{S} is an invertible matrix, thus only changing the basis of the code, and \mathbf{P} is a permutation matrix, thus giving a permutation equivalent code. In the encryption step the message is then encoded through \mathbf{G}' and an intentional error vector \mathbf{e} is added.

An equivalent [183] cryptosystem was proposed by Niederreiter in [204], where one uses the parity-check matrix \mathbf{H} , and the disguised parity-check matrix $\mathbf{H}' = \mathbf{SHP}$, instead of the generator matrix and the cipher is given by the syndrome of an error vector, i.e., $\mathbf{s} = \mathbf{H}'\mathbf{e}^\top$.

The code-based system proposed by Alekhnovich uses the initial idea of McEliece, but twists the disguising of the code, by adding a row to the parity-check matrix, which is a erroneous codeword, thus making the error vector the main part of the secret key. The idea of Alekhnovich, which is not considered practical has been the starting point of a new framework, the quasi-cyclic scheme.

A different idea has been proposed by Augot and Finiasz in [32]. Here the secret is given by the support of an error vector, which allows to insert an error of weight beyond the error correction capacity. Thus, again the code can be made completely public.

Finally, the McEliece framework has also been introduced for the rank metric by Gabidulin, Paramonov and Tretjakov and is usually denoted by the GPT system.

Clearly, all of these cryptosystems (except for Alekhnovich’s, which uses a random code) have been originally proposed for a specific code. In the following we will introduce the idea behind the systems as frameworks, thus without considering a specific code.

3.1 McEliece Framework

Although McEliece originally proposed in [193] to use a binary Goppa code as secret code, one usually denotes by the McEliece framework the following. Alice, the constructor of the system, chooses an $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q , which can efficiently decode t errors through the decoding algorithm \mathcal{D} . Instead of publishing a generator matrix \mathbf{G} of this code, which would then reveal to everyone the algebraic structure of \mathcal{C} and especially how to decode, one hides \mathbf{G} through some scrambling: we compute $\mathbf{G}' = \mathbf{S}\mathbf{G}\mathbf{P}$, for some invertible matrix $\mathbf{S} \in \text{GL}_k(\mathbb{F}_q)$ and an $n \times n$ permutation matrix \mathbf{P} . Hoping that the new matrix \mathbf{G}' and the code it generates \mathcal{C}' seem random (although \mathcal{C}' is permutation equivalent to \mathcal{C}), Alice then publishes this disguised matrix \mathbf{G}' and the error correction capacity t of \mathcal{C} .

Bob who wants to send a message $\mathbf{m} \in \mathbb{F}_q^k$ to Alice can then use the public generator matrix \mathbf{G}' to encode his message, i.e., $\mathbf{m}\mathbf{G}'$, and then adds a random error vector $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight up to t to it, i.e., the cipher is given by $\mathbf{c} = \mathbf{m}\mathbf{G}' + \mathbf{e}$.

An eavesdropper, Eve, only knows \mathbf{G}' , t and the cipher \mathbf{c} . In order to break the cryptosystem and to reveal the message \mathbf{m} , she would need to decode \mathcal{C}' , which seems random to her. Thus, she is facing an NP-complete problem and the best known solvers have an exponential cost.

However, Alice can reverse the disguising by computing $\mathbf{c}\mathbf{P}^{-1}$, which results in a codeword of \mathcal{C} added to some error vector of weight up to t . That is

$$\mathbf{c}\mathbf{P}^{-1} = \mathbf{m}\mathbf{S}\mathbf{G} + \mathbf{e}\mathbf{P}^{-1}.$$

Through the decoding algorithm \mathcal{D} Alice gets $\mathbf{m}\mathbf{S}$ and thus by multiplying with \mathbf{S}^{-1} , she recovers the message \mathbf{m} .

Exercise 156. Consider re-encryption: Given the public generator matrix \mathbf{G} . Bob encrypts the message \mathbf{m} getting $\mathbf{c}_1 = \mathbf{m}\mathbf{G} + \mathbf{e}_1$ and later with the same \mathbf{G} the same message \mathbf{m} again getting $\mathbf{c}_2 = \mathbf{m}\mathbf{G} + \mathbf{e}_2$. Is this safe?

Since this is the key part of this survey, we will provide a toy example explained in full detail.

Example 157. Let \mathcal{C} be the $[7, 4]$ binary Hamming code, which can efficiently correct 1 error. We take as generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

We choose $\mathbf{S} \in \text{GL}_4(\mathbb{F}_2)$ to be

$$\mathbf{S} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Table 7: McEliece Framework

ALICE	BOB
KEY GENERATION	
<p>Choose a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k and error correction capacity t. Let \mathbf{G} be a $k \times n$ generator matrix of \mathcal{C}.</p> <p>Choose randomly $\mathbf{S} \in \text{GL}_k(\mathbb{F}_q)$ and an $n \times n$ permutation matrix \mathbf{P}. Compute $\mathbf{G}' = \mathbf{S}\mathbf{G}\mathbf{P}$.</p> <p>The public key is given by $\mathcal{P} = (t, \mathbf{G}')$ and $\mathcal{S} = (\mathbf{G}, \mathbf{S}, \mathbf{P})$</p>	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
<p>Choose a message $\mathbf{m} \in \mathbb{F}_q^k$ and a random error vector $\mathbf{e} \in \mathbb{F}_q^n$ of weight at most t</p> <p>Encrypt the message $\mathbf{c} = \mathbf{m}\mathbf{G}' + \mathbf{e}$</p>	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
<p>Decrypt the cipher, by decoding $\mathbf{c}\mathbf{P}^{-1} = \mathbf{m}\mathbf{S}\mathbf{G} + \mathbf{e}\mathbf{P}^{-1}$ to get $\mathbf{m}\mathbf{S}$, and finally recover the message as $\mathbf{m} = (\mathbf{m}\mathbf{S})\mathbf{S}^{-1}$</p>	

and the permutation matrix \mathbf{P} to be

$$\mathbf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We thus compute

$$\mathbf{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

and publish $(\mathbf{G}', 1)$, since $t = 1$. The message we want to send is $\mathbf{m} = (1, 0, 1, 1) \in \mathbb{F}_2^4$ and thus we compute

$$\mathbf{m}\mathbf{G}' = (0, 1, 0, 1, 0, 1, 0).$$

Now, we choose an error vector $\mathbf{e} \in \mathbb{F}_2^7$ of Hamming weight 1, e.g.,

$$\mathbf{e} = (1, 0, 0, 0, 0, 0, 0).$$

Thus, the cipher is given by

$$\mathbf{c} = (1, 1, 0, 1, 0, 1, 0).$$

The constructor, who possesses \mathbf{P} can compute

$$\mathbf{c}\mathbf{P}^{-1} = \mathbf{c}\mathbf{P}^\top = (1, 1, 1, 1, 0, 0, 0).$$

We can now use the decoding algorithm of Hamming codes to recover $\mathbf{m}\mathbf{S} = (1, 1, 1, 0)$ and by multiplying with

$$\mathbf{S}^{-1} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

we recover the message $\mathbf{m} = (1, 0, 1, 1)$.

In this toy example, an attacker which sees $\mathbf{G}', t, \mathbf{c}$ has two possibilities:

1. recover the message directly,
2. recover the secret key.

The first type of attack could work as follows:

1. We bring \mathbf{G}' into a row-reduced form, that is for $\mathbf{G}' = [\mathbf{A} \mid \mathbf{B}]$ we compute $\mathbf{A}^{-1}\mathbf{G}'$, giving

$$\overline{\mathbf{G}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

With $\overline{\mathbf{G}} = [\text{Id}_4 \mid \mathbf{C}]$ we can also compute the parity-check matrix as $\overline{\mathbf{H}} = [\mathbf{C}^\top \mid \text{Id}_3]$, that is

$$\overline{\mathbf{H}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2. We can now compute the syndrome of \mathbf{c} through $\overline{\mathbf{H}}$, i.e.,

$$\mathbf{s} = \mathbf{c}\overline{\mathbf{H}}^\top = (1, 1, 0).$$

Note that this is also the syndrome of the error vector \mathbf{e} , i.e., $\mathbf{e}\overline{\mathbf{H}}^\top = \mathbf{s}$. Since there is only one entry of \mathbf{e} that is non-zero, we must have that the syndrome \mathbf{s} is equal to the column \mathbf{h}_i where $\mathbf{e}_i \neq 0$. And in fact, $\mathbf{s} = \mathbf{h}_1$, thus we have found

$$\mathbf{e} = (1, 0, 0, 0, 0, 0, 0)$$

and

$$\mathbf{c} - \mathbf{e} = \mathbf{m}\mathbf{G}' = (0, 1, 0, 1, 0, 1, 0).$$

Note that the moment we know the error vector, we can use linear algebra to recover the message. Since this is a toy example, we will also execute this step.

3. Denote by $\overline{\mathbf{m}} = \mathbf{m}\mathbf{A}$, then

$$(0, 1, 0, 1, 0, 1, 0) = \mathbf{m}\mathbf{G}' = \mathbf{m}\mathbf{A}\mathbf{A}^{-1}\mathbf{G}' = \overline{\mathbf{m}}\overline{\mathbf{G}}.$$

Since $\overline{\mathbf{G}} = [\text{Id}_4 \mid \mathbf{C}]$, we have that

$$\overline{\mathbf{m}}\overline{\mathbf{G}} = (\overline{\mathbf{m}}, \overline{\mathbf{m}}\mathbf{C}).$$

Hence, we can directly read off that $\overline{\mathbf{m}} = (0, 1, 0, 1)$ and by multiplying with \mathbf{A}^{-1} , we recover $\mathbf{m} = (1, 0, 1, 1)$.

The second type of attack, namely a key-recovery attack, is in nature more algebraic. Knowing that the secret code is a $[7, 4]$ binary code that can correct one error, the suspicion that the secret code is a Hamming code is natural. If not, one could proceed as follows.

1. We choose a set $I \subset \{1, \dots, n\}$ of size k , which is a possible information set. Let us denote by \mathbf{G}'_I the matrix consisting of the columns of \mathbf{G}' indexed by I .
2. We compute $(\mathbf{G}'_I)^{-1}\mathbf{G}'$ to get an identity matrix in the columns indexed by I .
3. Choose the permutation matrix \mathbf{P}' which brings the identity matrix in the columns indexed by I to the first k positions.

With this, if one chose $I = \{4, 2, 6, 3\}$ (the order matters here only for the permutation matrix) we recover \mathbf{G} and will now finally be able to read off the secret code and thus also know its decoding algorithm. With this, we can compute from \mathbf{G} and \mathbf{G}' the matrices \mathbf{S} and \mathbf{P} .

Although this example for the McEliece framework is clearly using a code that should not be used in practice, it shows in a few easy steps the main ideas of the attacks. For example, the minimum distance of a code should be large enough, since else an easy search for the error vector will reveal the message, and also the public code parameters should not reveal anything on the structure of the secret code, meaning that there should be many codes having such parameters.

These two different kind of attacks aim at solving two different problems the security of the McEliece system is based upon:

1. decoding the erroneous codeword, assuming that the code is random, should be hard,
2. the public code, which is permutation equivalent to the secret code, should not reveal the algebraic structure of the secret code.

Only if both of these points are fulfilled is the security of the cryptosystem guaranteed.

We will see more on this in Section 5.

3.2 Niederreiter Framework

The Niederreiter framework [204] uses the parity-check matrix instead of the generator matrix, resulting in an equivalently secure system [183]. Niederreiter originally proposed to use GRS codes as secret codes, however, we will consider with the Niederreiter framework the more general scheme.

Alice again chooses an $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q which can efficiently decode up to t errors. She then scrambles a parity-check matrix \mathbf{H} of \mathcal{C} by computing $\mathbf{H}' = \mathbf{SHP}$, for some invertible matrix $\mathbf{S} \in \text{GL}_{n-k}(\mathbb{F}_q)$ and an $n \times n$ permutation matrix \mathbf{P} . She publishes the seemingly random parity-check matrix \mathbf{H}' together with the error correction capacity t .

Bob can then encrypt a message $\mathbf{m} \in \mathbb{F}_q^n$ of Hamming weight up to t , simply by computing the syndrome of \mathbf{m} through the parity-check matrix \mathbf{H}' , i.e., the cipher is given by $\mathbf{c} = \mathbf{mH}'^\top$.

While Eve would only have access to \mathbf{H}' , which looks random to her, t and \mathbf{c} , she faces an NP-hard problem and can only apply exponential time algorithms in order to recover \mathbf{m} .

Alice, on the other hand, can recover the message by computing $\mathbf{S}^{-1}\mathbf{c}$, which results in a syndrome of her code \mathcal{C} , which she knows how to decode. That is

$$\mathbf{S}^{-1}\mathbf{c}^\top = \mathbf{HPm}^\top,$$

where \mathbf{Pm}^\top still has Hamming weight up to t . Thus, she recovers \mathbf{Pm}^\top and by multiplication with \mathbf{P}^{-1} , she recovers the message \mathbf{m} .

We provide the same toy example for the Niederreiter framework.

Example 158. This time, we start with a parity-check matrix \mathbf{H} of the $[7, 4]$ binary Hamming code, given by

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

We choose as invertible matrix $\mathbf{S} \in \text{G}_3(\mathbb{F}_2)$ the following

$$\mathbf{S} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

and as permutation matrix we choose

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Table 8: Niederreiter Framework

ALICE	BOB
KEY GENERATION	
Choose a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k that can efficiently correct t errors. Let \mathbf{H} be a $(n-k) \times n$ parity-check matrix of \mathcal{C}	
Choose randomly $\mathbf{S} \in \text{GL}_{n-k}(\mathbb{F}_q)$ and an $n \times n$ permutation matrix \mathbf{P} . Compute $\mathbf{H}' = \mathbf{SHP}$	
The public key is given by $\mathcal{P} = (t, \mathbf{H}')$	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
Choose a message $\mathbf{m} \in \mathbb{F}_q^n$ of weight at most t	
Encrypt the message $\mathbf{c}^\top = \mathbf{H}'\mathbf{m}^\top$	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
Decrypt the cipher by decoding $\mathbf{S}^{-1}\mathbf{c}^\top = \mathbf{HPm}^\top$ to get \mathbf{Pm}^\top , and finally recover the message as $\mathbf{m}^\top = \mathbf{P}^{-1}(\mathbf{Pm}^\top)$	

With this, we compute

$$\mathbf{H}' = \mathbf{SHP} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

The public key is given by \mathbf{H}' and $t = 1$. Assume that we want to send the message $\mathbf{m} = (0, 0, 1, 0, 0, 0, 0) \in \mathbb{F}_2^7$. For this, we compute the cipher as the syndrome of \mathbf{m} through \mathbf{H}' , i.e.,

$$\mathbf{c} = \mathbf{m}(\mathbf{H}')^\top = (1, 1, 0)$$

and send it to the constructor. The constructor which knows \mathbf{S} and \mathbf{P} first computes

$$\mathbf{S}^{-1}\mathbf{c}^\top = \mathbf{HPm}^\top = (0, 1, 0)^\top,$$

and then uses the decoding algorithm of the Hamming code to get

$$\mathbf{mP}^\top = (0, 0, 0, 0, 0, 1, 0).$$

Finally multiplying this with \mathbf{P}^{-1} we get the message $\mathbf{m} = (0, 0, 1, 0, 0, 0, 0)$.

The security is clearly equivalent to that of Example 157, due to the duality of \mathbf{G} and \mathbf{H} and the attacks from Example 157 work here as well.

3.3 Alekhnovich's Cryptosystems

Alekhnovich's cryptosystem [15] marks the first code-based cryptosystem with a security proof, i.e., it relies solely on the decoding problem. This seminal work lays the foundations of modern code-based cryptography, where researchers try to construct code-based cryptosystems with a provable reduction to the problem of decoding a random linear code.

There are two variants to this cryptosystem, both are relying on the following hard problem:

Problem 159. Given a code \mathcal{C} , distinguish a random vector from an erroneous codeword of \mathcal{C} .

Note that variations of these cryptosystem are used in [5, 20]. For the following description of the two variants we rely on the survey [269] and for more details we also refer to [269].

3.3.1 The First Variant

The idea is not to keep the parity-check matrix or generator matrix of the code hidden, but a random error vector. Thus, a random matrix \mathbf{A} is chosen and to this one adds the row $\mathbf{x}\mathbf{A} + \mathbf{e}$, thus an erroneous codeword of the code generated by \mathbf{A} is added resulting in the augmented matrix \mathbf{H} . Let us consider \mathcal{C} to be $\text{Ker}(\mathbf{H})$, that is the code having \mathbf{H} as parity-check matrix. One then publishes \mathbf{G} , a generator matrix of \mathcal{C} .

In this variant one only encrypts a single bit. One either sends as cipher an erroneous codeword of \mathcal{C}^\perp or a random vector, depending if 0 or 1 was encrypted. Finally, using the secret error vector \mathbf{e} , one can compute the standard inner product of the cipher and \mathbf{e} and will recover the message, with some decryption failure.

More in detail, if the cipher was given by $\mathbf{a}\mathbf{G} + \mathbf{e}'$, for a random $\mathbf{a} \in \mathbb{F}_2^{n-k}$ and a random error vector $\mathbf{e}' \in \mathbb{F}_2^n$ of weight t , then

$$\langle \mathbf{e}, \mathbf{a}\mathbf{G} + \mathbf{e}' \rangle = \langle \mathbf{e}, \mathbf{a}\mathbf{G} \rangle + \langle \mathbf{e}, \mathbf{e}' \rangle.$$

Note that $\langle \mathbf{e}, \mathbf{a}\mathbf{G} \rangle = 0$, since $\mathbf{e} \in \mathcal{C}^\perp$ by construction. In addition, since $\text{wt}_H(\mathbf{e}) = \text{wt}_H(\mathbf{e}') = t = o(\sqrt{n})$, we have that $\langle \mathbf{e}, \mathbf{e}' \rangle = 0$ with high probability. If the cipher was given by a random vector $\mathbf{c} \in \mathbb{F}_2^n$ instead, then with probability $1/2$ we get $\langle \mathbf{e}, \mathbf{c} \rangle = 1$.

Thus, there is a decryption failure in the case $m = 1$ of probability $1/2$. In order to get a reliable system one can encrypt the message multiple times. A systematic description of Alekhnovich's First Variant can be found in Table 9.

We give an example of the first variant.

Example 160. Let

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We choose $\mathbf{m} = (0, 1, 0, 1)$, $\mathbf{e} = (1, 0, 0, 0, 0, 0)$ and compute

$$\mathbf{m}\mathbf{A} + \mathbf{e} = (0, 0, 1, 1, 0, 1).$$

Table 9: Alekhnovich First Variant

ALICE	BOB
KEY GENERATION	
<p>Let $t \in o(\sqrt{n})$ and choose a random matrix $\mathbf{A} \in \mathbb{F}_2^{k \times n}$</p> <p>Let $\mathbf{e} \in \mathbb{F}_2^n$ be a random vector of weight t and let $\mathbf{x} \in \mathbb{F}_2^k$ be a random vector</p> <p>Compute $\mathbf{y} = \mathbf{x}\mathbf{A} + \mathbf{e}$ and $\mathbf{H}^\top = (\mathbf{A}^\top, \mathbf{y}^\top)$</p> <p>Let $\mathcal{C} = \ker(\mathbf{H})$ and choose a generator matrix $\mathbf{G} \in \mathbb{F}_2^{(n-k-1) \times n}$ of \mathcal{C}</p> <p>The public key is given by $\mathcal{P} = (\mathbf{G}, t)$ and the secret key is $\mathcal{S} = \mathbf{e}$</p>	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
<p>Choose a message $\mathbf{m} \in \mathbb{F}_2$</p> <p>If $\mathbf{m} = 0$: choose $\mathbf{a} \in \mathbb{F}_2^{n-k-1}$ and $\mathbf{e}' \in \mathbb{F}_2^n$ of weight t at random, send $\mathbf{c} = \mathbf{a}\mathbf{G} + \mathbf{e}'$</p> <p>If $\mathbf{m} = 1$: choose a random vector $\mathbf{c} \in \mathbb{F}_2^n$</p>	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
<p>Decrypt the cipher, by computing $\mathbf{b} = \langle \mathbf{e}, \mathbf{c} \rangle$.</p> <p>If $\mathbf{m} = 0$: $\mathbf{b} = 0$ with high probability</p> <p>If $\mathbf{m} = 1$: $\mathbf{b} = 1$ with probability $1/2$</p>	

If we append this to the matrix \mathbf{A} , we get the matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The dual code C of \mathbf{H} has a generator matrix

$$\mathbf{G} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

We encrypt 0 as

$$\mathbf{c}_0 = (0, 0, 0, 1, 1, 1) + (0, 1, 0, 0, 0, 0) = (0, 1, 0, 1, 1, 1),$$

and 1 as random vector

$$\mathbf{c}_1 = (1, 0, 1, 0, 0, 1).$$

To decrypt the cipher \mathbf{c} , we compute $\langle \mathbf{e}, \mathbf{c} \rangle$. If we receive \mathbf{c}_0 , we compute that $\langle \mathbf{e}, \mathbf{c}_0 \rangle = 0$. If we receive \mathbf{c}_1 , we see that $\langle \mathbf{e}, \mathbf{c}_1 \rangle = 1$.

3.3.2 The Second Variant

In this variant one generalizes the idea of the first variant and construct directly a matrix \mathbf{M} in which every row is an erroneous codeword.

This is achieved by choosing at random $\mathbf{A} \in \mathbb{F}_2^{n/2 \times n}$, $\mathbf{X} \in \mathbb{F}_2^{n \times n/2}$ and $\mathbf{E} \in \mathbb{F}_2^{n \times n}$ having row weight t . Then one computes the matrix $\mathbf{M} = \mathbf{X}\mathbf{A} + \mathbf{E}$.

Let \mathcal{C}_0 be a binary code of length n , that can correct codewords transmitted through a binary symmetric channel (BSC) with transition probability t^2/n . Let us consider

$$\begin{aligned} \varphi : \mathbb{F}_2^n &\rightarrow \mathbb{F}_2^n, \\ \mathbf{x} &\mapsto \mathbf{M}\mathbf{x}. \end{aligned}$$

Define

$$\mathcal{C}_1 = \varphi^{-1}(\mathcal{C}_0) = \{\mathbf{x} \in \mathbb{F}_2^n \mid \varphi(\mathbf{x}) \in \mathcal{C}_0\},$$

$\mathcal{C}_2 = \text{Ker}(\mathbf{A})$ and finally $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$. Let $\mathbf{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of \mathcal{C} . This generator matrix is made public, while the error vectors in \mathbf{E} are kept secret.

To encrypt a message $\mathbf{m} \in \mathbb{F}_2^{k/2}$ we first append a random vector $\mathbf{r} \in \mathbb{F}_2^{k/2}$ to get $\mathbf{x} = (\mathbf{m}, \mathbf{r}) \in \mathbb{F}_2^k$ and then compute

$$\mathbf{c} = \mathbf{x}\mathbf{G} + \mathbf{e},$$

for some random error vector $\mathbf{e} \in \mathbb{F}_2^n$ of weight t .

To decrypt we now compute

$$\begin{aligned} \mathbf{y}^\top &= \mathbf{E}\mathbf{c}^\top = \mathbf{E}(\mathbf{x}\mathbf{G} + \mathbf{e})^\top \\ &= \mathbf{E}(\mathbf{x}\mathbf{G})^\top + \mathbf{E}\mathbf{e}^\top \\ &= \mathbf{X}\mathbf{A}(\mathbf{x}\mathbf{G})^\top + \mathbf{M}(\mathbf{x}\mathbf{G})^\top + \mathbf{E}\mathbf{e}^\top \\ &= \mathbf{M}(\mathbf{x}\mathbf{G})^\top + \mathbf{E}\mathbf{e}^\top, \end{aligned}$$

where we have used that $\mathbf{A}\mathbf{a}^\top = 0$ for all $\mathbf{a} \in \mathcal{C}$, in particular also for $\mathbf{x}\mathbf{G}$. Note that $\mathbf{z}^\top = \mathbf{M}(\mathbf{x}\mathbf{G})^\top \in \mathcal{C}_0$, since $\mathcal{C} \subseteq \mathcal{C}_1$ and $\varphi(\mathcal{C}_1) = \mathcal{C}_0$. Finally, every row \mathbf{e}_i of \mathbf{E} has weight t and thus, $\langle \mathbf{e}_i, \mathbf{e} \rangle = 1$ with probability at most t^2/n . Thus, the decoding algorithm of \mathcal{C}_0 on \mathbf{y} gives \mathbf{z} with high probability. Finally, we can solve the linear system

$$\mathbf{x}\mathbf{G} = \varphi^{-1}(\mathbf{z})$$

to get \mathbf{x} and the first $k/2$ bits reveal the message \mathbf{m} .

Table 10: Alekhovich Second Variant

ALICE	BOB
KEY GENERATION	
<p>Choose random matrices $\mathbf{A} \in \mathbb{F}_2^{n/2 \times n}$, $\mathbf{X} \in \mathbb{F}_2^{n \times n/2}$ and $\mathbf{E} \in \mathbb{F}_2^{n \times n}$ of row weight t</p> <p>Set $\mathbf{M} = \mathbf{XA} + \mathbf{E} \in \text{GL}_n(\mathbb{F}_2)$</p> <p>Let \mathcal{C}_0 be a binary code of length n that can efficiently correct code-words transmitted through a BSC of transition probability t^2/n</p> <p>Let φ be the map $\mathbf{x} \mapsto \mathbf{Mx}$</p> <p>Let $\mathcal{C} = \varphi^{-1}(\mathcal{C}_0) \cap \text{Ker}(\mathbf{A})$</p> <p>Let $\mathbf{G} \in \mathbb{F}_2^{k \times n}$ be a generator matrix of \mathcal{C}</p> <p>The public key is given by $\mathcal{P} = (\mathbf{G}, t)$ and $\mathcal{S} = \mathbf{E}$</p>	
$\xrightarrow{\mathcal{P}}$	
ENCRIPTION	
<p>Choose a message $\mathbf{m} \in \mathbb{F}_2^{k/2}$ and choose randomly $\mathbf{r} \in \mathbb{F}_2^{k/2}$ and $\mathbf{e} \in \mathbb{F}_2^n$ of weight t</p> <p>Compute $\mathbf{x} = (\mathbf{m}, \mathbf{r}) \in \mathbb{F}_2^k$ and $\mathbf{c} = \mathbf{xG} + \mathbf{e}$</p>	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
<p>Decrypt the cipher, by computing $\mathbf{y}^\top = \mathbf{Ec}^\top = \mathbf{z}^\top + \mathbf{Ee}^\top$</p> <p>and use the decoding algorithm of \mathcal{C}_0 on \mathbf{y} to get \mathbf{z}</p> <p>Recover \mathbf{x} from the linear system $\mathbf{xG} = \varphi^{-1}(\mathbf{z})$ and thus \mathbf{m}</p>	

3.4 Quasi-Cyclic Scheme

The quasi-cyclic scheme is inspired by the scheme of Alekhovich, introduced in [9] and used in [5]. Similarly to Alekhovich's schemes, it is a probabilistic approach to encryption schemes and does not hide the initial code, which needs to be efficiently decodable. The message gets encrypted as codeword to which an error, too large to decode, gets added. With the knowledge of the private key parts of this error can be cancelled out resulting (with high probability) in a vector which can be decoded to recover the message.

We present the scheme in the Hamming metric, but note that the scheme can also be adapted to the rank metric.

Let n be a positive integer, q be a prime power and $\mathcal{R} = \mathbb{F}_q[x]/(x^n - 1)$. Recall from Section 2 that we identify vector $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ with the polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathcal{R}$ and vice versa.

The quasi-cyclic framework uses two types of codes:

1. An $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q , which can efficiently decode δ errors. A generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ is made public.
2. A random quasi-cyclic $[2n, n]$ code presented through a parity-check matrix

$$\mathbf{H} = \begin{pmatrix} \text{Id}_n & | & \text{rot}(\mathbf{h}) \end{pmatrix},$$

which does not require to be efficiently decodable and is also made public.

Recall that vector multiplication of any vector \mathbf{v} and \mathbf{h} is given by $\mathbf{v}\text{rot}(\mathbf{h})$, as this corresponds to the polynomial multiplication $v(x)h(x) \in \mathcal{R}$.

Let w , w_r and w_e be positive integers all in the range of $\sqrt{n}/2$. These are publicly known parameters.

The cryptosystem then proceeds as follows. Alice chooses a random $h \in \mathbb{F}_q^n$ and an $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q , that can efficiently correct t errors and chooses a generator matrix \mathbf{G} of \mathcal{C} .

Alice then also chooses two elements $\mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$, corresponding to the vector \mathbf{y}, \mathbf{z} both of Hamming weight w .

She publishes the generator matrix \mathbf{G} , the random element \mathbf{h} and $\mathbf{s} = \mathbf{y} + \mathbf{h}\mathbf{z}$, while \mathbf{y} and \mathbf{z} are kept secret and can clearly not be recovered from \mathbf{s} and \mathbf{h} . In fact, we can write

$$\mathbf{s} = (\mathbf{y}, \mathbf{z}) \begin{pmatrix} \text{Id}_n \\ \text{rot}(\mathbf{h}) \end{pmatrix},$$

thus $\mathbf{H} = (\text{Id}_n, \text{rot}(\mathbf{h}))^\top$ acts as quasi-cyclic parity-check matrix and (\mathbf{y}, \mathbf{z}) as unknown error vector.

Bob, who wants to send a message $\mathbf{m} \in \mathbb{F}_p^k$ to Alice, can choose $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight w_e and two elements $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{F}_q^n$, both of Hamming weight w_r . He then computes $\mathbf{u} = \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2$ and

$$\mathbf{v} = \mathbf{m}\mathbf{G} + \mathbf{s}\mathbf{r}_2 + \mathbf{e}.$$

The cipher is then given by $\mathbf{c} = (\mathbf{u}, \mathbf{v})$.

The message \mathbf{m} is thus encoded through the public \mathbf{G} and an error vector $\mathbf{s}\mathbf{r}_2 + \mathbf{e}$ is added, where both \mathbf{r}_2 and \mathbf{e} were randomly chosen by Bob. The only control Alice has on the error vector is in \mathbf{s} . This knowledge and also the additional information of Bob on \mathbf{r}_2 provided through the vector \mathbf{u} will allow Alice to decrypt the cipher.

In fact, Alice can use the decoding algorithm of \mathcal{C} on $\mathbf{v} - \mathbf{u}\mathbf{z}$, since

$$\begin{aligned} \mathbf{v} - \mathbf{u}\mathbf{z} &= \mathbf{m}\mathbf{G} + \mathbf{s}\mathbf{r}_2 + \mathbf{e} - (\mathbf{r}_1 + \mathbf{h}\mathbf{r}_2)\mathbf{z} \\ &= \mathbf{m}\mathbf{G} + (\mathbf{y} + \mathbf{h}\mathbf{z})\mathbf{r}_2 + \mathbf{e} - \mathbf{r}_1\mathbf{z} - \mathbf{h}\mathbf{r}_2\mathbf{z} \\ &= \mathbf{m}\mathbf{G} + (\mathbf{y}\mathbf{r}_2 - \mathbf{r}_1\mathbf{z} + \mathbf{e}). \end{aligned}$$

It follows that the decryption succeeds if $\text{wt}_H(\mathbf{y}\mathbf{r}_2 - \mathbf{r}_1\mathbf{z} + \mathbf{e}) \leq t$. Note that parameter sets should be chosen such that this happens with high probability, but clearly the framework does have a *decoding failure rate* (DFR).

Table 11: Quasi-Cyclic Scheme

ALICE	BOB
KEY GENERATION	
Choose an $[n, k]$ linear code \mathcal{C} over \mathbb{F}_q , which can efficiently decode t errors with generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ and choose $\mathbf{h} \in \mathbb{F}_q^n$ Choose $\mathbf{y}, \mathbf{z} \in \mathbb{F}_q^n$ of weight $\text{wt}_H(\mathbf{y}) = \text{wt}_H(\mathbf{z}) = w$, compute $\mathbf{s} = \mathbf{y} + \mathbf{h}\mathbf{z}$ The public key is $\mathcal{P} = (\mathbf{G}, \mathbf{h}, \mathbf{s}, w_e, w_r)$ and the secret key is $\mathcal{S} = (\mathbf{y}, \mathbf{z})$	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
Choose a message $\mathbf{m} \in \mathbb{F}_q^k$ Choose $\mathbf{e} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{e}) = w_e$ Choose $\mathbf{r}_1, \mathbf{r}_2 \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{r}_1) = \text{wt}_H(\mathbf{r}_2) = w_r$ Compute $\mathbf{u} = \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2$ Compute $\mathbf{v} = \mathbf{m}\mathbf{G} + \mathbf{s}\mathbf{r}_2 + \mathbf{e}$ The cipher is $\mathbf{c} = (\mathbf{u}, \mathbf{v})$	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
Compute $\mathbf{c}' = \mathbf{v} - \mathbf{u}\mathbf{z}$ and use the decoding algorithm of \mathcal{C} to recover \mathbf{m}	

Remark 161. The reason why we can make the generator matrix of the efficiently decodable code public, lies in the random choice of \mathbf{h} , which determines the parity-check matrix \mathbf{H} and in the fact that the error added to the codeword has a weight larger than the error correction capacity of the public code.

In fact, \mathbf{u} and \mathbf{s} are two syndromes through \mathbf{H} of a vector with given weight, as

$$\mathbf{u} = (\mathbf{r}_1, \mathbf{r}_2)\mathbf{H}^\top$$

and $\mathbf{s} = (\mathbf{y}, \mathbf{z})\mathbf{H}^\top$. In order to recover $(\mathbf{r}_1, \mathbf{r}_2)$ or (\mathbf{y}, \mathbf{z}) , an attacker would need to solve the NP-hard syndrome decoding problem. In addition, since $\text{wt}_H(\mathbf{s}\mathbf{r}_2 + \mathbf{e}) > t$ even with the knowledge of \mathbf{G} and \mathbf{v} an attacker can not uniquely determine the message \mathbf{m} .

Since the algebraic code, which is efficiently decodable, is publicly known, the security of this framework is different to that of the McEliece framework and the Niederreiter framework, as it does not rely on the indistinguishability of the code.

Remark 162. However, we want to stress the fact, that the SDP is NP-hard for a completely random code. The code with the double circulant parity-check matrix \mathbf{H} is in fact not completely random, and thus the question arises, if also this new problem lies in the complexity class of NP-hard problems.

Example 163. We choose $R = \mathbb{F}_2[x]/(x^7 + 1)$ and as code the binary repetition code of length 7, which can correct up to 3 errors. The generator matrix \mathbf{G} is given by

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and codewords with more ones than zeroes are decoded to $(1, 1, 1, 1, 1, 1, 1)$, everything else to $(0, 0, 0, 0, 0, 0, 0)$. Further, we choose

$$h(x) = 1 + x + x^2 \in \mathcal{R},$$

or equivalently $\mathbf{h} = (1, 1, 1, 0, 0, 0, 0)$ and $w = w_r = w_e = 1$. We pick $y(x) = 1$, $z(x) = x^3$, both in \mathcal{R} of weight $w = 1$, or equivalently $\mathbf{y} = (1, 0, 0, 0, 0, 0, 0)$, $\mathbf{z} = (0, 0, 0, 1, 0, 0, 0)$ and compute

$$s(x) = y(x) + h(x)z(x) = 1 + x^3 + x^4 + x^5.$$

Equivalently one can compute

$$\mathbf{s} = \mathbf{y} + \mathbf{z} \text{rot}(\mathbf{h}) = (1, 0, 0, 1, 1, 1, 0).$$

The public key is then given by

$$\mathcal{P} = (\mathbf{G}, \mathbf{h}, \mathbf{s}, w_e, w_r),$$

the secret key is the pair

$$\mathcal{S} = (\mathbf{y}, \mathbf{z}).$$

For this example, the message is $\mathbf{m} = (1) \in \mathbb{F}_2^1$. We also pick $e(x) = x \in \mathcal{R}$, that is $\mathbf{e} = (0, 1, 0, 0, 0, 0, 0)$ of weight $w_e = 1$ and $r_1(x) = r_2(x) = x^2$ in \mathcal{R} , that is $\mathbf{r}_1 = \mathbf{r}_2 = (0, 0, 1, 0, 0, 0, 0)$ of weight $w_r = 1$. We can then compute

$$u(x) = r_1(x) + h(x)r_2(x) = x^3 + x^4,$$

or equivalently

$$\mathbf{u} = \mathbf{r}_1 + \mathbf{r}_2 \text{rot}(\mathbf{h}),$$

hence $\mathbf{u} = (0, 0, 0, 1, 1, 0, 0)$, and since $s(x)r_2(x) = 1 + x^2 + x^5 + x^6$ of weight $5 > t$ we get

$$\begin{aligned} \mathbf{v} &= \mathbf{m}\mathbf{G} + \mathbf{s}\mathbf{r}_2 + \mathbf{e} = (1, 1, 1, 1, 1, 1, 1) + (1, 0, 1, 0, 0, 1, 1) + (0, 1, 0, 0, 0, 0, 0) \\ &= (0, 0, 0, 1, 1, 0, 0). \end{aligned}$$

We can then send the cipher

$$\mathbf{c} = (\mathbf{u}, \mathbf{v}) = ((0, 0, 0, 1, 1, 0, 0), (0, 0, 0, 1, 1, 0, 0)).$$

To decrypt the cipher, we compute with the knowledge of the secret key $\mathcal{S} = (\mathbf{y}, \mathbf{z}) = (1, x^3)$ that $u(x)z(x) = 1 + x^6$ and compute

$$\begin{aligned} \mathbf{v} - \mathbf{u}\mathbf{z} &= (0, 0, 0, 1, 1, 0, 0) - (1, 0, 0, 0, 0, 0, 1) \\ &= (1, 0, 0, 1, 1, 0, 1), \end{aligned}$$

which gets decoded to to the codeword $(1, 1, 1, 1, 1, 1, 1)$, from which we recover the message $\mathbf{m} = (1)$.

Exercise 164. Repeat this example with the fixed public parameters $\mathbf{G} = (1, 1, 1, 1, 1, 1, 1)$, $h(x) = 1 + x + x^2$, $s(x) = 1 + x^3 + x^4 + x^5$, $w_e = w_r = 1$ and the secret key $\mathcal{S} = (1, x^3)$, but now Bob chooses $e(x) = x^4$, $r_1(x) = 1$, $r_2(x) = x$. Is the decryption successful in this case?

3.5 Augot-Finiasz Cryptosystem

In its original version the Augot-Finiasz (AF) cryptosystem uses polynomial reconstructions, for this survey, however, we translate it into an easier formulation.

Similar to the quasi-cyclic framework, one can choose a code \mathcal{C} which can efficiently decode t errors and can make it public. The system does not rely on any hiding of the structured code. The idea of the AF and the FL system is publish a structured code $\mathcal{C} = \langle \mathbf{G} \rangle$ which can correct w erasures and t errors, usually this means that $d > 2t + w$. One then also publishes a corrupted codeword $\mathbf{y} = \mathbf{m}'\mathbf{G} + \mathbf{e}'$, where the error vector \mathbf{e}' has weight w , but keeps the support of \mathbf{e}' secret. Without the knowledge of the support, and as long as $w > \lfloor (d-1)/2 \rfloor$, an attacker cannot recover \mathbf{m}' or equivalently \mathbf{e}' .

To encrypt a message \mathbf{m} , one chooses at random a vector \mathbf{e} of weight t , a random $\alpha \in \mathbb{F}_q$, such that

$$\text{supp}(\alpha\mathbf{e}') = \text{supp}(\mathbf{e}')$$

and computes the cipher as

$$\mathbf{c} = \mathbf{m}\mathbf{G} + \alpha\mathbf{y} + \mathbf{e}.$$

Clearly, the cipher is still a corrupted codeword of \mathcal{C} , where the error vector is

$$\tilde{\mathbf{e}} = \alpha\mathbf{e}' + \mathbf{e}.$$

If \mathbf{e}' and \mathbf{e} are chosen at random then $\text{wt}_H(\tilde{\mathbf{e}}) \geq w - t$. Thus, as long as $w - t > \frac{d-1}{2}$ an attacker can still not decode the cipher without knowing the secret error support.

On the other hand, the constructor of the scheme knows $\text{supp}(\mathbf{e})$ and can use an erasure decoder to get rid off $\text{supp}(\mathbf{e}')$. Being left with at most t errors, the constructor of the system can use the error-decoder of the public code and compute the $\mathbf{m}' + \alpha\mathbf{m}$. Finally, knowing \mathbf{m}' and ensuring that α is visible in the vector $\alpha\mathbf{m}$, one recovers the message \mathbf{m} .

The decryption works, as

$$\mathbf{c} = (\mathbf{m} + \alpha(1, \mathbf{m}'))\mathbf{G} + \alpha\mathbf{e}' + \mathbf{e}$$

and $\alpha\mathbf{e}'$ has support in S . Thus,

$$\mathbf{c}_{SC} = (\mathbf{m} + \alpha(1, \mathbf{m}'))\mathbf{G} + \mathbf{e},$$

and since $\text{wt}_H(\mathbf{e}) \leq t$, we can decode the public code $\langle \mathbf{G} \rangle$ and recover the message $\mathbf{m} + \alpha(1, \mathbf{m}')$. Although, we do not know α , we have chosen the message of \mathbf{y} such that we can read α of the first entry, namely $(1, \mathbf{m}')$. Thus, we can remove $\alpha(1, \mathbf{m}')$ from the recovered message and recover \mathbf{m} .

Example 165. Let us give a toy example also for the AF system. Let us consider $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$, where $\alpha^4 = \alpha + 1$ and the Reed-Solomon code generated by

$$\mathbf{G} = \begin{pmatrix} 1 & \alpha & \alpha + 1 & \alpha^2 & \alpha^2 + 1 & \alpha^3 & \alpha^3 + \alpha \\ 1 & \alpha^2 & \alpha^2 + 1 & \alpha + 1 & \alpha & \alpha^3 + \alpha^2 & \alpha^3 \end{pmatrix}.$$

This code has minimum distance $d = n - k + 1 = 6$ and can thus correct 1 error and 3 erasures. We choose the secret error support $S = \{1, 2, 4\}$ and the error vector $\mathbf{e}' = (1, \alpha, 0, \alpha^2, 0, 0, 0)$. For the message $\mathbf{m}' = (1, 1)$ we get

$$\mathbf{y} = (1, 1)\mathbf{G} + \mathbf{e}' = (1, \alpha^2, \alpha^2 + \alpha, \alpha + 1, \alpha^2 + \alpha + 1, \alpha^2, \alpha).$$

Table 12: AF Cryptosystem

ALICE	BOB
KEY GENERATION	
Choose a generator matrix $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ which can correct t errors and w erasures	
Choose $\mathbf{e}' \in \mathbb{F}_q^n$ of weight w having support in S	
Choose $(1, \mathbf{m}') \in \mathbb{F}_q^k$	
Compute $\mathbf{y} = (1, \mathbf{m}')\mathbf{G} + \mathbf{e}'$	
The public key is $\mathcal{P} = (\mathbf{G}, \mathbf{y}, t)$ and the secret key is $\mathcal{S} = (\mathbf{e}')$	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
Choose $\mathbf{e} \in \mathbb{F}_q^n$ with $wt_H(\mathbf{e}) \leq t$	
Choose $\alpha \in \mathbb{F}_q$	
Encrypt $\mathbf{m} \in \mathbb{F}_q^k$ as $\mathbf{c} = \mathbf{m}\mathbf{G} + \alpha\mathbf{y} + \mathbf{e}$	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
Puncture \mathbf{c} in the positions indexed by S	
Decode \mathbf{c}_{SC} and recover $\alpha(1, \mathbf{m}') + \mathbf{m}$ and thus α as well as \mathbf{m} .	

Both \mathbf{G} and \mathbf{y} are made public. Bob wants to send the message $(0, \alpha^2)$ to Alice and chooses the scrambling $\alpha + 1$ and the error vector $\mathbf{e} = (0, 0, \alpha, 0, 0, 0, 0)$. The cipher is then given by

$$\begin{aligned} \mathbf{c} &= (0, \alpha^2)\mathbf{G} + (\alpha + 1)\mathbf{y} + \mathbf{e} \\ &= (\alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^3 + 1, 1, \alpha^3 + 1, 0). \end{aligned}$$

To decrypt, Alice first punctures in the secret positions $\{1, 2, 4\}$, thus only considering

$$\mathbf{c}_{SC} = (\alpha^3 + \alpha^2 + \alpha + 1, 1, \alpha^3 + 1, 0)$$

and decodes using the punctured Reed-Solomon code

$$\mathbf{G}_{SC} = \begin{pmatrix} \alpha + 1 & \alpha^2 + 1 & \alpha^3 & \alpha^3 + \alpha \\ \alpha^2 + 1 & \alpha & \alpha^3 + \alpha^2 & \alpha^3 \end{pmatrix},$$

getting the message $(\alpha + 1, \alpha^2 + \alpha + 1)$ and the error vector $(\alpha, 0, 0, 0)$. Due to the construction of the two messages, namely the first position of \mathbf{m} is zero and the first position of \mathbf{m}' is one, Alice can read of the first position the scrambling being $\alpha + 1$ and thus recovers the message

$$\mathbf{m} = (0, \alpha^2) = (1 + \alpha, \alpha^2 + \alpha + 1) - (\alpha + 1, \alpha + 1).$$

Exercise 166. 1. An attacker can guess $\alpha \in \mathbb{F}_q$ and attack the AF system. What is the security level of the above example?

2. Can we also choose different scramblings for \mathbf{y} ?

3. Repeat the example for Gabidulin codes and the rank metric.

The only requirement for the code \mathcal{C} is thus, that the punctured code can still efficiently decode.

The original system uses GRS codes, as a punctured GRS code is still a GRS code, and has been attacked in [97].

Clearly, this framework is independent of the metric and hence, one could also employ the rank metric. In fact, the rank-metric analog of the AF system has been proposed by Faure and Loidreau [119], relying the security on the hardness of reconstructing p -polynomials. Their original system proposes the use of Gabidulin codes and has been subject to algebraic attacks [129].

Many repair attempts [259, 224, 223, 176] have been made, unfortunately all have been broken in [78]. The idea of the attacks is to use list decoding of GRS codes, respectively of Gabidulin codes.

3.6 GPT Cryptosystem

The *Gabidulin-Paramonov-Tretjakov* (GPT) cryptosystem was introduced in [126] and is based on rank-metric codes. As usual, we pick an \mathbb{F}_q -basis of \mathbb{F}_{q^m} and use this to identify elements of \mathbb{F}_{q^m} with vectors in \mathbb{F}_q^m . The system we present is not following the original proposal, which was broken [209], but an adapted formulation, and as before we present the system as a framework, i.e., without choosing a family of codes for the secret code.

The GPT system proceeds as follows. Alice chooses an $[n, k]$ linear rank-metric code \mathcal{C} over \mathbb{F}_{q^m} with error correction capacity t and generator matrix \mathbf{G} . For some positive integer λ , she then chooses $\mathbf{S} \in \text{GL}_k(\mathbb{F}_{q^m})$, $\mathbf{P} \in \text{GL}_{n+\lambda}(\mathbb{F}_q)$ and $\mathbf{X} \in \mathbb{F}_{q^m}^{k \times \lambda}$ of rank $s \leq \lambda$. She publishes the scrambled matrix $\mathbf{G}' = \mathbf{S}[\mathbf{X} \mid \mathbf{G}]\mathbf{P}$ and the target weight t .

Bob can then encrypt his message $\mathbf{m} \in \mathbb{F}_{q^m}^k$, by computing

$$\mathbf{c} = \mathbf{m}\mathbf{G}' + \mathbf{e},$$

for some randomly chosen error vector $\mathbf{e} \in \mathbb{F}_{q^m}^{n+\lambda}$ with $\text{wt}_R(\mathbf{e}) = t$.

To decrypt, Alice can compute

$$\mathbf{c}\mathbf{P}^{-1} = \mathbf{m}\mathbf{S}[\mathbf{X} \mid \mathbf{G}] + \mathbf{e}\mathbf{P}^{-1}.$$

Since $\text{wt}_R(\mathbf{e}\mathbf{P}^{-1}) = t$, she can apply the decoding algorithm of the code \mathcal{C} to the last n positions of $\mathbf{c}\mathbf{P}^{-1}$ to recover $\mathbf{m}\mathbf{S}$ and thus also \mathbf{m} .

A systematic description of the GPT system can be found in Table 13.

This framework is closely related to the McEliece framework, as the algebraic code which can be efficiently decoded has to be kept secret and the matrix \mathbf{P} acts as an isometry. In fact, while for the Hamming metric \mathbf{P} is chosen a permutation matrix, which fixes the Hamming weight of a vector, in the rank metric we choose \mathbf{P} to be a full rank matrix over \mathbb{F}_q , which thus fixes the rank weight of a vector over \mathbb{F}_{q^m} .

Exercise 167. Establish the Niederreiter version of the GPT system using the parity-check matrix.

Table 13: GPT Cryptosystem

ALICE	BOB
KEY GENERATION	
<p>Choose a generator matrix $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$ of a rank-metric code of rank distance $d = 2t + 1$ and a positive integer λ</p> <p>Choose $\mathbf{S} \in \text{GL}_k(\mathbb{F}_{q^m})$, $\mathbf{P} \in \text{GL}_{n+\lambda}(\mathbb{F}_q)$</p> <p>Choose a matrix $\mathbf{X} \in \mathbb{F}_{q^m}^{k \times \lambda}$ of rank $s \leq \lambda$ and compute $\mathbf{G}' = \mathbf{S}[\mathbf{X} \mid \mathbf{G}]\mathbf{P}$.</p> <p>The public key is $\mathcal{P} = (\mathbf{G}', t)$ and the secret key is $\mathcal{S} = (\mathbf{G}, \mathbf{S}, \mathbf{X}, \mathbf{P})$</p>	
$\xrightarrow{\mathcal{P}}$	
ENCRYPTION	
<p>Choose $\mathbf{e} \in \mathbb{F}_{q^m}^{n+\lambda}$ with $wt_R(\mathbf{e}) \leq t$</p> <p>Encrypt $\mathbf{m} \in \mathbb{F}_{q^m}^k$ as $\mathbf{c} = \mathbf{m}\mathbf{G}' + \mathbf{e}$</p>	
$\xleftarrow{\mathbf{c}}$	
DECRYPTION	
<p>Compute $\mathbf{c}' = \mathbf{c}\mathbf{P}^{-1}$ and apply the decoding algorithm to the last n positions to recover $\mathbf{m}' = \mathbf{m}\mathbf{S}$</p> <p>Compute $\mathbf{m} = \mathbf{m}'\mathbf{S}^{-1}$</p>	

Example 168. We give an example for $n = 4$, $m = 5$, $k = 2$ and $s = \lambda = 1$. We identify $\mathbb{F}_{32} = \mathbb{F}_2[\alpha]$ with $\alpha^5 = \alpha^2 + 1$ and consider the Gabidulin code with generator matrix

$$\mathbf{G} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^3 + \alpha \end{pmatrix},$$

which can correct up to 1 error. We further need a $\mathbf{S} \in \text{GL}_2(\mathbb{F}_{32})$ and a $\mathbf{P} \in \text{GL}_5(\mathbb{F}_2)$ and \mathbf{X} of rank $s \leq \lambda = 1$, so we take

$$\mathbf{S} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix},$$

and for simplicity

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

and

$$\mathbf{X} = \begin{pmatrix} 1 \\ \alpha^2 + 1 \end{pmatrix}$$

We compute that

$$\mathbf{G}' = \mathbf{S}[\mathbf{X} \mid \mathbf{G}]\mathbf{P} = \begin{pmatrix} \alpha + 1 & \alpha^3 + \alpha & \alpha^3 + \alpha + 1 & \alpha^4 + \alpha^3 + \alpha^2 & 1 \\ 1 & \alpha^2 & \alpha^2 + 1 & \alpha^3 + \alpha & \alpha^4 \end{pmatrix}.$$

The public key is the pair

$$\mathcal{P} = (\mathbf{G}', 1),$$

the secret key is

$$\mathcal{P} = (\mathbf{G}, \mathbf{S}, \mathbf{X}, \mathbf{P}).$$

We want to encrypt the message

$$\mathbf{m} = (\alpha + 1, \alpha^2 + 1).$$

We choose the error vector

$$\mathbf{e} = (\alpha^3 + 1, 0, \alpha^3 + 1, \alpha^3 + 1, 0),$$

and compute

$$\mathbf{c} = \mathbf{m}\mathbf{G}' + \mathbf{e} = (\alpha^3 + 1, \alpha^3 + \alpha, \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^4 + \alpha^3 + 1).$$

To decrypt \mathbf{c} , we compute

$$\mathbf{c}' = \mathbf{c}\mathbf{P}^{-1} = (\alpha^2 + 1, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^4 + \alpha^3 + 1, \alpha^3 + \alpha^2 + \alpha + 1),$$

and use the decoding algorithm of Gabidulin codes to get

$$\mathbf{m}\mathbf{S} = (\alpha + 1, \alpha + 1),$$

and by multiplying with

$$\mathbf{S}^{-1} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

we recover \mathbf{m} .

4 Code-based Signature Schemes

We give two approaches of building a code-based signature, one is following the hash-and-sign approach [137] of the CFS scheme [98], which can also be adapted to the rank metric and the second one is through code-based ZK protocols, which can be turned into signature schemes via the Fiat-Shamir transform.

We later discuss their benefits and limitations, but in summary, hash-and-sign schemes often suffer from large public keys and distinguishing attacks, while signature schemes from ZK protocols suffer from large signature sizes. In Section 7.2 we will then present the novel submission to the additional standardization process of NIST and the respective solutions to these drawbacks.

4.1 Hash-and-Sign

Hash-and-sign schemes follow directly the usual approach of transforming a public-key encryption scheme into a signature scheme.

In fact, a public key encryption scheme relies on a trapdoor function f , which is easy to compute and hard to invert. For the public key encryption scheme one applies f on a message m and gets the cipher $c = f(m)$. In order to recover the message, an attacker has to invert f , which is mathematically a hard problem. However, the constructor with the secret key has access to f^{-1} .

Similarly, in a signature scheme, one can use the same trapdoor function f , or equivalently the hard problem of computing f^{-1} . However, only the signer should have access to the secret key and be able to sign in her name, thus, upon a message m the signer computes the signature $\sigma = f^{-1}(m)$ and everyone can verify the signature as $f(\sigma) = m$. For an impersonator, however, to find a valid signature for a message is difficult.

We present the first such code-based hash-and-sign scheme, CFS [98], and its rank-metric counterpart RankSign [27].

4.1.1 CFS Scheme

We present the CFS scheme as framework in Table 14.

In the CFS scheme, one starts with a message \mathbf{m} to sign, and hopes that the hash of this message is the syndrome of a low weight vector, i.e., $\text{Hash}(\mathbf{m}) = \mathbf{e}\mathbf{H}^\top$ for $\text{wt}_H(\mathbf{e}) \leq t$.

However, not many vectors are syndromes of low weight vectors.

Exercise 169. Show that in order for any vector to be a syndrome of a vector of weight up to $(d-1)/2$, we require a perfect code.

Since $\text{Hash}(\mathbf{m})$ is very likely not a syndrome of a vector of weight up to t , one introduces a counter i . That is, one checks whether $\text{Hash}(\mathbf{m}, i) = \mathbf{e}\mathbf{H}^\top$ for some \mathbf{e} of weight up to t , and if this is not the case one chooses a different i .

For certain codes, this requires many iterations, which makes the signing process slow.

Thus, the authors of [98] propose the use of the only family of codes, which is suitable for such an approach, namely high rate Goppa codes. In fact, high rate Goppa codes provide the existence of such error vectors for a non-negligible proportion of syndromes.

Unfortunately, the use of high rate Goppa codes is not safe, due to the distinguisher in [118]. Note that this distinguisher does not break the CFS scheme in general, as it only proves

that one of the two problems to which the security of the CFS scheme reduces can be solved in polynomial time.

In the key generation process, one chooses a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ of a binary code that can efficiently correct t errors. One then hides the parity-check matrix as in the Niederreiter framework, by choosing an $n \times n$ permutation matrix \mathbf{P} and computing $\mathbf{H}' = \mathbf{HP}$. The public key is then given by $\mathcal{P} = (\mathbf{H}', t)$ and the secret key by $\mathcal{S} = (\mathbf{H}, \mathbf{P})$.

In the signing process, given a message \mathbf{m} , one first chooses randomly i and uses the decoding algorithm of \mathcal{C} to find \mathbf{e} , such that $\text{wt}_H(\mathbf{e}) \leq t$ and

$$\mathbf{eH}^\top = \text{Hash}(\mathbf{m}, i),$$

if possible. The signature is then given by $\sigma = (i, \mathbf{eP})$.

In the verification, the verifier checks that $\text{wt}_H(\mathbf{eP}) \leq t$ and if

$$\mathbf{ePH}'^\top = \text{Hash}(\mathbf{m}, i).$$

Recall that **Hash** is a publicly known hash function.

Table 14: CFS

PROVER	VERIFIER
KEY GENERATION	
Choose a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ of \mathcal{C} , with error correction capacity t	
Choose an $n \times n$ permutation matrix \mathbf{P}	
Compute $\mathbf{H}' = \mathbf{HP}$. The public key is then given by $\mathcal{P} = (\mathbf{H}', t)$	
and the secret key by $\mathcal{S} = (\mathbf{H}, \mathbf{P})$	
$\xrightarrow{\mathcal{P}}$	
SIGNING	
Given a message \mathbf{m} , choose random i	
Use the decoding algorithm of \mathcal{C} to find \mathbf{e} , with $\text{wt}_H(\mathbf{e}) \leq t$ and $\mathbf{eH}^\top = \text{Hash}(\mathbf{m}, i)$	
Sign as $\sigma = (i, \mathbf{eP})$	
$\xrightarrow{m, s}$	
VERIFICATION	
Check if $\text{wt}_H(\mathbf{eP}) \leq t$ and if $\mathbf{ePH}'^\top = \text{Hash}(\mathbf{m}, i)$.	

Exercise 170. Show that $\mathbf{ePH}'^\top = \text{Hash}(\mathbf{m}, i)$.

Remark 171. The signing time is inversely related to the proportion of vectors, which are syndromes of error vectors of weight $t \leq \frac{d-1}{2}$ and this proportion scales badly with the error correction capacity of the code.

The benefits of the hash-and-sign approach is that the signature is a single vector and thus quite small.

The public key on the other hand, is, as in the McEliece framework, a scrambled secret parity-check matrix, and thus of size $(n - k)k$ bits.

Additionally, the schemes can be vulnerable to distinguishers, i.e., an attacker might retrieve the secret code, as seen in [98].

Example 172. Let us consider also here a small toy example. Let $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ and $\alpha^3 = \alpha + 1$.

Let us consider the Goppa polynomial

$$g(x) = x^2 + x + 1$$

and the evaluation points

$$1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + \alpha, \alpha^2 + 1, \alpha^2 + \alpha + 1.$$

We can compute

$$\begin{aligned} g(1)^{-1} &= 1, \\ g(\alpha)^{-1} &= g(\alpha + 1)^{-1} = \alpha^2, \\ g(\alpha^2)^{-1} &= g(\alpha^2 + 1)^{-1} = \alpha^2 + \alpha, \\ g(\alpha^2 + \alpha)^{-1} &= g(\alpha^2 + \alpha + 1)^{-1} = \alpha. \end{aligned}$$

Then,

$$\begin{aligned} \tilde{\mathbf{H}} &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha + 1 & \alpha^2 & \alpha^2 + \alpha & \alpha^2 + 1 & \alpha^2 + \alpha + 1 \end{pmatrix} \text{diag}(1, \alpha^2, \alpha^2, \alpha^2 + \alpha, \alpha, \alpha^2 + \alpha, \alpha) \\ &= \begin{pmatrix} 1 & \alpha^2 & \alpha^2 & \alpha^2 + \alpha & \alpha & \alpha^2 + \alpha & \alpha \\ 1 & \alpha + 1 & \alpha^2 + \alpha + 1 & \alpha^2 + 1 & \alpha^2 + \alpha + 1 & \alpha + 1 & \alpha^2 + 1 \end{pmatrix}. \end{aligned}$$

Using the basis $\Gamma = \{1, \alpha, \alpha^2\}$, the parity-check matrix of the Goppa code is then

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The Goppa code $\langle \mathbf{H} \rangle^\perp$ has minimum distance at least 3, and can thus correct at least $t = 1$ error.

The prover chooses the permutation matrix \mathbf{P} , permuting the first two columns and publishes

$$\mathbf{H}' = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Note that any syndrome of a weight 1 vector is simply given by one column of \mathbf{H} . Thus, there exist 7 possible syndromes.

Given a message \mathbf{m} and a random $i = (1, 0, 1, 1)$, the prover computes the hash of (\mathbf{m}, i) . We assume that the hash function outputs $(1, 0, 1, 0, 0, 1, 0)$.

Unfortunately, this is not a syndrome of a weight one vector. The prover chooses a different i and gets the hash $(1, 0, 0, 1, 0, 0)$. Using the syndrome decoder of the Goppa code, the prover finds

$$\mathbf{e} = (0, 1, 0, 0, 0, 0, 0)$$

and computes the signature

$$\sigma = (i, (1, 0, 0, 0, 0, 0, 0)).$$

The verifier checks that \mathbf{eP} has indeed weight 1 and computes

$$\mathbf{eP}\mathbf{H}'^\top = (1, 0, 0, 0, 0, 0, 0) \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}^\top = (1, 0, 1, 0, 0, 1, 0).$$

The verifier accepts the signature as

$$\text{Hash}(\mathbf{m}, i) = (1, 0, 1, 0, 0, 1, 0).$$

The random i , is usually chosen as a seed, denoted by $\text{seed} \in \{0, 1\}^\ell$.

4.1.2 RankSign

RankSign [27], as a framework, is the rank-metric analog of CFS. The authors propose to use augmented LRPC codes over an extension field \mathbb{F}_{q^m} and introduce a mixture of erasures and errors, which can be efficiently decoded.

In the key generation process, instead of hiding the parity-check matrix \mathbf{H} of the LRPC code over \mathbb{F}_{q^m} as usual, i.e., using \mathbf{SHP} , where $\mathbf{S} \in \text{GL}_{n-k}(\mathbb{F}_{q^m})$ and $\mathbf{P} \in \text{GL}_n(\mathbb{F}_q)$, we first add some random columns to \mathbf{H} . This is similar to the scrambling used in the GPT system.

Table 15: RankSign

PROVER	VERIFIER
KEY GENERATION	
Choose $\mathbf{S} \in \text{GL}_{n-k}(\mathbb{F}_{q^m}), \mathbf{P} \in \text{GL}_{n+t}(\mathbb{F}_q)$,	
Choose $r, \ell \in \mathbb{N}, \mathbf{X} \in \mathbb{F}_{q^m}^{(n-k) \times t'}$	
Choose $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ a parity-check matrix of a LRPC code	
Compute $\mathbf{H}' = \mathbf{S}(\mathbf{X} \mid \mathbf{H})\mathbf{P}$	
The keys are given by $\mathcal{S} = (\mathbf{S}, \mathbf{P}, \mathbf{X}, \mathbf{H})$,	
and $\mathcal{P} = (\mathbf{H}', \ell, r)$	
$\xrightarrow{\mathcal{P}}$	
SIGNING	
Choose $\tilde{\mathbf{e}} \in \mathbb{F}_{q^m}^t$ and a message \mathbf{m}	
Choose seed $\in \{0, 1\}^\ell$	
Compute $\mathbf{m}' = \text{Hash}(\mathbf{m} \mid \text{seed})$	
Set $\mathbf{s}' = \mathbf{m}'(\mathbf{S}^{-1})^\top - \tilde{\mathbf{e}}\mathbf{X}^\top$	
Find \mathbf{e}' , such that $\text{wt}_R(\mathbf{e}') = r$ and $\mathbf{e}'\mathbf{H}^\top = \mathbf{s}'$	
Set $\mathbf{e} = (\tilde{\mathbf{e}} \mid \mathbf{e}')(\mathbf{P}^\top)^{-1}$ and $\sigma = \xrightarrow{\mathbf{m}, \sigma} (\mathbf{e}, \text{seed})$	
VERIFICATION	
Check if $\text{wt}_R(\mathbf{e}) = r$ and if $\mathbf{e}\mathbf{H}'^\top = \text{Hash}(\mathbf{m}, \text{seed})$	

Let $\mathbf{S} \in \text{GL}_{n-k}(\mathbb{F}_{q^m}), \mathbf{P} \in \text{GL}_{n+t}(\mathbb{F}_q)$ and $\mathbf{X} \in \mathbb{F}_{q^m}^{(n-k) \times t'}$. Typically one sets $t' = t$, but one could also use other choices.

Then, one hides \mathbf{H} by computing $\mathbf{H}' = \mathbf{S}(\mathbf{X} \mid \mathbf{H})\mathbf{P}$.

While \mathbf{H}' and some integer ℓ are publicly known, the secret key is given by $\mathbf{X}, \mathbf{H}, \mathbf{S}, \mathbf{P}$.

In the signing process, one first chooses randomly $\tilde{\mathbf{e}} \in \mathbb{F}_{q^m}^t$ and hashes a message \mathbf{m} and a seed, denoted by $\text{seed} \in \{0, 1\}^\ell$ to get $\mathbf{m}' = \text{Hash}(\mathbf{m} \mid \text{seed}) \in \mathbb{F}_{q^m}^{n-k}$.

Then one sets a syndrome

$$\mathbf{s}' = \mathbf{m}'(\mathbf{S}^{-1})^\top - \tilde{\mathbf{e}}\mathbf{X}^\top$$

and tries to syndrome decode this syndrome \mathbf{s}' using \mathbf{H} .

If one succeeds, that is, there exists a $\mathbf{e}' \in \mathbb{F}_{q^m}^n$ of rank weight $r = t + r'$ and such that

$$\mathbf{e}'\mathbf{H}^\top = \mathbf{s}',$$

then one defines

$$\mathbf{e} = (\tilde{\mathbf{e}} \mid \mathbf{e}')(\mathbf{P}^\top)^{-1}$$

and sets the signature

$$\sigma = (\mathbf{e}, \text{seed}).$$

If not, this process needs to be repeated until one succeeds.

In the verification, the verifier checks that $\text{wt}_R(\mathbf{e}) = r = t + r'$, and if

$$\mathbf{e}\mathbf{H}'^\top = \mathbf{m}' = \text{Hash}(\mathbf{m} \mid \text{seed}).$$

Exercise 173. Show that $\mathbf{e}\mathbf{H}'^\top = \mathbf{m}'$.

We want to note here that this signature scheme was later attacked in [110].

4.2 Code-Based ZK Protocols

As described in Section 2.3.5, digital signature schemes can be constructed from a ZK protocol using the Fiat-Shamir transform [121]. In this section, we present two famous ZK protocols for this purpose, namely the scheme by Cayrel, Véron and El Yousfi Alaoui (CVE) [89] and scheme by Aguilar, Gaborit and Schrek (AGS) [3].

The CVE scheme [89] is an improvement of Stern's [249] and Véron's [258] protocols, which are both based on the hardness of decoding a random binary code [67]. The CVE scheme relies on codes over a large finite field. With this choice, the cheating probability for a single round is reduced from $2/3$ of Stern's 3-pass scheme to $\frac{q}{2(q-1)}$.

The idea of the scheme is the following: the secret key is given by a random error vector of weight t and the public key is a parity-check matrix together with the syndrome of this error vector. The challenges are requesting either a response that shows that the error vector has indeed weight t or a response that shows that the error vector solves the parity-check equations.

The scheme is of large interest, as it uses an actual random linear code, which is possible since no decoding process is required. The security of this scheme, thus, fully relies on the hardness of decoding a random linear code and not on the indistinguishability of a secret code.

Let σ be a permutation of $\{1, \dots, n\}$ and for $\mathbf{v} \in (\mathbb{F}_q^\star)^n$ and $\mathbf{a} \in \mathbb{F}_q^n$ we denote by

$$\sigma_{\mathbf{v}}(\mathbf{a}) = \sigma(\mathbf{v}) \star \sigma(\mathbf{a}),$$

where \star denotes the component-wise product.

We now show how the communication cost of this scheme is derived, following the reasoning of [41].

Table 16: CVE Scheme

PROVER	VERIFIER
KEY GENERATION	
Choose the parameters q, n, k, t and a hash function Hash	
Choose $\mathbf{e} \in B_H(t, n, q)$ and a parity-check matrix	
$\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$. Compute the syndrome	
$\mathbf{s} = \mathbf{e}\mathbf{H}^\top \in \mathbb{F}_q^{n-k}$.	
The public key is given by $\mathcal{P} = \xrightarrow{\mathcal{P}} (\mathbf{H}, \mathbf{s}, t)$	
VERIFICATION	
Choose $\mathbf{u} \in \mathbb{F}_q^n$, a permutation σ , $\mathbf{v} \in (\mathbb{F}_q^\times)^n$	
Set $c_0 = \text{Hash}(\sigma, \mathbf{v}, \mathbf{u}\mathbf{H}^\top)$	
Set $c_1 = \text{Hash}(\sigma_{\mathbf{v}}(\mathbf{u}), \sigma_{\mathbf{v}}(\mathbf{e}))$	
	$\xrightarrow{c_0, c_1}$
	Choose $z \in \mathbb{F}_q^\star$
	\xleftarrow{z}
Set $\mathbf{y} = \sigma_{\mathbf{v}}(\mathbf{u} + z\mathbf{e})$	
	$\xrightarrow{\mathbf{y}}$
	Choose $b \in \{0, 1\}$
	\xleftarrow{b}
If $b = 0$, set $r = (\sigma, \mathbf{v})$	
If $b = 1$, set $r = \sigma_{\mathbf{v}}(\mathbf{e})$	
	\xrightarrow{r}
If $b = 0$, accept if	
$c_0 = \text{Hash}(\sigma, \mathbf{v}, \sigma_{\mathbf{v}}^{-1}(\mathbf{y})\mathbf{H}^\top - z\mathbf{s})$	
or	
If $b = 1$, accept if $\text{wt}_H(\sigma_{\mathbf{v}}(\mathbf{e})) = t$ and	
$c_1 = \text{Hash}(\mathbf{y} - z\sigma_{\mathbf{v}}(\mathbf{e}), \sigma_{\mathbf{v}}(\mathbf{e}))$	

In order to represent a vector of length n and Hamming weight t over \mathbb{F}_q , we can either use the full vector, which requires $n \lceil \log_2(q) \rceil$ bits, or just consider its support, together with the ordered non-zero entries, resulting in

$$t(\lceil \log_2(n) \rceil + \lceil \log_2(q-1) \rceil)$$

bits. Thus the most convenient choice for a given set of parameters n , t and q is

$$\psi(n, q, t) = \min\{n \lceil \log_2(q) \rceil, t(\lceil \log_2(n) \rceil + \lceil \log_2(q-1) \rceil)\}.$$

Since random objects, such as the monomial transformation, are completely determined by the seed for the pseudo-random generator, they can also be compactly represented as such, whose length is denoted by l_{Seed} . Also the length of the hash values will be denoted by l_{Hash} . Using the compression technique for N rounds of the protocol we get the following average communication cost:

$$l_{\text{Hash}} + N \left(\lceil \log_2(q-1) \rceil + n \lceil \log_2(q) \rceil + 1 + l_{\text{Hash}} + \frac{\psi(n, q, t) + l_{\text{Seed}}}{2} \right).$$

For the maximal communication cost, we take the maximum size of the response, and thus we obtain

$$l_{\text{Hash}} + N \left(\lceil \log_2(q-1) \rceil + n \lceil \log_2(q) \rceil + 1 + l_{\text{Hash}} + \max\{\psi(n, q, t), l_{\text{Seed}}\} \right).$$

Let us fix $t = \lfloor (d_H - 1)/2 \rfloor$, for d_H denoting the minimum distance of the Gilbert-Varshamov bound. The authors of [89] have used the analysis due to Peters [212] to estimate the information set decoding complexity, and have proposed two parameters sets:

- $q = 256$, $n = 128$, $k = 64$, $t = 49$, for 87-bits security, having a communication cost of 3.472 kB;
- $q = 256$, $n = 208$, $k = 104$, $t = 78$, for 128-bits security, having a communication cost of 43.263 kB.

Exercise 174. Show the zero-knowledge property and the completeness property for the CVE scheme.

An easy attempt for an impersonator would be to guess the challenge b before sending the commitments.

Thus, the strategy if we guess $b = 0$, would be to choose an error vector \mathbf{e}' , which satisfies the parity-check equations, that is

$$\mathbf{s} = \mathbf{e}' \mathbf{H}^\top,$$

and to forget about the weight condition. This can easily be achieved using linear algebra. We denote by s_0 the strategy for $b = 0$, which in detail requires to choose randomly \mathbf{u}' , σ' and \mathbf{v}' according to the scheme and to send the commitments $c'_0 = \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}' \mathbf{H}^\top)$ and a random c'_1 . When the impersonator received a $z \in \mathbb{F}_q^*$, the impersonator now computes \mathbf{y}' according to the cheating error vector \mathbf{e}' , i.e.,

$$\mathbf{y}' = \sigma'_{\mathbf{v}'} (\mathbf{u}' + z \mathbf{e}').$$

The impersonator wins, if the verifier now asks for $b = 0$, since the verifier will check

$$\begin{aligned} c'_0 &= \text{Hash}(\sigma', \mathbf{v}', \sigma'_{\mathbf{v}'}^{-1}(\mathbf{y}') \mathbf{H}^\top - z \mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \sigma'_{\mathbf{v}'}^{-1}(\sigma'_{\mathbf{v}'}(\mathbf{u}' + z \mathbf{e}')) \mathbf{H}^\top - z \mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', (\mathbf{u}' + z \mathbf{e}') \mathbf{H}^\top - z \mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}' \mathbf{H}^\top + z \mathbf{e}' \mathbf{H}^\top - z \mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}' \mathbf{H}^\top + z \mathbf{s} - z \mathbf{s}). \end{aligned}$$

If the verifier asks for $b = 1$, the impersonator loses.

Whereas the strategy if we guess $b = 1$, would be to choose an error vector \mathbf{e}' , which has the correct weight, i.e., $\text{wt}_H(\mathbf{e}') = t$, but does not satisfy the parity-check equations. We denote by s_1 the strategy for $b = 1$, which in detail requires to choose randomly \mathbf{u}' , σ' and \mathbf{v}' according to the scheme and to send the commitments: a random c'_0 and $c'_1 = \text{Hash}(\sigma'_{\mathbf{v}'}(\mathbf{u}'), \sigma'_{\mathbf{v}'}(\mathbf{e}'))$. When the impersonator received a $z \in \mathbb{F}_q^*$, the impersonator now computes \mathbf{y}' according to the cheating error vector \mathbf{e}' , i.e.,

$$\mathbf{y}' = \sigma'_{\mathbf{v}'}(\mathbf{u}' + z\mathbf{e}').$$

The impersonator wins, if the verifier now asks for $b = 1$, since the verifier will check if $\text{wt}_H(\sigma'_{\mathbf{v}'}(\mathbf{e}')) = t$ and

$$\begin{aligned} c'_1 &= \text{Hash}(\mathbf{y}' - z\sigma'_{\mathbf{v}'}(\mathbf{e}'), \sigma'_{\mathbf{v}'}(\mathbf{e}')) \\ &= \text{Hash}(\sigma'_{\mathbf{v}'}(\mathbf{u}' + z\mathbf{e}') - z\sigma'_{\mathbf{v}'}(\mathbf{e}'), \sigma'_{\mathbf{v}'}(\mathbf{e}')) \\ &= \text{Hash}(\sigma'_{\mathbf{v}'}(\mathbf{u}') + \sigma'_{\mathbf{v}'}(z\mathbf{e}') - z\sigma'_{\mathbf{v}'}(\mathbf{e}'), \sigma'_{\mathbf{v}'}(\mathbf{e}')). \end{aligned}$$

If the verifier asks for $b = 0$, the impersonator loses.

With this easy strategy, one would get a cheating probability of $1/2$, which just corresponds to choosing the challenge b correctly. However, by also guessing z correctly one can improve the above strategy.

Proposition 175. *The cheating probability of the CVE scheme is $\frac{q}{2(q-1)}$.*

Proof. We modify the easy strategies s_i , following [89]:

Let us denote by s'_0 the improved strategy on s_0 , which works as follows: recall that \mathbf{e}' is chosen such that the parity-check equations are satisfied but not the weight condition. Instead of randomly choosing the commitment c'_1 , we choose a $z' \in \mathbb{F}_q^*$ and a second cheating error vector $\tilde{\mathbf{e}}$ of weight t , we compute a $\tilde{\mathbf{y}} = \sigma'_{\mathbf{v}'}(\mathbf{u}' + z'\mathbf{e}')$ with this guess and compute

$$c'_1 = \text{Hash}(\tilde{\mathbf{y}} - z'\tilde{\mathbf{e}}, \tilde{\mathbf{e}}).$$

When we receive a z from the verifier, we check if we made the correct choice, that is: if $z = z'$, we send the pre-computed $\tilde{\mathbf{y}}$, and if $z \neq z'$ we compute $\mathbf{y}' = \sigma'_{\mathbf{v}'}(\mathbf{u}' + z\mathbf{e}')$. If the verifier asks for $b = 0$, we use the usual strategy of s_0 and will get accepted, as before. If the verifier asks for $b = 1$, we send as answer $\tilde{\mathbf{e}}$. If we have guessed correctly and $z = z'$, we will get accepted also in this case as

$$c'_1 = \text{Hash}(\tilde{\mathbf{y}} - z\tilde{\mathbf{e}}, \tilde{\mathbf{e}})$$

by definition.

Let us denote by s'_1 the improved strategy on s_1 , which works as follows: recall that \mathbf{e}' is chosen having the correct weight. Instead of randomly choosing the commitment c'_0 , we choose a $z' \in \mathbb{F}_q^*$ and compute a $\tilde{\mathbf{y}} = \sigma'_{\mathbf{v}'}(\mathbf{u}' + z'\mathbf{e}')$ with this guess and compute

$$c'_0 = \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}'\mathbf{H}^\top + z'(\mathbf{e}'\mathbf{H}^\top - \mathbf{s})).$$

When we receive a z from the verifier, we check if we made the correct choice, that is: if $z = z'$, we send the pre-computed $\tilde{\mathbf{y}}$, and if $z \neq z'$ we compute $\mathbf{y}' = \sigma'_{\mathbf{v}'}(\mathbf{u}' + z\mathbf{e}')$. If the verifier asks for $b = 1$, we use the usual strategy of s_1 and will get accepted. If the verifier

asks for $b = 0$, we send as answer (σ', \mathbf{v}') . If we have guessed correctly and $z = z'$, we will get accepted also in this case as

$$\begin{aligned} c'_0 &= \text{Hash}(\sigma', \mathbf{v}', \sigma'_{\mathbf{v}'}^{-1}(\mathbf{y}')\mathbf{H}^\top - z\mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \sigma'_{\mathbf{v}'}^{-1}(\sigma'_{\mathbf{v}'}(\mathbf{u}' + z'\mathbf{e}'))\mathbf{H}^\top - z\mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', (\mathbf{u}' + z'\mathbf{e}')\mathbf{H}^\top - z\mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}'\mathbf{H}^\top + z'\mathbf{e}'\mathbf{H}^\top - z\mathbf{s}) \\ &= \text{Hash}(\sigma', \mathbf{v}', \mathbf{u}'\mathbf{H}^\top + z'\mathbf{s} - z\mathbf{s}). \end{aligned}$$

Thus, the probability that an impersonator following the strategy s'_i will get accepted is given by

$$P(b = i) + P(b = 1 - i) \cdot P(z = z') = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{q-1} = \frac{q}{2(q-1)},$$

which concludes this proof. \square

The second ZK protocol we want to present is the scheme by Aguilar, Gaborit and Schrek [3], which we will denote by AGS. This scheme is constructed upon quasi-cyclic codes over \mathbb{F}_2 . Let us consider a vector $\mathbf{a} \in \mathbb{F}_2^{jk}$ divided into j blocks of k entries each, that is,

$$\mathbf{a} = (a_1^{(1)}, \dots, a_k^{(1)}, \dots, a_1^{(j)}, \dots, a_k^{(j)}).$$

Let $\rho_i^{(k)}$ denote a function that performs a block-wise cyclic shift of \mathbf{a} by i positions, i.e.,

$$\rho_i^{(k)}(\mathbf{a}) = (a_{1-i \bmod k}^{(1)}, \dots, a_{k-i \bmod k}^{(1)}, \dots, a_{1-i \bmod k}^{(j)}, \dots, a_{k-i \bmod k}^{(j)}).$$

The idea is similar to that of the CVE scheme, but working with the generator matrix instead.

The secret key consists of a message and an error vector, while the public key consists of an erroneous codeword and the generator matrix. The challenges either require the proof of the error vector having the correct weight or of the knowledge of the message.

When performing N rounds, the average communication cost is

$$l_{\text{Hash}} + N \left(\lceil \log_2(k) \rceil + 1 + 2l_{\text{Hash}} + \frac{l_{\text{Seed}} + k + n + \psi(n, t, 2)}{2} \right),$$

while the maximum communication cost is

$$l_{\text{Hash}} + N \left(\lceil \log_2(k) \rceil + 1 + 2l_{\text{Hash}} + \max\{l_{\text{Seed}} + k, n + \psi(n, t, 2)\} \right).$$

In [3], three parameters sets are proposed:

- $n = 698$, $k = 349$, $t = 70$, for 81-bits security, having a communication cost of 2.5 kB;
- $n = 1094$, $k = 547$, $t = 109$, for 128-bits security, with communication cost of 28 kB.

Exercise 176. Show the zero-knowledge property and completeness for the AGS scheme.

We remark that in a code-based ZK protocol one does not require a code with an efficient decoding algorithm. Which stands in contrast to the requirements for many of the code-based public-key encryption schemes. Thus, choosing a random code the security of such schemes is much closer related to the actual NP-hard problem of decoding a random linear code.

Table 17: AGS Scheme

PROVER	VERIFIER
KEY GENERATION	
Choose the parameters n, k, t and a hash function Hash	
Choose $\mathbf{m} \in \mathbb{F}_2^k$ and $\mathbf{e} \in B_H(t, n, 2)$ and	
generator matrix $\mathbf{G} \in \mathbb{F}_2^{k \times n}$.	
Compute the erroneous codeword $\mathbf{c} = \mathbf{mG} + \mathbf{e} \in \mathbb{F}_2^n$	
The public key is given by $\mathcal{P} = \xrightarrow{\mathcal{P}} (\mathbf{G}, \mathbf{c}, t)$	
VERIFICATION	
Choose $\mathbf{u} \in \mathbb{F}_2^k$, a permutation σ	
Set $c_0 = \text{Hash}(\sigma)$	
Set $c_1 = \text{Hash}(\sigma(\mathbf{uG}))$	
	$\xrightarrow{c_0, c_1}$
	Choose $z \in \{1, \dots, k\}$
	\xleftarrow{z}
Set $c_2 = \text{Hash}(\sigma(\mathbf{uG} + \rho_z^{(k)}(\mathbf{e})))$	
	$\xrightarrow{c_2}$
	Choose $b \in \{0, 1\}$
	\xleftarrow{b}
If $b = 0$, set $r = (\sigma, \mathbf{u} + \rho_z^{(k)}(\mathbf{m}))$	
If $b = 1$, set $r = (\sigma(\mathbf{uG}), \sigma(\rho_z^{(k)}(\mathbf{e})))$	
	\xrightarrow{r}
If $b = 0$, accept if $c_0 = \text{Hash}(\sigma)$ and $c_2 = \text{Hash}((\mathbf{u} + \rho_z^{(k)}(\mathbf{m}))\mathbf{G} + \rho_z^{(k)}(\mathbf{c}))$	
If $b = 1$, accept if $\text{wt}_H(\rho_z^{(k)}(\mathbf{e})) = t$ and $c_1 = \text{Hash}(\sigma(\mathbf{uG}))$ and $c_2 = \text{Hash}(\sigma(\mathbf{uG} + \sigma(\rho_z^{(k)}(\mathbf{e})))$	

Clearly, using any of the two code-based ZK protocols presented above and the Fiat-Shamir transform one immediately gets a signature scheme.

5 Security Analysis

In the security analysis of a cryptographic scheme we make a difference between two main attack approaches:

1. structural attacks,
2. non-structural attacks.

A structural attack aims at exploiting the algebraic structure of the cryptographic system.

Whereas a non-structural attack tries to combinatorically recover the message or the secret key without exploiting any algebraic structure.

For example the security of the McEliece and Niederreiter type of cryptosystems rely on two assumptions. The first one being

The public code is not distinguishable from a random code.

A structural attack would usually aim at exactly this assumption, and try to recover the secret code, if the scrambled public version of it does not behave randomly.

Clearly, structural or algebraic attacks heavily depend on the chosen secret codes for the cryptosystem, if the system depends on an algebraic code that is efficiently decodable, and is not attacking the presented frameworks in general.

Assuming that this first assumption is met, however, the security of most code-based cryptosystems relies also on this second assumption

Decoding a random linear code is hard/ infeasible.

A non-structural attack on the McEliece cryptosystem would, thus, assume that the public code is in fact random, and rather try to decode this random code.

In general we also speak of attacks in terms of: *key-recovery attacks*, where an attacker tries to recover the secret key (usually structural attacks), and *message-recovery attacks*, where an attacker directly tries to decrypt the cipher without first recovering the secret key.

Code-based cryptography is rapidly advancing and new cryptosystems are basing their security on novel problems from algebraic coding theory.

In the following we list the main problems used in cryptography and discuss their hardness.

5.1 Problems from Coding Theory

The most prominent problem in algebraic coding theory is the decoding problem:

Problem 177. Decoding Problem (DP) Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{r} \in \mathbb{F}_q^n$ and $t \in \mathbb{N}$, is there a vector $\mathbf{m} \in \mathbb{F}_q^k$ and $\mathbf{e} \in \mathbb{F}_q^n$ of weight less than or equal to t such that $\mathbf{r} = \mathbf{m}\mathbf{G} + \mathbf{e}$?

Note that the DP formulated through the generator matrix is equivalent to the syndrome decoding problem, which is formulated through the parity-check matrix.

Problem 178. Syndrome Decoding Problem (SDP) Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and $t \in \mathbb{N}$, is there a vector $\mathbf{e} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{e}) \leq t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

These two problems are also equivalent to the Given Weight Codeword Problem:

Problem 179. Given Weight Codeword Problem (GWCP)

Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Let $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ and $w \in \mathbb{N}$, is there a vector $\mathbf{c} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{c}) = w$ and $\mathbf{c}\mathbf{H}^\top = \mathbf{0}_{n-k}$?

Theorem 180. *The DP, SDP and GWCP are equivalent.*

Proof. Let us start with showing that the DP and SDP are equivalent. For this we start with an instance of DP, i.e., $\mathbf{G}, \mathbf{r}, t$. We can then transform this instance to an instance of the SDP. In fact, we can bring \mathbf{G} into systematic form, that is

$$\mathbf{G}' = \begin{pmatrix} \text{Id}_k & \mathbf{A} \end{pmatrix}$$

and immediately get a parity-check matrix for the same code

$$\mathbf{H} = \begin{pmatrix} -\mathbf{A}^\top & \text{Id}_{n-k} \end{pmatrix}.$$

We can then multiply \mathbf{H} to the received vector $\mathbf{r} = \mathbf{m}\mathbf{G} + \mathbf{e}$, getting the syndrome

$$\mathbf{s} = \mathbf{r}\mathbf{H}^\top = \mathbf{e}\mathbf{H}^\top.$$

Hence, if we can solve the SDP on the instance $\mathbf{H}, \mathbf{s}, t$, thus finding \mathbf{e} , we have also solved DP.

On the other hand, given an instance of SDP, i.e., $\mathbf{H}, \mathbf{s}, t$, we can find an instance of DP. In fact, we can bring \mathbf{H} into systematic form and read of a generator matrix \mathbf{G} for the same code. We can now solve $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$ and since this is a linear system of $n - k$ equations in n unknowns, we get $N = q^k$ possible solutions for $\mathbf{x}_1, \dots, \mathbf{x}_N$. Note that for each of the q^k codewords $\mathbf{c}_1, \dots, \mathbf{c}_N$, we have that $\mathbf{c}_i + \mathbf{e}$ is a possible solution. Thus, each of the q^k solutions \mathbf{x}_i correspond to some $\mathbf{c}_i + \mathbf{e}$. Hence, any of the solutions \mathbf{x}_i can be used as received vector \mathbf{r} and we have recovered an instance of DP, as $\mathbf{G}, \mathbf{r}, t$. Hence, solving DP, i.e., finding \mathbf{e} , also solves the SDP instance.

Finally, it is enough to show that DP and SDP are also equivalent to GWCP.

Given an instance of DP, i.e., $\mathbf{G}, \mathbf{r}, t$ we can add \mathbf{r} as a row to the generator matrix, getting

$$\mathbf{G}' = \begin{pmatrix} \mathbf{G} \\ \mathbf{r} \end{pmatrix}.$$

Note that the code generated by \mathbf{G}' is also generated by

$$\begin{pmatrix} \mathbf{G} \\ \mathbf{e} \end{pmatrix},$$

as $\mathbf{r} = \mathbf{m}\mathbf{G} + \mathbf{e}$. The new code of dimension $k + 1$ has now as lowest weight codeword \mathbf{e} of weight t . Hence, we can compute the corresponding parity-check matrix \mathbf{H}' and solving the GWCP on the instance \mathbf{H}', t we recover the solution \mathbf{e} to the DP instance.

On the other hand, given an instance \mathbf{H}, w of GWCP, we can define an instance of SDP, by taking the same parity-check matrix and setting the syndrome $\mathbf{s} = \mathbf{0}$. Thus, a solver for SDP, searching for a weight w vector \mathbf{e} with $\mathbf{e}\mathbf{H}^\top = \mathbf{0}$ also solves the GWCP instance. \square

These three equivalent problems are the main problems used for code-based cryptography and will thus be the main focus of the survey. In the next section, we show that the DP,SDP and GWCP are NP-complete [67, 57].

There are, however, also other hard problems in coding theory. Recall from Section 2, that there are several notions of code equivalence in the Hamming metric. In the lightest version, we ask for two codes to be permutation equivalent.

Problem 181 (Permutation Equivalence Problem (PEP)). Given $\mathbf{G}, \mathbf{G}' \in \mathbb{F}_q^{k \times n}$, find φS_n , such that $\varphi(\langle \mathbf{G} \rangle) = \langle \mathbf{G}' \rangle$.

This problem is clearly contained in the linear equivalence problem.

Problem 182 (Linear Equivalence Problem (LEP)). Given $\mathbf{G}, \mathbf{G}' \in \mathbb{F}_q^{k \times n}$, find $\varphi \in (\mathbb{F}_q^*)^n \rtimes S_n$, such that $\varphi(\langle \mathbf{G} \rangle) = \langle \mathbf{G}' \rangle$.

On the other hand, we can also ask for a subcode-equivalence.

Problem 183 (Permuted Kernel Problem (PKP)). Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}, \mathbf{H}' \in \mathbb{F}_q^{(n-k') \times n}$ find a permutation matrix \mathbf{P} such that $\mathbf{H}'(\mathbf{GP})^\top = \mathbf{0}$.

This problem has first been introduced by Shamir in [239] and was formulated through parity-check matrices, thus the name *permuted kernel*. In [233] it has been observed, that the formulation of [239] is indeed equivalent to the subcode-equivalence problem.

Problem 184 (Subcode Equivalence Problem (SEP)). Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}, \mathbf{G}' \in \mathbb{F}_q^{k' \times n}$, find permutation matrix \mathbf{P} such that $\langle \mathbf{G}' \rangle \subset \langle \mathbf{GP} \rangle$.

Exercise 185. Show that PKP is equivalent to SEP.

In the following, we will thus only use the subcode equivalence formulation, also for PKP.

There also exists a relaxed version on PKP, which only asks to find a subcode of dimension 1.

Problem 186 (Relaxed PKP). Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}, \mathbf{G}' \in \mathbb{F}_q^{k' \times n}$, find $\mathbf{x} \in \mathbb{F}_q^k$ and a permutation matrix \mathbf{P} such that $\mathbf{xGP} \in \langle \mathbf{G}' \rangle$.

Since PKP only asks for permutation equivalence it contains PEP and clearly, PKP contains the Relaxed PKP.

The different code equivalence problems have a strong relation to the graph isomorphism problem and live in different complexity classes, which we will exploit in the next section.

Clearly, one can also consider the decoding problem or the code equivalence problem in a different metric.

Let us start with the Rank-metric analogue of the SDP.

Problem 187 (Rank SDP). Let \mathbb{F}_{q^m} be a finite field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}, \mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ and $t \in \mathbb{N}$, is there a vector $\mathbf{e} \in \mathbb{F}_{q^m}^n$ such that $\text{wt}_R(\mathbf{e}) \leq t$ and $\mathbf{eH}^\top = \mathbf{s}$?

Again, Rank SDP is equivalent to Rank DP or Rank GWCP, as the equivalence is independent of the metric. In [132] the authors provide a randomized reduction from the SDP to Rank SDP. While this gives great evidence of the hardness of the Rank SDP, it remains one of the largest open problems in code-based cryptography whether Rank SDP is NP-complete or not.

We do get a different problem, however, when considering \mathbb{F}_q -linear codes, i.e., matrix codes.

Problem 188 (MinRank Problem). Given $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$ $t \in \mathbb{N}$ and $\mathbf{R} \in \mathbb{F}_q^{m \times n}$, find $\mathbf{E} \in \mathbb{F}_q^{m \times n}$ of rank at most t , such that

$$\mathbf{R} = \lambda_1 \mathbf{G}_1 + \dots + \lambda_k \mathbf{G}_k + \mathbf{E},$$

for some $\lambda_1, \dots, \lambda_k \in \mathbb{F}_q$.

The MinRank problem is simply the DP for \mathbb{F}_q -linear codes in the rank metric and clearly equivalent to the respective SDP and GWCP. Note that unlike the Rank SDP, dealing with \mathbb{F}_q^m -linear codes, the MinRank problem is known to be NP-complete. We will see the proof in the next section and first cover some more hard problems.

Problem 189 (Lee SDP). Let \mathbb{F}_p be a prime field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$ and $t \in \mathbb{N}$, is there a vector $\mathbf{e} \in \mathbb{F}_p^n$ such that $\text{wt}_L(\mathbf{e}) \leq t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

The Lee SDP (again equivalent to Lee DP and Lee GWCP) has been proven to be NP-complete in [263]. Thus, marking the Lee metric as a promising alternative for the Hamming metric.

Problem 190 (Restricted SDP). Let \mathbb{F}_p be a prime field, $g \in \mathbb{F}_p$ have prime order z and define

$$\mathbb{E} = \{g^i \mid i \in \{0, \dots, z-1\}\}.$$

Let $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$ and $\mathbf{s} \in \mathbb{F}_p^{n-k}$, is there a vector $\mathbf{e} \in \mathbb{E}^n$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

The Restricted SDP is not exactly the SDP with a different metric, but rather than asking for \mathbf{e} to have a certain weight, the Restricted SDP asks for all entries of \mathbf{e} to live in a restricted set \mathbb{E} . Hence, we keep the linear condition $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and exchanged the non-linear constraint $\text{wt}(\mathbf{e}) \leq t$ with $\mathbf{e} \in \mathbb{E}^n$. In the next section, we give a proof on the NP-hardness of the Restricted SDP.

5.2 NP-completeness

In this section, we give the definitions of several complexity classes and the techniques in order to show that a problem belongs to such complexity class. We then show that DP (and thus also SDP and GWCP) are NP-complete. We also provide the reduction of PEP to graph isomorphism.

Let us start with a small introduction to complexity theory.

Let \mathcal{P} denote a problem. In order to estimate how hard it is to solve \mathcal{P} we have two main complexity classes.

Definition 191. \mathbf{P} denotes the class of problems that can be solved by a deterministic Turing machine in polynomial time.

The concept of deterministic and non-deterministic Turing machines will exceed the scope of this chapter, just note that "can be solved by a deterministic Turing machine in polynomial time" is the same as our usual "can be solved in polynomial time".

Example 192. Given a list S of n integers and an integer k , determine whether there is an integer $s \in S$ such that $s > k$? Clearly, this can be answered by going through the list and checking for each element whether it is greater than k , thus it has running time at most n and this problem is in P.

Definition 193. NP denotes the class of problems that can be solved by a non-deterministic Turing machine in polynomial time.

Thus, in contrary to the popular belief that NP stands for non-polynomial time, it actually stands for non-deterministic polynomial time. The difference is important: all problems in P live inside NP!

To understand NP better, we might use the equivalent definition: A problem \mathcal{P} is in NP if and only if one can check that a candidate is a solution to \mathcal{P} in polynomial time.

The example from before is thus also clearly in NP, since if given a candidate a , we can check in polynomial time whether $a \in S$ and whether $a > k$.

There are, however, interesting problems which are in NP, but we do not know whether they are in P. Let us change the previous example a bit.

Example 194. Given a list S of n integers and an integer k , is there a set of integers $T \subseteq S$, such that $\sum_{t \in T} t = k$? Since there are exponentially many subsets of S , there is no known algorithm to solve this problem in polynomial time and thus, we do not know whether it lives in P. But, if given a candidate T , we can check in polynomial time if all $t \in T$ are also in S and if $\sum_{t \in T} t = k$, which clearly places this problem inside NP.

The most important complexity class, for us, will be that of NP-hard problems. In order to define this class, we first have to define polynomial-time reductions.

A polynomial-time reduction from \mathcal{R} to \mathcal{P} follows the following steps:

1. take any instance I of \mathcal{R} ,
2. transform I to an instance I' of \mathcal{P} in polynomial time,
3. assume that (using an oracle) you can solve \mathcal{P} in the instance I' in polynomial time, getting the solution s' ,
4. transform the solution s' in polynomial time to get a solution s of the problem \mathcal{R} in the input I .

The existence of a polynomial-time reduction from \mathcal{R} to \mathcal{P} , informally speaking, means that if we can solve \mathcal{P} , we can also solve \mathcal{R} and thus solving \mathcal{P} is at least as hard as solving \mathcal{R} .

Definition 195. \mathcal{P} is NP-hard if for every problem \mathcal{R} in NP, there exists a polynomial-time reduction from \mathcal{R} to \mathcal{P} .

Informally speaking this class contains all problems which are at least as hard as the hardest problems in NP.

Example 196. One of the most famous examples for an NP-hard problem is the subset sum problem: given a set of integers S , is there a non-empty subset $T \subseteq S$, such that $\sum_{t \in T} t = 0$?

We want to remark here, that NP-hardness is only defined for *decisional* problems, that are problems of the form "decide whether there exists.." and not for *computational/search* problems, that are problems of the form "find a solution..". However, considering for example the SDP, in its decisional version, it asks whether there exists error vector \mathbf{e} with certain conditions. If one could solve the computational problem, that is to actually find such an error vector \mathbf{e} in polynomial time, then one would also be able to answer the decisional problem in polynomial time. Thus, not being very rigorous, we call also the computational SDP NP-hard.

In order to prove that a problem \mathcal{P} is NP-hard, fortunately we do not have to give a polynomial-time reduction to *every* problem in NP: there are already problems which are known to be NP-hard, thus it is enough to give a polynomial-time reduction from an NP-hard problem to \mathcal{P} .

Finally, NP-completeness denotes the intersection of NP-hardness and NP.

Definition 197. A problem \mathcal{P} is NP-complete, if it is NP-hard and in NP.

5.2.1 Decoding Problem

Berlekamp, McEliece and van Tilborg famously proved in [67] the NP-completeness of the syndrome decoding problem for the case of binary linear codes equipped with the Hamming metric. In [57], Barg generalized this proof to an arbitrary finite field. Finally, the NP-hardness proof has been generalized to arbitrary finite rings endowed with an additive weight in [263], thus including famous metrics such as the homogeneous and the Lee metric.

In this section we provide the proof of NP-completeness for the SDP as in [57].

Problem 198. Syndrome Decoding Problem (SDP) Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and $t \in \mathbb{N}$, is there a vector $\mathbf{e} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{e}) \leq t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

Note that the SDP is clearly in NP: given a candidate vector \mathbf{e} we can check in polynomial time if $\text{wt}_H(\mathbf{e}) \leq t$ and if $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$. Thus, we are only left with showing the NP-hardness of the SDP through a polynomial-time reduction. For this, we choose the 3-dimensional matching (3DM) problem, which is a well-known NP-hard problem.

Problem 199. 3-Dimensional Matching (3DM) Problem

Let T be a finite set and $U \subseteq T \times T \times T$. Given U, T , decide if there exists a set $W \subseteq U$ such that $|W| = |T|$ and no two elements of W agree in any coordinate.

Proposition 200. *The SDP is NP-complete.*

For the proof of Proposition 200 we follow closely [263].

Proof. We prove the NP-completeness by a polynomial-time reduction from the 3DM problem. For this, we start with a random instance of 3DM with T of size t , and $U \subseteq T \times T \times T$ of size u . Let us denote the elements in $T = \{b_1, \dots, b_t\}$ and in $U = \{\mathbf{a}_1, \dots, \mathbf{a}_u\}$. From this we build the matrix $\mathbf{H}^\top \in \mathbb{F}_q^{u \times 3t}$, as follows:

- for $j \in \{1, \dots, t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[1] = b_j$ and $h_{i,j} = 0$ else,
- for $j \in \{t+1, \dots, 2t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[2] = b_j$ and $h_{i,j} = 0$ else,
- for $j \in \{2t+1, \dots, 3t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[3] = b_j$ and $h_{i,j} = 0$ else.

With this construction, we have that each row of \mathbf{H}^\top corresponds to an element in U , and has weight 3. Let us set the syndrome \mathbf{s} as the all-one vector of length $3t$. Assume that we can solve the SDP on the instances \mathbf{H}, \mathbf{s} and t in polynomial time. Let us consider two cases.

Case 1: First, assume that the SDP solver returns as answer ‘yes’, i.e., there exists an $\mathbf{e} \in \mathbb{F}_q^u$, of weight less than or equal to t and such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

- We first observe that we must have $\text{wt}_H(\mathbf{e}) = |\text{supp}_H(\mathbf{e})| = t$. For this note that each row of \mathbf{H}^\top adds at most 3 non-zero entries to \mathbf{s} . Therefore, we need to add at least t rows to get \mathbf{s} , i.e., $|\text{supp}_H(\mathbf{e})| \geq t$ and hence $\text{wt}_H(\mathbf{e}) \geq t$. As we also have $\text{wt}_H(\mathbf{e}) \leq t$ by hypothesis, this implies that $\text{wt}_H(\mathbf{e}) = |\text{supp}_H(\mathbf{e})| = t$.
- Secondly, we observe that the weight t solution must be a binary vector. For this we note that the matrix \mathbf{H}^\top has binary entries and has constant row weight three, and since $|\text{supp}_H(\mathbf{e})| = t$, the supports of the t rows of \mathbf{H}^\top that sum up to the all-one vector have to be disjoint. Therefore, we get that the j -th equation from the system of equations $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ is of the form $e_i h_{i,j} = 1$ for some $i \in \text{supp}_H(\mathbf{e})$. Since $h_{i,j} = 1$, we have $e_i = 1$.

Recall from above that the rows of \mathbf{H}^\top correspond to the elements of U . The t rows corresponding to the support of \mathbf{e} are now a solution W to the 3DM problem. This follows from the fact that the t rows have disjoint supports and add up to the all-one vector, which implies that each element of T appears exactly once in each coordinate of the elements of W .

Case 2: Now assume that the SDP solver returns as answer ‘no’, i.e., there exists no $\mathbf{e} \in \mathbb{F}_q^u$ of weight at most t such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$. This response is now also the correct response for the 3DM problem. In fact, if there exists $W \subseteq U$ of size t such that all coordinates of its elements are distinct, then t rows of \mathbf{H}^\top should add up to the all one vector, which in turn means the existence of a vector $\mathbf{e} \in \{0, 1\}^u$ of weight t such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Thus, if such a polynomial time solver exists, we can also solve the 3DM problem in polynomial time. \square

Example 201. Let us consider $T = \{A, B, C, D\}$ and

$$U = \{(D, A, B), (C, B, A), (D, A, B), (B, C, D), (C, D, A), (A, D, A), (A, B, C)\}.$$

Then the above construction would yield

$$\mathbf{H}^\top = \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array} \right].$$

A solution to $\mathbf{e}\mathbf{H}^\top = (1, \dots, 1)$ would be $\mathbf{e} = (1, 0, 0, 1, 1, 0, 1)$ which corresponds to

$$W = \{(D, A, B), (B, C, D), (C, D, A), (A, B, C)\}.$$

Notice that the very same construction is used also in the problem of finding codewords with given weight.

Proposition 202. *The GWCP is NP-complete.*

Proof. We again prove the NP-completeness by a reduction from the 3DM problem. To this end, we start with a random instance of 3DM, i.e., T of size t , and $U \subseteq T \times T \times T$ of size u . Let us denote the elements in $T = \{b_1, \dots, b_t\}$ and in $U = \{\mathbf{a}_1, \dots, \mathbf{a}_u\}$. At this point, we build the matrix $\overline{\mathbf{H}}^\top \in \mathbb{F}_q^{u \times 3t}$, like in the proof of Proposition 200.

Then we construct $\mathbf{H}^\top \in \mathbb{F}_q^{(3tu+3t+u) \times (3tu+3t)}$ in the following way.

$$\mathbf{H}^\top = \begin{pmatrix} \overline{\mathbf{H}}^\top & \text{Id}_u & \cdots & \text{Id}_u \\ -\text{Id}_{3t} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & -\text{Id}_u & & \mathbf{0} \\ \vdots & & \ddots & \\ \mathbf{0} & \mathbf{0} & & -\text{Id}_u \end{pmatrix},$$

where we have repeated the size- u identity matrix $3t$ times in the first row. Let us set $w = 3t^2 + 4tM$ and assume that we can solve the GWCP on the instance given by \mathbf{H}, w in polynomial time. Let us again consider two cases.

Case 1: In the first case the GWCP solver returns as answer ‘yes’, since there exists a $\mathbf{c} \in \mathbb{F}_q^{3tu+3t+u}$, of weight equal to w , such that $\mathbf{c}\mathbf{H}^\top = \mathbf{0}_{3tu+3t}$. Let us write this \mathbf{c} as

$$\mathbf{c} = (\overline{\mathbf{c}}, \mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{3t}),$$

where $\overline{\mathbf{c}} \in \mathbb{F}_q^u$, $\mathbf{c}_0 \in \mathbb{F}_q^{3t}$ and $\mathbf{c}_i \in \mathbb{F}_q^u$ for all $i \in \{1, \dots, 3t\}$. Then, $\mathbf{c}\mathbf{H}^\top = \mathbf{0}_{3tu+3t}$ gives the equations

$$\begin{aligned} \overline{\mathbf{c}}\overline{\mathbf{H}}^\top - \mathbf{c}_0 &= \mathbf{0}, \\ \overline{\mathbf{c}} - \mathbf{c}_1 &= \mathbf{0}, \\ &\vdots \\ \overline{\mathbf{c}} - \mathbf{c}_{3t} &= \mathbf{0}. \end{aligned}$$

Hence, we have that $\text{wt}_H(\overline{\mathbf{c}}\overline{\mathbf{H}}^\top) = \text{wt}_H(\mathbf{c}_0)$ and

$$\text{wt}_H(\overline{\mathbf{c}}) = \text{wt}_H(\mathbf{c}_1) = \dots = \text{wt}_H(\mathbf{c}_{3t}).$$

Due to the coordinatewise additivity of the weight, we have that

$$\text{wt}_H(\mathbf{c}) = \text{wt}_H(\overline{\mathbf{c}}\overline{\mathbf{H}}^\top) + (3t+1)\text{wt}_H(\overline{\mathbf{c}}).$$

Since $\text{wt}_H(\overline{\mathbf{c}}\overline{\mathbf{H}}^\top) \leq 3t$, we have that $\text{wt}_H(\overline{\mathbf{c}}\overline{\mathbf{H}}^\top)$ and $\text{wt}_H(\overline{\mathbf{c}})$ are uniquely determined as the remainder and the quotient, respectively, of the division of $\text{wt}_H(\mathbf{c})$ by $3t+1$. In particular, if $\text{wt}_H(\mathbf{c}) = 3t^2 + 4t$, then we must have $\text{wt}_H(\overline{\mathbf{c}}) = t$ and $\text{wt}_H(\overline{\mathbf{c}}\overline{\mathbf{H}}^\top) = 3t$. Hence, the first u parts of the found solution \mathbf{c} , i.e., $\overline{\mathbf{c}}$, give a matching for the 3DM in a similar way as in the proof of Proposition 200. For this we first observe that $\overline{\mathbf{c}}\overline{\mathbf{H}}^\top$ is a full support vector and it

plays the role of the syndrome, i.e., $\bar{\mathbf{c}}\bar{\mathbf{H}}^\top = (x_1, \dots, x_{3t})$, where $x_i \in \mathbb{F}_q^*$. Now, using the same argument as in the proof of Proposition 200, we note that $\bar{\mathbf{c}}$ has exactly t non-zero entries, which corresponds to a solution of 3DM.

Case 2: If the solver returns as answer ‘no’, this is also the correct answer for the 3DM problem. In fact, if there exists a $W \subseteq U$ of size t , such that all coordinates of its elements are distinct, then t rows of $\bar{\mathbf{H}}^\top$ should add up to the all one vector, which in turn means the existence of a $\mathbf{e} \in \{0, 1\}^u$ of support size t such that $x\mathbf{e}\bar{\mathbf{H}}^\top = (x, \dots, x) =: \mathbf{c}_0$ for any $x \in \mathbb{F}_q^*$. And thus, with $\bar{\mathbf{c}} = x\mathbf{e}$ a solution \mathbf{c} to the GWCP with the instances constructed as above should exist.

Thus, if such a polynomial time solver for the GWCP exists, we can also solve the 3DM problem in polynomial time. \square

We remark that the bounded version of this problem, i.e., deciding if a codeword \mathbf{c} with $\text{wt}_H(\mathbf{c}) \leq w$ exists, can be solved by applying the solver of Problem 179 at most w many times.

The computational versions of Problems 179 and 178 are at least as hard as their decisional counterparts. Trivially, any operative procedure that returns a vector with the desired properties (when it exists) can be used as a direct solver for the above problems.

Note that the problem on which the McEliece system is based upon is not exactly equivalent to the SDP. In the McEliece system the parameter t is usually bounded by the error correction capacity of the chosen code. Whereas in the SDP, the parameter t can be chosen to be any positive integer. Thus, we are in a more restricted regime than in the SDP.

Problem 203 (Bounded SDP). Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and $d \in \mathbb{N}$, such that every set of $d-1$ columns of \mathbf{H} is linearly independent and $w = \lfloor \frac{d-1}{2} \rfloor$, is there a vector $\mathbf{e} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{e}) \leq w$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

This problem is conjectured to be NP-hard [57] and in [256] it is observed that this problem is not likely to be in NP, since already verifying that any $d-1$ columns are linearly independent is not possible in polynomial time.

There have been attempts [159] to transform the McEliece system in such a way that the underlying problem is closer or even exactly equivalent to the SDP, the actual NP-complete problem. This proposal has been attacked shortly after in [175]. However, using a different framework than the McEliece system, this is actually possible, for example by using the quasi-cyclic framework or the AF system.

We also want to remark here, that the following generalization of the GWCP, i.e., Problem 179, is also NP-complete [256]:

Problem 204. Let \mathbb{F}_q be a finite field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ and $w \in \mathbb{N}$, is there a vector $\mathbf{c} \in \mathbb{F}_q^n$ such that $\text{wt}_H(\mathbf{c}) \leq w$ and $\mathbf{c}\mathbf{H}^\top = \mathbf{0}_{n-k}$?

In [256] this problem was called the minimum distance problem, since if one could solve the above problem, then by running such solver on $w \in \{1, \dots, n\}$ until an affirmative answer is found, this would return the minimum distance of a code.

However, this does not mean that finding the minimum distance of a random code is NP-complete. In fact, with the above problem one can prove the NP-hardness of finding the minimum distance, but it is unlikely to be in NP, since in order to check whether a candidate solution d really is the minimum distance of the code, one would need to go through (almost) all codewords.

5.2.2 Code Equivalence Problems

Recall the different code equivalence problems, namely PEP, LEP, PKP and relaxed PKP:

Problem 205 (Permutation Equivalence Problem (PEP)). Given $\mathbf{G}, \mathbf{G}' \in \mathbb{F}_q^{k \times n}$, find $\varphi \in S_n$, such that $\varphi(\langle \mathbf{G} \rangle) = \langle \mathbf{G}' \rangle$.

Problem 206 (Linear Equivalence Problem (LEP)). Given $\mathbf{G}, \mathbf{G}' \in \mathbb{F}_q^{k \times n}$, find $\varphi \in (\mathbb{F}_q^*)^n \rtimes S_n$, such that $\varphi(\langle \mathbf{G} \rangle) = \langle \mathbf{G}' \rangle$.

Exercise 207. Show that $\text{PEP} \subset \text{LEP}$, by showing a reduction from PEP to LEP.

Problem 208. Permuted Kernel Problem (PKP) Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{G}' \in \mathbb{F}_q^{k' \times n}$, find permutation matrix \mathbf{P} such that $\langle \mathbf{G}' \rangle \subset \langle \mathbf{GP} \rangle$.

Exercise 209. Show that $\text{PEP} \subset \text{PKP}$.

Problem 210. Relaxed PKP Given $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, $\mathbf{G}' \in \mathbb{F}_q^{k' \times n}$, find $\mathbf{x} \in \mathbb{F}_q^k$ and a permutation matrix \mathbf{P} such that $\mathbf{xGP} \in \langle \mathbf{G}' \rangle$.

Exercise 211. Show that Relaxed PKP \subset PKP.

A graph \mathcal{G} is usually denoted through its vertices V and edges $E \subset V^2$, i.e., we write $\mathcal{G} = (V, E)$. We say that $\mathcal{G} = (V, E)$ with $|V| = v, |E| = e$ has *incidence matrix* $\mathbf{A} \in \mathbb{F}_2^{e \times v}$, if \mathbf{A} has entries $a_{i,j}$ with

$$a_{i,j} = \begin{cases} 1 & \text{if } i = (\ell, j) \in E, \\ 0 & \text{else.} \end{cases}$$

That is the rows correspond to the edges and the columns to the vertices. Considering the edge (a, b) , we set a 1 in the position a and in the position b .

Since we consider undirected graphs, the condition $e = (\ell, j) \in E$ should be read as unordered tuple, i.e., also $e = (j, \ell) \in E$.

Example 212. The graph \mathcal{G} with vertex set $V = \{1, 2, 3, 4\}$ and edge set $E = \{(1, 2), (2, 3), (3, 4)\}$ has incidence matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Clearly, there are different incidence matrices, depending on the ordering of the edges.

As mentioned before, the code equivalence problems have a relation to the Graph Isomorphism problem, which states the following.

Problem 213 (Graph Isomorphism (GI) problem). Given $\mathcal{G} = (V, E), \mathcal{G}' = (V, E')$, find $f : V \rightarrow V$, such that $\{u, v\} \in E \leftrightarrow \{f(u), f(v)\} \in E'$.

Theorem 214. *There exists a reduction from GI to PEP.*

We follow the proof of [213].

Proof. Let $\mathcal{G} = (V, E)$ and $\mathcal{G}' = (V, E')$ be an instance of GI. Let \mathbf{D} and \mathbf{D}' be two incidence matrices for \mathcal{G} , respectively \mathcal{G}' . We can transform this instance to an instance of PEP, by defining the two generator matrices in $\mathbb{F}_q^{e \times (3e+v)}$

$$\begin{aligned} \mathbf{G} &= \begin{pmatrix} \text{Id}_e & \text{Id}_e & \text{Id}_e & \mathbf{D} \end{pmatrix}, \\ \mathbf{G}' &= \begin{pmatrix} \text{Id}_e & \text{Id}_e & \text{Id}_e & \mathbf{D}' \end{pmatrix}. \end{aligned}$$

Let us consider two cases. In the first case, the answer to GI is "yes", as there exists a $f : V \rightarrow V$, such that $\{f(u), f(v)\} \in E'$ for all $\{u, v\} \in E$. Thus, there exists a permutation of V which maps one graph to the other and the two incidence matrices \mathbf{D} and \mathbf{D}' are such that

$$\mathbf{QDP} = \mathbf{D}'$$

for some $e \times e$ permutation matrix \mathbf{Q} and $v \times v$ permutation matrix \mathbf{P} . Clearly, the codes generated by \mathbf{G} and \mathbf{G}' are then also permutation equivalent.

In the second case, we assume that the two graphs are not isomorphic, hence there exists no permutation on V , which maps \mathcal{G} to \mathcal{G}' . Thus, no $v \times v$ permutation matrix \mathbf{P} and no $e \times e$ permutation matrix \mathbf{Q} exists for which $\mathbf{QDP} = \mathbf{D}'$.

The two codes generated by \mathbf{G}_1 and \mathbf{G}_2 are only permutation equivalent, if we can find $\mathbf{S} \in \text{GL}_n(\mathbb{F}_2)$ and $(3e + v) \times (3e + v)$ permutation matrix \mathbf{P} such that

$$\mathbf{SGP} = \begin{pmatrix} \mathbf{S} & \mathbf{S} & \mathbf{S} & \mathbf{SD} \end{pmatrix} \mathbf{P} = \mathbf{G}'.$$

Note that the first $3e$ columns of \mathbf{SG} consist of all unit vectors of length e , each appearing exactly three times. Hence, the first $3e$ columns of \mathbf{G}_2 are obtained by permuting the first $3e$ columns of \mathbf{SG} and thus, we also have the permutation matrix $\mathbf{P} = \text{diag}(\mathbf{S}^{-1}, \mathbf{S}^{-1}, \mathbf{S}^{-1}, \mathbf{T})$, where \mathbf{T} is a $v \times v$ permutation matrix. Hence, if such \mathbf{S}, \mathbf{P} exist, we must have $\mathbf{D}' = \mathbf{SDT}$, which is against the assumption that \mathcal{G} and \mathcal{G}' are not isomorphic. \square

Due to this result, we know that PEP (and thus also LEP) are at least as hard as GI.

Since PKP is a subcode-equivalence problem it is equivalent to the subgraph isomorphism problem and hence NP-complete [96]. However, the hardness of the relaxed version is not known.

Problem 215 (Open Problem). How hard is Relaxed PKP?

Recall that a random code has with high probability a trivial hull, i.e., $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. In [53], it was shown that a random instance of PEP, i.e., for codes with trivial hulls, PEP can be solved by graph isomorphism solvers, thus being at most quasi-polynomial.

For $q \leq 5$ we can reduce any instance of LEP to an instance of PEP which has a trivial hull, and thus LEP for $q \leq 5$ is also at most quasi-polynomial. However, for $q > 5$, we can still reduce LEP to PEP, but we get a self-orthogonal code, i.e., $\mathcal{C} \subset \mathcal{C}^\perp$. In this case it is not clear, whether a reduction to the graph isomorphism problem is possible.

Problem 216 (Open Problem). How hard is LEP for $q > 5$?

Even though it is not clear whether LEP is NP-hard for $q > 5$, it is considered to be hard, as only exponential cost solvers (classical and quantum) are known. Hence, it is a promising candidate for post-quantum cryptography.

We can also consider code equivalence for \mathbb{F}_q -linear codes endowed with the rank metric.

Problem 217 (Matrix Code Equivalence (MCE) Problem). Given $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$ and $\mathbf{G}'_1, \dots, \mathbf{G}'_k \in \mathbb{F}_q^{m \times n}$. Find $\mathbf{A} \in \text{GL}_m(\mathbb{F}_q), \mathbf{B} \in \text{GL}_n(\mathbb{F}_q)$, such that for all $\mathbf{C} \in \langle \mathbf{G}_1, \dots, \mathbf{G}_k \rangle$ we have $\mathbf{ACB} = \mathbf{C}'$ for some $\mathbf{C}' \in \langle \mathbf{G}'_1, \dots, \mathbf{G}'_k \rangle$.

Similar to LEP, the complexity class of MCE has not been determined and is believed to be hard. In fact, there exists a polynomial time reduction from the Hamming code equivalence problem in [99]. A nice summary on MCE can be found in [222].

Problem 218 (Open Problem). How hard is MCE?

5.2.3 Rank SDP

In [132], the authors provide a randomized reduction from the SDP to the Rank SDP. A randomized reduction is a polynomial time reduction, which only works with high probability.

Proposition 219. *There exists a randomized reduction from SDP to Rank SDP.*

Proof. Instead of using the SDP, we use the equivalent GWCP, in both metrics. We start with an instance of GWCP in the Hamming metric, namely $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ and t . Note that the Rank GWCP is only defined over extension fields, \mathbb{F}_{q^m} . Thus, we consider $\alpha \in \mathbb{F}_{q^m}^n$ a vector with \mathbb{F}_q -linearly independent entries.

Exercise 220. Show that for any $\mathbf{x} \in \mathbb{F}_q^n$ of $\text{wt}_H(\mathbf{x}) = t$ the componentwise product $\mathbf{x} \star \alpha \in \mathbb{F}_{q^m}^n$ has rank weight $\text{wt}_R(\mathbf{x} \star \alpha) = t$.

For the code $\mathcal{C} = \langle \mathbf{G} \rangle \subset \mathbb{F}_q^n$, we define $\mathcal{C}' = \langle \{\alpha \star \mathbf{c} \mid \mathbf{c} \in \mathcal{C}\} \rangle \subset \mathbb{F}_{q^m}^n$. Let \mathbf{G}' be a generator matrix of \mathcal{C}' . If the answer to the Hamming GWCP is yes, that is: there exists a $\mathbf{c} \in \mathcal{C}$ of Hamming weight t , then there also exists $\mathbf{c} \star \alpha$ in \mathcal{C}' of rank weight t . However, if there was no $\mathbf{c} \in \mathcal{C}$ of Hamming weight t , note that there might still be a codeword $\mathbf{c}' \in \mathcal{C}'$ of rank weight t , which is not of the form $\mathbf{c} \star \alpha$. In fact, since we are now over the extension field, we have generated many more codewords than simply those of the form $\mathbf{c} \star \alpha$.

With high probability, (details can be found in [132]), the only codewords of rank weight t are of the form $\mathbf{c} \star \alpha$ and thus the reduction works. \square

Example 221. Let us consider

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

which generates the code $\mathcal{C} \subset \mathbb{F}_2^3$. If we let $t = 1$, then clearly there is no codeword in \mathcal{C} of Hamming weight 1. However, for $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ and $\alpha^3 = \alpha + 1$ and the code

$$\mathcal{C}' = \langle \mathbf{c} \star (1, \alpha, \alpha^2 + \alpha + 1) \mid \mathbf{c} \in \mathcal{C} \rangle$$

we do have a codeword of rank weight 1, for example

$$\alpha(1, \alpha, \alpha^2 + \alpha + 1) \star (1, 0, 1) + (1, \alpha, \alpha^2 + \alpha + 1) \star (0, 1, 1) = (\alpha, \alpha, \alpha).$$

It remains one of the largest open problems in code-based cryptography, whether there exists a polynomial time reduction, which always works. That is

Problem 222 (Open Problem). Is the Rank SDP NP-hard?

As opposed to the Rank SDP, considering \mathbb{F}_{q^m} -linear codes endowed with the rank metric, for \mathbb{F}_q -linear codes the SDP is known to be NP-hard.

Theorem 223. *The MinRank Problem is NP-complete.*

Proof. We use a polynomial time reduction from the Hamming DP.

Exercise 224. Let $\mathbf{x} \in \mathbb{F}_q^n$ have Hamming weight t . Show that $\text{diag}(\mathbf{x}) \in \mathbb{F}_q^{n \times n}$ has rank weight t .

We start with an instance $\mathbf{G} = \begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_k \end{pmatrix} \in \mathbb{F}_q^{k \times n}$, $\mathbf{r} \in \mathbb{F}_q^n$ and $t \in \mathbb{N}$. We transform the

instance to a MinRank instance as

$$\mathbf{G}_1 = \text{diag}(\mathbf{g}_1), \dots, \mathbf{G}_k = \text{diag}(\mathbf{g}_k) \in \mathbb{F}_q^{n \times n}$$

and

$$\mathbf{R} = \text{diag}(\mathbf{r}) \in \mathbb{F}_q^{n \times n}.$$

Let us first assume that the Hamming DP instance has “yes” as a solution, i.e., there exists a $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t such that $\mathbf{r} - \mathbf{e} \in \langle \mathbf{G} \rangle$. In other words,

$$\mathbf{r} - \mathbf{e} = \lambda_1 \mathbf{g}_1 + \dots + \lambda_k \mathbf{g}_k$$

for some $\lambda_i \in \mathbb{F}_q$. Then the MinRank instance also has a solution “yes”. In fact, there exists $\mathbf{E} = \text{diag}(\mathbf{e})$ of rank weight t such that

$$\mathbf{R} - \mathbf{E} = \lambda_1 \mathbf{G}_1 + \dots + \lambda_k \mathbf{G}_k,$$

for the same $\lambda_i \in \mathbb{F}_q$. On the other hand, if the Hamming DP instance has “no” as a solution, i.e., there is no $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t , such that $\mathbf{r} - \mathbf{e} = \lambda_1 \mathbf{g}_1 + \dots + \lambda_k \mathbf{g}_k$, then the MinRank instance also gives “no” as a solution. In fact, assume by contradiction, a $\mathbf{E} \in \mathbb{F}_q^{n \times n}$ exists of rank weight t , such that

$$\mathbf{R} - \mathbf{E} = \lambda_1 \mathbf{G}_1 + \dots + \lambda_k \mathbf{G}_k$$

for some $\lambda_i \in \mathbb{F}_q$. Thus, if we denote by g_i^j the i th entry of \mathbf{g}_j , then

$$\begin{pmatrix} r_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & r_n \end{pmatrix} - \mathbf{E} = \lambda_1 \begin{pmatrix} g_1^1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & g_n^1 \end{pmatrix} + \dots + \lambda_k \begin{pmatrix} g_1^k & \dots & 0 \\ & \ddots & \\ 0 & \dots & g_n^k \end{pmatrix}.$$

Hence,

$$\mathbf{E} = \begin{pmatrix} r_1 - \sum_{i=1}^k \lambda_i g_1^i & \dots & 0 \\ & \ddots & \\ 0 & \dots & r_n - \sum_{i=1}^k \lambda_i g_n^i \end{pmatrix}.$$

Hence \mathbf{E} is again a diagonal matrix and we can denote its diagonal by \mathbf{e} . In order for \mathbf{E} to have rank weight t , we need that t many entries of \mathbf{e} are non-zero. Hence there exists a $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t , such that $e_j = r_j - \sum_{i=1}^k \lambda_i g_j^i$, i.e., $\mathbf{e} = \mathbf{r} - \sum_{i=1}^k \lambda_i \mathbf{g}_i$, which is a contradiction. \square

The natural question arises, why one cannot prove the NP-hardness of Rank SDP using the MinRank problem. In fact, starting with an instance of Rank SDP, i.e., an \mathbb{F}_{q^m} -linear code, one can always define the corresponding \mathbb{F}_q -linear code. However, for the polynomial time reduction from MinRank to Rank SDP, the other direction is needed. That is, starting with an instance of MinRank, transforming it to an instance of Rank SDP - and this already fails, as not all \mathbb{F}_q -linear codes can be lifted to an \mathbb{F}_{q^m} -linear code.

5.2.4 Lee SDP

Problem 225 (Lee SDP). Let \mathbb{F}_p be a prime field and $k \leq n$ be positive integers. Given $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$ and $t \in \mathbb{N}$, is there a vector $\mathbf{e} \in \mathbb{F}_p^n$ such that $\text{wt}_L(\mathbf{e}) \leq t$ and $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$?

The Lee SDP (again equivalent to Lee DP and Lee GWCP) has been proven to be NP-complete in [263]. Since the proof follows exactly in the same manner as the reduction for Hamming SDP, we leave it as an exercise.

Exercise 226. Show that Lee SDP is NP-complete using a reduction from 3DM.

5.2.5 Restricted SDP

The Restricted Syndrome Decoding Problem (R-SDP), first introduced in [41], reads as follows.

Problem 227 (Restricted SDP). Given $g \in \mathbb{F}_p^*$ of prime order z , $\mathbf{H} \in \mathbb{F}_p^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_p^{n-k}$, and $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$, decide if there exists $\mathbf{e} \in \mathbb{F}_p^n$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

The Restricted SDP is strongly related to other well-known hard problems. For example, when $z = p - 1$, the Restricted SDP is close to the classical SDP; if $z = 1$, the Restricted SDP is similar to the Subset Sum Problem (SSP) over finite fields. Consequently, it is unsurprising that the R-SDP is NP-complete for any choice of \mathbb{E} .

Theorem 228. *The Restricted SDP is NP-complete.*

The proof is again similar to the reduction provided for the SDP.

Proof. Recall the NP-hard 3-Dimensional Matching (3DM) problem, where one is given the instance $T = \{b_1, \dots, b_t\}$, with $|T| = t$, $U \subset T \times T \times T$ and $|U| = u$ and asks whether there exists a $W \subset U$ with $|W| = t$ and no two words in W coincide in any position.

Recall that the original SDP has a reduction from 3DM, through the following construction: let $\mathbf{H} \in \mathbb{F}_p^{(3t) \times u}$ be the incidence matrix, i.e., each column of \mathbf{H} corresponds to a word in U and the rows correspond to $T \times T \times T$, thus the rows $\{1, \dots, t\}$ correspond to the first position of the word \mathbf{u} , the rows $\{t+1, \dots, 2t\}$ correspond to the second position of \mathbf{u} and the rows $\{2t+1, \dots, 3t\}$ correspond to the third position of \mathbf{u} . More formally, let $T = \{b_1, \dots, b_t\}$, $U = \{\mathbf{a}_1, \dots, \mathbf{a}_u\}$ and

- for $j \in \{1, \dots, t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[1] = b_j$ and $h_{i,j} = 0$ else,
- for $j \in \{t+1, \dots, 2t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[2] = b_j$ and $h_{i,j} = 0$ else,
- for $j \in \{2t+1, \dots, 3t\}$, we set $h_{i,j} = 1$ if $\mathbf{a}_i[3] = b_j$ and $h_{i,j} = 0$ else.

We also set $\mathbf{s} \in \mathbb{F}_p^{3t}$ be the all one vector.

From the original reduction, we know that any solution $\mathbf{e} \in \mathbb{F}_p^u$ with $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$ has weight t and its support corresponds to the solution W . That is the columns of \mathbf{H} indexed by the support of \mathbf{e} are the t words in W .

The polynomial reduction from 3DM to R-SDP uses this construction as well. Let T of size t and $U \subset T \times T \times T$ of size u be an instance of 3DM. Let $\mathbf{H} \in \mathbb{F}_p^{(3t) \times u}$ be the incidence matrix and let

$$\tilde{\mathbf{H}} = \begin{pmatrix} \mathbf{H} & -g \star \mathbf{H} \\ \text{Id}_u & \text{Id}_u \end{pmatrix} \in \mathbb{F}_p^{(3t+u) \times 2u}$$

be a parity-check matrix. Let us consider the syndrome $(\mathbf{s}, \mathbf{s}') \in \mathbb{F}_p^{3t+u}$ with $\mathbf{s} = (1-g^2, \dots, 1-g^2) \in \mathbb{F}_p^{3t}$ and $\mathbf{s}' = (1+g, \dots, 1+g) \in \mathbb{F}_p^u$. Thus, the instance of R-SDP given by $\tilde{\mathbf{H}}$ and $(\mathbf{s}, \mathbf{s}')$ is asking for $(\mathbf{e}, \mathbf{e}') \in \mathbb{E}^{2u}$ such that

$$(\mathbf{e}, \mathbf{e}') \tilde{\mathbf{H}}^\top = (\mathbf{s}, \mathbf{s}'),$$

where $\mathbb{E} = \{g^i \mid i \in \{0, \dots, z-1\}\}$. By assumption of R-SDP, we use a g of order $2 < z < q-1$. We consider two cases.

1. Assume that the R-SDP solver returns “yes”, i.e., there exists $\mathbf{e}, \mathbf{e}' \in \mathbb{E}^u$ such that $(\mathbf{e}, \mathbf{e}') \tilde{\mathbf{H}}^\top = (\mathbf{s}, \mathbf{s}')$. Hence,

$$\begin{aligned} \mathbf{H}\mathbf{e}^\top - g \star \mathbf{H}\mathbf{e}'^\top &= (1-g^2, \dots, 1-g^2)^\top, \\ \mathbf{e} + \mathbf{e}' &= (1+g, \dots, 1+g). \end{aligned}$$

Hence, for each $i \in \{1, \dots, u\}$ we have $e_i + e'_i = 1+g$. Let us assume (we later show that this hypothesis is not needed, but it facilitates the proof) that the only elements in \mathbb{E} that add to $1+g$ is 1 and g .

Hence, whenever $e_i = 1$, we must have $e'_i = g$ and whenever $e_i = g$, we must have $e'_i = 1$. Thus, we split $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_g$ and $\mathbf{e}' = \mathbf{e}'_1 + \mathbf{e}'_g$ where $\mathbf{e}_1, \mathbf{e}'_1 \in \{0, 1\}^u$, $\mathbf{e}_g, \mathbf{e}'_g \in \{0, g\}^u$ and

$$\text{supp}(\mathbf{e}_1) = S = \text{supp}(\mathbf{e}'_g)$$

and

$$\text{supp}(\mathbf{e}'_1) = S^C = \text{supp}(\mathbf{e}_g).$$

From this also follows that

$$\mathbf{e}_g = g \star \mathbf{e}'_1$$

and

$$\mathbf{e}'_g = g \star \mathbf{e}_1.$$

The first parity-check equation can now be reformulated as

$$\begin{aligned} &\mathbf{H}\mathbf{e}^\top - g \star \mathbf{H}\mathbf{e}'^\top \\ &= \mathbf{H}\mathbf{e}_1^\top - g \star \mathbf{H}\mathbf{e}'_g^\top + \mathbf{H}\mathbf{e}_g^\top - g \star \mathbf{H}\mathbf{e}'_1^\top \\ &= \mathbf{H}\mathbf{e}_1^\top - g^2 \star \mathbf{H}\mathbf{e}_1^\top + g \star \mathbf{H}\mathbf{e}'_1^\top - g \star \mathbf{H}\mathbf{e}'_1^\top \\ &= (1-g^2) \star \mathbf{H}\mathbf{e}_1^\top \\ &= (1-g^2, \dots, 1-g^2) = \mathbf{s}', \end{aligned}$$

thus, $\mathbf{H}\mathbf{e}_1^\top = (1, \dots, 1)$ is such that $\text{supp}(\mathbf{e}_1)$ corresponds to a solution W of 3DM, as in the classical reduction.

2. Assume that the R-SDP solver returns “no”, i.e., there exists no $\mathbf{e}, \mathbf{e}' \in \mathbb{E}^u$ such that $(\mathbf{e}, \mathbf{e}') \tilde{\mathbf{H}}^\top = (\mathbf{s}, \mathbf{s}')$. Let us assume by contradiction, that the 3DM has a solution W . We can then define S to be the indices of words in U belonging to the solution W . Let us define $\mathbf{e}_1, \mathbf{e}'_1 \in \{0, 1\}^u$, $\mathbf{e}_g, \mathbf{e}'_g \in \{0, g\}^u$ with $\text{supp}(\mathbf{e}_1) = S = \text{supp}(\mathbf{e}'_g)$ and $\text{supp}(\mathbf{e}'_1) = S^C = \text{supp}(\mathbf{e}_g)$. From this also follows that $\mathbf{e}_g = g \star \mathbf{e}'_1$ and $\mathbf{e}'_g = g \star \mathbf{e}_1$. Then the vector $(\mathbf{e}_1 + \mathbf{e}_g, \mathbf{e}'_1 + \mathbf{e}'_g) \in \mathbb{E}^{2u}$ is a solution to the R-SDP, as in case 1, which gives the desired contradiction, to the R-SDP solver returning “no”.

Note that the hypothesis, that only 1 and g in \mathbb{E} add up to $1 + g$ is not necessary. For this assume that there exists $g^i, g^j \in \mathbb{E}$, with $0 \neq i < j < z$ such that $g^i + g^j = 1 + g$. Thus, the splitting of \mathbf{e} and \mathbf{e}' is a bit more complicated:

$$\begin{aligned}\mathbf{e} &= \mathbf{e}_1 + \mathbf{e}_g + \mathbf{e}_i + \mathbf{e}_j, \\ \mathbf{e}' &= \mathbf{e}'_1 + \mathbf{e}'_g + \mathbf{e}'_i + \mathbf{e}'_j,\end{aligned}$$

where $\mathbf{e}_1, \mathbf{e}'_1 \in \{0, 1\}^u, \mathbf{e}_g, \mathbf{e}'_g \in \{0, g\}^u, \mathbf{e}_i, \mathbf{e}'_i \in \{0, g^i\}^u, \mathbf{e}_j, \mathbf{e}'_j \in \{0, g^j\}^u$ with

$$\begin{aligned}\text{supp}(\mathbf{e}_1) &= S_1 = \text{supp}(\mathbf{e}'_g), \\ \text{supp}(\mathbf{e}_g) &= S'_1 = \text{supp}(\mathbf{e}'_1), \\ \text{supp}(\mathbf{e}_i) &= S_i = \text{supp}(\mathbf{e}'_j), \\ \text{supp}(\mathbf{e}_j) &= S'_i = \text{supp}(\mathbf{e}'_i),\end{aligned}$$

and the supports S_1, S'_1, S_i, S'_i are distinct and partition $\{1, \dots, u\}$. Again it follows that

$$\begin{aligned}\mathbf{e}_g &= g \star \mathbf{e}'_1, \\ \mathbf{e}'_g &= g \star \mathbf{e}_1, \\ \mathbf{e}_j &= g^{j-i} \star \mathbf{e}'_i, \\ \mathbf{e}'_j &= g^{j-i} \star \mathbf{e}_i.\end{aligned}$$

Thus, rewriting the first parity-check equation, we get

$$\begin{aligned}& \mathbf{H}\mathbf{e}^\top - g \star \mathbf{H}\mathbf{e}'^\top \\ &= \mathbf{H}\mathbf{e}_1^\top + \mathbf{H}\mathbf{e}_g^\top + \mathbf{H}\mathbf{e}_i^\top + \mathbf{H}\mathbf{e}_j^\top \\ & \quad - g \star \mathbf{H}\mathbf{e}'_1^\top - g \star \mathbf{H}\mathbf{e}'_g^\top - g \star \mathbf{H}\mathbf{e}'_i^\top - g \star \mathbf{H}\mathbf{e}'_j^\top \\ &= \mathbf{H}\mathbf{e}_1^\top + g \star \mathbf{H}\mathbf{e}'_1^\top + \mathbf{H}\mathbf{e}_i^\top + g^{j-i} \star \mathbf{H}\mathbf{e}'_i^\top \\ & \quad - g \star \mathbf{H}\mathbf{e}'_1^\top - g^2 \star \mathbf{H}\mathbf{e}_1^\top - g \star \mathbf{H}\mathbf{e}'_i^\top - g^{j-i+1} \star \mathbf{H}\mathbf{e}_i^\top \\ &= (1 - g^2) \star \mathbf{H}\mathbf{e}_1^\top + (1 - g^{j-i+1}) \star \mathbf{H}\mathbf{e}_i^\top + (g^{j-i} - g) \star \mathbf{H}\mathbf{e}'_i^\top \\ &= (1 - g^2, \dots, 1 - g^2) = \mathbf{s}'.\end{aligned}$$

Since $\mathbf{e}_1, \mathbf{e}_i, \mathbf{e}'_i$ all have different supports, the only way to get $1 - g^2$ in each entry, is to have $\mathbf{e}_i = \mathbf{e}'_i = 0$. In fact, any other sum leads to a contradiction:

- If $(1 - g^2) + (1 - g^{j-i+1}) = 1 - g^2$ then $1 = g^{j-i+1}$ and hence $j = i - 1$ which contradicts $j > i$.
- If $(1 - g^2) + (g^{j-i} - g) = 1 - g^2$ then $g^{j-i} = g$ and hence $j - i = 1$. However, as then $g^j + g^i = g^i(1 + g) = 1 + g$, it follows that $g^i = 1$, which contradicts $i \neq 0$.
- If $(1 - g^2) + (1 - g^{j-i+1}) + (g^{j-i} - g) = 1 - g^2$, then $1 + g^{j-i} = g^{j-i+1} + g = g(1 + g^{j-i})$ and thus $g = 1$, which contradicts $\mathbb{E} \neq \mathbb{F}_q^\star$.
- If $(1 - g^{j-i+1}) + (g^{j-i} - g) = 1 - g^2$, then $g^{j-i} - g^{j-i+1} = g - g^2$ and hence $g^{j-i}(1 - g) = g(1 - g)$ and thus $j - i = 1$, which is a contradiction again as in the second case.

□

5.3 Information Set Decoding

In this section we cover the main approach to solve the SDP, namely information set decoding (ISD) algorithms. For this we will follow closely [262].

In the McEliece and the Niederreiter framework the secret code is usually endowed with a particular algebraic structure to guarantee the existence of an efficient decoding algorithm and is then hidden from the public to appear as a random code. In different frameworks, such as the quasi-cyclic framework, the secret is actually purely the error vector and the algebraic code is made public. In both cases an adversary has to solve the NP-complete problem of decoding a random linear code.

An adversary would hence use the best generic decoding algorithm for random linear codes. Two main methods are known until today for decoding random linear codes: ISD and the generalized birthday algorithm (GBA). ISD algorithms are more efficient if the decoding problem has only a small number of solutions, whereas GBA is more efficient when there are many solutions. Also other ideas such as statistical decoding [12], gradient decoding [30] and supercode decoding [56] have been proposed but fail to outperform ISD algorithms.

ISD algorithms are an important aspect of code-based cryptography since they predict the key size achieving a given security level. ISD algorithms should not be considered as attacks in the classical sense, as they are not breaking a code-based cryptosystem, instead they determine the choice of parameters for a given security level.

Due to the duality of the decoding problem and the SDP also ISD algorithms can be formulated through the generator matrix or the parity-check matrix. Throughout this survey, we will stick to the parity-check matrix formulation.

The first ISD algorithm was proposed in 1962 by Prange [216] and interestingly, all improvements display the same structure: choose an information set, use Gaussian elimination to bring the parity-check matrix in a standard form, assuming a certain weight distribution on the error vector, we can go through smaller parts of the error vector and check if the parity-check equations are satisfied. The assumed weight distribution of the error vector thus constitutes the main part of an ISD algorithm.

In an ISD algorithm we fix a weight distribution and go through all information sets to find an error vector of this weight distribution. This is in contrast to ‘brute-force attacks’ where one fixes an information set and goes through all weight distributions of the error vector. In fact, due to this, ISD algorithms are in general not deterministic, since there are instances for which there exists no information set where the error vector has the sought after weight distribution. Clearly, a brute-force algorithm requires much more binary operations than an ISD algorithm, thus, in practice we only consider ISD algorithms.

For this section we will need to recall some notation: let $S \subseteq \{1, \dots, n\}$ be a set of size s , then for a vector $\mathbf{x} \in \mathbb{F}_q^n$ we denote by \mathbf{x}_S the vector of length s consisting of the entries of \mathbf{x} indexed by S . Whereas, for a matrix $\mathbf{A} \in \mathbb{F}_q^{k \times n}$, we denote by \mathbf{A}_S the matrix consisting of the columns of \mathbf{A} indexed by S . For a set S we denote by S^C its complement. For $S \subseteq \{1, \dots, n\}$ of size s we denote by $\mathbb{F}_q^n(S)$ the vectors in \mathbb{F}_q^n having support in S . The projection of $\mathbf{x} \in \mathbb{F}_q^n(S)$ to \mathbb{F}_q^s is then canonical and denoted by $\pi_S(\mathbf{x})$. On the other hand, we denote by $\sigma_S(\mathbf{x})$ the canonical embedding of a vector $\mathbf{x} \in \mathbb{F}_q^s$ to $\mathbb{F}_q^n(S)$.

5.3.1 General Algorithm

We are given a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ of a code \mathcal{C} , a positive integer t and a syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$, such that there exists a vector $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight less than or equal to t with syndrome \mathbf{s} , i.e., $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$. The aim of the algorithm is to find such a vector \mathbf{e} .

1. Find an information set $I \subset \{1, \dots, n\}$ of size k for \mathcal{C} .
2. Bring \mathbf{H} into the systematic form corresponding to I , i.e., find an invertible matrix $\mathbf{U} \in \mathbb{F}_q^{(n-k) \times (n-k)}$, such that $(\mathbf{UH})_I = \mathbf{A}$, for some $\mathbf{A} \in \mathbb{F}_q^{(n-k) \times k}$ and $(\mathbf{UH})_{I^c} = \text{Id}_{n-k}$.
3. Go through all error vectors $\mathbf{e} \in \mathbb{F}_q^n$ having the assumed weight distribution (and in particular having Hamming weight t).
4. Check if the parity-check equations, i.e., $\mathbf{e}\mathbf{H}^\top \mathbf{U}^\top = \mathbf{s}\mathbf{U}^\top$ are satisfied.
5. If they are satisfied, output \mathbf{e} , if not start over with a new choice of I .

Since the iteration above has to be repeated several times, the cost of such algorithm is given by the cost of one iteration times the number of required iterations.

Clearly, the average number of iterations required is given as the reciprocal of the success probability of one iteration and this probability is completely determined by the assumed weight distribution.

5.3.2 Overview Algorithms

The first ISD algorithm was proposed in 1962 by Prange [216] and is sometimes referred to as plain ISD. In this algorithm Prange makes use of an information set of a code, that in fact contains all the necessary information to decode, in a clever way. For this we have to assume that there is an information set where the error vector has weight 0 (thus all t errors are outside of this information set). One now only has to bring the parity-check matrix into systematic form according to this information set, which has a polynomial cost, this is called an iteration of the algorithm. However, one has to find such an information set first. This is done by trial and error, which results in a large number of iterations. Indeed, the assumption that no errors happen in the information set is not very likely and thus the success probability of one iteration is very low.

All the improvements that have been suggested to Prange's simplest form of ISD (see for example [82, 84, 83, 116, 170, 181, 255]) assume a more likely weight distribution of the error vector, which results in a higher cost of one iteration but give overall a smaller cost, since less iterations have to be performed.

The improvements split into two directions: the first direction is following the idea of Lee and Brickell [178] where they ask for v errors in the information set and $t - v$ outside. The second direction is Dumer's approach [116], 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. Clearly, the second direction includes the first direction by setting $\ell = 0$.

Following the first direction, Leon [181] generalizes Lee-Brickell's algorithm by introducing a set of size ℓ outside the information set called zero-window, where no errors happen. In 1988, Stern [248] adapted the algorithm by Leon and proposed to partition the information

set into two sets and ask for v errors in each part and $t - 2v$ errors outside the information set (and outside the zero-window). In 2010, with the rise of code-based cryptography over a general finite field \mathbb{F}_q , Peters generalized these algorithms to \mathbb{F}_q [212].

In 2011, Bernstein, Lange and Peters proposed the ball-collision algorithm [72], where 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. This algorithm and its speed-up techniques were then generalized to \mathbb{F}_q by Interlando, Khathuria, Rohrer, Rosenthal and Weger in [157]. In 2016, Hirose [152] generalized the nearest neighbor algorithm over \mathbb{F}_q and applied it to the generalized Stern algorithm.

An illustration of these algorithms is given in Figure 2, where we assume for simplicity that the information set is in the first k positions and the zero-window is in the adjacent ℓ positions.

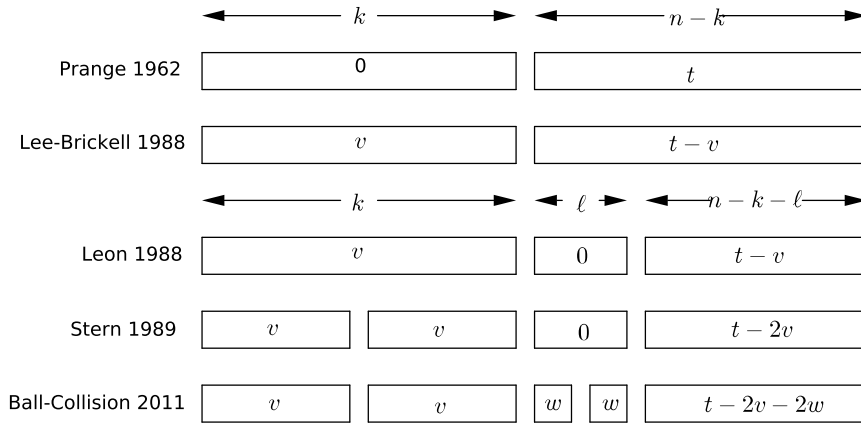


Figure 2: Overview of algorithms following the splitting of Lee-Brickell, adapted from [72].

The second direction has resulted in many improvements, for example in 2009 Finiasz and Sendrier [122] 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 [203] in 2010 improved the performance of ISD algorithms over \mathbb{F}_q based on the idea of Finiasz and Sendrier.

In 2011, May, Meurer and Thomae [191] proposed the use of the representation technique introduced by Howgrave-Graham and Joux [156] for the subset sum problem. Further improvements have been proposed by Becker, Joux, May and Meurer [60] in 2012 by introducing overlapping supports. We will refer to this algorithm as BJMM. In 2015, May-Ozerov [192] used the nearest neighbor algorithm to improve BJMM and finally in 2017, the nearest neighbor algorithm over \mathbb{F}_q was applied to the generalized BJMM algorithm by Gueye, Klamti and Hirose [149].

These new approaches do not use set partitions of the support but rather a sum partition of the weight. An illustration of these algorithms is given in Figure 3, where we again assume that the $k + \ell$ bits containing an information set are in the beginning. The overlapping sets

are denoted by X_1 and X_2 and their intersection of size $2\alpha(k + \ell)$ is in blue. The amount of errors within the intersection is denoted by δ .

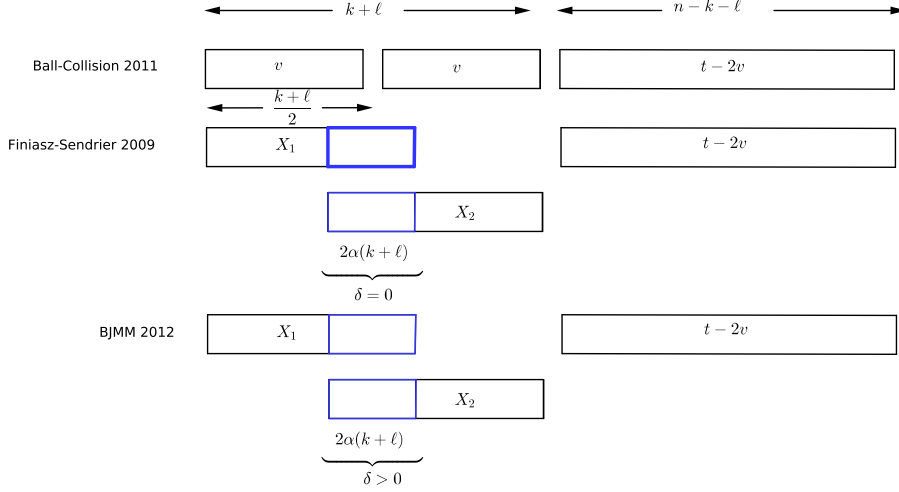


Figure 3: Overview of the weight splitting in the different algorithms.

A very introductory reading on ISD algorithms is in the thesis of Weger [262], which we also follow closely and for binary ISD algorithms, a very informative reading is the thesis of Meurer [195].

It is important to remark (see [195]) that the BJMM algorithm, even if having the smallest complexity until today, 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} (which is a reasonable restriction), BJMM and the ball-collision algorithm are performing almost the same.

What is the possible impact on the cost of ISD algorithms when using a capable quantum computer? In [68] the authors expect that quantum computers result in a square root speed up for ISD algorithms, since Grover's search algorithm [146, 147] needs only $O(\sqrt{N})$ operations to find an element in a set of size N , instead of $O(N)$ many. Thus, intuitively, the search of an information set will become faster and thus the number of iterations needed in an ISD algorithm will decrease.

Since all the improvements upon Prange's algorithm were only focusing on decreasing this number of iterations, the speed up for these algorithms will be smaller, than for the original algorithm by Prange. Hence the authors predict that on a capable quantum computer Prange's algorithm will result as the fastest.

5.3.3 Techniques

In the following we introduce some speed-up techniques for ISD algorithms, mostly introduced in [72] over \mathbb{F}_2 and later generalized to \mathbb{F}_q in [157].

First of all, we want to fix the cost that we consider throughout this chapter of one addition and one multiplication over \mathbb{F}_q , i.e., we assume that one addition over \mathbb{F}_q costs $\lceil \log_2(q) \rceil$ binary operations and one multiplication costs $\lceil \log_2(q) \rceil^2$ binary operations. The cost of the multiplication is clearly not using the fastest algorithm known but will be good enough for our purposes. Also for the cost of multiplying two matrices we will always stick to a broad estimate given by school book long multiplication, i.e., multiplying \mathbf{AB} , where $\mathbf{A} \in \mathbb{F}_q^{k \times n}$ and $\mathbf{B} \in \mathbb{F}_q^{n \times r}$ will cost $nkr \left(\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2 \right)$ binary operations.

Number of Iterations One of the main parts in the cost of an information set decoding algorithm is the *average number of iterations* needed. This number depends on the success probability of one iteration. In turn, the success probability is completely given by the assumed weight distribution of the error vector. Since in one iteration we consider a fixed information set, the success probability of an iteration is given by the fraction of how many vectors there are with the assumed weight distribution, divided by how many vectors there are in general with the target weight t .

Example 229. For example, we are looking for $\mathbf{e} \in \mathbb{F}_q^n$ of Hamming weight t , and we assume that the error vector has no errors inside an information set I , and thus all t errors appear in I^C of size $n - k$. Since there are $\binom{n-k}{t}(q-1)^t$ many vectors having support of size t in a set of size $n - k$ and the total number of vectors of support t in a set of size n is given by $\binom{n}{t}(q-1)^t$, we have that the success probability of one iteration is given by

$$\binom{n-k}{t} \binom{n}{t}^{-1},$$

and hence the number of iterations needed on average is given by

$$\binom{n-k}{t}^{-1} \binom{n}{t}.$$

Early Abort In some of the algorithms we have to perform a computation and the algorithm only proceeds if the result of this computation satisfies a certain condition. In our case, the condition is that the weight of the resulting vector does not exceed a target weight.

We thus compute one entry of the result and check the weight of this entry, before proceeding to the next entry. As soon as the weight of the partially computed vector is above the target weight, we can stop the computation, hence the name *early abort*.

Example 230. To provide an example also for this technique, assume that we have to compute \mathbf{xA} , for $\mathbf{x} \in \mathbb{F}_q^k$ of Hamming weight t and $\mathbf{A} \in \mathbb{F}_q^{k \times n}$. Usually computing \mathbf{xA} would cost $nt \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$ binary operations.

However, assuming our algorithm only proceeds if $\text{wt}_H(\mathbf{xA}) = w$, we can use the method of early abort, i.e., computing one entry of the resulting vector and checking its weight simultaneously. For this we assume that the resulting vector is uniformly distributed. Since we are over \mathbb{F}_q , the probability that an entry adds to the weight of the full vector is given

by $\frac{q-1}{q}$. Hence we can expect that after computing $\frac{q}{q-1}w$ entries the resulting vector should have reached the weight w , and after computing $\frac{q}{q-1}(w+1)$ entries we should have exceeded the target weight w and can abort. Since computing only one entry of the resulting vector costs $t \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$ binary operations, the cost of this step is given by

$$\frac{q}{q-1}(w+1)t \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$$

binary operations, instead of

$$nt \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right).$$

Clearly, this is a speed up, whenever $\frac{q}{q-1}(w+1) < n$.

Number of Collisions In some algorithms we want to check if a certain condition is verified and only then we would proceed. This condition depends on two vectors \mathbf{x} and \mathbf{y} living in some sets S , respectively T . Hence the algorithm would go through all the vectors $\mathbf{x} \in S$ and then through all the vectors $\mathbf{y} \in T$ in their respective sets and check if the condition is satisfied for a fixed pair (\mathbf{x}, \mathbf{y}) . If this is the case, such a pair is called a *collision*. The subsequent steps of the algorithm would be performed on all the collisions, thus multiplying the cost of these steps with the size of the set of all (\mathbf{x}, \mathbf{y}) , i.e., $|S| |T|$.

Instead, we can compute the *average number of collisions* we can expect on average.

Example 231. Let us also give an example for this technique; assume that we only proceed whenever

$$\mathbf{x} + \mathbf{y} = \mathbf{s},$$

for a fixed $\mathbf{s} \in \mathbb{F}_q^k$ and for all $\mathbf{x} \in \mathbb{F}_q^k$ of Hamming weight v and all $\mathbf{y} \in \mathbb{F}_q^k$ of Hamming weight w . To verify this condition we have to go through all possible \mathbf{x} and \mathbf{y} , thus costing

$$\binom{k}{v} \binom{k}{w} (q-1)^{v+w} \min\{k, v+w\} \log_2(q)$$

binary operations. As a subsequent step one would compute for all such (\mathbf{x}, \mathbf{y}) the vector $\mathbf{Ax} - \mathbf{By}$, for some fixed $\mathbf{A} \in \mathbb{F}_q^{n \times k}$ and $\mathbf{B} \in \mathbb{F}_q^{n \times k}$. Usually one would do this for all elements in $S = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^k, \text{wt}_H(\mathbf{x}) = v, \text{wt}_H(\mathbf{y}) = w\}$, giving this step a cost of

$$\binom{k}{v} \binom{k}{w} (q-1)^{v+w} \min\{k, v+w\} n (\log_2(q) + \log_2(q)^2).$$

However, we only have to perform the subsequent steps as many times as on average we expect a collision, i.e., a pair (\mathbf{x}, \mathbf{y}) such that $\mathbf{x} + \mathbf{y} = \mathbf{s}$. Assuming a uniform distribution, this amount is given by

$$\frac{|S|}{q^n} = \frac{\binom{k}{v} \binom{k}{w} (q-1)^{v+w}}{q^n} < \binom{k}{v} \binom{k}{w} (q-1)^{v+w-n}.$$

Thus computing $\mathbf{Ax} - \mathbf{By}$ for all $(\mathbf{x}, \mathbf{y}) \in S$ costs on average

$$\binom{k}{v} \binom{k}{w} (q-1)^{v+w-n} \min\{k, v+w\} n (\log_2(q) + \log_2(q)^2)$$

binary operations, which is clearly less than the previous cost.

Intermediate Sums In some algorithms we have to do a certain computation for all vectors in a certain set. The idea of *intermediate sums* is to do this computation in the easiest case and to use the resulting vector to compute the results for harder cases. This will become clear with an example.

Example 232. Let $\mathbf{A} \in \mathbb{F}_2^{k \times n}$ and assume that we want to compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_2^k$ of Hamming weight t . This would usually cost

$$nt \binom{k}{t}$$

binary operations.

Using the concept of intermediate sums helps to speed up this computation: we first compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_2^k$ of Hamming weight 1, thus just outputting the rows of \mathbf{A} which is for free. As a next step, we compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_2^k$ of Hamming weight 2, which is the same as adding two rows of \mathbf{A} and hence costs $\binom{k}{2}n$ binary operations. As a next step, we compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_2^k$ of Hamming weight 3. This is the same as adding one row of \mathbf{A} to one of the already computed vectors from the previous step, thus this costs $\binom{k}{3}n$ binary operations. If we proceed in this way, until we compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_2^k$ of Hamming weight t , this step costs

$$nL(k, t)$$

binary operations, where

$$L(k, t) = \sum_{i=2}^t \binom{k}{i}.$$

This is a speed up to the previous cost, since

$$n \sum_{i=2}^t \binom{k}{i} = n \left(\binom{k}{2} + \cdots + \binom{k}{t} \right) < nt \binom{k}{t}.$$

When generalizing this result to \mathbb{F}_q , computing \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_q^k$ of Hamming weight 1 does not come for free anymore. Instead we have to compute $\mathbf{A} \cdot \lambda$ for all $\lambda \in \mathbb{F}_q^*$ which costs $kn \lceil \log_2(q) \rceil^2$ binary operations. Further, if we want to compute \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_q^k$ of Hamming weight 2, we have to add two multiples of rows of \mathbf{A} . While there are still $\binom{k}{2}$ many rows, we now have $(q-1)^2$ multiples. Thus, this step costs $\binom{k}{2}(q-1)^2 n \lceil \log_2(q) \rceil$ binary operations. Proceeding in this way, the cost of computing \mathbf{xA} for all $\mathbf{x} \in \mathbb{F}_q^k$ of Hamming weight t , is given by

$$L_q(k, t) n \lceil \log_2(q) \rceil + kn \lceil \log_2(q) \rceil^2$$

binary operations, where

$$L_q(k, t) = \sum_{i=2}^t \binom{k}{i} (q-1)^i.$$

Which is clearly less than the previous cost of

$$\binom{k}{t} (q-1)^t nt \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$$

binary operations.

5.3.4 Prange's Algorithm

In Prange's algorithm we assume that there exists an information set I that is disjoint to the support of the error vector $\text{supp}(\mathbf{e})$, i.e.,

$$I \cap \text{supp}(\mathbf{e}) = \emptyset.$$

Of course, such an assumption comes with a probability whose reciprocal defines how many iterations are needed on average if the algorithm ends. Note that Prange's algorithm is not deterministic, i.e., there are instances which Prange's algorithm can not solve. For an easy example, one can just take an instance where $\text{wt}_H(\mathbf{e}) = t > n - k = |I^C|$. For a more elaborate example, which also allows unique decoding, assume that we have a parity-check matrix, which is such that each information set includes the first position. Then an error vector with non-zero entry in the first position could never be found through Prange's algorithm.

To illustrate the algorithm, let us assume that the information set is $I = \{1, \dots, k\}$, and let us denote by $J = I^C$. To bring the parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$ into systematic form, we multiply by an invertible matrix $\mathbf{U} \in \mathbb{F}_q^{(n-k) \times (n-k)}$. Since we assume that no errors occur in the information set, we have that $\mathbf{e} = (\mathbf{0}_k, \mathbf{e}_J)$ with $\text{wt}_H(\mathbf{e}_J) = t$. We are in the following situation:

$$\mathbf{e}\mathbf{H}^\top \mathbf{U}^\top = \begin{pmatrix} \mathbf{0}_k & \mathbf{e}_J \end{pmatrix} \begin{pmatrix} \mathbf{A}^\top \\ \text{Id}_{n-k} \end{pmatrix} = \mathbf{s}\mathbf{U}^\top,$$

for $\mathbf{A} \in \mathbb{F}_q^{(n-k) \times k}$.

It follows that $\mathbf{e}_J = \mathbf{s}\mathbf{U}^\top$ and hence we are only left with checking the weight of $\mathbf{s}\mathbf{U}^\top$.

We will now give the algorithm of Prange in its full generality, i.e., we are not restricting to the choice of I and J that we made before for simplicity.

Algorithm 1 Prange's Algorithm over \mathbb{F}_q in the Hamming metric

Input: $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $t \in \mathbb{N}$.

Output: $\mathbf{e} \in \mathbb{F}_q^n$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and $\text{wt}_H(\mathbf{e}) = t$.

- 1: Choose an information set $I \subset \{1, \dots, n\}$ of size k and define $J = I^C$.
- 2: Compute $\mathbf{U} \in \mathbb{F}_q^{(n-k) \times (n-k)}$, such that

$$(\mathbf{U}\mathbf{H})_I = \mathbf{A} \quad \text{and} \quad (\mathbf{U}\mathbf{H})_J = \text{Id}_{n-k},$$

where $\mathbf{A} \in \mathbb{F}_q^{(n-k) \times k}$.

- 3: Compute $\mathbf{s}' = \mathbf{s}\mathbf{U}^\top$.
 - 4: **if** $\text{wt}_H(\mathbf{s}') = t$ **then**
 - 5: Return \mathbf{e} such that $\mathbf{e}_I = \mathbf{0}_k$ and $\mathbf{e}_J = \mathbf{s}'$.
 - 6: Start over with Step 1 and a new selection of I .
-

Theorem 233. *Prange's algorithm over \mathbb{F}_q requires on average*

$$\binom{n-k}{t}^{-1} \binom{n}{t} (n-k)^2 (n+1) \left(\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2 \right)$$

binary operations.

Proof. One iteration of Algorithm 1 only consists of bringing \mathbf{H} into systematic form and applying the same row operations on the syndrome; thus, the cost can be assumed equal to that of computing $\mathbf{U} \begin{pmatrix} \mathbf{H} & \mathbf{s}^\top \end{pmatrix}$, i.e.,

$$(n-k)^2 (n+1) (\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2)$$

binary operations.

The success probability is given by having chosen the correct weight distribution of \mathbf{e} . In this case, we require that no errors happen in the chosen information set, hence the probability is given by

$$\binom{n-k}{t} \binom{n}{t}^{-1}.$$

Then, the estimated overall cost of Prange's ISD algorithm over \mathbb{F}_q is given as in the claim. \square

Let us consider an example for Prange's algorithm.

Example 234. Over \mathbb{F}_5 , we are given

$$\mathbf{H} = \begin{pmatrix} 3 & 2 & 1 & 4 & 3 & 0 & 4 & 4 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 & 2 & 3 & 2 & 4 & 2 \\ 3 & 0 & 3 & 1 & 4 & 0 & 2 & 2 & 0 & 0 \\ 2 & 3 & 0 & 2 & 3 & 1 & 4 & 4 & 3 & 0 \\ 0 & 2 & 3 & 0 & 2 & 0 & 3 & 4 & 2 & 4 \\ 2 & 3 & 4 & 0 & 2 & 2 & 0 & 0 & 1 & 2 \end{pmatrix},$$

$\mathbf{s} = (2, 4, 0, 2, 0, 4)$ and $t = 2$. We start by choosing an information set, since $I_1 = \{1, 2, 3, 4\}$ is not an information set, our first choice might be $I_2 = \{1, 2, 3, 5\}$. As a next step we compute \mathbf{U} to get \mathbf{H} into systematic form. For this information set we have that

$$\mathbf{U}_2 \mathbf{H} = \begin{pmatrix} 3 & 4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 3 & 0 & 4 & 1 & 0 & 0 & 0 & 0 \\ 4 & 4 & 2 & 0 & 4 & 0 & 1 & 0 & 0 & 0 \\ 1 & 4 & 4 & 0 & 3 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We apply the same on the syndrome, getting

$$\mathbf{s}'_2 = \mathbf{s}\mathbf{U}_2^\top = (3, 2, 4, 3, 4, 1),$$

which is now unfortunately not of Hamming weight 2. Thus, we have to choose another information set. This procedure repeats until the chosen information set succeeds. For example for $I = \{7, 8, 9, 10\}$. In fact, if we now compute the systematic form we get

$$\mathbf{U}\mathbf{H} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 4 & 2 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 4 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 3 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 4 & 3 \end{pmatrix}$$

and $\mathbf{s}' = \mathbf{s}\mathbf{U}^\top = (2, 0, 0, 4, 0, 0)$, which has Hamming weight 2. Thus,

$$\mathbf{e} = (\mathbf{s}', \mathbf{0}) = (2, 0, 0, 4, 0, 0, 0, 0, 0, 0).$$

5.3.5 Stern's Algorithm

Stern's algorithm [248] is one of the most used ISD algorithms, as it is considered one of the fastest algorithms on a classical computer. In this algorithm we use the idea of Lee-Brickell and allow errors inside the information set and in addition we partition the information set into two sets and ask for v errors in both of them. Further, we also use the idea of Leon [181] to have a *zero-window* of size ℓ outside the information set, where no errors happen.

Stern's algorithm is given in Algorithm 2. But first we explain the algorithm and illustrate it.

The steps are the usual: we first choose an information set and then bring the parity-check matrix into systematic form according to this information set. We partition the information set into two sets and define the sets S and T , where S takes care of all vectors living in one partition and T takes care of all vectors living in the other partition. We can now check whether two of such fixed vectors give us the wanted error vector.

To illustrate the algorithm, we assume that the information set is $I = \{1, \dots, k\}$ and that the zero-window is $Z = \{k+1, \dots, k+\ell\}$. Further, let us define $J = (I \cup Z)^C = \{k+\ell+1, \dots, n\}$. We again denote by \mathbf{U} the matrix that brings the parity-check matrix into systematic form and write the error vector partitioned into the information set part I , the zero-window part Z and the remaining part J , as $\mathbf{e} = (\mathbf{e}_I, \mathbf{0}_\ell, \mathbf{e}_J)$, with $\text{wt}_H(\mathbf{e}_I) = 2v$ and $\text{wt}_H(\mathbf{e}_J) = t - 2v$. Thus, we get the following:

$$\mathbf{e}\mathbf{H}^\top\mathbf{U}^\top = \begin{pmatrix} \mathbf{e}_I & \mathbf{0}_\ell & \mathbf{e}_J \end{pmatrix} \begin{pmatrix} \mathbf{A}^\top & \mathbf{B}^\top \\ \text{Id}_\ell & \mathbf{0}_{\ell \times (n-k-\ell)} \\ \mathbf{0}_{(n-k-\ell) \times \ell} & \text{Id}_{n-k-\ell} \end{pmatrix} = \begin{pmatrix} \mathbf{s}_1 & \mathbf{s}_2 \end{pmatrix} = \mathbf{s}\mathbf{U}^\top,$$

where $\mathbf{A} \in \mathbb{F}_q^{\ell \times k}$ and $\mathbf{B} \in \mathbb{F}_q^{(n-k-\ell) \times k}$.

From this we get the following two conditions

$$\mathbf{e}_I \mathbf{A}^\top = \mathbf{s}_1, \quad (5.1)$$

$$\mathbf{e}_I \mathbf{B}^\top + \mathbf{e}_J = \mathbf{s}_2. \quad (5.2)$$

We partition the information set I into the sets X and Y , for the sake of simplicity, assume that k is even and $m = k/2$. Assume that $X = \{1, \dots, m\}$ and $Y = \{m+1, \dots, k\}$. Hence, we can write $\mathbf{e}_I = (\mathbf{e}_X, \mathbf{e}_Y)$, and Condition (5.1) becomes

$$\sigma_X(\mathbf{e}_X) \mathbf{A}^\top = \mathbf{s}_1 - \sigma_Y(\mathbf{e}_Y) \mathbf{A}^\top. \quad (5.3)$$

Observe that the σ_X is needed, as \mathbf{e}_X has length m but we want to multiply it to $\mathbf{A}^\top \in \mathbb{F}_q^{k \times \ell}$. In the algorithm we will not use the embedding σ_X but rather $\mathbb{F}_q^k(X)$, thus \mathbf{e}_X will have length k , but only support in X .

In the algorithm, we define a set S that contains all vectors of the form $\sigma_X(\mathbf{e}_X) \mathbf{A}^\top$, i.e., of the left side of (5.3) and a set T that contains all vectors of the form $\mathbf{s}_1 - \sigma_Y(\mathbf{e}_Y) \mathbf{A}^\top$, i.e., of the right side of (5.3). Whenever a vector in S and a vector in T coincide, we call such a pair a collision.

For each collision we define \mathbf{e}_J such that Condition (5.2) is satisfied, i.e.,

$$\mathbf{e}_J = \mathbf{s}_2 - \mathbf{e}_I \mathbf{B}^\top$$

and if the weight of \mathbf{e}_J is the remaining $t - 2v$, we have found the sought-after error vector.

We now give the algorithm of Stern in its full generality, i.e., we are not restricting to the choice of I, J and Z , that we made before for illustrating the algorithm.

Theorem 235. *Stern's algorithm over \mathbb{F}_q requires on average*

$$\begin{aligned} & \binom{m_1}{v}^{-1} \binom{m_2}{v}^{-1} \binom{n-k-\ell}{t-2v}^{-1} \binom{n}{t} \\ & \cdot \left((n-k)^2(n+1) \left(\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2 \right) + (m_1 + m_2)\ell \lceil \log_2(q) \rceil^2 \right. \\ & + \ell \left(L_q(m_1, v) + L_q(m_2, v) + \binom{m_2}{v} (q-1)^v \right) \lceil \log_2(q) \rceil \\ & + \frac{\binom{m_1}{v} \binom{m_2}{v} (q-1)^{2v}}{q^\ell} \min \left\{ n-k-\ell, \frac{q}{q-1} (t-2v+1) \right\} \\ & \cdot 2v \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right) \end{aligned}$$

binary operations.

Proof. As in Prange's algorithm, as a first step we bring \mathbf{H} into systematic form and apply the same row operations on the syndrome; a broad estimate for the cost is given by

$$(n-k)^2(n+1) \left(\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2 \right)$$

binary operations.

Algorithm 2 Stern's Algorithm over \mathbb{F}_q in the Hamming metric

Input: $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $t \in \mathbb{N}$, $k = m_1 + m_2$, $\ell < n - k$ and $v < \min\{m_1, m_2, \lfloor \frac{t}{2} \rfloor\}$.

Output: $\mathbf{e} \in \mathbb{F}_q^n$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and $\text{wt}_H(\mathbf{e}) = t$.

- 1: Choose an information set $I \subset \{1, \dots, n\}$ of size k and choose a zero-window $Z \subset I^C$ of size ℓ , and define $J = (I \cup Z)^C$.
- 2: Partition I into X of size m_1 and Y of size $m_2 = k - m_1$.
- 3: Compute $\mathbf{U} \in \mathbb{F}_q^{(n-k) \times (n-k)}$, such that

$$(\mathbf{U}\mathbf{H})_I = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix}, \quad (\mathbf{U}\mathbf{H})_Z = \begin{pmatrix} \text{Id}_\ell \\ \mathbf{0}_{(n-k-\ell) \times \ell} \end{pmatrix} \quad \text{and} \quad (\mathbf{U}\mathbf{H})_J = \begin{pmatrix} \mathbf{0}_{\ell \times (n-k-\ell)} \\ \text{Id}_{n-k-\ell} \end{pmatrix},$$

where $\mathbf{A} \in \mathbb{F}_q^{\ell \times k}$ and $\mathbf{B} \in \mathbb{F}_q^{(n-k-\ell) \times k}$.

- 4: Compute $\mathbf{s}\mathbf{U}^\top = \begin{pmatrix} \mathbf{s}_1 & \mathbf{s}_2 \end{pmatrix}$, where $\mathbf{s}_1 \in \mathbb{F}_q^\ell$ and $\mathbf{s}_2 \in \mathbb{F}_q^{n-k-\ell}$.
- 5: Compute the set S

$$S = \{(\mathbf{e}_X \mathbf{A}^\top, \mathbf{e}_X) \mid \mathbf{e}_X \in \mathbb{F}_q^k(X), \text{wt}_H(\mathbf{e}_X) = v\}.$$

- 6: Compute the set T

$$T = \{(\mathbf{s}_1 - \mathbf{e}_Y \mathbf{A}^\top, \mathbf{e}_Y) \mid \mathbf{e}_Y \in \mathbb{F}_q^k(Y), \text{wt}_H(\mathbf{e}_Y) = v\}.$$

- 7: **for** $(\mathbf{a}, \mathbf{e}_X) \in S$ **do**
 - 8: **for** $(\mathbf{a}, \mathbf{e}_Y) \in T$ **do**
 - 9: **if** $\text{wt}_H(\mathbf{s}_2 - (\mathbf{e}_X + \mathbf{e}_Y)\mathbf{B}^\top) = t - 2v$ **then**
 - 10: Return \mathbf{e} such that $\mathbf{e}_I = \mathbf{e}_X + \mathbf{e}_Y$, $\mathbf{e}_Z = \mathbf{0}_\ell$ and $\mathbf{e}_J = \mathbf{s}_2 - (\mathbf{e}_X + \mathbf{e}_Y)\mathbf{B}^\top$.
 - 11: Start over with Step 1 and a new selection of I .
-

To compute the set S , we can use the technique of intermediate sums. We want to compute $\mathbf{e}_X \mathbf{A}^\top$ for all $\mathbf{e}_X \in \mathbb{F}_q^k(X)$ of Hamming weight v . Using intermediate sums, this costs

$$L_q(m_1, v) \ell \lceil \log_2(q) \rceil + m_1 \ell \lceil \log_2(q) \rceil^2$$

binary operations.

Similarly, we can build set T : we want to compute $\mathbf{s}_1 - \mathbf{e}_Y \mathbf{A}^\top$, for all $\mathbf{e}_Y \in \mathbb{F}_q^k(Y)$ of Hamming weight v . Using intermediate sums, this costs

$$L_q(m_2, v) \ell \lceil \log_2(q) \rceil + m_2 \ell \lceil \log_2(q) \rceil^2 + \binom{m_2}{v} (q-1)^v \ell \lceil \log_2(q) \rceil$$

binary operations. Note that the $L_q(m_2, v) \ell \lceil \log_2(q) \rceil + m_2 \ell \lceil \log_2(q) \rceil^2$ part comes from computing $\mathbf{e}_Y \mathbf{A}^\top$, whereas the $\binom{m_2}{v} (q-1)^v \ell \lceil \log_2(q) \rceil$ part comes from subtracting from each of the vectors $\mathbf{e}_Y \mathbf{A}^\top$ the vector \mathbf{s}_1 .

In the remaining steps we go through all $(\mathbf{a}, \mathbf{e}_X) \in S$ and all $(\mathbf{a}, \mathbf{e}_Y) \in T$, thus usually the cost of these steps should be multiplied by the size of $S \times T$. However, since the algorithm

first checks for a collision, we can use instead of $|S| + |T|$ the number of collisions we expect on average.

More precisely: since S consists of all $\mathbf{e}_X \in \mathbb{F}_q^k(X)$ of Hamming weight v , S is of size $\binom{m_1}{v}(q-1)^v$ and similarly T is of size $\binom{m_2}{v}(q-1)^v$.

The resulting vectors $\mathbf{e}_X \mathbf{A}^\top$, respectively, $\mathbf{s}_1 - \mathbf{e}_Y \mathbf{A}^\top$ live in \mathbb{F}_q^ℓ , and we assume that they are uniformly distributed. Hence, we have to check on average

$$\frac{\binom{m_1}{v} \binom{m_2}{v} (q-1)^{2v}}{q^\ell}$$

many collisions.

For each collision we have to compute

$$\mathbf{s}_2 - (\mathbf{e}_X + \mathbf{e}_Y) \mathbf{B}^\top.$$

Since the algorithm only proceeds if the weight of

$$\mathbf{s}_2 - (\mathbf{e}_X + \mathbf{e}_Y) \mathbf{B}^\top$$

is $t - 2v$, we can use the concept of early abort.

Computing one entry of the vector $\mathbf{s}_2 - (\mathbf{e}_X + \mathbf{e}_Y) \mathbf{B}^\top$ costs

$$2v \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$$

binary operations. Thus, we get that this step costs on average

$$\frac{q}{q-1} (t - 2v + 1) 2v \left(\lceil \log_2(q) \rceil^2 + \lceil \log_2(q) \rceil \right)$$

binary operations.

Finally, the success probability is given by having chosen the correct weight distribution of \mathbf{e} ; this is exactly the same as over \mathbb{F}_2 and given by

$$\binom{m_1}{v} \binom{m_2}{v} \binom{n-k-\ell}{t-2v} \binom{n}{t}^{-1}.$$

Thus, we can conclude. □

Note that we usually set in Stern's algorithm the parameter $m_1 = \lfloor \frac{k}{2} \rfloor$. Hence assuming that k is even we get a nicer formula for the cost, being

$$\begin{aligned} & \binom{k/2}{v}^{-2} \binom{n-k-\ell}{t-2v}^{-1} \binom{n}{t} \left(\left(\lceil \log_2(q) \rceil + \lceil \log_2(q) \rceil^2 \right) \right. \\ & \cdot \left((n-k)^2(n+1) + \binom{k/2}{v}^2 (q-1)^{2v-\ell} \min \left\{ n-k-\ell, \frac{q}{q-1} (t-2v+1) \right\} 2v \right) \\ & \left. + k\ell \lceil \log_2(q) \rceil^2 + \ell \left(2L_q(k/2, v) + \binom{k/2}{v} (q-1)^v \right) \lceil \log_2(q) \rceil \right) \end{aligned}$$

binary operations.

5.3.6 BJMM Algorithm

In what follows we cover the BJMM algorithm proposed in [60], this is considered to be the fastest algorithm over the binary, for this reason we will stick to the binary case also for this paragraph.

In the previous ISD algorithms one always represented the entries of the error vector as $0 = 0 + 0$ and $1 = 1 + 0 = 0 + 1$, that is one was looking for a set partition of the support. The novel idea of the algorithm is to use also the other representations, i.e., $0 = 0 + 0 = 1 + 1$. Thus, the search space for the smaller error vector parts become larger but the probability to find the correct error becomes larger as well.

The idea of the BJMM algorithm is to write a vector \mathbf{e} of some length n and weight v as $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2$, where \mathbf{e}_1 and \mathbf{e}_2 are both of length n and of weight $v/2 + \varepsilon$, thus we are asking for an overlap in ε positions, which will cancel out.

The first part of all algorithms, which belong to the second direction of improvements, is to perform a partial Gaussian elimination (PGE) step, that is for some positive integer $\ell \leq n - k$ one wants to find an invertible matrix $\mathbf{U} \in \mathbb{F}_2^{(n-k) \times (n-k)}$, such that (after some permutation of the columns)

$$\mathbf{UH} = \begin{pmatrix} \text{Id}_{n-k-\ell} & \mathbf{A} \\ \mathbf{0} & \mathbf{B} \end{pmatrix},$$

where $\mathbf{A} \in \mathbb{F}_2^{(n-k-\ell) \times (k+\ell)}$ and $\mathbf{B} \in \mathbb{F}_2^{\ell \times (k+\ell)}$. Hence we are looking for $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2)$, with $\mathbf{e}_1 \in \mathbb{F}_2^{n-k-\ell}$ of weight $t - v$ and $\mathbf{e}_2 \in \mathbb{F}_2^{k+\ell}$, of weight v . For the parity-check equations, we also split the new syndrome $\mathbf{sU}^\top = (\mathbf{s}_1, \mathbf{s}_2)$ with $\mathbf{s}_1 \in \mathbb{F}_2^{n-k-\ell}$ and $\mathbf{s}_2 \in \mathbb{F}_2^\ell$, that is we want to solve

$$\mathbf{UHe}^\top = \begin{pmatrix} \text{Id}_{n-k-\ell} & \mathbf{A} \\ \mathbf{0} & \mathbf{B} \end{pmatrix} \begin{pmatrix} \mathbf{e}_1^\top \\ \mathbf{e}_2^\top \end{pmatrix} = \begin{pmatrix} \mathbf{s}_1^\top \\ \mathbf{s}_2^\top \end{pmatrix}.$$

The parity-check equations can thus be written as

$$\begin{aligned} \mathbf{e}_1^\top + \mathbf{A}\mathbf{e}_2^\top &= \mathbf{s}_1^\top, \\ \mathbf{B}\mathbf{e}_2^\top &= \mathbf{s}_2^\top. \end{aligned}$$

The idea of the algorithms using PGE is to solve now the second equation, i.e., to search for \mathbf{e}_2 of length $k + \ell$ and weight v such that $\mathbf{e}_2\mathbf{B}^\top = \mathbf{s}_2$ and then to define $\mathbf{e}_1 = \mathbf{s}_1 - \mathbf{e}_2\mathbf{A}^\top$ and to check if this has then the remaining weight $t - v$.

Note that this is now a smaller instance of a syndrome decoding problem, for which we want to find a list of solutions. The success probability of such a splitting of \mathbf{e} is then given by

$$\binom{k+\ell}{v} \binom{n-k-\ell}{t-v} \binom{n}{t}^{-1}.$$

An important part of such algorithms is how to merge two lists of parts of the error vector together. For this we consider two lists $\mathcal{L}_1, \mathcal{L}_2$, a positive integer $u < k$, which denotes the number of positions on which one merges, a target vector $\mathbf{t} \in \mathbb{F}_2^u$ and a target weight w . For a vector \mathbf{x} , let us denote by $\mathbf{x}_{|u}$ the vector consisting of the first u entries of \mathbf{x} .

Algorithm 3 Merge

Input: The input lists $\mathcal{L}_1, \mathcal{L}_2$, the positive integers $0 < u < k$ and $0 \leq v \leq n$, the matrix $\mathbf{B} \in \mathbb{F}_2^{k \times (k+\ell)}$ and the target $\mathbf{t} \in \mathbb{F}_2^u$.

Output: $\mathcal{L} = \mathcal{L}_1 \bowtie \mathcal{L}_2$.

- 1: Lexicographically sort \mathcal{L}_1 and \mathcal{L}_2 according to $(\mathbf{B}\mathbf{x}_i^\top)_{|u}$, respectively $(\mathbf{B}\mathbf{y}_j^\top)_{|u} + \mathbf{t}$ for $\mathbf{x}_i \in \mathcal{L}_1$ and $\mathbf{y}_j \in \mathcal{L}_2$.
 - 2: **for** $(\mathbf{x}_i, \mathbf{y}_j) \in \mathcal{L}_1 \times \mathcal{L}_2$ with $(\mathbf{B}\mathbf{x}_i^\top)_{|u} = (\mathbf{B}\mathbf{y}_j^\top)_{|u} + \mathbf{t}$ **do**
 - 3: **if** $\text{wt}_H(\mathbf{x}_i + \mathbf{y}_j) = w$ **then**
 - 4: $\mathcal{L} = \mathcal{L} \cup \{\mathbf{x}_i + \mathbf{y}_j\}$.
 - 5: **Return** \mathcal{L} .
-

Lemma 236. *The average cost of the merge algorithm (Algorithm 3) is given by*

$$(L_1 + L_2)u(k + \ell) + L_1 \log(L_1) + L_2 \log_2(L_2) + (k + \ell)(L_1 \cdot L_2 2^{-u}),$$

where $L_i = |\mathcal{L}_i|$ for $i = 1, 2$.

Exercise 237. Prove Lemma 236.

The algorithm will use this merging process three times.

For the internal parameter v (which can be optimized), we also choose the positive integers $\varepsilon_1, \varepsilon_2$ (also up to optimization), and define

$$\begin{aligned} v_1 &= v/2 + \varepsilon_1, \\ v_2 &= v_1/2 + \varepsilon_2. \end{aligned}$$

We start with creating the two base lists \mathcal{B}_1 and \mathcal{B}_2 , which depend on a partition P_1, P_2 of $\{1, \dots, k + \ell\}$, of same size, i.e., $\frac{k+\ell}{2}$:

$$\mathcal{B}_i = \{\mathbf{x} \in \mathbb{F}_2^{k+\ell}(P_i) \mid \text{wt}_H(\mathbf{x}) = v_2/2\}.$$

These lists have size

$$B = \binom{(k + \ell)/2}{v_2/2}.$$

We now choose $\mathbf{t}_1^{(1)} \in \mathbb{F}_2^{u_1}$, which determines $\mathbf{t}_2^{(1)} = (\mathbf{s}_2)_{|u_1} + \mathbf{t}_1^{(1)}$. We also choose $\mathbf{t}_1^{(2)}, \mathbf{t}_3^{(2)} \in \mathbb{F}_2^{u_2}$, which define

$$\begin{aligned} \mathbf{t}_2^{(2)} &= (\mathbf{t}_1^{(1)})_{|u_2} + \mathbf{t}_1^{(2)}, \\ \mathbf{t}_4^{(2)} &= (\mathbf{t}_2^{(1)})_{|u_2} + \mathbf{t}_3^{(2)}. \end{aligned}$$

Then, for a positive integer u_2 and the four target vectors $\mathbf{t}_i^{(2)}$, for $i \in \{1, \dots, 4\}$ we perform the first four merges using Algorithm 3 to get $\mathcal{L}_i^{(2)} = \mathcal{B}_1 \bowtie \mathcal{B}_2$ on u_2 positions, weight v_2 and target vector $\mathbf{t}_i^{(2)}$ for $i \in \{1, \dots, 4\}$. The lists $\mathcal{L}_i^{(2)}$ are expected to be of size $L_2 = \binom{k+\ell}{v_2} 2^{-u_2}$.

With the four new lists we then perform another two merges yielding

$$\mathcal{L}_i^{(1)} = \mathcal{L}_{2i-1}^{(2)} \bowtie \mathcal{L}_{2i}^{(2)}$$

on u_1 positions, with weight v_1 and target vectors $\mathbf{t}_i^{(1)}$ for $i \in \{1, 2\}$. These lists are expected to be of size $L_1 = \binom{k+\ell}{v_1} 2^{-u_1}$.

As a last step we then merge the two new lists to get the final list

$$\mathcal{L} = \mathcal{L}_1^{(1)} \bowtie \mathcal{L}_2^{(1)}$$

on ℓ positions, with weight v and target vector \mathbf{s}_2 . The final list is expected to be of size $L = \binom{k+\ell}{v} 2^{-\ell}$.

One important aspect of such algorithms is the following

We have to make sure that at least one representation of the solution lives in each list.

This can either be done by employing the probability of this happening in the success probability, thus increasing the number of iterations or by choosing u , the number of positions on which one merges in such a way that we can expect that at least one representation lives in the lists.

In [60] the authors chose the second option: observe that the number of tuples $(\mathbf{e}_1^{(1)}, \mathbf{e}_2^{(1)}) \in \mathcal{L}_1^{(1)} \times \mathcal{L}_2^{(1)}$ that represent a single solution $\mathbf{e}_2 \in \mathcal{L}$ is given by

$$U_1 = \binom{v}{v/2} \binom{k+\ell-v}{\varepsilon_1}.$$

Hence choosing $u_1 = \log_2(U_1)$ ensures that $L \geq 1$. Similarly, since we also represent $\mathbf{e}_i^{(1)}$ as sum of two overlapping vectors $(\mathbf{e}_{2i-1}^{(2)}, \mathbf{e}_{2i}^{(2)})$, we have that for each $\mathbf{e}_i^{(1)}$ we have approximately

$$U_2 = \binom{v_1}{v_1/2} \binom{k+\ell-v_1}{\varepsilon_2}$$

many representations. Thus, we can choose $u_2 = \log_2(U_2)$.

Proposition 238. *Algorithm 4 has an average cost of*

$$\begin{aligned} & \binom{n}{t} \binom{n-k-\ell}{t-v}^{-1} \binom{k+\ell}{v}^{-1} \cdot [(n-k-\ell)^2(n+1) \\ & + 4(2Bu_2(k+\ell) + 2B \log(B) + (k+\ell)B^2 2^{-u_2}) \\ & + 2(2L_2u_1(k+\ell) + 2L_2 \log(L_2) + (k+\ell)L_2^2 2^{-u_1}) \\ & + (2L_1\ell(k+\ell) + 2L_1 \log(L_1) + (k+\ell)L_1^2 2^{-\ell}) \\ & + \binom{k+\ell}{v} 2^{-\ell} 2(t-v+1)v] \end{aligned}$$

binary operations.

Algorithm 4 BJMM

Input: $0 \leq \ell \leq n - k$, $0 \leq u_2 \leq u_1 \leq \ell$, $\varepsilon_1, \varepsilon_2$, $t, v < t$, $\mathbf{H} \in \mathbb{F}_2^{(n-k) \times n}$ and $\mathbf{s} \in \mathbb{F}_2^{n-k}$.

Output: $\mathbf{e} \in \mathbb{F}_2^n$ with $\text{wt}_H(\mathbf{e}) = t$ and $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$.

- 1: Choose an $n \times n$ permutation matrix \mathbf{P} .
- 2: Find $\mathbf{U} \in \mathbb{F}_2^{(n-k) \times (n-k)}$, such that

$$\mathbf{UHP} = \begin{pmatrix} \text{Id}_{n-k-\ell} & \mathbf{A} \\ \mathbf{0} & \mathbf{B} \end{pmatrix},$$

where $\mathbf{A} \in \mathbb{F}_2^{(n-k-\ell) \times (k+\ell)}$ and $\mathbf{B} \in \mathbb{F}_2^{\ell \times (k+\ell)}$.

- 3: Compute $\mathbf{Us}^\top = \begin{pmatrix} \mathbf{s}_1^\top \\ \mathbf{s}_2^\top \end{pmatrix}$, where $\mathbf{s}_1 \in \mathbb{F}_2^{n-k-\ell}$, $\mathbf{s}_2 \in \mathbb{F}_2^\ell$.
- 4: Choose partitions P_1, P_2 of $\{1, \dots, k + \ell\}$ of size $(k + \ell)/2$.
- 5: Set

$$\mathcal{B}_j = \left\{ \mathbf{x} \in \mathbb{F}_2^{k+\ell}(P_j) \mid \text{wt}_H(\mathbf{x}) = v_2/2 \right\}$$

for $j \in \{1, 2\}$.

- 6: Choose $\mathbf{t}_1^{(1)} \in \mathbb{F}_2^{u_1}$, set $\mathbf{t}_2^{(1)} = (\mathbf{s}_2)_{|u_1} + \mathbf{t}_1^{(1)}$
 - 7: Choose $\mathbf{t}_1^{(2)}, \mathbf{t}_3^{(2)} \in \mathbb{F}_2^{u_2}$, set $\mathbf{t}_2^{(2)} = (\mathbf{t}_1^{(1)})_{|u_2} + \mathbf{t}_1^{(2)}$ and $\mathbf{t}_4^{(2)} = (\mathbf{t}_2^{(1)})_{|u_2} + \mathbf{t}_3^{(2)}$
 - 8: **for** $i \in \{1, \dots, 4\}$ **do**
 - 9: Compute $\mathcal{L}_i^{(2)} = \mathcal{B}_1 \bowtie \mathcal{B}_1$ using Algorithm 3 on u_2 positions to get weight v_2 and target vectors $\mathbf{t}_i^{(2)}$.
 - 10: **for** $i \in \{1, 2\}$ **do**
 - 11: Compute $\mathcal{L}_i^{(1)} = \mathcal{L}_{2i-1}^{(2)} \bowtie \mathcal{L}_{2i}^{(2)}$ using Algorithm 3 on u_1 positions to get weight v_1 and target vectors $\mathbf{t}_i^{(1)}$.
 - 12: Compute $\mathcal{L} = \mathcal{L}_1^{(1)} \bowtie \mathcal{L}_2^{(1)}$ using Algorithm 3 on ℓ positions to get weight v and target vector \mathbf{s}_2 .
 - 13: **for** $\mathbf{e}_2 \in \mathcal{L}$ **do**
 - 14: **if** $\text{wt}_H(\mathbf{s}_1 - \mathbf{e}_2 \mathbf{A}^\top) = t - v$ **then**
 - 15: Set $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2)$.
 - 16: Return \mathbf{Pe} .
 - 17: Else start over at step 1.
-

5.3.7 Generalized Birthday Decoding Algorithms

In the syndrome decoding problem (SDP) we are given a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, a syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and a weight $t \in \mathbb{N}$ and want to find an error vector $\mathbf{e} \in \mathbb{F}_q^n$, such that $\mathbf{s} = \mathbf{e}\mathbf{H}^\top$ and $\text{wt}_H(\mathbf{e}) = t$.

The first step of a generalized birthday algorithm (GBA) decoder is the partial Gaussian elimination step, i.e., for some positive integer $\ell \leq n - k$ we bring the parity-check matrix into the form

$$\mathbf{H}' = \begin{pmatrix} \text{Id}_{n-k-\ell} & \mathbf{A} \\ 0 & \mathbf{B} \end{pmatrix},$$

up to permutation of columns. We recall from the BJMM algorithm, that this leaves us with solving the smaller SDP instance: find $\mathbf{e}_2 \in \mathbb{F}_q^{k+\ell}$ of Hamming weight $v \leq t$, such that

$$\mathbf{e}_2 \mathbf{B}^\top = \mathbf{s}_2,$$

for $\mathbf{s}_2 \in \mathbb{F}_q^\ell$ and $\mathbf{B} \in \mathbb{F}_q^{\ell \times (k+\ell)}$.

This second step is usually performed using Wagner's algorithm on a levels.

By abuse of notation, we write for the rest $\mathbf{e}\mathbf{B}^\top = \mathbf{s}$, instead of $\mathbf{e}_2 \mathbf{B}^\top = \mathbf{s}_2$. In a Lee-Brickell approach, one would now go through all possible $\mathbf{e} \in \mathbb{F}_q^{k+\ell}$ of weight v and check if they satisfy the parity-check equations. The idea of GBA is to split the vector \mathbf{e} further. Let us start with GBA on one level, that is

$$\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2)$$

with $\mathbf{e}_i \in \mathbb{F}_q^{(k+\ell)/2}$ of weight $v/2$, for $i \in \{1, 2\}$. Hence we define $\mathbf{B} = \begin{pmatrix} \mathbf{B}_1 & \mathbf{B}_2 \end{pmatrix}$, with $\mathbf{B}_i \in \mathbb{F}_q^{\ell \times (k+\ell)/2}$, for $i \in \{1, 2\}$ and split the syndrome $\mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2$. We hence want that

$$\mathbf{e}_1 \mathbf{B}_1^\top + \mathbf{e}_2 \mathbf{B}_2^\top = \mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2.$$

For this we define two lists

$$\begin{aligned} \mathcal{L}_1 &= \{(\mathbf{e}_1, \mathbf{e}_1 \mathbf{B}_1^\top - \mathbf{s}_1) \mid \mathbf{e}_1 \in \mathbb{F}_q^{(k+\ell)/2}, \text{wt}_H(\mathbf{e}_1) = v/2\}, \\ \mathcal{L}_2 &= \{(\mathbf{e}_2, \mathbf{e}_2 \mathbf{B}_2^\top - \mathbf{s}_2) \mid \mathbf{e}_2 \in \mathbb{F}_q^{(k+\ell)/2}, \text{wt}_H(\mathbf{e}_2) = v/2\}. \end{aligned}$$

We are then looking for an element

$$((\mathbf{e}_1, \mathbf{x}_1), (\mathbf{e}_2, \mathbf{x}_2)) \in \mathcal{L}_1 \times \mathcal{L}_2,$$

such that $\mathbf{x}_1 + \mathbf{x}_2 = 0$, which will then imply that

$$\mathbf{e}_1 \mathbf{B}_1^\top + \mathbf{e}_2 \mathbf{B}_2^\top = \mathbf{s} = \mathbf{s}_1 + \mathbf{s}_2.$$

This idea can be generalized to a levels, thus splitting

$$\mathbf{e} = (\mathbf{e}_1^{(1)}, \dots, \mathbf{e}_{2^a}^{(1)}),$$

where $\mathbf{e}_i^{(1)} \in \mathbb{F}_q^{(k+\ell)/2^a}$ of weight $v/(2^a)$ and writing

$$\mathbf{B} = \begin{pmatrix} \mathbf{B}_1 & \cdots & \mathbf{B}_{2^a} \end{pmatrix},$$

where $\mathbf{B}_i \in \mathbb{F}_q^{\ell \times (k+\ell)/2^a}$ and splitting $\mathbf{s} = \mathbf{s}_1 + \cdots + \mathbf{s}_{2^a}$. For this we will need the merging positions $0 \leq u_1 \leq \cdots \leq u_a = \ell$. One first constructs the base lists

$$\mathcal{L}_j^{(1)} = \{(\mathbf{e}_j^{(1)}, \mathbf{e}_j^{(1)} \mathbf{B}_j^\top - \mathbf{s}_j) \mid \mathbf{e}_j^{(1)} \in \mathbb{F}_q^{(k+\ell)/2^a}, \text{wt}_H(\mathbf{e}_j^{(1)}) = v/2^a\},$$

for $j \in \{1, \dots, 2^a\}$ and then performs a merges: in the i -th merge we are given a parameter $0 \leq u_i \leq v$ and we want to merge

$$\mathcal{L}_j^{(i+1)} = \mathcal{L}_{2j-1}^{(i)} \bowtie_{u_i} \mathcal{L}_{2j}^{(i)}.$$

For this let us define the merge $\mathcal{L} = \mathcal{L}_1 \bowtie_u \mathcal{L}_2$ first formally. Given $\mathcal{L}_i = \{(\mathbf{e}_i, \mathbf{x}_i)\}$, for $i \in \{1, 2\}$ and u

$$\mathcal{L}_1 \bowtie_u \mathcal{L}_2 = \{((\mathbf{e}_1, \mathbf{e}_2), \mathbf{x}_1 + \mathbf{x}_2) \mid \mathbf{x}_1 + \mathbf{x}_2 =_u \mathbf{0}\},$$

where $\mathbf{a} =_u \mathbf{b}$, denotes that \mathbf{a} and \mathbf{b} are equal on the first u positions. The merging process follows the following algorithm

1. Lexicographically order the elements $(\mathbf{e}_i, \mathbf{x}_i) \in \mathcal{L}_i$ for $i \in \{1, 2\}$ according to the first u positions,
2. Search for a collision, i.e., $\mathbf{x}_1 + \mathbf{x}_2 =_u \mathbf{0}$ and if found insert the corresponding $((\mathbf{e}_1, \mathbf{e}_2), \mathbf{x}_1 + \mathbf{x}_2)$ in \mathcal{L} .

The general idea of GBA is that we will not use the probability that we can split \mathbf{e} into $(\mathbf{e}_1, \dots, \mathbf{e}_{2^a})$ each having weight $v/2^a$, but rather we want that the merging process of will produce a solution with high probability. The average size of \mathcal{L} is given by

$$L = |\mathcal{L}_1 \bowtie_u \mathcal{L}_2| = \frac{|\mathcal{L}_1| |\mathcal{L}_2|}{q^u},$$

and thus, whenever $L \geq 1$ we can be assured that this algorithm returns (on average) a solution \mathbf{e} .

This is only possible for large weights v . If we are in this case, there exists a further improvement on the algorithm, where one does not take the whole lists $\mathcal{L}_i^{(1)}$ but only 2^b many such elements, and thus the algorithm works as long as $\frac{2^{2b}}{q^u} \geq 1$.

Stern's ISD algorithm is a special case of Wagner's algorithm on one level, where $\ell = 0$ and $\mathbf{s}_1 = \mathbf{0}$. However, in Stern's algorithm one employs the probability of splitting the error vector into $(\mathbf{e}_1, \mathbf{e}_2)$, rather than asking for

$$\frac{|\mathcal{L}_1| |\mathcal{L}_2|}{q^\ell} \geq 1.$$

The idea of GBA or more precisely of Wagner's approach was used in famous ISD papers such as BJMM and MMT, where 3 levels turned out to be an optimal choice.

5.3.8 Asymptotic Cost

An important aspect of ISD algorithms (apart from the cost) is their asymptotic cost. The idea of the asymptotic cost is that we are interested in the exponent $e(R, q)$ such that for large n the cost of the algorithm is given by $q^{(e(R, q) + o(1))n}$. This is crucial in order to compare different algorithms.

We consider codes of large length n , and consider the dimension and the error correction capacity as functions in n , i.e., $k, t : \mathbb{N} \rightarrow \mathbb{N}$. For these we define

$$\begin{aligned}\lim_{n \rightarrow \infty} t(n)/n &= T, \\ \lim_{n \rightarrow \infty} k(n)/n &= R.\end{aligned}$$

If $c(n, k, t, q)$ denotes the cost of an algorithm, for example Prange's algorithm, then we are now interested in

$$C(q, R, T) = \lim_{n \rightarrow \infty} \frac{1}{n} \log_q(c(n, k, t, q)).$$

For this we often use Stirlings formula, that is

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log_q \left(\frac{(\alpha + o(1))n}{(\beta + o(1))n} \right) = \alpha \log_q(\alpha) - \beta \log_q(\beta) - (\alpha - \beta) \log_q(\alpha - \beta).$$

One of the most important aspects in computing the asymptotic cost, is that random codes attain the asymptotic Gilbert-Varshamov bound with high probability, thus we are allowed to choose a relative minimum distance δ such that $R = 1 - H_q(\delta)$.

Example 239. The asymptotic cost of Prange's algorithm is easily computed as

$$\begin{aligned}\lim_{n \rightarrow \infty} \frac{1}{n} \log_q \left(\binom{n-k}{t}^{-1} \binom{n}{t} \right) &= \\ &= -(1-T) \log_q(1-T) - (1-R) \log_q(1-R) + (1-R-T) \log_q(1-R-T).\end{aligned}$$

Exercise 240. Prove that the asymptotic cost of Prange is equal to

$$H_q(T) - (1-R)H_q(T/(1-R)).$$

For the more sophisticated algorithms such as Stern and BJMM, we will also have internal parameters, such as ℓ, v , which will be chosen optimal, i.e., giving the smallest cost.

Note that we assume half-distance decoding, i.e., $T = \delta/2$, thus $C(q, R, \delta/2) = e(R, q)$ and then compute the largest value of $e(R^*, q)$ by taking

$$R^* = \operatorname{argmax}_{0 < R < 1} e(R, q).$$

With the asymptotic cost, we can now compare different ISD algorithms. For this, we will restrict ourselves to the binary case, since we presented the BJMM algorithm only over the binary. In the following table BJMM refers to the algorithm presented in [60], MMT to [191], BCD to the algorithm from [72] and Stern and Prange refer to the algorithms of [248], respectively [216].

Algorithm	$e(R^*, 2)$
BJMM	0.1019
MMT	0.115
BCD	0.1163
Stern	0.1166
Prange	0.1208

Table 18: Asymptotic cost of different ISD algorithms over the binary

5.3.9 Rank-metric ISD Algorithms

Finally, we want to conclude this section on ISD algorithms explaining the idea of rank-metric ISD algorithms.

For this we first recall that the Hamming support of an error vector $\mathbf{e} \in \mathbb{F}_{q^m}^n$ is defined as

$$\text{supp}_H(\mathbf{e}) = \{i \in \{1, \dots, n\} \mid \mathbf{e}_i \neq 0\}.$$

The Hamming weight of \mathbf{e} is then given by the size of the Hamming support, i.e.,

$$\text{wt}_H(\mathbf{e}) = |\text{supp}_H(\mathbf{e})| \leq n.$$

If we would want to go through all error vectors of a given Hamming weight t , there are

$$\binom{n}{t} (q^m - 1)^t$$

many choices. This concept changes when we move to the rank-metric. The rank support of an error vector $\mathbf{e} \in \mathbb{F}_{q^m}^n$ is usually defined as the \mathbb{F}_q -vector space spanned by the entries of \mathbf{e} :

$$\text{supp}(\mathbf{e}) = \langle \mathbf{e}_1, \dots, \mathbf{e}_n \rangle_{\mathbb{F}_q}.$$

The rank weight of \mathbf{e} is then defined as the \mathbb{F}_q -dimension of the rank support, i.e.,

$$\text{wt}_R(\mathbf{e}) = \dim_{\mathbb{F}_q}(\text{supp}(\mathbf{e})).$$

If we want to go through all vectors of a given rank weight t , there are

$$\begin{bmatrix} m \\ t \end{bmatrix}_q = \prod_{i=0}^{t-1} \frac{q^m - q^i}{q^t - q^i} \sim q^{(m-t)t}$$

many choices. Thus, it is quite clear, that to look for an error vector in the rank metric poses a more costly problem than its Hamming metric counterpart.

However, depending whether m or n are smaller, we could also consider the row or column support.

Example 241. Let us consider $\mathbf{e} = (1, \alpha) \in \mathbb{F}_8^2$, where $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$ and the basis $\Gamma = \{1, \alpha, \alpha^2\}$. Then $\mathbf{e} = \mathbf{c}\mathbf{R}$, where $\mathbf{c} = (1, \alpha)$ and $\mathbf{R} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Thus, the column support of \mathbf{e} is given by

$$\text{supp}_C(\mathbf{e}) = \langle \Gamma(\mathbf{c})^\top \rangle = \langle (1, 0, 0), (0, 1, 0) \rangle \subset \mathbb{F}_2^3$$

of dimension 3. Whereas the row support of \mathbf{e} is given by

$$\text{supp}_R(\mathbf{e}) = \langle \mathbf{R} \rangle = \langle (1, 0), (0, 1) \rangle \subset \mathbb{F}_2^2.$$

Note that the column and row support can also be read of

$$\Gamma(\mathbf{e}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

as

$$\text{supp}_R(\mathbf{e}) = \text{rowsp}(\Gamma(\mathbf{e})) \subset \mathbb{F}_q^n$$

and

$$\text{supp}_C(\mathbf{e}) = \text{colsp}(\Gamma(\mathbf{e})) \subset \mathbb{F}_q^m.$$

Thus,

1. if $m \leq n$, we consider the column support of \mathbf{e} . In this case we have $\begin{bmatrix} m \\ t \end{bmatrix}_q$ vector spaces to go through.
2. If $n \leq m$, we row support of \mathbf{e} . In this case we have $\begin{bmatrix} n \\ t \end{bmatrix}_q$ many vector spaces.

In the following we give only the ideas of the combinatorial and algebraic algorithms to solve the rank SDP. First observe that we can write $\mathbf{e} = \beta \mathbf{E}$, where $\beta = (\beta_1, \dots, \beta_t)$ is a basis of the support of the error vector \mathbf{e} and $\mathbf{E} \in \mathbb{F}_q^{t \times n}$.

The first proposed rank ISD algorithm [90] performs a basis enumeration. That is, we want to enumerate all possible choices for β . Since if we know β , then solving $\beta \mathbf{E} \mathbf{H}^\top = \mathbf{s}$ has quadratic complexity. This attack has approximately a complexity of q^{tm} operations.

The second proposed rank ISD algorithm [207] enumerates all possible matrices \mathbf{E} instead, resulting in a cost of approximately $q^{(t-1)(k+1)}$ operations. These approaches are called combinatorial attacks, as they solve the rank SDP through enumerations.

In [130] the authors give a Prange-like rank metric ISD algorithm. The algorithm is usually called GRS, as abbreviation for the authors Gaborit, Ruatta, Schrek, not to be confused with generalized Reed-Solomon codes. One first chooses whether to guess the row or column support of \mathbf{e} , depending whether $n \leq m$, or $m \leq n$. Let us first assume that $m \leq n$ and hence we guess the column support.

Recalling that $\mathbf{e} = \mathbf{c}\mathbf{R}$, if we know a basis of the column support $\{\gamma_1, \dots, \gamma_t\}$ with $\gamma_i \in \mathbb{F}_q^m$, such that $\Gamma(c_i) = \gamma_i$, we can write for each $i \in \{1, \dots, n\}$

$$e_i = \sum_{j=1}^t c_j r_{i,j}.$$

And over \mathbb{F}_q

$$\Gamma(e_i) = \sum_{j=1}^t \gamma_j r_{i,j}.$$

Thus, we have nt unknowns $r_{i,j}$ and from $\mathbf{s} = \mathbf{e}\mathbf{H}^\top$ we have $m(n-k)$ equations.

Example 242. Let us consider $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$ and basis $\Gamma = \{1, \alpha, \alpha^2\}$. We are given the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha & 1 \end{pmatrix}$$

and the syndrome $\mathbf{s} = (\alpha^2, \alpha + 1)$ and $t = 1$.

We guess the column support of \mathbf{e} to be $\langle (1, 1, 0) \subset \mathbb{F}_2^3$, this corresponds to $\mathbf{c} = (\alpha + 1)$. Hence

$$e_i = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} r_i.$$

We consider the 2 syndrome equations

$$\begin{aligned} e_1 + e_3 + \alpha^2 e_4 &= s_1 = \alpha^2 \\ e_2 + \alpha e_3 + e_4 &= s_2 = \alpha + 1. \end{aligned}$$

In order to write these equations over \mathbb{F}_2 we observe that $\alpha^2 e_4 = \alpha^2(\alpha + 1)r_4 = (\alpha^2 + \alpha + 1)r_4$ and $\alpha e_3 = \alpha(\alpha + 1)r_3 = (\alpha^2 + \alpha)r_3$. Hence we get the linear system of equations

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

After solving the system, we get the unique solution $r_1 = 1, r_2 = 0, r_3 = 0, r_4 = 1$ and recompute $\mathbf{e} = \mathbf{c}\mathbf{R} = (\alpha + 1, 0, 0, \alpha + 1)$, which indeed has rank weight 1.

Exercise 243. Perform the same example but guess the column support to be $(1, 0, 0)$.

If we know the row support $\{\mathbf{r}_1, \dots, \mathbf{r}_t\}$ for $\text{Supp}_R(\mathbf{e}) \subset \mathbb{F}_q^n$, i.e., the rows of \mathbf{R} , then we can write for each $i \in \{1, \dots, n\}$

$$e_i = \sum_{j=1}^t c_j r_{i,j},$$

and using the basis Γ of \mathbb{F}_{q^m} over \mathbb{F}_q we can write

$$\Gamma(e_i) = \sum_{j=1}^t \Gamma(c_j) r_{i,j}.$$

Thus, over \mathbb{F}_q we have mt unknowns and $m(n-k)$ equations.

Let us use a neat trick for the next example: in order to bring the parity-check equations to the base field, we need to know what to do with a multiplication. Let $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ be a basis of \mathbb{F}_{q^m} over \mathbb{F}_q . The multiplication with $a \in \mathbb{F}_{q^m}$ is given by

$$\begin{aligned} m_a : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_{q^m} \\ x &\mapsto xa. \end{aligned}$$

This map can be extended to \mathbb{F}_q as

$$\begin{aligned} \mathbf{M}_a : \mathbb{F}_{q^m} &\rightarrow \mathbb{F}_q^m \\ x &\mapsto \mathbf{M}_a \Gamma(x), \end{aligned}$$

where $\mathbf{M}_a \in \mathbb{F}_q^{m \times m}$ is defined through having the columns $\Gamma(a\gamma_1), \dots, \Gamma(a\gamma_m)$.

Example 244. Let us consider $\mathbb{F} - 8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$ and the basis $\Gamma = \{1, \alpha, \alpha^2\}$. Multiplication with α^2 is given by the matrix

$$\mathbf{M}_{\alpha^2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Then for any $x \in \mathbb{F}_8$, we get that $\Gamma(\alpha^2 x) = \mathbf{M}_{\alpha^2} \Gamma(x)$.

Algorithm 5 GRS Algorithm

Input: $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ and $t \leq r \leq n-k$.

Output: $\mathbf{e} \in \mathbb{F}_{q^m}^n$ with $\text{wt}_R(\mathbf{e}) = t$ and $\mathbf{H}\mathbf{e}^\top = \mathbf{s}^\top$.

- 1: Choose random subspace $\mathcal{S} = \langle \mathbf{s}_1, \dots, \mathbf{s}_r \rangle \subset \mathbb{F}_q^n$ of dimension r .
 - 2: Write the error vector in terms of the basis $\mathbf{s}_1, \dots, \mathbf{s}_t$ as $e_i = \sum_{j=1}^r e_{ij} \mathbf{s}_j$, with unknowns $e_{ij} \in \mathbb{F}_q$.
 - 3: Solve the linear system of equations (over \mathbb{F}_q) implied by $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ to obtain the e_{ij} .
 - 4: **if** $\text{wt}_R(\mathbf{e}) \leq t$ **then**
 - 5: Return \mathbf{e} .
 - 6: Else, go to Step 1.
-

The cost of the GRS algorithm is only given by guessing a subspace $\mathcal{S} \subset \mathbb{F}_q^n$ of dimension r , which contains $\text{supp}_R(\mathbf{e})$.

Thus the success probability of one iteration is given by

$$P = \frac{|\{\mathcal{S} \subset \mathbb{F}_q^n \mid \dim(\mathcal{S}) = r, \text{supp}_R(\mathbf{e}) \subset \mathcal{S}\}|}{|\{\mathcal{S} \subset \mathbb{F}_q^n \mid \dim(\mathcal{S}) = r\}|} = \frac{\begin{bmatrix} n-t \\ r-t \end{bmatrix}_q \begin{bmatrix} n \\ r \end{bmatrix}_q^{-1}}{1}.$$

All the other steps, namely writing \mathbf{e} in terms of the basis of \mathcal{S} and solving the linear system of equations can be done in polynomial time.

Thus, the GRS algorithm costs

$$\begin{bmatrix} n \\ r \end{bmatrix}_q \begin{bmatrix} n-t \\ r-t \end{bmatrix}_q^{-1} \sim q^{(n-r)t}.$$

In order to get an overdetermined system and thus a candidate solution for \mathbf{e} , we only require to have more equations than unknowns. Since there are rn many unknowns e_{ij} , and we have $m(n-k)$ equations over \mathbb{F}_q , this forces us to choose $r \leq n-k$.

Proposition 245. *The GRS algorithm has an asymptotic cost of*

$$\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1} \sim q^{kt}.$$

Example 246. Let us consider $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ with $\alpha^3 = \alpha + 1$ and basis $\Gamma = \{1, \alpha, \alpha^2\}$. We are given the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha & 1 \end{pmatrix},$$

the syndrome $\mathbf{s} = (\alpha^2, \alpha + 1)$ and $t = 1$.

We guess the row support of \mathbf{e} to be $\langle (1, 0, 0, 1) \rangle \subset \mathbb{F}_2^4$. Hence $e_1 = e_4 = c$ and $e_2 = e_3 = 0$. We consider the 2 syndrome equations

$$\begin{aligned} e_1 + e_3 + \alpha^2 e_4 e_1 + \alpha^2 e_4 &= s_1 = \alpha^2 \\ e_2 + \alpha e_3 + e_4 e_4 &= s_2 = \alpha + 1. \end{aligned}$$

Using \mathbf{M}_{α^2} , we can write the equations as

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} + \begin{pmatrix} c_1 \\ c_1 + c_2 \\ c_0 + c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

From here we can already solve the system and get $\mathbf{c} = (\alpha + 1)$. We recompute $\mathbf{e} = \mathbf{c}\mathbf{R} = (\alpha + 1, 0, 0, \alpha + 1)$, which indeed has rank weight 1.

Exercise 247. Perform the same example but guess the row support to be $(1, 1, 0, 0)$.

We say that the GRS algorithm is the rank-metric analog of Prange, as it searches for \mathcal{S} of dimension $n-k$ with $\text{Supp}(\mathbf{e}) \subset \mathcal{S}$. While Prange's algorithm in the Hamming metric searches for I^C of size $n-k$ with $\text{Supp}_H(\mathbf{e}) \subset I^C$.

Indeed, while Prange's algorithm in the Hamming metric has the cost

$$\binom{n}{t} \binom{n-k}{t}^{-1},$$

the rank-metric analog has the cost

$$\begin{bmatrix} n \\ t \end{bmatrix}_q \begin{bmatrix} n-k \\ t \end{bmatrix}_q^{-1}.$$

The algebraic approach aims at translating the notion of the rank metric into an algebraic setting. For example via linearized polynomials: in [130] and [29] it was observed that for $\mathbf{e} \in \mathbb{F}_{q^m}^n$ there exists a linearized polynomial of q -degree t of the form

$$f(x) = \sum_{i=0}^t f_i x^{q^i}$$

annihilating the error vector, i.e., $f(\mathbf{e}_i) = 0$ for all $i \in \{1, \dots, n\}$. This algorithm works well for small choices of t , giving an approximate cost [130] of

$$\mathcal{O}\left((n-k)^3 q^{t\lceil \frac{(k+1)m}{n} \rceil - n}\right).$$

Recently, a new benchmark for the complexity of the rank SDP has been achieved by the paper [52], which solves the rank SDP using the well studied MinRank problem from multivariate cryptography. This might be one of the major reasons why NIST did not choose to finalize any of the code-based cryptosystem based on the rank metric, although they were achieving much lower public key sizes; this area of code-based cryptography needs further research before we can deem it secure.

5.3.10 Attacks on other Code-Based Problems

we have seen that ISD is the fastest algorithm to solve the Decoding Problem, the Syndrome Decoding Problem or the Given Weight Codeword Problem, whether we use the Hamming or the rank metric. This stays true also for the Lee metric [263] or restricted errors [76, 45], clearly, adapted to the considered metrics.

When considering code-equivalence problems, one could expect other algorithms to be faster. However, also in this case the fastest known algorithms rely on ISD [73]. In fact, we have seen in Section 2, that two equivalent codes \mathcal{C} and \mathcal{C}' have the same weight enumerator

$$W_i(\mathcal{C}) = |\{\mathbf{c} \in \mathcal{C} \mid \text{wt}(\mathbf{c}) = i\}| = W_i(\mathcal{C}').$$

Thus, the main algorithm to solve the code equivalence problem asks to find some low weight codewords in \mathcal{C} and \mathcal{C}' using ISD, ordering them as

$$S = \{b_{c_1}, \dots, b_{c_N}\},$$

respectively

$$S' = \{c'_1, \dots, c'_N\}$$

and then searching for an isometry that maps S to S' . Recall, that a code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k has on average

$$|B(q, n, r)| q^{k-n}$$

many codewords of weight r , where $B(q, n, r)$ denotes the balls of radius r in the respective metric.

If we search for codewords of very small weight, we thus get smaller sets S, S' and it becomes easier to find an isometry between the two sets. However, searching for a small weight increases the cost of the ISD algorithm to find them. On the other hand, when searching for a moderate weight r , the ISD algorithm has a small cost, but due to the large size of S, S' it becomes harder to find an isometry.

5.4 Algebraic Attacks

In this section, we present some techniques which are used for algebraic attacks on certain code-based cryptosystems. Most famously, is the square code attack, which is in general a distinguisher attack. *Distinguishers* a priori want to show that the public code is in fact not behaving randomly but like an algebraically structured code. Distinguishers can then further imply a strategy on how to recover the structure of the secret code, e.g. the evaluation points of a GRS code, or be used directly in a message recovery.

Definition 248. Let $v = (v_1, \dots, v_n), w = (w_1, \dots, w_n) \in \mathbb{F}_q^n$ be two vectors. The *Schur product* $v * w$ of v and w is the coordinatewise product of v and w , i.e.,

$$v * w := (v_1 w_1, \dots, v_n w_n).$$

With this definition we can also define the Schur product of two linear codes.

Definition 249. Let $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{F}_q^n$ be two linear codes. The Schur product of \mathcal{C}_1 and \mathcal{C}_2 is defined as the \mathbb{F}_q -span generated by the Schur product of all combinations of elements, i.e.,

$$\mathcal{C}_1 * \mathcal{C}_2 := \langle \{\mathbf{c}_1 * \mathbf{c}_2 \mid \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\} \rangle \subset \mathbb{F}_q^n.$$

For a linear code $\mathcal{C} \subset \mathbb{F}_q^n$, we call $\mathcal{C} * \mathcal{C}$ the *square code* of \mathcal{C} and denote it with $\mathcal{C}^{(2)}$.

Clearly for any code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k , we have that

$$\dim(\mathcal{C}^{(2)}) \leq \min \left\{ \frac{k(k+1)}{2}, n \right\}.$$

However, for codes which have a lot of algebraic structure, this square code dimension might be much smaller.

Proposition 250. Let $k \leq n \leq q$ be positive integers. Then,

$$\dim(\text{GRS}_{n,k}(\alpha, \beta)) = \min\{2k - 1, n\}.$$

Exercise 251. Prove Proposition 250.

Whereas for a random linear code of dimension k , the expected dimension of its square code is typically quadratic in the dimension k :

Theorem 252 ([85, Theorem 2.3]). For a random linear code \mathcal{C} over \mathbb{F}_q of dimension k and length n , we have with high probability that

$$\dim(\mathcal{C}^{(2)}) = \min \left\{ \binom{k+1}{2}, n \right\}.$$

This clearly provides a distinguisher between random codes and algebraically structured codes. Let us list some of the codes, which suffer from such a distinguisher

1. GRS codes: Proposition 250,
2. low-codimensional subcodes of GRS codes: [265],
3. Reed-Muller codes: [79],

4. Polar codes: [114],
5. some Goppa codes: [105],
6. high rate alternant codes: [118],
7. algebraic geometry codes [104, 103].

Note that square code attacks often need to be performed on a modified version of the public code, for example

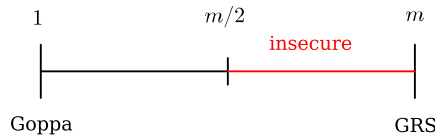
1. the sum of two GRS codes: [100, 106],
2. GRS codes with additional random entries: [102],
3. expanded GRS codes: [101].

McEliece proposed to use classical binary Goppa codes as secret codes in [193], and no algebraic attack on this system has been developed. Thus, they are considered to be reasonably secure and were chosen as the finalists for the NIST standardization process [14].

Recall that Goppa codes are heavily connected to GRS codes: let us consider a GRS code over \mathbb{F}_q^m and some $1 \leq \lambda \leq m$. The code \mathcal{C} which contains all codewords of the GRS code living in a fixed λ -dimensional \mathbb{F}_q -vector subspace of \mathbb{F}_q^m is called a *subspace subcode* of a GRS code.

- If we choose $\lambda = m$ we get a GRS code, which provides very low key sizes for the McEliece cryptosystem due to their large error correction capacity and only considering ISD attacks. They are however insecure due to the square code attack.
- If we choose $\lambda = 1$ we get a Goppa code, which suffers from very large key sizes due to their small correction capacity, but they are deemed to be secure against algebraic attacks.

The proposal [166] and also [64] propose to use a different λ in the McEliece system, trying to find a balance between the two extreme points and profiting from both advantages: smaller key sizes than Goppa codes would provide and thwarting the vulnerability of GRS codes. But also this suggestion has been attacked for $\lambda \geq m/2$ by the square code attack in [101]:



Let us summarize this in Table 19.

Note that for the rank-metric based cryptosystems a similar distinguisher exists for the rank analogues of the Reed-Solomon codes, namely the Gabidulin codes: these attacks all stem from the original attack of Overbeck [209] on the proposal [126] to use Gabidulin codes in the GPT framework, but also includes the attack of [155] on its generalization [184, 219]. Their main tool here is that instead of taking the square code, one performs the Frobenius map on the code.

Code \mathcal{C}	$\dim(\mathcal{C}^{(2)})$
Random Code	$\min\left\{\frac{k(k+1)}{2}, n\right\}$ (with high probability)
RS Code	$\min\{2k - 1, n\}$
Binary Goppa Codes [$n, k = n - mr$]	$\min\left\{\frac{k(k+1)}{2} - \frac{mr}{2}(2r \log_2(r) - r - 1), n\right\}$ (with high probability)
Expanded GRS Code [mn, mk]	$\min\{\mathcal{O}(mk^2), n\}$ (with high probability)

Table 19: Square code dimension of different codes

Let us consider an extension field \mathbb{F}_{q^m} of the base field \mathbb{F}_q . We denote by $[i]$ the i th Frobenius power, q^i . The Frobenius map can be applied to a matrix or a vector by doing so coordinatewise, i.e., for a matrix $\mathbf{M} \in \mathbb{F}_{q^m}^{k \times n}$ with entries $(m_{j,\ell})$ we denote by $\mathbf{M}^{[i]}$ the matrix with entries $(m_{j,\ell}^{[i]})$.

Definition 253. Let $\mathbf{M} \in \mathbb{F}_{q^m}^{k \times n}$ and $\ell \in \mathbb{N}$, then we define the operator Λ_ℓ as

$$\Lambda_\ell : \mathbb{F}_{q^m}^{k \times n} \rightarrow \mathbb{F}_{q^m}^{(\ell+1)k \times n},$$

$$\mathbf{M} \mapsto \Lambda_\ell(\mathbf{M}) = \begin{pmatrix} \mathbf{M} \\ \mathbf{M}^{[1]}, \\ \vdots \\ \mathbf{M}^{[\ell]} \end{pmatrix}.$$

The Frobenius attack now considers the rowspan of this new matrix.

Proposition 254 ([209], Lemma 5.1). *If \mathbf{M} is the generator matrix of an $[n, k]$ Gabidulin code and $\ell \leq n - k - 1$, then the subvector space spanned by the rows of $\Lambda_\ell(\mathbf{M})$ is an $[n, k + \ell]$ Gabidulin code.*

Note that this is similar to Proposition 250, where one shows that the square code of a GRS code is again a GRS code. And as the square code dimension of a GRS code is $2k - 1$, in this case the dimension of the rowspace of the Frobenius of a Gabidulin code is $k + \ell$.

However, for a random code \mathcal{C} , the Frobenius of this code should have dimension of order $k\ell$.

Theorem 255 ([186]). *Let $\mathbf{M} \in \mathbb{F}_{q^m}^{k \times n}$ be a random matrix of full column rank over \mathbb{F}_q . Then $\Lambda_\ell(\mathbf{M})$ has rank*

$$\min\{(\ell + 1)k, n\},$$

with probability at least $1 - 4q^{-m}$.

The Frobenius map can thus distinguish between a Gabidulin code and a random code.

5.5 Other Attacks

We want to note here, that there exist also several other attacks on code-based cryptosystems, such as: side-channel attacks and chosen-ciphertext attacks. Since these attacks are less mathematically involved, we will just quickly cover them and refer interested readers to [87].

Side-channel attacks try to get information from the implementation of the cryptosystem, which includes timing information, power consumption and many more. Thus, side-channel attacks complement the algebraic and non-structural attacks we have discussed before by considering also the physical security of the cryptosystem.

There have been many side-channel attacks on the McEliece cryptosystem (see for example [251, 35, 250, 91, 225]) which aim for example at the timing/reaction attacks based on the error weight or recover the error weight using a simple power analysis on the syndrome computation.

Note that recently the information gained through side-channel attacks was used in ISD algorithms in [153].

Another line of attacks is the *chosen-ciphertext attack* (CCA): in a chosen-ciphertext attack we consider the scenario in which the attacker has the ability to choose ciphertexts c_i and to view their corresponding decryptions, i.e., the messages m_i . In this scenario we might speak of an oracle that is queried with ciphertexts. The aim of the attacker is to gain the secret key or to get as much information as possible on the attacked system.

In an *adaptive chosen-ciphertext attack* (CCA2) the attacker wants to distinguish a target ciphertext without consulting the oracle on this target. Thus, the attacker may query the oracle on many ciphertext but the target one. This means that the new ciphertexts are created based on responses (being the corresponding messages) received previously.

In this context we also speak of ciphertext indistinguishability, meaning that an attacker can not distinguish ciphertexts based on the message they encrypt. We have two main definitions:

1. *Indistinguishability under chosen-plaintext attack* (IND-CPA),
2. *Indistinguishability under adaptive chosen-ciphertext attack* (IND-CCA2).

These are usually defined over a game, which is played between an attacker and a *challenger*, where we assume that we have a public-key encryption scheme with a secret key \mathcal{S} and a publicly known public key \mathcal{P} .

For IND-CPA, the attacker and the challenger are playing the following game.

1. The attacker sends two distinct messages m_1, m_2 to the challenger.
2. The challenger selects one of the messages m_i and sends the *challenge* c_i , which is the encrypted message m_i .
3. The attacker tries to guess i .

We say that a system is *IND-CPA secure* if an attacker has only a negligible advantage over randomly guessing i .

For IND-CCA2, the attacker and the challenger are playing the following game.

1. The attacker sends two distinct messages m_1, m_2 to the challenger.
2. The challenger selects one of the messages m_i and sends the *challenge* c_i , which is the encrypted message m_i .
3. The attacker may query a decryption oracle on any cipher but the target cipher c_i .
4. The attacker tries to guess i .

We say that a system is *IND-CCA2 secure* if an attacker has only a negligible advantage over randomly guessing i .

Let us consider the McEliece framework from Section 3.1.

The IND-CPA security for this framework translates as: the challenger performs the key generation, getting the secret key $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ and sends the public key $\mathbf{G}' \in \mathbb{F}_q^{k \times n}$ to the attacker. The attacker chooses two messages $\mathbf{m}_1, \mathbf{m}_2 \in \mathbb{F}_q^k$ and sends them to the challenger. The challenger now chooses $b \in \{1, 2\}$ and encrypts \mathbf{m}_b as

$$\mathbf{c} = \mathbf{m}_b \mathbf{G}' + \mathbf{e},$$

for some random error vector of Hamming weight t . The challenger sends \mathbf{c} back to the attacker. The attacker tries to figure out whether \mathbf{m}_1 or \mathbf{m}_2 was encrypted.

Proposition 256. *The classic McEliece framework is not IND-CPA secure.*

Proof. The attacker can easily recover which message was encrypted by computing

$$\begin{aligned} \mathbf{c}_1 &= \mathbf{m}_1 \mathbf{G}', \\ \mathbf{c}_2 &= \mathbf{m}_2 \mathbf{G}', \end{aligned}$$

and testing whether the received \mathbf{c} has distance t from one of the codewords. Indeed, if \mathbf{m}_1 was encrypted, then

$$\mathbf{c} - \mathbf{c}_1 = \mathbf{m}_1 \mathbf{G}' - \mathbf{m}_1 \mathbf{G}' + \mathbf{e} = \mathbf{e}$$

has weight t , whereas

$$\mathbf{c} - \mathbf{c}_2 = \mathbf{m}_1 \mathbf{G}' - \mathbf{m}_2 \mathbf{G}' + \mathbf{e} = (\mathbf{m}_1 - \mathbf{m}_2) \mathbf{G}' + \mathbf{e}$$

has weight larger than t , as any codeword (thus also $(\mathbf{m}_1 - \mathbf{m}_2) \mathbf{G}'$) has weight at least $2t + 1$ and adding \mathbf{e} , we can decrease the weight to at least $t + 1$. \square

Exercise 257. Show that the Niederreiter framework is not IND-CPA secure.

An easy fix for this issue is called *random padding*. Instead of choosing the message $\mathbf{m} \in \mathbb{F}_q^k$, we only choose a part of the message, say $\mathbf{m}' \in \mathbb{F}_q^\ell$ and choose the remaining $k - \ell$ position at random, called \mathbf{r} .

Proposition 258. *The McEliece framework using random padding is IND-CPA secure.*

Proof. The attacker has now chosen $\mathbf{m}_1, \mathbf{m}_2 \in \mathbb{F}_q^\ell$ and sends them to the challenger. Assume the challenger encrypts \mathbf{m}_1 as

$$\mathbf{c} = (\mathbf{m}_1, \mathbf{r})\mathbf{G}' + \mathbf{e},$$

and sends this back to the attacker. Let us split the public generator matrix into $\mathbf{A} \in \mathbb{F}_q^{\ell \times n}$ and $\mathbf{B} \in \mathbb{F}_q^{(k-\ell) \times n}$, hence the ciphertext is

$$\mathbf{c} = \mathbf{m}_1\mathbf{A} + \mathbf{rB} + \mathbf{e}.$$

The attacker can now compute

$$\mathbf{c}_1 = \mathbf{m}_1\mathbf{A},$$

$$\mathbf{c}_2 = \mathbf{m}_2\mathbf{A}.$$

Taking these away from the received ciphertext, the attacker gets

$$\mathbf{c} - \mathbf{c}_1 = \mathbf{rB} + \mathbf{e},$$

$$\mathbf{c} - \mathbf{c}_2 = \mathbf{rB} + (\mathbf{m}_1 - \mathbf{m}_2)\mathbf{A} + \mathbf{e}.$$

However, the only way to recover \mathbf{r} or \mathbf{e} is to solve the SDP. □

Note that in [169] the authors gave conversions of the McEliece system to achieve CCA2 security.

For digital signature schemes, we have a similar notion to CCA and CPA, called Existential UnForgeability under Chosen Message Attack (EUF-CMA).

The new game works as follows.

1. The challenger generates a secret key \mathcal{S} and a public key \mathcal{P} and sends \mathcal{P} to the attacker.
2. The attacker chooses messages m_1, \dots, m_N and sends them to the challenger.
3. The challenger generates the signatures $(\sigma_1, \dots, \sigma_N)$ and sends them to the attacker.
4. The attacker wins, if the attacker is able to generate a valid signature σ for some message $m \neq m_i$.

The signature scheme is called EUF-CMA secure if no (efficient) adversary has a non-negligible advantage in winning the game. Note that EUF-CMA security, thus, also asks for signatures to behave indistinguishably from some random distribution.

6 Historical Overview

There have been many proposals especially for the McEliece framework. We will here only list a small choice of them, which we hope represent well the major difficulties in proposing new code-based cryptosystems.

McEliece proposed to use binary Goppa codes for his framework, and while the initially proposed parameters are now broken with information set decoding [70], algebraic attacks are only known for specific parameter sets of Goppa codes [105, 118]. In fact, for most parameter sets, there is no algebraic property of binary Goppa codes known which distinguishes them from a random code. The drawback of binary Goppa codes, however, is that they can only correct a small amount of errors, leading to large generator matrices for cryptosystems to reach a fixed security level, resulting in large key sizes.

Other proposals have tried to avoid this problem by using other classes of algebraic codes. Several proposals are based on GRS codes, since these codes have the largest possible error correction capability, but were ultimately broken: Sidelnikov-Shestakov proposed an attack [244] which recovers parameters for the Niederreiter scheme [204], where GRS codes were originally proposed.

Attempts to avoid this weakness [65, 42, 44, 47, 77, 167, 204, 166, 61] were often unsuccessful, as GRS codes can be distinguished from random codes with the help of the square code [265, 100, 106, 101, 177], since the square code of a GRS code has a very low dimension.

Other proposals have been made using non-binary Goppa codes [71], algebraic geometry codes [160], LDPC and MDPC codes [46, 198, 197], Reed-Muller codes [245] and convolutional codes [187], but most of them were unsuccessful in hiding the structure of the private code [104, 105, 172, 196, 206].

The first rank-metric code based cryptosystem called GPT was proposed in 1991 by Gabidulin, Paramonov and Tretjakov [126]. The authors suggest the use of Gabidulin codes, which can be seen as the rank-metric analog of GRS codes. Similar to the distinguisher on GRS codes, namely the square code attack, also Gabidulin codes suffer from a distinguisher by Overbeck [209] using the Frobenius map. The GPT system was then generalized in [219], but still suffers from an extended Frobenius distinguisher [155]. Since this proposal some authors have tried to fix this security issue by tweaking the Gabidulin code [63, 218]. Other rank-metric systems include [185, 127, 154].

Next, we want to list some of the most important proposals for code-based signature schemes. The first code-based signature scheme was proposed in 2001 by Courtois, Finiasz and Sendrier (CFS) [98]. Again this can be considered as a framework, but the code suggested by the authors was a high rate Goppa code, for which, unfortunately, a distinguisher exists [118]. Another way to approach this problem is to relax the weight condition on the error vector. This idea has been followed in [43] where low-density generator matrices were proposed, in [141], where convolutional codes were suggested, and in [179], where they use Reed-Muller codes. The proposals [43, 141] have been attacked in [214, 199] respectively.

Also notable are the signature schemes in [162, 163, 59, 131], which can at most be considered as one-time signatures due to the attack in [88, 205].

In [151] the authors propose binary $(U, U + V)$ codes in a signature scheme and the security relies on the problem of finding a closest codeword. However, the hull of such a code is typically much larger than for a random linear code of the same length and dimension. Thus, this proposal has been attacked in [108]. This problem has later been solved by the

Code	proposed in	attack
Goppa	[193, 14]	
Wild Goppa	[71]	[105]
Interleaved Goppa	[117]	
GRS	[204]	[244]
Twisted RS	[61]	[177]
low-codimensional subcodes of GRS	[65]	[265]
Sum of GRS	[42, 167]	[100]
Expanded GRS	[166]	[101]
Subspace Subcodes of GRS	[64]	[101]
GRS and random columns	[261, 264]	[102]
$(U, U + V)$ RS	[190]	
Reed-Muller	[245]	[79, 196]
Polar	[243]	[114]
Algebraic geometry	[160]	[104, 103]
LDPC	[46, 198]	[206]
MDPC	[197]	[206]
Convolutional	[187]	[172]
Ordinary concatenated	[236]	[237]
Generalized concatenated	[217]	

Table 20: Proposals for the McEliece Framework

Code	proposed in	attack
Gabidulin	[126, 219]	[209, 155]
Subspace subcodes of Gabidulin	[63]	
Twisted Gabidulin	[218]	

Table 21: Proposals for the GPT framework

authors of Wave [109], by using generalized $(U, U + V)$ codes over the ternary and basing the security on the farthest codeword problem. In addition, Wave provides a proof of the preimage sampleable property (first introduced in [138]), which thwarts all attacks trying to

Code	proposed in	attack
GRS (list decoding)	[33]	[97]
Gabidulin (list decoding)	[119]	[129]
Interleaved Gabidulin	[259, 224, 223]	[78]
Gabidulin	[176]	[78]

Table 22: Proposals for the AF framework

exploit the knowledge of signatures.

In [247] the authors propose a code-based signature scheme from the Lyubashevsky framework, which was then broken in [17].

Also the code-equivalence problem has been used for a code-based signature scheme in [74], which was attacked in [73]. The LESS signature scheme resolved the vulnerability in [36].

A one-time signature scheme from quasi-cyclic codes has been proposed in [211]. Also this proposal has been attacked in [232].

The signature scheme RaCoSS [230] submitted to NIST standardization process is similar to the hash-and-sign approach of CFS but depending on some Bernoulli distributed vector. This proposal has been broken (either see [266] or the comment section on the NIST website¹).

Finally, the signature scheme pqsigRM [179] is an adaption of the broken CFS scheme [98], where the authors propose the use of Reed-Muller codes instead of Goppa codes, this proposal has also been cryptanalyzed².

In the rank metric, one of the most notable signature schemes is that of RankSign [27], which has been attacked in [110]. Other rank-metric signature schemes include Durandal [25], which is in the Lyubashevsky framework and MURAVE [174]. Note that, even though Durandal has an EUF-CMA security proof, it has recently been broken [26].

Due to the Fiat-Shamir transform, we also include code-based ZK protocols here, although the proposals until now all suffer from large signature sizes. The ZK protocols usually use random codes, thus we will often not specify a particular proposed code.

The first code-based ZK protocol was proposed by Stern in 1993 [249] and recently after also by Véron [258]. In this survey we have covered two improvements on their idea, namely CVE [89] and AGS [3].

In a recent paper [41] the authors propose to use restricted error vectors in CVE, which leads to smaller signature sizes.

Another approach to reduce the signature sizes is the quasi-cyclic version of Stern’s ZK protocol, proposed in [75].

Also rank-metric ZK protocols have been proposed in the recent paper [62], with the aim of turning it into a fully fledged rank-metric signature scheme.

¹<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/RaCoSS.pdf>

²<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/pqsigRM.pdf>

7 Submissions to NIST

In 2016 the National Institute of Standards and Technology (NIST) started a competition to establish post-quantum cryptographic standards for public-key cryptography and signature schemes. Initially, 82 proposals were submitted of which 69 could participate in the first round. 19 of these submissions were based on coding theory.

In 2020, the third round was announced. Of the initial candidates, 9 public-key systems and 6 signature schemes still remain in this round. Three of the 9 public-key cryptosystems are code-based, one of them being Classic McEliece [14], a Niederreiter-based adaption of the initial McEliece cryptosystem.

The other two candidates put effort on avoiding the drawback of large public-key sizes. BIKE [20] achieves this by combining circulant matrices with MDPC codes, whereas HQC [5] is a proposal based on the quasi-cyclic scheme, which does not require using the algebraic structure of the error-correcting code.

In this section, we will study these candidates in depth, for this we provide tables summarizing the submissions that were eliminated in round 1, round 2 and finally the finalists of round 3.

Table 23 contains all public-key encryption and key-encapsulation mechanism candidates, which were eliminated in round one. All candidates use the Hamming metric (HM) or the rank metric (RM). Key sizes will be given in kilobytes, pk denotes the public key and sk the secret key.

Due to space limitations, we will sometimes abbreviate the McEliece framework with MF, the Niederreiter framework with NF, the framework of Alekhnovich by AF, the quasi-cyclic framework by QCF and finally a Diffie-Hellman approach by DH.

In addition to acronyms that were already introduced, we also abbreviate quasi-cyclic (QC), Ideal Code (IC) and double-circulant (DC).

The given key sizes are for the parameter sets that were proposed for 128 bits of security (however, some proposals contained multiple suggestions for parameter sets for this security level).

All data is taken from the supporting documentations of the NIST proposals BIG QUAKE [50], DAGS [48], Edon-K [140], LAKE [23], LEDAkem [38], LEDApkc [39], Lepton [268], LOCKER [24], McNie [135], Ouroboros-R [7], QC-MDPC KEM [267], Ramstake [252] and RLCE-KEM [261].

The reason for the drop out of BIG QUAKE was mainly discussed at CBC 2019³, and is due to the large key sizes of the proposal, as it is "still worse than completely unstructured lattice KEM." The reason for Lepton's drop out, is a security issue that can be found in the comment section of the NIST website⁴.

³<https://drive.google.com/file/d/1nruEobwdeJbtwouJssbjZCK0WQiBN7rW/view>

⁴<https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/official-comments/Lepton-official-comment.pdf>

Candidate	Framework	Code	Metric	Pk Size	Reason for Drop Out
BIG QUAKE	NF	QC Goppa	HM	25 – 103	large key sizes
DAGS	MF	dyadic GS	HM	8.1	broken [54]
Edon K	MF	binary Goppa	HM	2.6	broken [182]
LAKE	NF	IC, DC, LRPC	RM	0.4	merged (ROLLO)
LEDAskem	NF	QC LDPC	HM	3.5 – 6.4	merged (LedAcrypt)
LEDApkc	MF	QC LDPC	HM	3.5 – 6.4	merged (LedAcrypt)
Lepton	AF	BCH	HM	1.0	cryptanalysis
LOCKER	NF	IC, DC, LRPC	RM	0.7	merged (ROLLO)
McNie	MF/NF	QC LRPC	RM	0.3 – 0.5	broken [28] [173]
Ouroboros-R	QCF	DC LRPC	RM	1.2	merged (ROLLO)
QC-MDPC KEM	MF	QC MDPC	HM	1.2 – 2.6	N/A
Ramstake	DH	RS	HM	26.4	broken [253]
RLCE-KEM	MF	GRS	HM	118 – 188	broken [102]

Table 23: Code-based PKE/KEM submissions to NIST, eliminated in round 1

In Table 24 we list all code-based signature schemes that were eliminated during round one, which in every case was due to cryptanalysis.

The table contains their signature sizes, public key sizes, secret key sizes (all in kilobytes) and the recommended number of rounds necessary to ensure verification with a very high probability.

For this a security level of 128-bit is fixed in the respective scheme. The signature size of pqsigRM is taken from [180], all other data is taken from the supporting documentations pqsigRM [179], RaCoSS [230] and RankSign [27].

Candidate	Signature Size	Pk Size	Sk Size	Rounds
pqsigRM	0.5	262	138	100
RaCoSS	0.3	169	100	100
RankSign	1.4 – 1.5	10	1.4 – 1.5	N/A

Table 24: Code-based signature submissions to NIST, eliminated in round 1

Table 25 contains all PKE/KEM candidates that were eliminated during round two. There are no code-based signature schemes that made it to round two or further.

All data is taken from the supporting documentations of LEDAcrypt [40], NTS-KEM [13], ROLLO [4] and RQC [6].

Candidate	Framework	Code	Metric	Pk Size	Reason for Drop Out
LEDAcrypt	McE/N	QC LDPC	HM	1.4 – 2.7	broken [16]
NTS-KEM	Niederreiter	binary Goppa	HM	319	merged (Classic McE)
ROLLO	Niederreiter	IC, LRPC	RM	0.7	cryptanalysis [51]
RQC	Quasi-Cyclic	IC, Gabidulin	RM	1.8	N/A

Table 25: Code-based PKE/KEM submissions to NIST, eliminated in round 2

Finally, there are three candidates that made it to the final round, round three. Classic McEliece, as main candidate, and BIKE and HQC as alternative candidates.

As before, the public key (pk) size is given in kilobytes, data is taken from the proposed parameters for the 128-bit security level.

Candidate	Framework	Code	Metric	pk size
Classic McEliece	Niederreiter	binary Goppa	Hamming	261
BIKE	Niederreiter	MDPC	Hamming	1.5
HQC	Quasi-Cyclic	decodable code of choice, QC	Hamming	2.2

Table 26: Final round code-based PKE submissions to NIST

7.1 Round 4 Candidates: Classic McEliece, BIKE and HQC

In this section, we present the three code-based proposals Classic McEliece, BIKE and HQC, which are in the fourth round of the NIST standardization call from 2016. For each one, we give a mathematical description and the proposed parameters.

7.1.1 Classic McEliece

The NIST submission Classic McEliece uses the Niederreiter framework (Section 3.2) with binary Goppa codes (Definition 49) as secret codes. This subsection is based on the round 3 submission [14].

Let us start with the description of the scheme. Let m be a positive integer, $q = 2^m$, $n \leq q$ and $t \geq 2$ be positive integers such that $mt < n$ and set $k = n - mt$.

Further, pick a monic irreducible polynomial $f(z) \in \mathbb{F}_2[z]$ of degree m and identify \mathbb{F}_q with $\mathbb{F}_2[z]/f(z)$. Note that under this identification, every element in \mathbb{F}_{2^m} can be written as

$$u_0 + u_1z + \dots + u_{m-1}z^{m-1}$$

for a unique vector $(u_0, u_1, \dots, u_{m-1}) \in \mathbb{F}_2^m$.

With these preliminaries set, we can describe the public-key encryption scheme:

- **Key Generation:**

1. Generate a random monic irreducible polynomial $g(x) \in \mathbb{F}_q[x]$ of degree t and n random distinct elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$.
2. Compute a parity-check matrix $\tilde{\mathbf{H}} = \{\tilde{h}_{ij}\}_{ij}$ of the binary Goppa code with parameters $(g, \alpha_1, \dots, \alpha_n)$ by computing $\tilde{h}_{ij} = \alpha_j^{i-1}/g(\alpha_j)$.
3. Apply an invertible matrix to $\tilde{\mathbf{H}}$ and permute the columns of this matrix to get a matrix in systematic form $\mathbf{H} = (\text{Id}_{n-k} | \mathbf{T})$.
Denote with $(\alpha'_1, \dots, \alpha'_n)$ the n -tuple obtained by applying the same permutation to $(\alpha_1, \dots, \alpha_n)$.
Note that $(\text{Id}_{n-k} | \mathbf{T})$ is a parity-check matrix of the Goppa code defined by $(g, \alpha'_1, \dots, \alpha'_n)$.

- **Private Key:** The private key is the $(n+1)$ -tuple $\Gamma' = (g, \alpha'_1, \dots, \alpha'_n)$.
- **Public Key:** The public key is the $(n-k) \times (n-k)$ matrix \mathbf{T} and the number t .
- **Encryption:** Encode the message as weight t vector $\mathbf{e} \in \mathbb{F}_2^n$ and compute

$$\mathbf{c}_0 = \mathbf{H}\mathbf{e}^\top \in \mathbb{F}_2^{n-k}.$$

- **Decryption:** Extend \mathbf{c}_0 to $\mathbf{v} = (\mathbf{c}_0^\top, 0, \dots, 0) \in \mathbb{F}_2^n$. The parameters Γ' of the private key define a Goppa code, so we can use a decoding algorithm for Goppa codes to find a codeword \mathbf{c} with distance $\leq t$ to \mathbf{v} (if it exists).

We then recover \mathbf{e} as $\mathbf{e} = \mathbf{v} + \mathbf{c}$ and check that it indeed satisfies $\mathbf{H}\mathbf{e}^\top = \mathbf{c}_0$ and is of weight t .

Remark 259. The decryption works for the following reason: we have that $\mathbf{H} = (\text{Id}_{n-k} | \mathbf{T})$, so

$$\mathbf{H}\mathbf{v}^\top = \text{Id}_{n-k}\mathbf{c}_0 = \mathbf{c}_0.$$

Thus, it follows that

$$\mathbf{H}(\mathbf{v} + \mathbf{e})^\top = 0,$$

and $\mathbf{c} = \mathbf{v} + \mathbf{e}$ is a codeword of the Goppa code defined by Γ' .

Since this code has minimum distance at least $2t + 1$, we get that $\mathbf{v} + \mathbf{e}$ is also the unique codeword of distance up to t from \mathbf{v} , so we may recover the error vector as $\mathbf{e} = \mathbf{v} + \mathbf{c}$.

7.1.2 Proposed Parameters for Classic McEliece

We give an overview of the proposed parameter sets, input and output sizes for the expected security levels. Level 1 corresponds to 128 bits, level 3 corresponds to 192 bits and level 5 corresponds to 256 bits of security. The key sizes and ciphertext size are given in bytes.

Parameter set	m	n	t	Public key	Private key	Ciphertext	Security level
mceliece348864	12	3488	64	261120	6492	128	1
mceliece460896	13	4608	96	524160	13608	188	3
mceliece6688128	13	6688	128	1044992	13932	240	5
mceliece6960119	13	6960	119	1047319	13948	226	5
mceliece8192128	13	8192	128	1357824	14120	240	5

Table 27: Parameters for Classic McEliece

The Classic McEliece submission is considered the main candidate for standardization by NIST. It is clearly based on the original proposal of McEliece [193] and thus a rather conservative choice by NIST. The main advantage of Classic McEliece is thus its well studied security, as there are no known algebraic attacks on the original proposal of McEliece since 1978, but it still suffers from the same disadvantage, i.e., the large size of its public keys.

7.1.3 BIKE

The NIST submission Bit Flipping Key Encapsulation (BIKE) combines circulant matrices with the idea of moderate density parity-check matrices (Definition 74). The usage of circulant matrices keeps key sizes small while using moderate density parity-check matrices allows efficient decoding with a Bit-Flipping algorithm. We follow the NIST round 3 submission [20] and give a ring-theoretic description of the system. Note however that BIKE can also be fully described with matrices.

Let r be prime number such that 2 is primitive modulo r , i.e., 2 generates the multiplicative group $\mathbb{Z}/r\mathbb{Z}^*$. The parameter r denotes the block size, from which we obtain the code length $n = 2r$. We further pick an even row weight $w \approx \sqrt{n}$ such that $w/2$ is odd and an error weight $t \approx \sqrt{n}$.

We then set $R := \mathbb{F}_2[x]/(x^r - 1)$. Any element $a \in R$ can be represented as polynomials of degree less or equal than $r - 1$ and can uniquely be written as linear combination of the form

$$a = \sum_{i=0}^{r-1} a_i x^i,$$

where $a_i \in \mathbb{F}_2$ for all $i \in \{0, 1, \dots, r - 1\}$.

This gives us a natural notion of the weight of a , which we denote with $\text{wt}(a)$, i.e.,

$$\text{wt}(a) = |\{i \in \{0, 1, \dots, r - 1\} \mid a_i \neq 0\}|.$$

Remark 260. The choice of r ensures that the irreducible factors of $x^r - 1$ are $x - 1$ and $x^{r-1} + x^{r-2} + \dots + 1$ (see Exercise 263). As a consequence of this, an element $a \in R$ is invertible if and only if $\text{wt}(a)$ is odd and $\text{wt}(a) \neq r$.

- **Key Generation:** Pick a pair $(h_0, h_1) \in R^2$ such that $\text{wt}(h_0) = \text{wt}(h_1) = w/2$. Then compute $h = h_1 h_0^{-1} \in R$.
- **Private Key:** The private key is the pair (h_0, h_1) .
- **Public Key:** The public key is the element $h \in R$ and the integer t .
- **Encryption:** The message gets encoded as error $(e_0, e_1) \in R^2$ such that $\text{wt}(e_0) + \text{wt}(e_1) = t$ and then encrypted as $s = e_0 + e_1 h$.
- **Decryption:** We compute $sh_0 = e_0 h_0 + e_1 h_1$. Since h_0 and h_1 are of moderate density, this can be decoded efficiently with a Bit-Flipping algorithm to recover the pair (e_0, e_1) .

Remark 261. The difficulty of attacking BIKE lies in finding an element $\tilde{h} \in R$ of at most moderately high weight, such that $h\tilde{h}$ is also of at most moderately high weight.

Remark 262. BIKE can also be described with matrices: for

$$a = \sum_{i=0}^{r-1} a_i x^i \in R$$

and

$$b = \sum_{i=0}^{r-1} b_i x^i,$$

we are considering the code with parity-check matrix

$$\mathbf{H} = \left(\begin{array}{ccccc|ccccc} a_0 & a_1 & \cdots & a_{r-2} & a_{r-1} & b_0 & b_1 & \cdots & b_{r-2} & b_{r-1} \\ a_{r-1} & a_0 & \cdots & a_{r-3} & a_{r-2} & b_{r-1} & b_0 & \cdots & b_{r-3} & b_{r-2} \\ \vdots & & \ddots & & \vdots & \vdots & & \ddots & & \vdots \\ a_2 & a_3 & \cdots & a_0 & a_1 & b_2 & b_3 & \cdots & b_0 & b_1 \\ a_1 & a_2 & \cdots & a_{r-1} & a_0 & b_1 & b_2 & \cdots & b_{r-1} & b_0 \end{array} \right).$$

In this case, the errors $e_0 = \sum_{i=0}^{r-1} e_{0,i}x^i$ and $e_1 = \sum_{i=0}^{r-1} e_{1,i}x^i$ may be viewed as vectors

$$\tilde{\mathbf{e}}_j = (e_{j,0}, e_{j,r-1}, e_{j,r-2}, \dots, e_{j,1})$$

for all $j \in \{1, 2\}$. We then compute syndromes by

$$\mathbf{H}(\tilde{\mathbf{e}}_1 \mid \tilde{\mathbf{e}}_2)^\top.$$

Exercise 263. Let r be a prime such that 2 generates $\mathbb{Z}/r\mathbb{Z}^\star$. Show that the irreducible factors of $x^r - 1 \in \mathbb{F}_2[x]$ are $x - 1$ and $x^{r-1} + x^{r-2} + \dots + 1$. You may use the following steps:

1. Let $p(x)$ be a monic irreducible factor of $x^{r-1} + x^{r-2} + \dots + 1$ and α a root of $p(x)$ in the algebraic closure. Show that r is the smallest positive integer such that $\alpha^r = 1$.
2. Justify that the roots of $p(x)$ are the elements of the set $\{\alpha^{(2^n)} \mid n \in \mathbb{N}_{\geq 1}\}$.
3. Show that $\{\alpha^{(2^n)} \mid n \in \mathbb{N}_{\geq 1}\}$ contains exactly $r - 1$ elements and conclude that $p(x) = x^{r-1} + x^{r-2} + \dots + 1$.

7.1.4 Proposed Parameters for BIKE

We now present the proposed parameters for three levels of security, where again level 1 is 128 bits of security, level 3 is 192 bits, and level 5 is 256 bits of security. We also include an estimate for the decoding failure rate (DFR) and key and ciphertext sizes in bytes.

Security	r	w	t	Private key	Public key	Ciphertext	DFR
Level 1	12323	142	134	281	1541	1573	2^{-128}
Level 3	24659	206	199	419	3083	3115	2^{-192}
Level 5	40973	274	264	580	5122	5154	2^{-256}

Table 28: Parameters for BIKE

It can be seen that BIKE has small public key sizes, which is a big advantage over the other systems.

7.1.5 HQC

The submission Hamming Quasi-Cyclic (HQC) is based on the quasi-cyclic framework (see Section 3.4) and uses a combination of a decodable code of choice and circulant matrices.

The third round proposal suggests to use concatenated Reed-Muller and Reed-Solomon codes (Definitions 78, 75, 44), in the initial NIST submission [8, Section 1.6] a tensor product code of a BCH and a repetition code was proposed. An important feature of HQC is the fact that the used codes are not secret.

We follow the NIST submission [5] for the detailed description.

Let n be such that $(x^n - 1)/(x - 1)$ is irreducible over \mathbb{F}_2 . We pick a positive integer $k < n$ and an $[n, k]$ linear code \mathcal{C} with an efficient decoding algorithm, whose error correcting

capacity is given by t . We are further given error weights w , w_r and w_e , all in the range of $\frac{\sqrt{n}}{2}$. We set $R := \mathbb{F}_2[x]/(x^n - 1)$. Recall that any element $a \in R$ can be written as

$$a = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_0$$

for unique $a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_2$. For such an element we denote its Hamming weight as

$$\text{wt}_H(a) = |\{i \in \{0, 1, \dots, n-1\} \mid a_i \neq 0\}|.$$

Note also that we can identify a vector $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_2^n$ with the element $a = \sum_{i=0}^{n-1} a_i x^i \in R$ and vice versa. In the following description any bold letter, e.g. \mathbf{u} , refers to the associated vector in \mathbb{F}_2^n of an element in R , e.g. $u \in R$.

- **Key Generation:** Given the parameters (n, k, t, w, w_e, w_r) , choose a generator matrix \mathbf{G} of the code \mathcal{C} and generate a random $h \in R$.
- **Private Key:** The private key is a randomly generated pair $(y, z) \in R^2$ such that $\text{wt}_H(y) = \text{wt}_H(z) = w$.
- **Public Key:** We compute $s = y + hz \in R$. The public key is given by (\mathbf{G}, h, s, t) .

- **Encryption:** We randomly generate an element $e \in R$ such that $\text{wt}(e) = w_e$ and a pair $(r_1, r_2) \in R^2$ such that $\text{wt}_H(r_1) = \text{wt}_H(r_2) = w_r$.

Let $\mathbf{m} \in \mathbb{F}_2^k$ be the message, which gets encrypted as the pair $\mathbf{c} = (\mathbf{u}, \mathbf{v}) \in R^2$, where $u = r_1 + hr_2$ and $\mathbf{v} = \mathbf{m}\mathbf{G} + \mathbf{s}r_2 + \mathbf{e}$.

- **Decryption:** As mentioned in the quasi-cyclic framework, we compute that

$$\mathbf{v} - \mathbf{u}z = \mathbf{m}\mathbf{G} + (\mathbf{y}r_2 - \mathbf{r}_1z + \mathbf{e}).$$

The term $\mathbf{y}r_2 - \mathbf{r}_1z + \mathbf{e}$ has Hamming weight $\leq t$ with high probability (this follows non-trivially from the choice of the parameters). If this is the case, we can use the decoding algorithm of \mathcal{C} to recover the message \mathbf{m} .

7.1.6 Proposed Parameters for HQC

The following table contains the proposed parameters for HQC together with an upper estimate on the decoding failure rate (DFR) and ciphertext size and key sizes. The key and ciphertext sizes are given in bytes and as before, security levels 1,3 and 5 correspond to 128-bit, 192-bit and 256-bit security respectively.

Security	n	w	$w_r = w_e$	Public key	Private key	Ciphertext	DFR
Level 1	17669	66	75	2249	40	4481	2^{-128}
Level 3	35851	100	114	4522	40	9026	2^{-192}
Level 5	57637	131	149	7245	40	14469	2^{-256}

Table 29: Parameters for HQC

The advantages of HQC are its efficient implementation and its small key sizes. However, HQC suffers from a low encryption rate.

7.2 Code-Based Signature Schemes

In 2023, NIST has opened an additional standardization call for post-quantum signature schemes. Out of the 50 submitted schemes, 40 have been found complete and proper and have been published as official round 1 candidates.

Among the 40 schemes, we find

- 12 multivariate schemes,
- 7 lattice-based schemes,
- 4 symmetric schemes,
- 1 isogeny-based scheme,
- 5 schemes that have been grouped as “other”,
- 11 code-based schemes.

Within the first 2 months, 11 of the schemes have been attacked. At the moment of this writing, we have 29 surviving schemes, out of which we find

- 9 multivariate schemes,
- 5 lattice-based schemes,
- 4 symmetric schemes,
- 1 isogeny-based scheme,
- 1 scheme that has been grouped as “other”,
- 9 code-based schemes.

The interested reader can compare the 29 survivors on

<https://pqshield.github.io/nist-sigs-zoo/>

In the following, we will only consider the 11 submitted code-based signatures.

Recall the three different approaches to construct a signature scheme, with the benefits and limitations:

Hash-and-Sign		
Needs	Limitations	Advantages
Trapdoor Secret code	Large public keys Slow signing	Small signatures
ZK Protocol and Fiat-Shamir Transform		
Needs	Limitations	Advantages
Hard problem	Large signatures	Small public keys
ZK Protocol and MPCitH		
Needs	Limitations	Advantages
Hard problem $(N - 1)$ -private MPC	Slow signing Slow verifying	Small signatures Small public keys

Table 30: Comparison of the different techniques to construct a code-based signature scheme.

7.2.1 Hash-and-sign schemes

Let us start with the three code-based hash-and-sign schemes.

Trapdoor	Secret Code	Scheme	Comment
Lee SDP	Quasi-cyclic code	FuLeeca	Broken
SDP	Reed-Muller code	Enhanced pqsigRM	Broken
SDP	$(U, U + V)$ -code	WAVE	Large public keys

Table 31: Hash-and-sign schemes submitted to the additional call of NIST for signature schemes.

1. FuLeeca

FuLeeca [226] is the first cryptosystem based on the Lee metric. It uses a secret quasi-cyclic code with low Lee weight generators \mathbf{a}, \mathbf{b} , i.e., $\text{wt}_L(\mathbf{a}, \mathbf{b}) = w_{key}$, defining the two circulant matrices \mathbf{A}, \mathbf{B} which give the secret generator matrix

$$\mathbf{G} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \end{pmatrix}.$$

The public generator matrix is given by \mathbf{G} in systematic form,

$$\mathbf{G}' = \begin{pmatrix} \text{Id}_k & \mathbf{T} \end{pmatrix},$$

Level	Public key size	Signature size	Signing time	Verification time
I	1.3	1.1	1803	1.4
III	1.9	1.6	2139	2.5
V	2.6	2.1	11805	3.8

Table 32: Performance of FuLeeca. Sizes are in kilobytes and timings in MCycles.

for

$$\mathbf{T} = \mathbf{A}^{-1}\mathbf{B}.$$

Clearly, it is enough to publish one row of \mathbf{T} .

In order to sign a message \mathbf{m} , the signer hashes \mathbf{m} getting $\mathbf{c} = \text{Hash}(\mathbf{m})$ and iteratively searches for a small \mathbf{x} , such that $\mathbf{v} = \mathbf{xG}$ satisfies two conditions

- (a) $\text{wt}_L(\mathbf{v}) \in [w_{sig} - 2w_{key}, w_{sig}]$,
- (b) $\text{LMP}(\mathbf{v}, \mathbf{c}) > \lambda + 64$.

The first assumption ensures that an impersonator has to solve the Lee SDP in order to forge a signature, and the second conditions binds the message to the signature. On a high level, the hash of the message should have many signs matching with the codeword. By setting their LMP larger than λ , one ensures that an impersonator has to go through 2^λ randomly chosen \mathbf{v} before finding enough signs matching. Since the codeword $\mathbf{v} = (\mathbf{y}, \mathbf{yT})$, the signature is then given by \mathbf{y} .

A verifier first recovers $\mathbf{v} = (\mathbf{y}, \mathbf{yT})$ checks exactly these two conditions

- (a) $\text{wt}_L(\mathbf{v}) \in [w_{sig} - 2w_{key}, w_{sig}]$,
- (b) $\text{LMP}(\mathbf{v}, \mathbf{c}) > \lambda + 64$,

in order to accept the signature \mathbf{y} .

The signature scheme shines with very small public key and signature sizes, one of the only code-based schemes to achieve both.

Unfortunately, the scheme was broken by van Woerden and Hörmann. The attack makes use of the following facts:

- The \mathbf{x} used to get the codeword $\mathbf{v} = \mathbf{xG} \bmod p$ is chosen so small, there is no modular reduction necessary. That is $\mathbf{v} = \mathbf{xG}$ also over \mathbb{Z} . This allows the attackers to directly use the integer lattice $L(\mathbf{G})$.
- The quasi-cyclic structure of the code allows the attackers further to only search for a solution in one part, i.e., $\mathbf{G} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \end{pmatrix}$ and it is enough to work with $L(\mathbf{A})$.
- Finally, using BKZ [234], the attacker can find short Euclidean vectors in $L(\mathbf{A})$. Usually, one would expect exponentially many such short vectors and only very few of those are also of small Lee weight. However, the chosen instances of FuLeeca allow for this attack to work fast.

Level	Public key size	Signature size	Signing time	Verification time
I	2000	1.03	2.2	0.2

Table 33: Performance of Enhanced pqsigRM. Sizes are in kilobytes and timings in MCycles.

2. Enhanced pqsigRM

This proposals [93] follows closely the original idea of CFS using a modified Reed-Muller code.

Thus, the secret code is given by a Reed-Muller code having parity-check matrix \mathbf{H} and the public code is a scrambled parity-check matrix $\mathbf{H}' = \mathbf{H}\mathbf{P}$. Upon a message \mathbf{m} , one hashes the messages $\text{Hash}(\mathbf{m})$ and hopes that it is the syndrome of a low weight vector \mathbf{e} , i.e., $\mathbf{e}\mathbf{H}^\top = \text{Hash}(\mathbf{m})$. In this case, one sends $\mathbf{e}\mathbf{P}$ as signature. The verifier can easily check that $\mathbf{e}\mathbf{P}\mathbf{P}^\top\mathbf{H}^\top = \text{Hash}(\mathbf{m})$.

Note that a scrambled Reed-Muller code can be distinguished and the secret code can be recovered using the attack [196]. Thus, Enhanced pqsigRM proposes a modified Reed-Muller code. Recall from Section 2, that Reed-Muller codes are $(U, U + V)$ codes. The original attack makes use of the fact that the hull of such a code, i.e., $\mathcal{C} \cap \mathcal{C}^\perp$ only consists of (U, U) -codewords, which helps to reveal the secret code. To avoid this, the proposed code is designed so that $\dim(U^\perp \cap V)$ is large.

Nevertheless, Enhanced pqsigRM has been broken by Debris-Alazard, Loisel and Vasseur again exploiting the $(U, U + V)$ structure to recover the secret code.

3. WAVE

WAVE [49] is a hash-and-sign scheme, whose trapdoor is based on permuted generalized $(U, U + V)$ -codes. Unlike most code-based schemes, WAVE does not rely on finding small weight codewords, but rather large weight codewords. In fact, until the Hamming weight $\frac{q-1}{q}(n - k)$ it is hard to find low weight codewords and similarly after the Hamming weight $k + \frac{q-1}{q}(n - k)$ it is again hard to find large weight codewords.

Again a signer starts with a secret generalized $(U, U + V)$ code and scrambles it to publish the parity-check matrix $\mathbf{H}' = \mathbf{H}\mathbf{P}$.

Upon a message \mathbf{m} the signer computes the hash $\text{Hash}(\mathbf{m})$ and hopes that it is the syndrome of a *large* weight vector, i.e., $\text{Hash}(\mathbf{m}) = \mathbf{e}\mathbf{H}^\top$. In order to find such large weight \mathbf{e} , WAVE makes use of the secret generalized $(U, U + V)$ code and performing ISD in the V part.

In this case, the signer sends the signature $\mathbf{e}\mathbf{P}$. A verifier can then easily check that $\text{Hash}(\mathbf{m}) = \mathbf{e}\mathbf{P}\mathbf{P}^\top\mathbf{H}^\top$.

The main advantage of WAVE is in its security, in fact a large amount of work has been performed using rejection sampling and smartly choosing the distribution, such that the preimage sampleable property is achieved, which thwarts all attacks trying to exploit the knowledge of signatures.

As limitations, WAVE has quite large public key sizes in the range of 3 MB.

Level	Public key size	Signature size	Signing time	Verification time
I	3677	0.8	1160	205
III	7867	1.2	3507	464
V	13632	1.6	7936	813

Table 34: Performance of WAVE. Sizes are in kilobytes and timings in MCycles.

7.2.2 ZK Protocols and Fiat-Shamir Transform

In the additional call 3 code-based signature schemes using ZK protocols have been submitted, namely **CROSS** based on restricted errors, **LESS** based on LEP and **MEDS** based on MCE.

Let us start with the three code-based hash-and-sign schemes.

Hard Problem	Scheme	Comment
Restricted SDP	CROSS	
LEP	LESS	Large total size
MCE	MEDS	Large total size

Table 35: Signatures from ZK protocols submitted to the additional call of NIST for signature schemes.

1. CROSS

The signature scheme **CROSS** [37] uses an adapted version of the code-based ZK protocol CVE (see Section 4.2). However, instead of using SDP and thus σ a linear isometry in the Hamming metric, **CROSS** relies on the Restricted SDP. This allows not only to represent vectors $\mathbf{e} \in \mathbb{E}^n$ using only the exponents $\ell(\mathbf{e}) \in \mathbb{F}_z^n$, thus having size $n \lceil \log_2(z) \rceil$, but also the maps that act transitively on \mathbb{E}^n are given by componentwise multiplication with vectors in \mathbb{E}^n .

CROSS makes use of several techniques to compress sizes, such as Merkle trees and weighted challenge vectors, $\mathbf{b} \in \{0, 1\}^t$. In fact, seeing that one of the responses (where $b_i = 1$) has a much smaller size to send than the other, in order to reduce the signature size one would sample challenge vectors \mathbf{b} of large weight. Note that this information could potentially be used by an attacker. Thus, **CROSS** adapted the forgery attack [164] in order to choose the weight w of \mathbf{b} and the number of rounds t , in a secure way.

CROSS provides several variants, one relying on Restricted SDP, denoted by R-SDP, one relying on Restricted SDP in a subgroup G , denoted by R-SDP(G). The “f” variant stands for *fast*, the “b” variant provides a *balanced* solution and the “s” variant provides a *small* solution.

Variant	Level	Public key size	Signature size	Signing time	Verification time
R-SDP-f	I	0.06	19	1.28	0.78
R-SDP-b	I	0.06	12	2.38	1.44
R-SDP-s	I	0.06	10	8.96	5.84
R-SDP(G)-f	I	0.03	12	0.94	0.55
R-SDP(G)-b	I	0.03	9.2	1.85	1.09
R-SDP(G)-s	I	0.03	7.9	6.54	3.96
R-SDP-f	III	0.09	42	2.75	1.69
R-SDP-b	III	0.09	28	4.97	2.89
R-SDP-s	III	0.09	23	12.2	6.8
R-SDP(G)-f	III	0.06	27	2.04	1.21
R-SDP(G)-b	III	0.06	23	2.63	1.53
R-SDP(G)-s	III	0.06	18	9.67	5.61
R-SDP-f	V	0.12	76	4.93	3.04
R-SDP-b	V	0.12	51	8.26	5
R-SDP-s	V	0.12	43	15.69	9.37
R-SDP(G)-f	V	0.07	48	3.93	2.32
R-SDP(G)-b	V	0.07	40	4.99	2.96
R-SDP(G)-s	V	0.07	32	14.12	7.73

Table 36: Performance of CROSS. Sizes are in kilobytes and timings in MCycles.

Variant	Level	Public key size	Signature size	Signing time	Verification time
LESS-1b	I	13.7	8.4	878.7	890.8
LESS-1i	I	41.1	6.1	876.6	883.6
LESS-1s	I	95.9	5.2	703.6	714.7
LESS-3b	III	34.5	18.4	7224	7315
LESS-3s	III	68.9	14.1	8527	8608
LESS-5b	V	64.6	32.5	33787	34014
LESS-5s	V	129	26.1	22621	22703

Table 37: Performance of LESS. Sizes are in kilobytes and timings in MCycles.

2. LESS

LESS [36] is a code-based signature scheme based on LEP and using a ZK protocol with the Fiat-Shamir transform.

On a high level, the idea of LESS is as follows. A prover publishes $\mathbf{G} \in \mathbb{F}_q^{k \times n}$ chosen at random and chooses a secret permutation matrix \mathbf{P} and a $\mathbf{v} \in (\mathbb{F}_q^*)^n$ at random. The prover computes and publishes $\mathbf{G}' = \mathbf{G}\mathbf{P}\text{diag}(\mathbf{v})$, while the monomial transformation $\mathbf{P}\text{diag}(\mathbf{v})$ is kept secret. In order to prove knowledge of the monomial transformation, the prover also computes the commitment $\mathbf{G}'' = \mathbf{G}\mathbf{P}'\text{diag}(\mathbf{v}')$ for some permutation matrix \mathbf{P}' and $\mathbf{v}' \in (\mathbb{F}_q^*)^n$. The prover can thus easily provide the monomial transformation from \mathbf{G} to \mathbf{G}'' (being $\mathbf{P}'\text{diag}(\mathbf{v}')$) or the linear isometry from \mathbf{G}' to \mathbf{G}'' (being $\mathbf{P}^{-1}\text{diag}(\mathbf{v})^{-1}\mathbf{P}'\text{diag}(\mathbf{v}')$) without revealing any information on the secret monomial from \mathbf{G} to \mathbf{G}' (being $\mathbf{P}\text{diag}(\mathbf{v})$).

Clearly such ZK protocol comes with a cheating probability of $1/2$. LESS decreases the cheating probability by using multiple public keys. In more details, one chooses several monomial transformations $\mathbf{Q}_1, \dots, \mathbf{Q}_N$ and publishes $\mathbf{G}\mathbf{Q}_1, \dots, \mathbf{G}\mathbf{Q}_N$. The verifier now chooses from which $\mathbf{G}\mathbf{Q}_i$ the monomial transformation to \mathbf{G}'' should be revealed, thus increasing the challenge space to $N + 1$ and the cheating probability to $\frac{1}{N+1}$.

Since the \mathbf{G} was chosen at random it is enough to send a seed as public key. A drawback that comes with LESS is that the commitments and the responses are structured matrices, thus needing a lot of bits to be sent.

LESS also makes use of several compression techniques such as seed trees and weighted challenges.

Also LESS provides several variants: a *balanced* configuration, denoted with “b”, where public key and signature are roughly of the same size, and a *small* configuration, denoted with “s”, providing a small signature at the cost of larger public keys. Finally, for level I also an *intermediate* configuration, denoted with “i” is given.

Note that at the moment of this writing, the contributors of LESS suggested a novel approach to shorten the signatures. In [95] the authors propose to use canonical forms of matrices, this corresponds to a short representative of a certain equivalence class. As a first step, the monomial transformations are split as $(\mathbf{P}, \mathbf{v}, \mathbf{P}', \mathbf{v}')$ for \mathbf{P} a $k \times k$

Variant	Level	Public key size	Signature size
LESS-1c	I	13.9	2.4
LESS-1f	I	41.8	1.8
LESS-3c	III	35	5.6
LESS-3f	III	105.2	4.4
LESS-5c	V	65.8	10
LESS-5f	V	197.3	7.8

Table 38: New sizes of LESS. Sizes are in kilobytes.

permutation matrix, \mathbf{P}' a $(n - k) \times (n - k)$ permutation matrix and $\mathbf{v} \in (\mathbb{F}_q^\star)^k, \mathbf{v}' \in (\mathbb{F}_q^\star)^{n-k}$, thus getting \mathbf{G} and \mathbf{G}' are monomially equivalent if there exist $(\mathbf{P}, \mathbf{v}, \mathbf{P}', \mathbf{v}')$ such that

$$\mathbf{G} = \mathbf{S}\mathbf{G}' \begin{pmatrix} \mathbf{P}\text{diag}(\mathbf{v}) & \mathbf{0} \\ \mathbf{0} & \mathbf{P}'\text{diag}(\mathbf{v}') \end{pmatrix},$$

for some $\mathbf{S} \in \text{GL}_k(\mathbb{F}_q)$.

Since one sends the generator matrices in systematic form, this allows the authors to restrict the monomial transformation to the redundant $k \times (n - k)$ part and only send $\mathbf{P}^{-1}\text{diag}(\mathbf{v})^{-1}\mathbf{P}'\text{diag}(\mathbf{v}')$.

The resulting sizes are much smaller now, as shown in Table 38.

3. MEDS

MEDS [94] uses the same strategy as LESS, but adapted to matrix codes and the rank metric.

A prover publishes $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$ chosen at random and chooses the secret matrices $\mathbf{A} \in \text{GL}_m(\mathbb{F}_q), \mathbf{B} \in \text{GL}_n(\mathbb{F}_q)$ at random. The prover computes and publishes $\mathbf{G}'_i = \mathbf{A}\mathbf{G}_i\mathbf{B}$, while the rank-metric isometry (\mathbf{A}, \mathbf{B}) is kept secret. In order to prove knowledge of the monomial transformation, the prover also computes the commitment $\mathbf{G}''_i = \mathbf{A}'\mathbf{G}_i\mathbf{B}'$ for some $\mathbf{A}' \in \text{GL}_m(\mathbb{F}_q), \mathbf{B}' \in \text{GL}_n(\mathbb{F}_q)$. The prover can thus easily provide the transformation from $\mathcal{C} = \langle \mathbf{G}_1, \dots, \mathbf{G}_k \rangle$ to $\mathcal{C}' = \langle \mathbf{G}''_1, \dots, \mathbf{G}''_k \rangle$ (being \mathbf{A}', \mathbf{B}') or the isometry from $\mathcal{C}' = \langle \mathbf{G}'_1, \dots, \mathbf{G}'_k \rangle$ to $\mathcal{C}'' = \langle \mathbf{G}''_1, \dots, \mathbf{G}''_k \rangle$ (being $\mathbf{A}'\mathbf{A}^{-1}, \mathbf{B}^{-1}\mathbf{B}'$) without revealing any information on the secret isometry from \mathcal{C} to \mathcal{C}' (being \mathbf{A}, \mathbf{B}).

The signature scheme MEDS also makes use of the same compression techniques as LESS, namely seed trees, fixed weight challenges and multiple public keys.

Similar to LESS, also MEDS results in quite total sizes, being the size of the signature added to the size of the public key.

The MEDS proposal also gives two different parameter sets for each security level, one being tuned for small signatures, and the other for fast signing and verifying.

Variant	Level	Public key size	Signature size	Signing time	Verification time
MEDS-9923	I	9.9	9.8	518	515.6
MEDS-13220	I	13.2	12.98	88.9	87.48
MEDS-41711	III	41.7	41	1467	1462
MEDS-55604	III	55.6	54.7	387.3	380.7
MEDS-134180	V	134.2	132.6	1629.9	1612.6
MEDS-167717	V	167.7	165.5	961.8	938.9

Table 39: Performance of MEDS. Sizes are in kilobytes and timings in MCycles.

7.2.3 ZK Protocols and MPCitH

In the additional round for post-quantum signature schemes, one finds 5 code-based schemes which are using ZK protocols and using the MPCitH technique.

Hard Problem	MPC	Scheme
SDP	hypercube, threshold	SDitH
Rank SDP	hypercube additive	RYDE
Relaxed PKP	BG splitting	PERK
MinRank	additive hypercube, linearized polynomials	MIRA
MinRank	Kipnis-Shamir modeling	MiRitH

Table 40: Signatures from ZK protocols and MPCitH technique submitted to the additional call of NIST for signature schemes.

1. SDitH:

The SDitH signature scheme [10] relies on the SDP and an MPC protocol which efficiently checks whether a given shared input corresponds to the solution of a SDP instance. The used MPC protocol is called *hypercube technique* [11] and instead traditional additive sharings, SDitH uses low-threshold linear secret sharings to exploit their error-correcting feature, called *threshold approach* [22].

First of all, recall that due to the systematic form of a parity-check matrix

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \text{Id}_{n-k} \end{pmatrix},$$

any syndrome

$$\mathbf{s} = (\mathbf{e}, \mathbf{e}')\mathbf{H}^\top = \mathbf{e}\mathbf{A}^\top + \mathbf{e}'.$$

Thus, it is enough to use \mathbf{e} for the secret sharing.

Variant	Level	Public key size	Signature size	Signing time	Verification time
SDitH-gf256-L1-hyp	I	0.1	8.2	13.4	12.5
SDitH-gf251-L1-hyp	I	0.1	8.2	22.1	21.2
SDitH-gf256-L1-thr	I	0.1	10.1	5.1	1.6
SDitH-gf251-L1-thr	I	0.1	10.1	4.4	0.6
SDitH-gf256-L3-hyp	III	0.2	19.1	30.5	27.7
SDitH-gf251-L3-hyp	III	0.2	19.1	51.1	49
SDitH-gf256-L3-thr	III	0.2	24.9	14.8	4.9
SDitH-gf251-L3-thr	III	0.2	24.9	11.7	1.5
SDitH-gf256-L5-hyp	V	0.2	33.4	59.2	54.4
SDitH-gf251-L5-hyp	V	0.2	33.4	94.8	91.3
SDitH-gf256-L5-thr	V	0.2	43.9	30.5	10.2
SDitH-gf251-L5-thr	V	0.2	43.9	23.9	3.2

Table 41: Performance of SDitH. Sizes are in kilobytes and timings in MCycles.

Let $\mathbb{F}_q = \{f_1, \dots, f_q\}$. The MPC protocol is based on four polynomials,

$$S(x), P(x), Q(x), F(x),$$

defined as

- $S(x) \in \mathbb{F}_q[x]$ of degree up to $n - 1$ such that $S(f_i) = e_i$,
- $Q(x) \in \mathbb{F}_q[x]$ of degree $t = \text{wt}_H(\mathbf{e}', \mathbf{e})$ such that $Q(x) = \prod_{i \in \text{supp}(\mathbf{e}', \mathbf{e})} (x - f_i)$,
- $F(x) \in \mathbb{F}_q[x]$ of degree n such that $F(x) = \prod_{i=1}^n (x - f_i)$,
- $P(x) \in \mathbb{F}_q[x]$ of degree up to $t - 1$, such that $P(x) = \frac{S(x)Q(x)}{F(x)}$.

The correctness of the SDP solution amounts to verifying the relation:

$$S(x)Q(x) = P(x)F(x).$$

While $F(x)$ is made public, the prover wants to convince the verifier of the knowledge of $P(x), Q(x)$, such that $S(f_i)Q(f_i) = P(f_i)F(f_i) = 0$ for all $i \in \{1, \dots, n\}$.

The soundness of the MPC protocol is based on the fact that $\text{wt}_H(\mathbf{e}', \mathbf{e}) = t$ is equivalent to the existence of $P(x), Q(x)$ of degree up to $t - 1$, respectively t , such that $S(x)Q(x) = P(x)F(x)$. The parties thus get as shares $(\mathbf{e}, P(x), Q(x))$, locally compute $(\mathbf{e}', \mathbf{e})$ and $S(x)$ by Lagrange interpolation and verify that $S(x)Q(x) = P(x)F(x)$.

SDitH provides for each security level 4 parameter sets, two for the hypercube approach and two for the threshold approach. There is a clear trade-off between the two variants, as the hypercube approach achieves smaller signatures, while the threshold approach is faster.

2. RYDE:

RYDE [18] is based on the Rank SDP and using the (ℓ, N) -threshold linear secret sharing scheme as MPC protocol. For this a secret s is split into N shares $[[s]] = (s_1, \dots, s_N)$, such that the secret can be recovered from any $\ell + 1$ shares s_i .

RYDE uses an additive (N, N) -threshold linear secret sharing scheme, as explained in Section 2.3.6, that is the shares of s are given by

$$(r_1, \dots, r_{N-1}, s - \sum_{i=1}^{N-1} r_i),$$

for some random r_i .

In more details, the MPC protocol works as follows. We are given a parity-check matrix

$$\mathbf{H} = \begin{pmatrix} \mathbf{A} & \text{Id}_{n-k} \end{pmatrix} \in \mathbb{F}_{q^m}^{(n-k) \times n},$$

a syndrome $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ and a weight t . Let $(\mathbf{e}, \mathbf{e}')$ be a solution to the Rank SDP instance. Each party is then given a share of $[[\mathbf{e}]]$. Let \mathcal{S} be the error support of $(\mathbf{e}, \mathbf{e}')$, i.e., $\mathcal{S} = \langle e_1, \dots, e_n \rangle$ of \mathbb{F}_q -dimension t . Then \mathcal{S} has an annihilator polynomial

$$f(x) = \prod_{s \in \mathcal{S}} (x - s).$$

The parties also take the following as shares $\mathbf{b}, \mathbf{a}, c$, where $\mathbf{b} \in \mathbb{F}_{q^m}^t$ is a vector containing the coefficients of

$$L = \sum_{i=1}^t b_i (x^{q^i} - x),$$

$\mathbf{a} \in \mathbb{F}_{q^{m\eta}}^t$ is randomly sampled and $c = -\langle \mathbf{b}, \mathbf{a} \rangle$. The parties now proceed as

- (a) sample at random $(\gamma_1, \dots, \gamma_n, \varepsilon) \in \mathbb{F}_{m \cdot \eta}^{n+1}$,
- (b) locally compute $\mathbf{e}' = \mathbf{s} - \mathbf{A}\mathbf{e}$,
- (c) locally compute $z = -\sum_{j=1}^n \gamma_j (e_j^{q^t} - e_j)$,
- (d) locally compute $w_i = \sum_{j=1}^n \gamma_j (e_j^{q^i} - e_j)$ for all $i \in \{1, \dots, t-1\}$,
- (e) locally compute and open $\alpha = \varepsilon \mathbf{w} + \mathbf{a}$,
- (f) locally compute and open $v = \varepsilon z - \langle \alpha, \mathbf{b} \rangle - c$,
- (g) and they accept if $v = 0$.

RYDE is able to achieve smaller signatures than SDitH, however at the cost of a slower signing and verifying process. In Table 42, we can see the two parameter sets for each security level, one denoted by “F” for a *fast* version and one denoted by “S” for a *small* version.

Variant	Level	Public key size	Signature size	Signing time	Verification time
RYDE-128F	I	0.09	7.4	5.4	4.4
RYDE-128S	I	0.09	6	23.4	20.1
RYDE-192F	III	0.13	16.4	12.2	10.7
RYDE-192S	III	0.13	13	49.6	44.8
RYDE-256	V	0.2	29.1	26	22.7
RYDE-256	V	0.2	22.8	105.5	94.9

Table 42: Performance of RYDE. Sizes are in kilobytes and timings in MCycles.

3. PERK:

PERK [1] is based on the relaxed PKP, that is, one publishes a parity-check matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, a vector $\mathbf{e} \in \mathbb{F}_q^n$ and a permuted syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$, i.e., there exists some $\sigma \in S_n$ such that $\mathbf{H}\sigma(\mathbf{e})^\top = \mathbf{s}^\top$. Hence, the secret is given by the permutation σ . PERK is based on the BG ZK protocol introduced in [21], and employs a simple MPC protocol.

The BG protocol works as follows: one samples randomly permutations $\sigma_2, \dots, \sigma_N \in S_n$, and vectors $\mathbf{v}_2, \dots, \mathbf{v}_N \in \mathbb{F}_q^n$. One computes the commitments c_i from the hashes of the used seeds to generate σ_i, \mathbf{v}_i .

One then computes the permutation $\sigma_1 = \sigma_2^{-1} \circ \dots \circ \sigma_N^{-1} \circ \sigma$ and samples a random $\mathbf{v}_1 \in \mathbb{F}_q^n$. The commitment c_1 is given by the hash of σ_1 , and the seed for \mathbf{v}_1 . One then computes

$$\mathbf{v} = \mathbf{v}_N + \sum_{i=1}^{N-1} \sigma_N \circ \dots \circ \sigma_{i+1}(\mathbf{v}_i)$$

and the commitment c which is the hash of the syndrome $\mathbf{v}\mathbf{H}^\top$.

The first challenge of the verifier is some $\beta \in \mathbb{F}_q$, with this the prover computes $\tilde{\mathbf{e}}_0 = \beta \mathbf{e}$ and for all $i \in \{1, \dots, N\}$ the vectors $\tilde{\mathbf{e}}_i = \sigma_i(\tilde{\mathbf{e}}_{i-1}) + \mathbf{v}_i$. The first response is given by the hash of all the $\tilde{\mathbf{e}}_i$. The verifier can then challenge any $i \in \{1, \dots, N\}$ and the prover responds with $c_i, \tilde{\mathbf{e}}_i$ and in the case $i = 1$ also with σ_1 .

The employed MPC protocol asks N parties to perform the BG steps $i \in \{1, \dots, N\}$

- if $i \neq 1$ sample random $(\sigma_i, \mathbf{v}_i) \in S_n \times \mathbb{F}_q^n$ and compute the commitment $c_i = \text{Hash}(\sigma_i, \mathbf{v}_i)$ (actually of their seeds),
- if $i = 1$ sample random $\mathbf{v}_1 \in \mathbb{F}_q^n$ and compute σ_1 as usual, i.e., $\sigma_1 = \sigma_2^{-1} \circ \dots \circ \sigma_N^{-1} \circ \sigma$ and the commitment $c_1 = \text{Hash}(\sigma_1, \mathbf{v}_1)$,
- upon the challenge β one sets $\tilde{\mathbf{e}}_0 = \beta \mathbf{e}$ and each party computes $\tilde{\mathbf{e}}_i = \sigma_i(\tilde{\mathbf{e}}_{i-1}) + \mathbf{v}_i$.
- The verifier has to recompute the commitments and $\tilde{\mathbf{e}}_i$ for each $i \in \{1, \dots, N\}$.

We will denote this MPC protocol as “BG splitting”.

Variant	Level	Public key size	Signature size	Signing time	Verification time
PERK-I-fast3	I	0.15	8.35	7.6	5.3
PERK-I-fast5	I	0.24	8.03	7.2	5.1
PERK-I-short3	I	0.15	6.56	39	27
PERK-I-short5	I	0.24	6.06	36	25
PERK-III-fast3	III	0.23	18.8	16	13
PERK-III-fast5	III	0.37	18	15	12
PERK-III-short3	III	0.23	15	82	65
PERK-III-short5	III	0.37	13.8	77	60
PERK-V-fast3	V	0.31	33.3	36	28
PERK-V-fast5	V	0.51	31.7	34	26
PERK-V-short3	V	0.31	26.4	185	143
PERK-V-short5	V	0.51	24.2	171	131

Table 43: Performance of PERK. Sizes are in kilobytes and timings in MCycles.

4. MIRA:

MIRA [19] is based on the MinRank problem, i.e., the decoding problem for Matrix codes endowed with the rank metric. The MPC protocol used in MIRA is an additive sharing. That is for a secret s , the shares are $(r_1, \dots, r_{N-1}, s - \sum_{i=1}^{N-1} r_i)$, for some random r_i .

The MPC protocol is similar to the one in RYDE; we have the generating matrices $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$, one chooses a secret $\mathbf{x} \in \mathbb{F}_q^k$ and publishes \mathbf{E} of rank t and $\mathbf{R} = \mathbf{E} - \sum_{i=1}^k \mathbf{G}_i x_i$.

Each party received $\mathbf{x} \in \mathbb{F}_q^k$ and the coefficients $b_i \in \mathbb{F}_{q^m}$ of the annihilating polynomial

$$L(x) = \sum_{i=1}^t b_i x^{q^i},$$

a random $\mathbf{a} \in \mathbb{F}_{q^{m\eta}}^t$ and $c = -\langle \mathbf{a}, \mathbf{b} \rangle$. The parties proceed as follows

- (a) sample random $(\gamma_1, \dots, \gamma_n, \varepsilon) \in \mathbb{F}_{q^{m\eta}}^{n+1}$,
- (b) compute $\mathbf{E} = \mathbf{R} + \sum_{i=1}^k x_i \mathbf{G}_i$,
- (c) set $e_i \in \mathbb{F}_{q^m}$ associated to the i th column of \mathbf{E} , that is for some basis Γ of \mathbb{F}_{q^m} over \mathbb{F}_q compute $e_i = \Gamma^{-1}(\mathbf{E}_{\{i\}})$,
- (d) compute $z = -\sum_{j=1}^n \gamma_j e_j^{q^t}$,
- (e) compute $w_i = \sum_{j=1}^n \gamma_j e_j^{q^i}$ for all $i \in \{1, \dots, t\}$,

Variant	Level	Public key size	Signature size	Signing time	Verification time
MIRA-128F	I	0.09	7.4	37.4	36.7
MIRA-128S	I	0.09	5.6	46.8	43.9
MIRA-192F	III	0.12	15.5	107.2	107
MIRA-192S	III	0.12	11.8	119.7	116.2
MIRA-256F	V	0.15	27.7	322.3	323.2
MIRA-256S	V	0.15	20.8	337.7	331.4

Table 44: Performance of MIRA. Sizes are in kilobytes and timings in MCycles.

- (f) open the shares to compute $\alpha = \varepsilon \mathbf{w} + \mathbf{a}$,
- (g) open the shares to compute $v = \varepsilon z - \langle \alpha, \mathbf{b} \rangle - c$,
- (h) and accept if $v = 0$.

MIRA has two parameter sets for each security level, given in Table 44. One parameter set is denoted by “F” for a *fast* version and one denoted by “S” for a *small* version. Compared to RYDE, which uses the same MPC protocol but is based on the rank decoding problem for \mathbb{F}_{q^m} -linear codes instead of \mathbb{F}_q -linear codes, we can observe that MIRA is able to achieve slightly smaller signature sizes than RYDE, however at the cost of a much slower signing and verification process.

5. MiRitH:

Also MiRitH [2] is based on the MinRank problem and uses an MPC protocol. However, MiRitH uses a Kipnis-Shamir [168] modeling, instead of the linearized polynomials used in MIRA. This leads to faster verification and signing.

Recall that in MinRank, the generating matrices $\mathbf{G}_1, \dots, \mathbf{G}_k \in \mathbb{F}_q^{m \times n}$, a received matrix $\mathbf{R} \in \mathbb{F}_q^{m \times n}$ are made public, and the task is to find $\mathbf{x} \in \mathbb{F}_q^k$ such that $\mathbf{E} = \mathbf{R} - \sum_{i=1}^k \mathbf{G}_i x_i$ has rank at most t .

The Kipnis-Shamir modeling is based on the following fact, if there exists a vector $\mathbf{x} \in \mathbb{F}_q^k$ and a matrix $\mathbf{K} \in \mathbb{F}_q^{t \times (n-t)}$, such that

$$\left(\mathbf{R} - \sum_{i=1}^k x_i \mathbf{G}_i \right) \begin{pmatrix} \mathbf{S} \\ \mathbf{K} \end{pmatrix} = \mathbf{0}, \quad (7.1)$$

for some invertible $\mathbf{S} \in \mathbb{F}_q^{(n-t) \times (n-t)}$ then \mathbf{x} is a solution to the MinRank instance $\mathbf{R}, \mathbf{G}_1, \dots, \mathbf{G}_k$. Thus, if we write $\mathbf{R} = \begin{pmatrix} \mathbf{R}' & \mathbf{R}'' \end{pmatrix}$ and $\mathbf{G}_i = \begin{pmatrix} \mathbf{G}'_i & \mathbf{G}''_i \end{pmatrix}$, for each $i \in \{1, \dots, k\}$ then we can transform Equation (7.1) to

$$\mathbf{R}' - \sum_{i=1}^k x_i \mathbf{G}'_i = \left(\mathbf{R}'' - \sum_{i=1}^k x_i \mathbf{G}''_i \right) \mathbf{K}.$$

Variant	Level	Public key size	Signature size	Signing time	Verification time
MiRitH-Iaf	I	0.13	7.7	4.8	4.5
MiRitH-Ias	I	0.13	5.7	42.9	42.7
MiRitH-Ibf	I	0.14	8.8	6.4	5.9
MiRitH-Ibs	I	0.14	6.3	51.5	51.8
MiRitH-IIIaf	III	0.2	16.7	11.2	10.4
MiRitH-IIIsas	III	0.2	12.4	94.5	94.2
MiRitH-IIIbf	III	0.2	17.9	13.3	12.3
MiRitH-IIIsbs	III	0.2	13.1	112.2	112
MiRitH-Vaf	V	0.25	29.6	23.9	22.2
MiRitH-Vas	V	0.25	21.8	196.7	194.6
MiRitH-Vbf	V	0.27	32	28.3	26.3
MiRitH-Vbs	V	0.27	23.1	241.6	241

Table 45: Performance of MiRitH. Sizes are in kilobytes and timings in MCycles.

Thus, let us write $\mathbf{R}_x = \mathbf{R} - \sum_{i=1}^k x_i \mathbf{G}_i$ and as before $\mathbf{R}_x = \begin{pmatrix} \mathbf{R}'_x & \mathbf{R}''_x \end{pmatrix}$, hence the Kipnis-Shamir modeling amounts to showing that $\mathbf{R}'_x = \mathbf{R}''_x \mathbf{K}$.

Thus, each party gets the additive sharings $[[\mathbf{x}]]$ and $[[\mathbf{K}]]$ and $[[\mathbf{A}]]$ for a random $\mathbf{A} \in \mathbb{F}_q^{s \times t}$ and $[[\mathbf{C}]]$ for $\mathbf{C} = \mathbf{A}\mathbf{K}$. The parties then proceed as follows

- (a) locally compute sharings $[[\mathbf{R}'_x]]$ and $[[\mathbf{R}''_x]]$,
- (b) sample a random matrix $\mathbf{X} \in \mathbb{F}_q^{s \times m}$,
- (c) locally compute

$$[[\mathbf{Y}]] = \mathbf{X}[[\mathbf{R}''_x]] + [[\mathbf{A}]]$$

and open the sharings, so each party gets \mathbf{Y} ,

- (d) locally compute

$$[[\mathbf{V}]] = \mathbf{Y}\mathbf{K} - \mathbf{X}[[\mathbf{R}'_x]] - \mathbf{C}$$

and open the sharings, so that each party gets \mathbf{V} ,

- (e) accept if $\mathbf{V} = \mathbf{0}$.

MiRitH presents four parameter sets for each security level, two denoted with “a”, and two denoted with “b”, where the “b” variant achieves a greater security level to leave some margins for possible further improvements on solving PKP. The parameter sets denoted by “f” are a *fast* variant, while the “s” denotes the *small* variant. We can see a clear difference in the timings compared to MIRA.

Another variant of MiRitH is using the hypercube technique, which allows to get even shorter signatures. While the hypercube variant presents several parameter sets for short signatures, we chose only the shortest variant.

Variant	Level	Public key size	Signature size	Signing time	Verification time
MiRitH-hyper-Iaf	I	0.13	6.2	4.1	3.4
MiRitH-hyper-Ias	I	0.13	3.9	3122	3066
MiRitH-hyper-Ibf	I	0.14	6.7	5.3	4.4
MiRitH-hyper-Ibs	I	0.14	4.1	3184	3156
MiRitH-hyper-IIIaf	III	0.21	13.4	9	8.2
MiRitH-hyper-IIIas	III	0.21	8.7	5149	5120
MiRitH-hyper-IIIbf	III	0.21	13.8	10.2	9.1
MiRitH-hyper-IIIbs	III	0.21	8.8	5278	5250
MiRitH-hyper-Vaf	V	0.25	23.9	17.4	14.8
MiRitH-hyper-Vas	V	0.25	15.1	9730	9800
MiRitH-hyper-Vbf	V	0.27	25	21.2	18.2
MiRitH-hyper-Vbs	V	0.27	15.4	9767	9811

Table 46: Performance of MiRitH using Hypercube. Sizes are in kilobytes and timings in MCycles.

Remark 264. Note that all the reported timings are from the respective documentations and based on different implementations. For signature sizes, we have taken the average sizes.

8 Conclusion

In this book chapter, we presented a comprehensive collection of code-based cryptography, concerning its history and most famous schemes, until the latest advances, especially in signature schemes.

There are several open question within this research area, prominent ones include

- Is the Rank Syndrome Decoding Problem NP-hard?
- Can we distinguish classical Goppa codes?
- How to improve the code-equivalence solvers?
- How to construct an efficient and secure hash-and-sign scheme?

.. and many more.

We hope that this book chapter helps young researchers to get into code-based cryptography, so that we can advance in these open question together.

Any comments, typos or additions can be sent to violetta.weger@tum.de and we will update the ArXiv version regularly.

Acknowledgement

The authors would like to thank Jean-Pierre Tillich, Nicolas Sendrier and Thomas Debris-Alazard for fruitful discussions. The authors would also like to thank Giovanni Tognolini and the anonymous reviewers for pointing out some of the typos.

Violetta Weger is supported by the Swiss National Science Foundation grant number 195290 and by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 899987.

Niklas Gassner and Joachim Rosenthal are supported by armasuisse Science and Technology (Project Nr.: CYD C-2020010).

Bibliography

- [1] Najwa Aaraj, Slim Bettaieb, Loïc Bidoux, Alessandro Budroni, Victor Dyesryn, Andre Esser, Philippe Gaborit, Mukul Kulkarni, Victor Mateu, Marco Palumbi, Lucas Perin, and Jean-Pierre Tillich. PERK. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [2] Gora Adj, Luis Rivera-Zamarripa, Javier Verbel, Emanuele Bellini, Stefano Barbero, Andre Esser, Carlo Sanna, and Floyd Zweyninger. MiRitH. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [3] Carlos Aguilar, Philippe Gaborit, and Julien Schrek. A new zero-knowledge code based identification scheme with reduced communication. In *2011 IEEE Information Theory Workshop*, pages 648–652. IEEE, 2011.
- [4] 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. *NIST PQC Call for Proposals*, 2020. Round 2 Submission.
- [5] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Arnaud Dion, Philippe Gaborit, Jérôme Lacan, Edoardo Persichetti, Jean-Marc Robert, Pascal Véron, and Gilles Zémor. Hamming Quasi-Cyclic (HQC). *NIST PQC Call for Proposals*, 2022. Round 4 Submission.
- [6] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Maxime Bros, Alain Couvreur, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Rank Quasi-Cyclic (RQC). *NIST PQC Call for Proposals*, 2020. Round 2 Submission.
- [7] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, and Gilles Zémor. Ouroboros-R. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [8] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor. Hamming Quasi-Cyclic (HQC). *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [9] Carlos Aguilar-Melchor, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Transactions on Information Theory*, 64(5):3927–3943, 2018.
- [10] Carlos Aguilar Melchor, Thibault Feneuil, Nicolas Gama, Shay Gueron, James Howe, David Joseph, Antoine Joux, Edoardo Persichetti, Tovahery H. Randrianarisoa, Matthieu Rivain, and Dongze Yue. SDitH. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [11] Carlos Aguilar-Melchor, Nicolas Gama, James Howe, Andreas Hülsing, David Joseph, and Dongze Yue. The return of the SDitH. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 564–596. Springer, 2023.

- [12] Abdulrahman Al Jabri. A statistical decoding algorithm for general linear block codes. In *IMA International Conference on Cryptography and Coding*, pages 1–8. Springer, 2001.
- [13] Martin Albrecht, Carlos Cid, Kenneth G. Paterson, Cen Jung Tjhai, and Martin Tomlinson. NTS-KEM - Second round submission. *NIST PQC Call for Proposals*, 2019. Round 2 Submission.
- [14] Martin R. Albrecht, Daniel J. Bernstein, Tung Chou, Carlos Cid, Jan Gilcher, Tanja Lange, Varun Maram, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Kenneth G. Paterson, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, Cen Jung Tjhai, Martin Tomlinson, and Wen Wang. Classic McEliece: Conservative Code-Based Cryptography. *NIST PQC Call for Proposals*, 2022. Round 4 Submission.
- [15] M. Alekhnovich. More on average case vs approximation complexity. In *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings.*, pages 298–307, 2003.
- [16] Daniel Apon, Ray Perlner, Angela Robinson, and Paolo Santini. Cryptanalysis of LEDAcrypt. Cryptology ePrint Archive, Report 2020/455, 2020. <https://ia.cr/2020/455>.
- [17] Nicolas Aragon, Marco Baldi, Jean-Christophe Deneuville, Karan Khathuria, Edoardo Persichetti, and Paolo Santini. Cryptanalysis of a code-based full-time signature. *Designs, Codes and Cryptography*, 89(9):2097–2112, 2021.
- [18] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Deryn, Thibault Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, and Adrien Vincotte. RYDE. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [19] Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Deryn, Thibault Feneuil, Philippe Gaborit, Romaric Neveu, Matthieu Rivain, and Jean-Pierre Tillich. MIRA. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [20] Nicolas Aragon, Paulo S.L.M. Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre tillich, Valentin Vasseur, and Gilles Zémor. BIKE: Bit Flipping Key Encapsulation. *NIST PQC Call for Proposals*, 2022. Round 4 Submission.
- [21] Nicolas Aragon, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Thibault Feneuil, Philippe Gaborit, Romaric Neveu, and Matthieu Rivain. MIRA: a digital signature scheme based on the minrank problem and the mpc-in-the-head paradigm. *arXiv preprint arXiv:2307.08575*, 2023.
- [22] Nicolas Aragon, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Thibault Feneuil, Philippe Gaborit, Romaric Neveu, and Matthieu Rivain. Mira: a digital signature scheme based on the minrank problem and the mpc-in-the-head paradigm, 2023.

- [23] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LAKE - Low rank parity check codes Key Exchange. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [24] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LOCKER - Low rank parity Check codes EncRyption. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [25] 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*, pages 728–758. Springer, 2019.
- [26] Nicolas Aragon, Victor Deryn, and Philippe Gaborit. Analysis of the security of the pssi problem and cryptanalysis of the durandal signature scheme. *Cryptology ePrint Archive*, 2023.
- [27] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, and Gilles Zémor. RankSign - a signature proposal for the NIST’s call. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [28] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. Improvement of generic attacks on the rank syndrome decoding problem. 2017.
- [29] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. A new algorithm for solving the rank syndrome decoding problem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2421–2425. IEEE, 2018.
- [30] Alexei Ashikhmin and Alexander Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.
- [31] Jaakko Astola. On the asymptotic behaviour of Lee-codes. *Discrete applied mathematics*, 8(1):13–23, 1984.
- [32] Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 229–240. Springer, 2003.
- [33] Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 229–240. Springer, 2003.
- [34] Jean-Philippe Aumasson, Daniel J. Bernstein, Ward Beullens, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, and Bas Westerbaan. Sphincs⁺. *NIST PQC Call for Proposals*, 2022. Selected for Standardization.
- [35] Roberto Avanzi, Simon Hoerder, Dan Page, and Michael Tunstall. Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *Journal of Cryptographic Engineering*, 1(4):271–281, 2011.

- [36] Marco Baldi, Alessandro Barenghi, Luke Beckwith, Jean-François Biasse, Andre Esser, Kris Gaj, Kamyar Mohajerani, Gerardo Pelosi, Edoardo Persichetti, Markku-Juhani O. Saarinen, Paolo Santini, and Robert Wallace. LESS. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [37] Marco Baldi, Alessandro Barenghi, Sebastian Bitzer, Patrick Karl, Felice Manganiello, Alessio Pavoni, Gerardo Pelosi, Paolo Santini, Jonas Schupp, Freeman Slaughter, Antonia Wachter-Zeh, and Violetta Weger. CROSS. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [38] Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, and Paolo Santini. LEDAkem. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [39] Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, and Paolo Santini. LEDApkc. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [40] Marco Baldi, Alessandro Barenghi, Franco Chiaraluce, Gerardo Pelosi, and Paolo Santini. LEDAcrypt: Low-density parity-check code-based cryptographic systems - version 3.0. *NIST PQC Call for Proposals*, 2020. Round 2 Submission.
- [41] Marco Baldi, Massimo Battaglioni, Franco Chiaraluce, Anna-Lena Horlemann-Trautmann, Edoardo Persichetti, Paolo Santini, and Violetta Weger. A new path to code-based signatures via identification schemes with restricted errors. *arXiv preprint arXiv:2008.06403*, 2020.
- [42] 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*, number 7, pages 173–182. HAL-Inria, 2011.
- [43] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, and Davide Schipani. Using LDGM codes and sparse syndromes to achieve digital signatures. In *International Workshop on Post-Quantum Cryptography*, pages 1–15. Springer, 2013.
- [44] Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Jakob Rosenthal, Davide Mose, et al. Method and apparatus for public-key cryptography based on error correcting codes, November 17 2015. US Patent 9,191,199.
- [45] Marco Baldi, Sebastian Bitzer, Alessio Pavoni, Paolo Santini, Antonia Wachter-Zeh, and Violetta Weger. Zero knowledge protocols and signatures from the restricted syndrome decoding problem. *PKC 2024*, 2024.
- [46] 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*, pages 246–262. Springer, 2008.
- [47] Marco Baldi, Franco Chiaraluce, Joachim Rosenthal, Paolo Santini, and Davide Schipani. Security of generalised Reed–Solomon code-based cryptosystems. *IET Information Security*, 13(4):404–410, 2019.
- [48] Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler,

- Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti, and Jefferson E. Ricardini. DAGS: Key Encapsulation from Dyadic GS Codes. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [49] Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karpman, Johanna Loyer, Ruben Niederhagen, Nicolas Sendrier, Benjamin Smith, and Jean-Pierre Tillich. WAVE. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
 - [50] Magali Bardet, Élise Barelli, Olivier Blazy, Rodolfo Canto-Torres, Alain Couvreur, Philippe Gaborit, Otmani Ayoub, Nicolas Sendrier, and Jean-Pierre Tillich. BIG QUAKE: BInary Goppa QUAsi-cyclic Key Encapsulation. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
 - [51] Magali Bardet, Pierre Briaud, Maxime Bros, Philippe Gaborit, Vincent Neiger, Olivier Ruatta, and Jean-Pierre Tillich. An algebraic attack on rank metric code-based cryptosystems. *CoRR*, abs/1910.00810, 2019.
 - [52] Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier Verbel. Improvements of algebraic attacks for solving the rank decoding and MinRank problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 507–536. Springer, 2020.
 - [53] Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha. Permutation code equivalence is not harder than graph isomorphism when hulls are trivial. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2464–2468. IEEE, 2019.
 - [54] Élise Barelli and Alain Couvreur. An efficient structural attack on NIST submission DAGS. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 93–118, Cham, 2018. Springer International Publishing.
 - [55] Alexander Barg and G David Forney. Random codes: Minimum distances and error exponents. *IEEE Transactions on Information Theory*, 48(9):2568–2573, 2002.
 - [56] Alexander Barg, Evgueni Krouk, and Henk CA van Tilborg. On the complexity of minimum distance decoding of long linear codes. *IEEE Transactions on Information Theory*, 45(5):1392–1405, 1999.
 - [57] S Barg. Some new NP-complete coding problems. *Problemy Peredachi Informatsii*, 30(3):23–28, 1994.
 - [58] Jessica Bariffi, Hannes Bartz, Gianluigi Liva, and Joachim Rosenthal. On the properties of error patterns in the constant Lee weight channel. In *International Zurich Seminar on Information and Communication (IZS 2022). Proceedings*, pages 44–48. ETH Zurich, 2022.
 - [59] Paulo SLM Barreto, Rafael Misoczki, and Marcos A Simplicio Jr. One-time signature scheme from syndrome decoding over generic error-correcting codes. *Journal of Systems and Software*, 84(2):198–204, 2011.

- [60] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 520–536. Springer, 2012.
- [61] Peter Beelen, Martin Bossert, Sven Puchinger, and Johan Rosenkilde. Structural properties of twisted Reed-Solomon codes with applications to cryptography. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 946–950. IEEE, 2018.
- [62] Emanuele Bellini, Florian Caullery, Philippe Gaborit, Marc Manzano, and Victor Mateu. Improved Veron identification and signature schemes in the rank metric. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1872–1876. IEEE, 2019.
- [63] Thierry P Berger, Philippe Gaborit, and Olivier Ruatta. Gabidulin matrix codes and their application to small ciphertext size cryptosystems. In *International Conference on Cryptology in India*, pages 247–266. Springer, 2017.
- [64] Thierry P Berger, Cheikh Thiécoumba Gueye, and Jean Belo Klamti. Generalized subspace subcodes with application in cryptology. *IEEE Transactions on Information Theory*, 65(8):4641–4657, 2019.
- [65] Thierry P. Berger and Pierre Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35:63–79, 2005.
- [66] Elwyn Berlekamp. *Algebraic coding theory*. World Scientific, 2015.
- [67] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
- [68] Daniel J Bernstein. Grover vs. McEliece. In *International Workshop on Post-Quantum Cryptography*, pages 73–80. Springer, 2010.
- [69] Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-Quantum Cryptography*. Springer-Verlag, Berlin-Heidelberg, 2009.
- [70] Daniel J Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the McEliece cryptosystem. In *International Workshop on Post-Quantum Cryptography*, pages 31–46. Springer, 2008.
- [71] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Wild McEliece. In *International Workshop on Selected Areas in Cryptography*, pages 143–158. Springer, 2010.
- [72] Daniel J Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: ball-collision decoding. In *Annual Cryptology Conference*, pages 743–760. Springer, 2011.
- [73] Ward Beullens. Not enough LESS: An improved algorithm for solving code equivalence problems over \mathbb{F}_q . In *International Conference on Selected Areas in Cryptography*, pages 387–403. Springer, 2020.

- [74] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. LESS is more: Code-based signatures without syndromes. In *International Conference on Cryptology in Africa*, pages 45–65. Springer, 2020.
- [75] Loïc Bidoux, Philippe Gaborit, and Nicolas Sendrier. Quasi-cyclic Stern proof of knowledge. *arXiv preprint arXiv:2110.05005*, 2021.
- [76] Sebastian Bitzer, Alessio Pavoni, Violetta Weger, Paolo Santini, Marco Baldi, and Antonia Wachter-Zeh. Generic decoding of restricted errors. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 246–251. IEEE, 2023.
- [77] Jessalyn Bolkema, Heide Gluesing-Luerssen, Christine A Kelley, Kristin E Lauter, Beth Malmskog, and Joachim Rosenthal. Variations of the McEliece cryptosystem. In *Algebraic geometry for coding theory and cryptography*, pages 129–150. Springer, 2017.
- [78] Maxime Bombar and Alain Couvreur. Decoding supercodes of Gabidulin codes and applications to cryptanalysis. *arXiv preprint arXiv:2103.02700*, 2021.
- [79] Mikhail A Borodin and Ivan V Chizhov. Effective attack on the McEliece cryptosystem based on Reed-Muller codes. *Discrete Mathematics and Applications*, 24(5):273–280, 2014.
- [80] Eimear Byrne, Anna-Lena Horlemann, Karan Khathuria, and Violetta Weger. Density of free modules over finite chain rings. *Linear Algebra and its Applications*, 651:1–25, 2022.
- [81] Eimear Byrne and Violetta Weger. Bounds in the Lee metric and optimal codes. *Finite Fields and Their Applications*, 87:102151, 2023.
- [82] Anne Canteaut and Hervé Chabanne. *A further improvement of the work factor in an attempt at breaking McEliece’s cryptosystem*. PhD thesis, INRIA, 1994.
- [83] 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. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998.
- [84] Anne Canteaut and Nicolas Sendrier. Cryptanalysis of the original McEliece cryptosystem. In *International conference on the theory and application of cryptology and information security*, pages 187–199. Springer, 1998.
- [85] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor. Squares of random linear codes. *IEEE Transactions on Information Theory*, 61(3):1159–1173, 2015.
- [86] Dario Catalano, Ronald Cramer, Giovanni Di Crescenzo, Ivan Damgård, David Pointcheval, Tsuyoshi Takagi, Ronald Cramer, and Ivan Damgård. Multiparty computation, an introduction. *Contemporary cryptography*, pages 41–87, 2005.
- [87] Pierre-Louis Cayrel, Cheikh T Gueye, Ousmane Ndiaye, and Robert Niebuhr. Critical attacks in code-based cryptography. *International Journal of Information and Coding Theory*, 3(2):158–176, 2015.

- [88] Pierre-Louis Cayrel, Ayoub Otmani, and Damien Vergnaud. On Kabatianskii-Krouk-Smeets signatures. In *International Workshop on the Arithmetic of Finite Fields*, pages 237–251. Springer, 2007.
- [89] Pierre-Louis Cayrel, Pascal Véron, and Sidi Mohamed El Yousfi Alaoui. A zero-knowledge identification scheme based on the q -ary syndrome decoding problem. In *International Workshop on Selected Areas in Cryptography*, pages 171–186. Springer, 2010.
- [90] Florent Chabaud and Jacques Stern. The cryptographic security of the syndrome decoding problem for rank distance codes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 368–381. Springer, 1996.
- [91] Cong Chen, Thomas Eisenbarth, Ingo Von Maurich, and Rainer Steinwandt. Differential power analysis of a McEliece cryptosystem. In *International Conference on Applied Cryptography and Network Security*, pages 538–556. Springer, 2015.
- [92] Lily Chen, Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. *Report on post-quantum cryptography*, volume 12. US Department of Commerce, National Institute of Standards and Technology, 2016.
- [93] Jinkyu Cho, Jong-Seon No, Yongwoo Lee, Young-Sik Kim, and Zahyun Koo. Enhanced pqsigRM. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [94] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Lars Ran, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. MEDS. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [95] Tung Chou, Edoardo Persichetti, and Paolo Santini. On linear equivalence, canonical forms, and digital signatures. *Cryptology ePrint Archive*, 2023.
- [96] Stephen A Cook. The complexity of theorem-proving procedures. In *Logic, Automata, and Computational Complexity: The Works of Stephen A. Cook*, pages 143–152. 2023.
- [97] Jean-Sebastien Coron. Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem. In *International Workshop on Public Key Cryptography*, pages 14–27. Springer, 2004.
- [98] Nicolas T Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 157–174. Springer, 2001.
- [99] Alain Couvreur, Thomas Debris-Alazard, and Philippe Gaborit. On the hardness of code equivalence problems in rank metric. *arXiv preprint arXiv:2011.04611*, 2020.
- [100] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes. *Designs, Codes and Cryptography*, 73(2):641–666, 2014.

- [101] Alain Couvreur and Matthieu Lequesne. On the security of subspace subcodes of Reed–Solomon codes for public key encryption. *IEEE Transactions on Information Theory*, 2021.
- [102] Alain Couvreur, Matthieu Lequesne, and Jean-Pierre Tillich. Recovering short secret keys of RLCE in polynomial time. In *International Conference on Post-Quantum Cryptography*, pages 133–152. Springer, 2019.
- [103] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. In *2014 IEEE International Symposium on Information Theory*, pages 1446–1450. IEEE, 2014.
- [104] Alain Couvreur, Irene Márquez-Corbella, and Ruud Pellikaan. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. *IEEE Transactions on Information Theory*, 63(8):5404–5418, 2017.
- [105] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial time attack on wild McEliece over quadratic extensions. *IEEE Transactions on Information Theory*, 63(1):404–427, 2016.
- [106] Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich, and Valérie Gauthier-Umana. A polynomial-time attack on the BBCRS scheme. In *IACR International Workshop on Public Key Cryptography*, pages 175–193. Springer, 2015.
- [107] Matthew C Davey and David JC MacKay. Reliable communication over channels with insertions, deletions, and substitutions. *IEEE Transactions on Information Theory*, 47(2):687–698, 2001.
- [108] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. The problem with the SURF scheme. *arXiv preprint arXiv:1706.08065*, 2017.
- [109] 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*, pages 21–51. Springer, 2019.
- [110] Thomas Debris-Alazard and Jean-Pierre Tillich. Two attacks on rank metric code-based schemes: RankSign and an IBE scheme. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 62–92. Springer, 2018.
- [111] Ph Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of combinatorial theory, Series A*, 25(3):226–241, 1978.
- [112] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.
- [113] Jintai Ding, Jason E Gower, and Dieter S Schmidt. *Multivariate public key cryptosystems*, volume 25. Springer Science & Business Media, 2006.
- [114] Vlad Drăgoi, Valeriu Beiu, and Dominic Bucerzan. Vulnerabilities of the McEliece variants based on polar codes. In *International Conference on Security for Information Technology and Communications*, pages 376–390. Springer, 2018.

- [115] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium. *NIST PQC Call for Proposals*, 2022. Selected for Standardization.
- [116] Il'ya Isaakovich Dumer. Two decoding algorithms for linear codes. *Problemy Peredachi Informatsii*, 25(1):24–32, 1989.
- [117] Molka Elleuch, Antonia Wachter-Zeh, and Alexander Zeh. A public-key cryptosystem from interleaved Goppa codes. *arXiv preprint arXiv:1809.03024*, 2018.
- [118] Jean-Charles Faugère, Valérie Gauthier-Umaña, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate McEliece cryptosystems. *IEEE Transactions on Information Theory*, 59(10):6830–6844, 2013.
- [119] Cédric Faure and Pierre Loidreau. A new public-key cryptosystem based on the problem of reconstructing p -polynomials. In *International Workshop on Coding and Cryptography*, pages 304–315. Springer, 2005.
- [120] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. *Journal of cryptology*, 1(2):77–94, 1988.
- [121] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986.
- [122] 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*, pages 88–105. Springer, 2009.
- [123] G David Forney. Concatenated codes. 1965.
- [124] Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. *NIST PQC Call for Proposals*, 2022. Selected for Standardization.
- [125] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy peredachi informatsii*, 21(1):3–16, 1985.
- [126] Ernst M Gabidulin, AV Paramonov, and OV Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 482–489. Springer, 1991.
- [127] Ernst M Gabidulin, Haitham Rashwan, and Bahram Honary. On improving security of GPT cryptosystems. In *2009 IEEE International Symposium on Information Theory*, pages 1110–1114. IEEE, 2009.
- [128] Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC*, volume 2013, 2013.
- [129] Philippe Gaborit, Ayoub Otmani, and Hervé Talé Kalachi. Polynomial-time key recovery attack on the Faure–Loidreau scheme based on Gabidulin codes. *Designs, Codes and Cryptography*, 86(7):1391–1403, 2018.

- [130] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2015.
- [131] Philippe Gaborit and Julien Schrek. Efficient code-based one-time signature from automorphism groups with syndrome compatibility. In *2012 IEEE International Symposium on Information Theory Proceedings*, pages 1982–1986. IEEE, 2012.
- [132] Philippe Gaborit and Gilles Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Transactions on Information Theory*, 62(12):7245–7252, 2016.
- [133] Maximilien Gadouneau and Zhiyuan Yan. Properties of codes with the rank metric. In *IEEE Globecom 2006*, pages 1–5. IEEE, 2006.
- [134] Robert Gallager. Low-density parity-check codes. *IRE Transactions on information theory*, 8(1):21–28, 1962.
- [135] Lucky Galvez, Jon-Lark Kim, Myeong Jae Kim, Young-Sik Kim, and Nari Lee. McNie: Compact McEliece-Niederreiter Cryptosystem. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [136] Danièle Gardy and Patrick Solé. Saddle point techniques in asymptotic coding theory. In *Workshop on Algebraic Coding*, pages 75–81. Springer, 1991.
- [137] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206, 2008.
- [138] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206, 2008.
- [139] Edgar N Gilbert. A comparison of signalling alphabets. *The Bell system technical journal*, 31(3):504–522, 1952.
- [140] Danilo Gligoroski and Kristian Gjøsteen. Post-quantum Key Encapsulation Mechanism Edon-K. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [141] Danilo Gligoroski, Simona Samardjiska, Håkon Jacobsen, and Sergey Bezzateev. McEliece in the world of Escher. *IACR Cryptol. ePrint Arch.*, 2014:360, 2014.
- [142] Valerii Denisovich Goppa. A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3):24–30, 1970.
- [143] Valerii Denisovich Goppa. A rational representation of codes and (l, g) -codes. *Problemy Peredachi Informatsii*, 7(3):41–49, 1971.
- [144] Valerii Denisovich Goppa. Binary symmetric channel capacity is attained with irreducible codes. *Problems of Information Transmission*, 10:89–90, 1974.
- [145] Elisa Gorla. Rank-metric codes. *arXiv preprint arXiv:1902.02650*, 2019.

- [146] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
- [147] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2):325, 1997.
- [148] Anina Gruica and Alberto Ravagnani. Common complements of linear subspaces and the sparseness of MRD codes. *arXiv preprint arXiv:2011.02993*, 2020.
- [149] 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 *International Conference on Codes, Cryptology, and Information Security*, pages 96–109. Springer, 2017.
- [150] Venkat Guruswami and Eric Blais. Introduction to Coding Theory, Notes 6: Reed-Solomon, BCH, Reed-Muller, and concatenated codes. February 2010. Lecture Notes.
- [151] Amir Herzberg and Dalit Naor. Surf ‘N’Sign: Client signatures on web documents. *IBM Systems Journal*, 37(1):61–71, 1998.
- [152] 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*, pages 115–126. Springer, 2016.
- [153] Anna-Lena Horlemann, Sven Puchinger, Julian Renner, Thomas Schamberger, and Antonia Wachter-Zeh. Information-set decoding with hints. Technical report, Cryptology ePrint Archive, Report 2021/279. <https://eprint.iacr.org/2021/279>, 2021.
- [154] Anna-Lena Horlemann-Trautmann, Kyle Marshall, and Joachim Rosenthal. Considerations for rank-based cryptosystems. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2544–2548. Ieee, 2016.
- [155] Anna-Lena Horlemann-Trautmann, Kyle Marshall, and Joachim Rosenthal. Extension of Overbeck’s attack for Gabidulin-based cryptosystems. *Designs, Codes and Cryptography*, 86(2):319–340, 2018.
- [156] Nick Howgrave-Graham and Antoine Joux. New generic algorithms for hard knapsacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 235–256. Springer, 2010.
- [157] Carmelo Interlando, Karan Khathuria, Nicole Rohrer, Joachim Rosenthal, and Violetta Weger. Generalization of the ball-collision algorithm. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 7(2):195–207, 2020.
- [158] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Zero-knowledge from secure multiparty computation. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 21–30, 2007.
- [159] Fedor Ivanov, Grigory Kabatiansky, Eugeny Krouk, and Nikita Rumenko. A new code-based cryptosystem. In *Code-Based Cryptography Workshop*, pages 41–49. Springer, 2020.

- [160] Heeralal Janwa and Oscar Moreno. McEliece public key cryptosystems using algebraic-geometric codes. *Designs, Codes and Cryptography*, 8(3):293–307, 1996.
- [161] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.
- [162] Gregory Kabatianskii, Evgenii Krouk, and Ben Smeets. A digital signature scheme based on random error-correcting codes. In *IMA International Conference on Cryptography and Coding*, pages 161–167. Springer, 1997.
- [163] Grigorii Kabatiansky, Evgenii Krouk, and Sergei Semenov. *Error correcting coding and security for data networks: analysis of the superchannel concept*. John Wiley & Sons, 2005.
- [164] Daniel Kales and Greg Zaverucha. An attack on some signature schemes constructed from five-pass identification schemes. In *International Conference on Cryptology and Network Security*, pages 3–22. Springer, 2020.
- [165] Hiroshi Kamabe and Shusaku Kobota. Simple improvements of bit-flipping decoding. In *2010 The 12th International Conference on Advanced Communication Technology (ICACT)*, volume 1, pages 113–118. IEEE, 2010.
- [166] Karan Khathuria, Joachim Rosenthal, and Violetta Weger. Encryption scheme based on expanded Reed-Solomon codes. *Advances in Mathematics of Communications*, 15(2):207, 2021.
- [167] Karan Khathuria, Joachim Rosenthal, and Violetta Weger. Weight two masking of the Reed-Solomon structure in conjunction with list decoding. *Proceedings of 23rd International Symposium on Mathematical Theory of Networks and Systems*, pages 309–314, 2018.
- [168] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.
- [169] Kazukuni Kobara and Hideki Imai. Semantically secure McEliece public-key cryptosystems-conversions for McEliece PKC. In *International Workshop on Public Key Cryptography*, pages 19–35. Springer, 2001.
- [170] Evgenii Avramovich Kruk. Decoding complexity bound for linear block codes. *Problemy Peredachi Informatsii*, 25(3):103–107, 1989.
- [171] Alexander Kshevetskiy and Ernst Gabidulin. The new construction of rank codes. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 2105–2108. IEEE, 2005.
- [172] 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*, pages 102–117. Springer, 2013.

- [173] Terry Shue Chien Lau and Chik How Tan. Key recovery attack on McNie based on low rank parity check codes and its reparation. In Atsuo Inomata and Kan Yasuda, editors, *Advances in Information and Computer Security*, pages 19–34, Cham, 2018. Springer International Publishing.
- [174] Terry Shue Chien Lau and Chik How Tan. MURAVE: A new rank code-based signature with multiple rank verification. In *Code-Based Cryptography Workshop*, pages 94–116. Springer, 2020.
- [175] Terry Shue Chien Lau and Chik How Tan. Polynomial-time plaintext recovery attacks on the IKKR code-based cryptosystems. *Advances in Mathematics of Communications*, 2021.
- [176] Julien Lavauzelle, Pierre Loidreau, and Ba-Duc Pham. RAMESSES, a rank metric encryption scheme with short keys. *arXiv preprint arXiv:1911.13119*, 2019.
- [177] Julien Lavauzelle and Julian Renner. Cryptanalysis of a system based on twisted Reed–Solomon codes. *Designs, Codes and Cryptography*, 88(7):1285–1300, 2020.
- [178] Pil Joong Lee and Ernest F Brickell. An observation on the security of McEliece’s public-key cryptosystem. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 275–280. Springer, 1988.
- [179] Wijik Lee, Young-Sik Kim, Yong-Woo Lee, and Jong-Seon No. pqsigRM - Post quantum signature scheme based on modified Reed-Muller code. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [180] Yongwoo Lee, Wijik Lee, Young Sik Kim, and Jong-Seon No. Modified pqsigRM: RM Code-Based Signature Scheme. *IEEE Access*, 8:177506–177518, 2020.
- [181] Jeffrey S Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, 1988.
- [182] Matthieu Lequesne and Jean-Pierre Tillich. Attack on the Edon-K key encapsulation mechanism. *CoRR*, abs/1802.06157, 2018.
- [183] Y. X. Li, R. H. Deng, and X. M. Wang. On the Equivalence of McEliece’s and Niederreiter’s Public-Key Cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.
- [184] Pierre Loidreau. Designing a rank metric based McEliece cryptosystem. In *International Workshop on Post-Quantum Cryptography*, pages 142–152. Springer, 2010.
- [185] Pierre Loidreau. Designing a rank metric based McEliece cryptosystem. In *Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings 3*, pages 142–152. Springer, 2010.
- [186] Pierre Loidreau and Raphael Overbeck. Decoding rank errors beyond the error correcting capability. *Proc. of ACCT-10, Zvenigorod*, pages 168–190, 2006.
- [187] Carl Löndahl and Thomas Johansson. A new version of McEliece PKC based on convolutional codes. In *International Conference on Information and Communications Security*, pages 461–470. Springer, 2012.

- [188] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.
- [189] Telex Magloire, Nkouatchah Ngatched, Martin Bossert, Achim Fahrner, and Fambirai Takawira. Two bit-flipping decoding algorithms for low-density parity-check codes. *IEEE transactions on communications*, 57(3):591–596, 2009.
- [190] Irene Márquez-Corbella and Jean-Pierre Tillich. Using Reed-Solomon codes in the $(u|u+v)$ construction and an application to cryptography. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 930–934. IEEE, 2016.
- [191] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $\tilde{\gamma}(2^{0.054n})$. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 107–124. Springer, 2011.
- [192] 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*, pages 203–228. Springer, 2015.
- [193] Robert J. McEliece. A public-key cryptosystem based On algebraic coding theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.
- [194] Robert J. McEliece and Dilip V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.
- [195] Alexander Meurer. *A coding-theoretic approach to cryptanalysis*. PhD thesis, Ruhr-Universität Bochum, 2012.
- [196] Lorenz Minder and Amin Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 347–360. Springer, 2007.
- [197] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *2013 IEEE international symposium on information theory*, pages 2069–2073. IEEE, 2013.
- [198] C. Monico, J. Rosenthal, and A. Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. In *Proceedings of the 2000 IEEE International Symposium on Information Theory*, page 215, Sorrento, Italy, 2000.
- [199] Dustin Moody and Ray Perlner. Vulnerabilities of “McEliece in the world of Escher”. In *Post-Quantum Cryptography*, pages 104–117. Springer, 2016.
- [200] Eliakim Hastings Moore. A two-fold generalization of Fermat’s theorem. 1896.
- [201] D. E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the I.R.E. Professional Group on Electronic Computers*, EC-3(3):6–12, 1954.
- [202] Alessandro Neri, Anna-Lena Horlemann-Trautmann, Tovohery Randrianarisoa, and Joachim Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

- [203] 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. *International journal of information and Coding Theory*, 4(1):47–78, 2017.
- [204] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory* 15, 1(6):159–166, 1986.
- [205] Ayoub Otmani and Jean-Pierre Tillich. An efficient attack on all concrete KKS proposals. In *International Workshop on Post-Quantum Cryptography*, pages 98–116. Springer, 2011.
- [206] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*, 3(2):129–140, 2010.
- [207] Alexei V Ourivski and Thomas Johansson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3):237–246, 2002.
- [208] Samuel Ouzan and Yair Be’ery. Moderate-density parity-check codes. *arXiv preprint arXiv:0911.3262*, 2009.
- [209] Raphael Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *Journal of cryptology*, 21(2):280–301, 2008.
- [210] Chris Peikert. A decade of lattice cryptography. *Cryptology ePrint Archive*, 2015.
- [211] Edoardo Persichetti. Efficient one-time signatures from quasi-cyclic codes: A full treatment. *Cryptography*, 2(4):30, 2018.
- [212] Christiane Peters. Information-set decoding for linear codes over \mathbb{F}_q . In *International Workshop on Post-Quantum Cryptography*, pages 81–94. Springer, 2010.
- [213] Erez Petrank and Ron M Roth. Is code equivalence easy to decide? *IEEE Transactions on Information Theory*, 43(5):1602–1604, 1997.
- [214] Aurélie Phesso and Jean-Pierre Tillich. An efficient attack on a code-based signature scheme. In *Post-Quantum Cryptography*, pages 86–103. Springer, 2016.
- [215] John Pierce. Limit distribution of the minimum distance of random linear codes. *IEEE Transactions on Information Theory*, 13(4):595–599, 1967.
- [216] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.
- [217] Sven Puchinger, Sven Muelich, Karim Ishak, and Martin Bossert. Code-based cryptosystems using generalized concatenated codes. In *Special Sessions in Applications of Computer Algebra*, pages 397–423. Springer, 2015.
- [218] Sven Puchinger, Julian Renner, and Antonia Wachter-Zeh. Twisted Gabidulin codes in the GPT cryptosystem. *arXiv preprint arXiv:1806.10055*, 2018.

- [219] Haitham Rashwan, Ernst M Gabidulin, and Bahram Honary. A smart approach for GPT cryptosystem based on rank codes. In *2010 IEEE International Symposium on Information Theory*, pages 2463–2467. IEEE, 2010.
- [220] I. Reed. A class of multiple-error-correcting codes and the decoding scheme. *Transactions of the IRE Professional Group on Information Theory*, 4(4):38–49, 1954.
- [221] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.
- [222] Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Hardness estimates of the code equivalence problem in the rank metric. *Cryptology ePrint Archive*, 2022.
- [223] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. Interleaving Loidreau’s rank-metric cryptosystem. In *2019 XVI International Symposium” Problems of Redundancy in Information and Control Systems”(REDUNDANCY)*, pages 127–132. IEEE, 2019.
- [224] Julian Renner, Sven Puchinger, and Antonia Wachter-Zeh. LIGA: a cryptosystem based on the hardness of rank-metric list and interleaved decoding. *Designs, Codes and Cryptography*, 89(6):1279–1319, 2021.
- [225] Tania Richmond, Martin Petrvalsky, and Milos Drutarovsky. A side-channel attack against the secret permutation on an embedded McEliece cryptosystem. In *3rd Workshop on Trustworthy Manufacturing and Utilization of Secure Devices-TRUDEVICE*, 2015.
- [226] Stefan Ritterhoff, Sebastian Bitzer, Patrick Karl, Georg Maringer, Thomas Schamberger, Jonas Schupp, Georg Sigl, Antonia Wachter-Zeh, and Violetta Weger. FuLeeca. In *First Round Submission to the additional NIST Postquantum Cryptography Call*, 2023.
- [227] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [228] Ron M Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE transactions on Information Theory*, 37(2):328–336, 1991.
- [229] Ron M Roth. Introduction to coding theory. *IET Communications*, 47, 2006.
- [230] Partha Sarathi Roy, Rui Xu, Kazuhide Fukushima, Shinsaku Kiyomoto, Kirill Morozov, and Tsuyoshi Takagi. Supporting Documentation of RaCoSS (Random Code-based Signature Scheme). *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [231] Gerald E Sacks. Multiple error correction by means of parity checks. *IRE transactions on information theory*, 4(4):145–147, 1958.
- [232] Paolo Santini, Marco Baldi, and Franco Chiaraluce. Cryptanalysis of a one-time code-based digital signature scheme. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2594–2598. IEEE, 2019.
- [233] Paolo Santini, Marco Baldi, and Franco Chiaraluce. Computational hardness of the permuted kernel and subcode equivalence problems. *IEEE Transactions on Information Theory*, 2023.

- [234] Claus-Peter Schnorr and Martin Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical programming*, 66:181–199, 1994.
- [235] Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehle, and Jintai Ding. CRYSTALS-KYBER. In *Selected Algorithm for the NIST Postquantum Cryptography Call*, 2022.
- [236] Nicolas Sendrier. *On the structure of randomly permuted concatenated code*. PhD thesis, INRIA, 1995.
- [237] Nicolas Sendrier. On the concatenated structure of a linear code. *Applicable Algebra in Engineering, Communication and Computing*, 9(3):221–242, 1998.
- [238] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [239] Adi Shamir. *An efficient identification scheme based on permuted kernels*. Springer, 1990.
- [240] Keisuke Shiromoto. Singleton bounds for codes over finite rings. *Journal of Algebraic Combinatorics*, 12:95–99, 2000.
- [241] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
- [242] Victor Shoup. A proposal for an ISO standard for public key encryption, 2001. sho@zurich.ibm.com 11676 received 20 Dec 2001.
- [243] Sujan Raj Shrestha and Young-Sik Kim. New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pages 368–372. IEEE, 2014.
- [244] Vladimir M. Sidel’nikov and Sergey O. Shestakov. On an encoding system constructed on the basis of generalized Reed–Solomon codes. *Diskretnaya Matematika*, 4(3):57–63, 1992.
- [245] Vladimir Michilovich Sidelnikov. A public-key cryptosystem based on binary Reed–Muller codes. *Discrete Mathematics and Applications*, 4(3):191–208, 1994.
- [246] RCRC Singleton. Maximum distance q -nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.
- [247] Yongcheng Song, Xinyi Huang, Yi Mu, Wei Wu, and Huaxiong Wang. A code-based signature scheme from the Lyubashevsky framework. *Theoretical Computer Science*, 835:15–30, 2020.
- [248] Jacques Stern. A method for finding codewords of small weight. In *International Colloquium on Coding Theory and Applications*, pages 106–113. Springer, 1988.
- [249] Jacques Stern. A new identification scheme based on syndrome decoding. In *Annual International Cryptology Conference*, pages 13–21. Springer, 1993.

- [250] Falko Strenzke. A timing attack against the secret permutation in the McEliece PKC. In *International Workshop on Post-Quantum Cryptography*, pages 95–107. Springer, 2010.
- [251] Falko Strenzke, Erik Tews, H Gregor Molter, Raphael Overbeck, and Abdulhadi Shoufan. Side channels in the McEliece PKC. In *International Workshop on Post-Quantum Cryptography*, pages 216–229. Springer, 2008.
- [252] Alan Szepieniec. Ramstake - KEM Proposal for NIST PQC Project. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [253] Marcel Tiepelt and Jan-Pieter D’Anvers. Exploiting decryption failures in Mersenne number cryptosystems. pages 45–54, 2020.
- [254] Jacobus Hendricus Van Lint. *Introduction to coding theory*, volume 86. Springer Science & Business Media, 2012.
- [255] Johan van Tilburg. On the McEliece public-key cryptosystem. In *Conference on the Theory and Application of Cryptography*, pages 119–131. Springer, 1988.
- [256] Alexander Vardy. Algorithmic complexity in coding theory and the minimum distance problem. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 92–109, 1997.
- [257] Rom Rubenovich Varshamov. Estimate of the number of signals in error correcting codes. *Doklady Akad. Nauk, SSSR*, 117:739–741, 1957.
- [258] Pascal Véron. A fast identification scheme. In *Proceedings of 1995 IEEE International Symposium on Information Theory*, page 359. IEEE, 1995.
- [259] Antonia Wachter-Zeh, Sven Puchinger, and Julian Renner. Repairing the Faure-Loidreau public-key cryptosystem. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 2426–2430. IEEE, 2018.
- [260] Tadashi Wadayama, Keisuke Nakamura, Masayuki Yagita, Yuuki Funahashi, Shogo Usami, and Ichi Takumi. Gradient descent bit flipping algorithms for decoding LDPC codes. In *2008 International Symposium on Information Theory and Its Applications*, pages 1–6. IEEE, 2008.
- [261] Yongge Wang. RLCE Key Encapsulation Mechanism (RLCE-KEM) Specification. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [262] Violetta Weger. *Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities*. PhD thesis, University of Zurich, 2020.
- [263] Violetta Weger, Karan Khathuria, Anna-Lena Horlemann, Massimo Battaglioni, Paolo Santini, and Edoardo Persichetti. On the hardness of the Lee syndrome decoding problem. *Advances in Mathematics of Communications*, page 0, 2022.
- [264] Christian Wieschebrink. Two NP-complete problems in coding theory with an application in code based cryptography. In *2006 IEEE International Symposium on Information Theory*, pages 1733–1737. IEEE, 2006.

- [265] Christian Wieschebrink. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. volume 6061, pages 61–72, 05 2010.
- [266] Keita Xagawa. Practical attack on RaCoSS-r. *Tc*, 1:0, 2018.
- [267] Atsushi Yamada, Edward Eaton, Kassem Kalach, Philip Lafrance, and Alex Parent. QC-MDPC KEM: A Key Encapsulation Mechanism Based on the QC-MDPC McEliece Encryption Scheme. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [268] Yu Yu and Jiang Zhang. Lepton: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise. *NIST PQC Call for Proposals*, 2017. Round 1 Submission.
- [269] Gilles Zémor. Notes on Alekhnovich’s cryptosystems. 2016.