Evolution of the McEliece Public Key Encryption Scheme

Dominic Bucerzan[1], Vlad Dragoi[2(✉)], and Hervé Talé Kalachi[2,3]

[1] Department of Mathematics and Computer Science,
Aurel Vlaicu University of Arad, 310330 Arad, Romania
dominic@bbcomputer.ro
[2] Laboratoire LITIS - EA 4108 Université de Rouen - UFR Sciences et Techniques,
76800 Saint Etienne du Rouvray, France
{vlad.dragoi1,herve.tale-kalachi1}@univ-rouen.fr
[3] Departament de Mathématiques, Université de Yaounde 1, Yaounde, Cameroun

Abstract. The evolution of the McEliece encryption scheme is a long and thrilling research process. The code families supposed to securely reduce the key size of the original scheme were often cryptanalyzed and thus the future of the code-based cryptography was many times doubted. Yet from this long evolution emerged a great comprehension and understanding of the main difficulties and advantages that coding theory can offer to the field of public key cryptography. Nowadays code-based cryptography has become one of the most promising solutions to post-quantum cryptography. We analyze in this article the evolution of the main encryption variants coming from this field. We stress out the main security issues and point out some new ideas coming from the Rank based cryptography. A summary of the remaining secure variants is given in Fig. 2.

Keywords: Post-quantum cryptography · Coding theory · McEliece encryption scheme

1 Introduction

Code-based cryptography appeared for the first time in 1978, when McEliece proposed the first public key encryption scheme which is not based on number theory primitives [McE78]. Instead he built a scheme for which the security stands on two problems, namely the hardness of the Syndrome Decoding Problem [BMvT78] and the difficulty to distinguish between a binary Goppa code and a random linear code [CFS01,FGO+13]. The scheme disposes of various advantages like

– the complexity of the encryption and decryption algorithms are equivalent to those of symmetric schemes and thus are very efficient compared to other public key schemes.

P. Farshim and E. Simion (Eds.): SecITC 2017, LNCS 10543, pp. 129–149, 2017.
https://doi.org/10.1007/978-3-319-69284-5_10

– the best attacks for solving the Syndrome Decoding Problem are exponential in the code length, which makes code-based schemes of high potential for post-quantum cryptography.

However code-based cryptography came with a big disadvantage: the size of the public keys was about five hundred thousands bits which was unacceptable at that time. Nevertheless the scientific community made a huge progress in reducing the key size of the McEliece PKC by proposing different structures like quasi-cyclic or quasi-dyadic codes. Nowadays the key size is no longer an issue and several practical implementations of the McEliece prove the efficiency and potential of the scheme [BS08, Str10b, CHP12, BCS13, HvMG13, MOG15].

Ever since Peter Shor introduced a polynomial time quantum computer algorithm for factoring integers over $\mathbb{Z}$ and for computing logarithms in the multiplicative group $\mathbb{F}_p$ [Sho94], the code-based cryptography became a serious candidate for public-key cryptography. The interest of the scientific community in this field is nowadays motivated by the latest announcement of the National Institute of Standards and Technology (NIST). They initiated the Post-Quantum crypto Project which aims to define new standards for quantum resistant cryptography and fixed the deadline for public key cryptographic algorithm submissions, for November 2017 (NIST-PQcrypto Project) (http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html). The purpose of this article is to give a complete evolution of the code-based encryption schemes and rank based encryption schemes. Proposing a global state-of-the-art, that includes both Rank distance and Hamming distance came in a natural manner since there are several facts relating these two topics

– both Hamming distance based schemes and Rank distance schemes sustain their security on the same problem, namely the Syndrome/Rank Syndrome Decoding Problem.
– the similarities do not end here since the properties of the code families that were used are quite equivalent, take for example the case of LRPC (in Rank metric) and LDPC codes (in Hamming metric) or Gabidulin (in Rank metric) and GRS codes (in Hamming metric).
– also the construction techniques are rather similar, for example the QC-LRPC (in Rank metric) and the QC-MDPC (in Hamming metric).

The article also provides a full section dedicated to the security arguments and analyze the main types of attack and it is organized as following. We begin with a preliminary section on the coding theory (Sect. 2). Then we give the necessary details on the McEliece scheme and the actual security arguments for it (see Sect. 3). In Sect. 4 we give the evolution of the McEliece variants starting with the binary Goppa codes up to nowadays. The same analysis is done in Sect. 5, for the Rank based encryption schemes. We conclude with some perspectives in this area.

2 Coding Theory

2.1 Preliminaries

Through this paper, we adopt the following notations: $\mathbb{F}_q$ denotes the finite field with q elements, $\mathsf{GL}_k(\mathbb{F})$ denotes the set of $k \times k$ invertible matrices over a field $\mathbb{F}$. An $[n, k]$ linear code $\mathscr{C}$ over $\mathbb{F}_{q^m}$ is a linear subspace of dimension k of the vector space $\mathbb{F}_{q^m}^n$. Any element in $\mathscr{C}$ is called a *codeword*. A *generator matrix* for a $[n, k]$ linear code is a $k \times n$ matrix (often denoted by $\boldsymbol{G}$) whose rows form a basis for the code. The *dual* of $\mathscr{C}$ denoted by $\mathscr{C}^\perp$ is the linear code which consists of all vectors $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ such that $\forall\ \boldsymbol{c} \in \mathscr{C} \quad \boldsymbol{y} \cdot \boldsymbol{c}^T = 0$. A *parity-check matrix* of $\mathscr{C}$ is a generator matrix of its dual. It is also a $(n-k) \times n$ matrix $\boldsymbol{H}$ of full rank that satisfies $\boldsymbol{H}\boldsymbol{c}^T = \boldsymbol{0}$ for all $\boldsymbol{c} \in \mathscr{C}$.

Minimum distance of a code. There are several metrics over the vector space $\mathbb{F}_{q^m}^n$ that are known in the literature like the Lee distance, the Hamming distance, the Rank distance etc. In code-based cryptography there are only two of them that became famous: The Hamming distance $\mathsf{d_H}$, that denotes the number of coordinates on which two vectors differ and The Rank distance $\mathsf{d_R}$ defined as follows.

Definition 1 (Rank distance). *The* rank weight *of a vector* $\boldsymbol{x} = (x_1, x_2, ..., x_n)$ *in* $\mathbb{F}_{q^m}^n$ *denoted by* $|\boldsymbol{x}|_q$ *is the dimension of the* $\mathbb{F}_q$*-vector space generated by* $\{x_1, \ldots, x_n\}$

$$|\boldsymbol{x}|_q = \dim \sum_{i=1}^{n} \mathbb{F}_q x_i.$$

The rank distance $\mathsf{d_R}(\boldsymbol{x}, \boldsymbol{y})$ *is then given by:*

$$\mathsf{d_R}(\boldsymbol{x}, \boldsymbol{y}) = |\boldsymbol{x} - \boldsymbol{y}|_q$$

In the sequel, for a given vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, $|\boldsymbol{x}|$ will denote the Hamming weight of $\boldsymbol{x}$.

Definition 2 (Minimum distance). *The minimum distance of a linear code is:*

$$\mathsf{d}_{\min}(\mathscr{C}) = \min_{\substack{(\boldsymbol{c}, \boldsymbol{c}^*) \in \mathscr{C} \times \mathscr{C} \\ \boldsymbol{c} \neq \boldsymbol{c}^*}} \mathsf{d}(\boldsymbol{c}, \boldsymbol{c}^*)$$

where d *is any of the aforementioned distances.*

2.2 The General Decoding Problem

The initial purpose of a linear code is to provide an efficient tool for a reliable communication process and it was introduced by Claude Shannon [Sha48]. We explain here a simple case, namely binary linear codes over the Binary Symmetric Channel. Let $\mathscr{C}$ be a $[n, k, d]$ binary linear code with generator matrix $\boldsymbol{G}$ and

parity check matrix $\boldsymbol{H}$, where d is the minimum distance of the code. Encoding a message $\boldsymbol{m}$ into a codeword $\boldsymbol{c}$ is equivalent to compute $\boldsymbol{c} = \boldsymbol{mG}$. Then the codeword $\boldsymbol{c}$ is sent over a BSC(p), where p is the probability of flipping a bit. In other words the receiver obtains $\boldsymbol{z} = \boldsymbol{c} \oplus \boldsymbol{e} \in \mathbb{F}_2^n$ where $\boldsymbol{e}$ is the error vector. The problem the receiver needs to solve here is to recover $\boldsymbol{c}$ from $\boldsymbol{z}$, which is called the *general decoding problem.*

Since for any codeword $\boldsymbol{c}$ of $\mathscr{C}$ we have $\boldsymbol{Hc}^T = \boldsymbol{0}_{n-k}$ we deduce that $\boldsymbol{Hz}^T = \boldsymbol{He}^T$. Therefore the dual version of the later problem can be defined generally as follows:

Definition 3 (Syndrome Decoding Problem).
Instance: *A full rank matrix* $\boldsymbol{H} \in \mathcal{M}_{n-k,n}(\mathbb{F}_{q^m})$*, a vector* $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ *and an integer* $\omega > 0$.
Question: *Is there a vector* $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ *of weight* $\leq \omega$*, such that* $\boldsymbol{Hx}^T = \boldsymbol{s}$?

In the case of the Hamming distance we call it the Syndrome Decoding Problem and Rank Syndrome Decoding Problem in the case of the Rank distance. These problems are NP-complete [BMvT78, GZ16].

There are code families for which the later problem is no longer difficult and for which efficient decoding algorithms are known. In the next part we recall some of the linear codes that are used for cryptographic purpose.

2.3 Some Code Families

Reed-Muller codes. The Reed-Muller codes were introduced by David Muller [Mul54] and rediscovered shortly after with an efficient decoding algorithm by Irving Reed [Ree54].[1] The scientific community was highly interested in this family of codes and therefore discovered many structural properties of Reed-Muller codes. Recently Kudekar et al. proved that Reed-Muller codes achieve the capacity of the Erasure channel [KKM+17].

Definition 4 (Reed-Muller codes). *Let* m *and* r *be two integers such that* $1 \leq r \leq m$ *and let* $n \stackrel{def}{=} 2^m$*. Then the* r^{th} *order Reed-Muller code* $\mathscr{R}(r, m)$ *is the binary linear code defined as the set of all vectors* $(g(v_1, \ldots, v_m))_{(v_1,\ldots,v_m)\in\mathbb{F}_2^m} \in \mathbb{F}_2^n$*, where* g *ranges over the set of polynomials over* $\mathbb{F}_2$ *in* m *variables with degree at most* r.

$$\mathscr{R}(r,m) \stackrel{def}{=} \left\{ (g(v_1,\ldots,v_m))_{(v_1,\ldots,v_m)\in\mathbb{F}_2^m} \mid g \in \mathbb{F}_2[x_1,\ldots,x_m] \ \deg g \leq r \right\}.$$

Generalized Reed-Solomon and Goppa codes. Generalized Reed-Solomon codes, or shortly GRS codes, were introduced by Reed and Solomon in [ISR60] and represent a powerful family of codes with many applications. Ten years after, a new class of codes, binary Goppa codes, was introduced by Valery Goppa [Gop70]. The main reason we detail Goppa codes in the same paragraph with GRS codes is because Goppa codes can be defined as subfield subcodes of GRS codes.

[1] Although it seems that these codes were firstly discovered by Mitani in 1951 [Mit51], they became popular only after the article of Muller and Reed.

Definition 5 (Generalized Reed-Solomon codes). *Let k and n be two integers such that $1 \leq k < n \leq q$ where $q = p^m$ is a power of a prime number p. Let $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n$ be a pair such that $\boldsymbol{x}$ is an n-tuple of distinct elements of $\mathbb{F}_q$ and the elements y_i are nonzero elements in $\mathbb{F}_q$. Then the Generalized Reed-Solomon code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ is given by:*

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} \{(y_1 f(x_1), \ldots, y_n f(x_n)) \mid f \in \mathbb{F}_q[x],\ \deg(f) < k\}\,.$$

The vector $\boldsymbol{x}$ is called the support of the code and $\boldsymbol{y}$ the multiplier vector. One can easily deduce that a generator matrix of $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ is given by

$$\boldsymbol{G} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{k-1} & x_2^{k-1} & \ldots & x_n^{k-1} \end{pmatrix} \begin{pmatrix} y_1 & & & \\ & y_2 & & 0 \\ & & \ddots & \\ 0 & & & y_n \end{pmatrix}.$$

Proposition 1 ([MS86]Theorem 4, Chap. 10). *The dual of a GRS code is also a GRS code and we have*

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\perp} = \mathbf{GRS}_{n-k}(\boldsymbol{x}, \boldsymbol{z}),$$

where $\boldsymbol{z}$ is a non-zero codeword of the $(n, 1, n)$ GRS code $\mathbf{GRS}_{n-1}(\boldsymbol{x}, \boldsymbol{y})^{\perp}$.

We notice that the vector $\boldsymbol{z}$ with $\forall\ 1 \leq i \leq n, z_i \neq 0$ exists since any non zero codeword of a $[n, 1, n]$ GRS code has a Hamming weight equal to n.

Definition 6 (Alternant codes). *A p-ary alternant code of order r associated to $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_{p^m}^n \times \mathbb{F}_{p_m}^n$ denoted by $\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y})$ is*

$$\mathbf{Alt}_r(\boldsymbol{x}, \boldsymbol{y}) \stackrel{def}{=} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp} \cap \mathbb{F}_p^n.$$

Definition 7 (Binary Goppa codes). *Let $\boldsymbol{x} \in \mathbb{F}_{2^m}^n$ be a $n-$tuple of distinct elements and $g \in \mathbb{F}_{2^m}[x]$ be a polynomial of degree t such that $\forall\ i, g(x_i) \neq 0$. Let $\boldsymbol{y} \stackrel{def}{=} (1/g(x_i), \ldots, 1/g(x_n))$ then the binary Goppa code is defined by*

$$\boldsymbol{\Gamma}(\boldsymbol{x}, g) \stackrel{def}{=} \mathbf{Alt}_t(\boldsymbol{x}, \boldsymbol{y}).$$

There are several decoding techniques for Goppa codes like for example the Berlekamp-Massey algorithm, the Extended Euclidean Algorithm or the Patterson algorithm [MS86, Chap. 12].

LDPC and MDPC codes. Another important class of linear codes is the family of low density parity check (LDPC) codes discovered by Gallager [Gal63]. He was motivated by the problem of finding "random-like" codes that could be decoded near the channel capacity with quasi-optimal performance and feasible complexity. Since LDPC were too complex for the technology at that time, they were forgotten for more than 30 years, and rediscovered by MacKay [Mac99] and Sipser and Spielman [SS96]. These codes were extended in a natural way to moderate density parity check codes in [OB09]. LDPC codes have many applications in communication field as well as in cryptography.

Definition 8 (LDPC/MDPC codes). *A (n, k, ω)-code is a linear code defined by a $k \times n$ parity-check matrix ($k < n$) where each row has weight ω.*

A LDPC *code is a (n, k, ω)-code with $\omega = O(1)$, when $n \to \infty$. [Gal63]*
A MDPC *code is a (n, k, ω)-code with $\omega = O(\sqrt{n})$, when $n \to \infty$. [OB09]*

The theory of error correcting codes is not only a highly important tool in the communication field, it is also applied to public key cryptography. One of the oldest public key encryption scheme, namely the McEliece PKC [McE78], is based on several aspects from coding theory.

3 McEliece and Niederreiter Encryption Scheme

3.1 Description

The McEliece public key encryption scheme [McE78] is composed of three algorithms: *key generation* (KeyGen), *encryption* (Encrypt) and *decryption* (Decrypt). The key generation algorithm takes as input the integers n, m, k, t, q such that $k < n$ and $t < n$ and outputs the public key/private key pair $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{KeyGen}(n, m, k, t, q) = (\mathsf{pk}, \mathsf{sk})$

1. Pick a generator matrix $\boldsymbol{G}$ of a $[n, k]$ code $\mathscr{C}$ that can corrects t errors.
2. Pick at random $\boldsymbol{S}$ in $\mathsf{GL}_k(\mathbb{F}_{q^m})$ and a $n \times n$ permutation matrix $\boldsymbol{P}$.
3. Compute $\boldsymbol{G}_{\text{pub}} \stackrel{\text{def}}{=} \boldsymbol{SGP}$.
4. Return

$$\mathsf{pk} = (\boldsymbol{G}_{\text{pub}}, t) \text{ and } \mathsf{sk} = (\boldsymbol{S}, \boldsymbol{P}).$$

In order to encrypt a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$ one applies the following function

$\mathsf{Encrypt}(\boldsymbol{m}, \mathsf{pk}) = \boldsymbol{z}$

1. Generate a random error-vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $|\boldsymbol{e}| \leq t$
2. Return $\boldsymbol{z} = \boldsymbol{mG}_{\text{pub}} \oplus \boldsymbol{e}$

The decryption takes as input a ciphertext $\boldsymbol{z}$ and the private key sk and outputs the corresponding message $\boldsymbol{m}$

$\mathsf{Decrypt}(\boldsymbol{z}, \mathsf{sk}) = \boldsymbol{m}$

1. Compute $\boldsymbol{z}^* = \boldsymbol{zP}^{-1}$ and $\boldsymbol{m}^* = \mathcal{D}ecode(\boldsymbol{z}^*, \boldsymbol{H})$
2. Return $\boldsymbol{m}^* \boldsymbol{S}^{-1}$.

$\mathcal{D}ecode(.,.)$ is an efficient decoding algorithm for $\mathscr{C}$. Notice that multiplying the error vector by a permutation does not change the weight of the vector. One can easily verify the correctness of the scheme by checking

$$\mathsf{Decrypt}(\mathsf{Encrypt}(\boldsymbol{m}, \mathsf{pk}), \mathsf{sk}) = \boldsymbol{m}.$$

The Niederreiter public-key encryption scheme [Nie86] is similar to the McEliece's scheme. It uses the dual code and thus the public key is a parity check matrix for the code. The message will be an error vector that is encrypted into a syndrome. In [LDW94] it is showed that the two schemes are equivalent in term of security.

3.2 Security Arguments

The security of all the variants à la McEliece is based on two facts: firstly the public code is supposed to be indistinguishable from a random code. If the later supposition is satisfied then in order to decrypt a cyphertext one has to solve the Syndrome Decoding Problem for a random code (see Definition 3), which is known as a difficult problem. There are three types of attacks known in the literature: Distinguishing Attacks, Message Recovery Attacks (MRA) and Key Recovery Attacks (KRA).

Distinguishing attacks. Even though the indistinguishably of the public code in the original McEliece scheme was not proved, there is a strong believe that this problem is hard. However, a recent breakthrough in this area was the distinguisher for high rate Goppa codes, proposed in [FGO+13]. It is based on the star product of two codes and uses the dimension of the square code in order to distinguish between a random linear code and a high rate Goppa code. This technique also works on high rate Alternant codes [FGO+13], Reed-Solomon codes [CGG+14], Reed-Muller codes [CB13, OTK15] etc.

Message Recovery Attacks. In this scenario an adversary aim to recover the plaintext from a given ciphertext. If the public code is indistinguishable from a random code then the MRA become equivalent to solving the Syndrome Decoding Problem. The most efficient algorithm to solve the Syndrome Decoding Problem is the Information Set Decoding (ISD). Details about the different variants of ISD and their complexity analysis are given in [CTS16]. However, the best variant has a complexity which is exponential in the codes parameters.

Key Recovery Attacks. The key recovery adversary aims to retrieve the private key from a given public key. If the cryptanalyst manages to efficiently recover the private key, then he can also decode and find all the messages that have been encrypted with that key. Therefore it is considered as the most powerful possible attack. In the KRA scenario the adversary is often reduced to solve the following problem.

Definition 9 (Permutation Code Equivalence Problem). *Let* $\boldsymbol{G}$ *and* $\boldsymbol{G}^*$ *be the generating matrices for two* $[n, k]$ *binary linear codes. Given* $\boldsymbol{G}$ *and* $\boldsymbol{G}^*$ *does there exist a* $k \times k$ *binary invertible matrix* $\boldsymbol{S}$ *and* $n \times n$ *permutation matrix* $\boldsymbol{P}$ *such that* $\boldsymbol{G}^* = \boldsymbol{SGP}$*?*

The computational problem was studied by Petrank and Roth over the binary field [PR97], in which the authors proved that the problem is not NP-complete. The most common algorithm used to solve this problem is the Support Splitting Algorithm (SSA) [Sen00]. This algorithm is very efficient in the random case, but cannot be used in the case of codes with large Hulls or codes with large Permutation group such as Goppa codes, Reed-Muller codes, ... When the SSA is infeasible, other efficient technique can be employed such as the *Minimum Weight Codewords* approach. The idea is to use the subcode spanned by the set of minimum weight codewords and solve the code equivalence problem for the

later code. Indeed, in the case of many linear codes, the code spanned by the set of minimum weight codewords is almost the entire code. This is the case of Polar codes and more generally of any Decreasing Monomial codes (see [BDOT16]). This technique was used to solve the code equivalence problem for Reed-Muller codes [MS07] and Polar codes [BCD+16]. The main step of this technique is the minimum weight codewords searching. The most efficient algorithms for this are derived from the Information Set Decoding algorithm.

Side-channel attacks. The importance of practical issues is crucial for designing a cryptosystem. A designer should be able to prove that the scheme can be securely implemented and that eventual side-channel attacks can easily be countered. In this scenario the attacker has the capability to access and monitor different parameters of the implementation, like for example a particular function in the decryption process. In a successful side-channel attack, the aforementioned advantage reveals information on the private message or on the private key of the scheme.

4 McEliece Variants

In the previous section, several security issues are revealed, fact that raised a fundamental question: *What is the most appropriate code family for the McEliece scheme?*

4.1 Binary Irreducible Goppa Codes

They were proposed in the original paper of McEliece [McE78]. Even though the original parameters were broken in [BLP08], they proposed a new set of secured parameters (see Fig. 1). Despite their well known structure there are no efficient key recovery or decoding attacks against binary irreducible Goppa codes. A **distinguisher** exists in the case of high rate Goppa codes [FGO+13]. But despite of this potential vulnerability there is no efficient algorithm for the moment exploiting the knowledge and the properties of the distinguisher. The existence of **weak keys** for Goppa codes was raised by Sendrier and Loidreau in [LS01].

We notice from Fig. 1 that the size of the public key is a real disadvantage of the McEliece scheme compared to the well known RSA encryption scheme [RSA78]. Therefore reducing the size of the keys is one of the starting points of a continuous research interest in this field. We mention the existence of a

Security level(-bit)	$[n, k]$	t	Public Key size (bits)	RSA - Public key size (bits)
80	[1632, 1269]	33	460647	512
128	[2960, 2288]	56	1537536	3072
256	[6624, 5129]	115	7667855	15360

Fig. 1. Parameters and key size for McEliece with Goppa codes from [BLP08] and key size for the RSA scheme

compact variant of the McEliece scheme based on quasi-dyadic Goppa codes due to Misoczki and Barreto [MB09], variant that is not yet broken in the binary case. The binary Goppa codes were also the most cryptanalyzed scheme from side-channel perspective. There are mainly two types of side-channel attacks classified by their goal:

1. Recover the secret message [STM+08, AHPT11];
2. Recover the private key (fully or partially) [Str13, Str10a, SSMS09, BCDR16].

In each article the authors propose to counter the leak and thus step towards a secure implementation of the scheme. Countermeasures and secured implementations are also proposed in [CHP12, DCCR13, BCS13].

4.2 Generalized Reed-Solomon Codes

This family was proposed for the first time by Niederreiter in [Nie86] but turned out to be an insecure solution. Indeed, six years after the article was published, Sidelnikov and Shestakov proposed a polynomial time attack against this variant [SS92]. Nevertheless the idea of using GRS codes was reconsidered more than ten years after by Berger and Loidreau when they proposed to consider subcodes of GRS codes [BL05]. Unfortunately this technique was also attacked in two steps by Wieschebrink [Wie06a, Wie09], using the **square code structure**.

Other attempts to repair the Niederreiter variant were proposed by Wieschebrink [Wie06b] who's idea was to add random column to the generator matrix. But this variant turned out to be extremely unsecure against **square code type attacks** [CGG+14]. Nevertheless GRS codes are still of high interest for this community since several modified version of the McEliece scheme use this family of codes. For example Baldi et al. [BBC+16] proposed to change the permutation matrix, Tillich et al. [MCT16] propose to use them in a "$u \mid u + v$" construction, Wang [Wan16] propose to use a technique derived from Wieschebrink's idea.

4.3 Reed-Muller Codes

Reed-Muller codes were proposed by Sidelnikov's in [Sid94] and was firstly attacked by Minder and Shokrollahi [MS07]. In the case of Reed-Muller codes the Key Recovery Attack is reduced to solving the code equivalence problem since there is only one $\mathscr{R}(r, m)$. Minder and Shokrollahi managed to solve this problem using a filtration type attack based on the structure properties of the minimum weight codewords. The complexity of their algorithm was dominated by the minimum weight codewords searching algorithm.

Recently, Chizhov and Borodin [CB14] proposed another attack that could solve the code equivalence problem, for some of the parameters of the Reed-Muller codes, in polynomial time. Their idea was to use two simple operations in order to find the first order Reed-Muller code given the r^{th} order Reed-Muller code. Indeed they noticed that the dual and the **square code** of a Reed-Muller code is still a Reed-Muller code. So they combined these operations in order to

approach the $\mathscr{R}(1, m)$. A modified version using the masking technique introduced by Wieschebrink was proposed in [GM13] and recently broken by Otmani and Talé-Kalachi [OTK15] using a **square code** type attack.

4.4 Algebraic-Geometry Codes

This family of codes was suggested by Janwa and Moreno [JM96]. Several articles discussed the potential vulnerabilities of this variant and proposed algorithms that could be deployed to attack in some particular cases [FM08,SS92]. Nevertheless they can not be generalized and suffer in terms of efficiency. In [CMCP14] Couvreur, Marquez-Corbella and Pellikaan proposed a polynomial type algorithm that works on codes from curves of arbitrary genus.

4.5 Concatenated Codes

Concatenated codes were the first family of probabilistic codes analyzed from a cryptographic point of view. Sendrier detailed in [Sen94,Sen98] the main vulnerabilities of ordinary concatenated codes.

4.6 LDPC Codes

Monico, Rosenthal and Shokrollahi were the first ones to propose and analyze a McEliece variant using low density parity check codes in [MRAS00]. Using the idea of Gaborit to consider quasi-cyclic codes [Gab05][2] the new QC-LDPC cryptosystem was presented by Baldi and Chiaraluce in [BC07]. Both BCH codes and LDPC codes with quasi-cyclic structure were successfully cryptanalyzed by Otmani, Tillich and Dallot [OTD08]. In order to prevent the last attack, a modification based on increasing the weight of the codewords in the public code was proposed in [BBC08]. In the book of Baldi [Bal14] all the details about the thrilling combats defeating and attacking the LDPC codes are given.

4.7 Wild Goppa Codes

This code family is a natural extension from binary Goppa codes to non binary fields. It was proposed by Bernstein, Lange and Peters in [BLP10] and [BLP11]. Many of the proposed parameters were broken by Couvreur, Otmani and Tillich using **filtration type techniques** [COT14a,COT14b], for quadratic extensions.

4.8 Srivastava Codes

Srivastava codes were proposed in [Per12] in order to reduce the key length of the original McEliece scheme. The author uses Quasi-Dyadic Srivastava codes and gives another application of these types of codes for signature schemes. Even though the parameters for the signature were broken in [FOP+16], the parameters for the encryption scheme are still valid.

[2] In [Gab05] the author proposes BCH codes with quasi-cyclic structure. The idea of adding the quasi cyclic structure became one of the main techniques for reducing the key size in the McEliece scheme.

4.9 MDPC Codes

Moderate Density Parity-Check codes are probably the most suitable codes in a McEliece type scheme [MTSB13]. Many cryptographic arguments are in favour of this family of codes like efficiency, small key size when used with a quasi-cyclic structure and the most important to our opinion the lack of algebraic structure. Another security argument is the fact that the usual distinguisher does not work for MDPC codes. In a recent paper, weak keys of the QC-MDPC scheme are revealed [BDLO16]. However the authors show how to avoid vulnerable parameters.

4.10 Convolutional Codes

Convolutional codes represented among the shortest term solutions since between the proposed article by Londahl and Johansson [LJ12] and the efficient attack by Landais and Tillich [LT13] only one year passed.

4.11 Polar Codes

This family of codes was as unfortunate as convolutional code. The first variant using Polar codes was proposed by Shrestha and Kim [SK14] while the second one using subcodes of Polar codes was given in [HSEA14]. In [BCD+16] the first variant was attacked using the structure of the minimum weight codewords. The authors managed to solve the code equivalence problem for Polar codes and thus completely break the scheme.

To close this section we emphasize that there are code families which are not appropriate in this context due to their structural properties, namely the GRS codes, the Reed-Muller codes, the Polar codes ... However several classes of codes remain secure in a McEliece PKC such as original binary Goppa codes, LDPC and MDPC codes etc. A complete summary of the remaining secure code families is also given in Fig. 2. Meanwhile the scientific community developed a new idea, that consists in working with another metric, for instance the rank-metric. Nowadays, this part of the public-key cryptography is known under the name of rank-based cryptography.

5 Rank Based Encryption Schemes

The first rank-metric scheme was proposed in [GPT91] by Gabidulin, Paramonov and Tretjakov which is now called the GPT cryptosystem. This scheme can be seen as an analogue of the McEliece public key cryptosystem based on the class of Gabidulin codes. In the following, we present the class Gabidulin codes. In order to simplify the notation, for any x in $\mathbb{F}_{q^m}$ and for any integer i, the quantity x^{q^i} is denoted by $x^{[i]}$.

Definition 10 (Gabidulin code). *Let $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$ such that $|\boldsymbol{g}|_q = n$. The $(n,k)-$ Gabidulin code denoted by $\mathscr{G}_k(\boldsymbol{g})$ is the code with a generator matrix $\boldsymbol{G}$ where:*

$$\boldsymbol{G} = \begin{pmatrix} g_1^{[0]} & \cdots & g_n^{[0]} \\ \vdots & & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}. \tag{1}$$

A matrix of the form (1) is called a $q-$ Vandermonde matrix. Gabidulin codes are known to have a good decoding capability [GPT91].

5.1 The General GPT Cryptosystem

The key generation algorithm of the general GPT cryptosystem takes as input the integers k, ℓ, n and m such that $k < n \leq m$ and $\ell \ll n$ and outputs the public key/private key pair $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{KeyGen}(n, m, k, \ell, q) = (\mathsf{pk}, \mathsf{sk})$

1. Let $\boldsymbol{G} \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ be a generator matrix of the Gabidulin code $\mathscr{G}_k(\boldsymbol{g})$
2. Pick $\boldsymbol{S} \in \mathsf{GL}_k(\mathbb{F}_{q^m})$, $\boldsymbol{X} \in \mathcal{M}_{k,\ell}(\mathbb{F}_{q^m})$ and $\boldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$.
3. Compute $\boldsymbol{G}_{\text{pub}} \stackrel{\text{def}}{=} \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P}$ and $t = \frac{n-k}{2}$
4. Return

$$\mathsf{pk} = (\boldsymbol{G}_{\text{pub}}, t) \text{ and } \mathsf{sk} = (\boldsymbol{S}, \boldsymbol{P}).$$

To encrypt a message $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, apply the following function

$\mathsf{Encrypt}(\boldsymbol{m}, \mathsf{pk}) = \boldsymbol{z}$

1. Generate a random error-vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ with $|\boldsymbol{e}|_q \leq t$
2. Return $\boldsymbol{z} = \boldsymbol{m}\boldsymbol{G}_{\text{pub}} \oplus \boldsymbol{e}$

The decryption takes as input a ciphertext $\boldsymbol{z}$ and the private key sk and outputs the corresponding message $\boldsymbol{m}$. $\mathsf{Decrypt}(\boldsymbol{z}, \mathsf{sk})$ firstly computes $\boldsymbol{z}\boldsymbol{P}^{-1} = \boldsymbol{m}\boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G}) + \boldsymbol{e}\boldsymbol{P}^{-1}$. The last n components of $\boldsymbol{z}\boldsymbol{P}^{-1}$ will satisfy $\boldsymbol{z}' = \boldsymbol{m}\boldsymbol{S}\boldsymbol{G} + \boldsymbol{e}'$ where $\boldsymbol{e}'$ is a sub-vector of $\boldsymbol{e}\boldsymbol{P}^{-1}$ hence $|\boldsymbol{e}'|_q \leq t$. It then applies a fast decoding algorithm of $\mathscr{G}_k(\boldsymbol{g})$ to $\boldsymbol{z}'$ and obtain $\boldsymbol{m}\boldsymbol{S}$ and hence $\boldsymbol{m}$.

Security. In [Ove08], Overbeck proposed a very efficient attack on the GPT cryptosystem. Several works propose to resist to Overbeck's attack either by taking a column scrambler matrix defined over the extension field $\mathbb{F}_{q^m}$ [Gab08, GRH09, RGH11, GP14] or by taking special distortion matrix as in [Loi10, RGH10]. We describe in the following all existing variant of the GPT cryptosystem after the apparition of Overbeck's attacks, and we give the state of the security of each variant.

5.2 GPT Cryptosystem with Column Scrambler on the Extension Field

The first paper that consider column scrambler matrix over the extension field is Gabidulin's paper [Gab08]. The important points are Key generation and decryption; the encryption phase is without change. The author proposed to describe the system as follows:

Description of the Scheme. The key generation algorithm works as for the general GPT scheme, with the difference: $\boldsymbol{P}$ in $\mathsf{GL}_{n+\ell}(\mathbb{F}_{q^m})$ is such that there exist $\boldsymbol{Q}_{11}$ in $\mathcal{M}_{\ell,\ell}(\mathbb{F}_{q^m})$, $\boldsymbol{Q}_{21}$ in $\mathcal{M}_{n,\ell}(\mathbb{F}_{q^m})$, $\boldsymbol{Q}_{22}$ in $\mathcal{M}_{n,n}(\mathbb{F}_q)$ and $\boldsymbol{Q}_{12}$ in $\mathcal{M}_{\ell,n}(\mathbb{F}_{q^m})$ with $|\boldsymbol{Q}_{12}| = s < t$ so that

$$\boldsymbol{P}^{-1} = \begin{pmatrix} \boldsymbol{Q}_{11} & \boldsymbol{Q}_{12} \\ \boldsymbol{Q}_{21} & \boldsymbol{Q}_{22} \end{pmatrix}. \tag{2}$$

The public key is $(\boldsymbol{G}_{\text{pub}}, t_{\text{pub}})$ with $t_{\text{pub}} = t - s$ and $\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G})\boldsymbol{P}$.

Decryption. We have $\boldsymbol{c}\boldsymbol{P}^{-1} = \boldsymbol{m}\boldsymbol{S}(\boldsymbol{X} \mid \boldsymbol{G}) + \boldsymbol{e}\boldsymbol{P}^{-1}$. Suppose that $\boldsymbol{e} = (\boldsymbol{e}_1 \mid \boldsymbol{e}_2)$ where $\boldsymbol{e}_1 \in \mathbb{F}_{q^m}^{\ell}$ and $\boldsymbol{e}_2 \in \mathbb{F}_{q^m}^{n}$. We have:

$$\boldsymbol{e}\boldsymbol{P}^{-1} = (\boldsymbol{e}_1\boldsymbol{Q}_{11} + \boldsymbol{e}_2\boldsymbol{Q}_{21} \mid \boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}) \tag{3}$$

It is clear that

$$|\boldsymbol{e}_1\boldsymbol{Q}_{12} + \boldsymbol{e}_2\boldsymbol{Q}_{22}| \leq |\boldsymbol{e}_1\boldsymbol{Q}_{12}| + |\boldsymbol{e}_2\boldsymbol{Q}_{22}| \leq s + t - s.$$

So the plaintext $\boldsymbol{m}$ is recovered by applying the decoding algorithm only to the last n components of $\boldsymbol{c}\boldsymbol{P}^{-1}$.

Several authors also proposed other constructions of the column scrambler on the extension field. In [GRH09,RGH11] it is proposed for instance to choose a column scrambler matrix $\boldsymbol{P}^* = \boldsymbol{T}\boldsymbol{P}$ such that

$$\boldsymbol{P}^{-1} = (\boldsymbol{Q}_1 \mid \boldsymbol{Q}_2) \tag{4}$$

where $\boldsymbol{Q}_1 \in \mathcal{M}_{n,s}(\mathbb{F}_{q^m})$ while $\boldsymbol{Q}_2 \in \mathcal{M}_{n,(n-s)}(\mathbb{F}_q)$. This construction can be seen as a variant of the more general construction given in [Gab08] (see [OTKN16] for more details). In [GP13,GP14], another variant is also proposed. This variant consists to use a column scrambler matrix $\boldsymbol{P}$ such that

$$\boldsymbol{P}^{-1} = \boldsymbol{T} + \boldsymbol{Z} \tag{5}$$

$\boldsymbol{T} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ and $\boldsymbol{Z} \in \mathcal{M}_{n+\ell,n+\ell}(\mathbb{F}_{q^m})$ with $|\boldsymbol{Z}| = s$. However, this last variant was shown in [UG14] to be equivalent to the general GPT cryptosystem [GO01] and hence not secure.

Security. In was recently shown in [OTKN16] that the Gabidulin's general construction [Gab08] is not secured, even if a more general column scrambler $\boldsymbol{P}^* = \boldsymbol{T}\boldsymbol{P}\boldsymbol{Q}$ is considered ($\boldsymbol{T}, \boldsymbol{Q} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ and $\boldsymbol{P}$ being a matrix that the inverse is given by Eq. 2). This attack also implies and attack on the variant of [GRH09,RGH11] since the construction of [Gab08] is a generalization of the constructions given in [GRH09,RGH11,GP14,GP13].

5.3 GPT Cryptosystems with a Special Distortion Matrix

Loidreau reparation. The main objective of the Loidreau reparation [Loi10] is not to propose a new system, but to propose parameters that would prevent Overbeck's attack. The idea is to take a very large ℓ ($\ell >>> n-k$) and use a matrix $\boldsymbol{X} \in \mathcal{M}_{k,\ell}(\mathbb{F}_{q^m})$ with a very low rank s such that $s(n-k) \leq \ell - a$ where a is a given integer. Even if the keys sizes of this reparation are small compared to what we have in the McEliece encryption scheme [McE78], they remain very large. It is the reason why the author of [RGH10] proposed the "smart approach" that aim to avoid Overbeck's attack while keeping small keys sizes.

The smart approach. As in the Loidreau's reparation, the only difference is on the generation of $\boldsymbol{X}$. The authors proposed to take a distortion matrix $\boldsymbol{X} \in \mathcal{M}_{k,\ell}(\mathbb{F}_{q^m})$ that is a concatenation of a $q-$Vandermonde matrix $\boldsymbol{X}_1 \in \mathcal{M}_{k,a}(\mathbb{F}_{q^m})$ and a random matrix $\boldsymbol{X}_2 \in \mathcal{M}_{k,\ell-a}(\mathbb{F}_{q^m})$ with $0 < a < \ell$. More precisely, to design the public generator matrix, let $\boldsymbol{S} \in \mathsf{GL}_k(\mathbb{F}_{q^m})$, $\boldsymbol{X}_2 \in \mathcal{M}_{k,\ell-a}(\mathbb{F}_{q^m})$, $\boldsymbol{b} = (b_1, \cdots, b_a)$ and

$$\boldsymbol{X}_1 = \begin{pmatrix} b_1^{[0]} & \cdots & b_a^{[0]} \\ \vdots & & \vdots \\ b_1^{[k-1]} & \cdots & b_a^{[k-1]} \end{pmatrix}. \tag{6}$$

Select $\boldsymbol{P} \in \mathsf{GL}_{n+\ell}(\mathbb{F}_q)$ and compute

$$\boldsymbol{G}_{\text{pub}} = \boldsymbol{S}\,(\boldsymbol{X}_1 \mid \boldsymbol{X}_2 \mid \boldsymbol{G})\,\boldsymbol{P}$$

Security. A successful cryptanalysis of the previous variants was recently propose in [HMR15]. We also emphasise that there is a recent Message Recovery Attack against the aforementioned variants by [GRS16, HTMR16].

5.4 LRPC Cryptosystem

Beside the Gabidulin codes and inspired by the class of MDPC/LDPC codes in Hamming metric, a new class of rank metric codes was recently proposed in [GMRZ13] namely Low Rank Parity Check codes. They are the adaptation of the MDPC/LDPC codes in the rank metric. The LRPC cryptosystem [GMRZ13] is thus the analogue of the MDPC McEliece scheme. The main advantage of the scheme is that it comes, as the MDPC PKC, with a quasi-cyclic version, which allows to drastically reduce the key size. The QC-LRPC scheme is therefore one of the most promising rank-based encryption scheme since it has many security arguments in its favour: compared to the Gabidulin codes, the LRPC codes have a weak algebraic structure and thus seem much more fitted for a cryptographic purpose. Secondly the QC-LRPC scheme is equivalent to the NTRU [HPS98] and thus benefit of a quite long research experience from a cryptanalytic point of view.

Security level(-bit)	Binary Goppa [BLP08]	Wild Goppa [BLP10]	QD - Srivastava [Per12]	QC - LDPC [Bal14]	QC - MDPC [MTSB13]	LRPC [GMRZ13]
80	460647	-	36288	-	4801	1681
128	1537536	1523278	37440	12351	9857	2809

Fig. 2. Key size in bits for the remaining secure code families in the McEliece scheme

6 Conclusion and Perspectives

In this article we have given a state-of-the-art of the McEliece encryption scheme. We have also detailed the main security threats for the scheme and for each of the mentioned variants. The general idea is to choose an appropriate private code that will be masked into a public one. This technique opens a general security question of indistinguishability of the public code from a random code. Even though several variants remain secured against existing attacks there is no theoretical guaranty of their security. By that we mean there is no security proof for the aforementioned variants. For instance there is no formal proof of the indistinguishability of the public code from a random one. The table bellow summarizes the remaining secure code families in the McEliece scheme. We emphasize that this table is not complete, but the variants given are the principal ones known with parameters.

Following McEliece's idea a possible solution for this problem would be to find a new masking technique for which there is a formal proof of the indistinguishability of the public code from a random one. In [Wan16] the author propose a masking technique for which he proves that the public code is equivalent to a random code and thus reintroduce in the context all the structural codes that have been broken. Another solution was already proposed by Alekhnovich who proposed an innovative approach based on the difficulty of decoding purely random codes [Ale11]. Several authors were inspired by his work [DMN12, DV13, KMP14, ABD+16]. This two approaches open a new perspective for code-based cryptography.

References

[ABD+16] Aguilar, C., Blazy, O., Deneuville, J.-C., Gaborit, P., Zémor, G.: Efficient encryption from random quasi-cyclic codes. arXiv preprint (2016). arXiv:1612.05572

[AHPT11] Avanzi, R., Hoerder, S., Page, D., Tunstall, M.: Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. J. Cryptogr. Eng. **1**(4), 271–281 (2011)

[Ale11] Alekhnovich, M.: More on average case vs approximation complexity. Comput. Complex. **20**(4), 755–786 (2011)

[Bal14] Baldi, M.: QC-LDPC Code-Based Cryptography. SpringerBriefs in Electrical and Computer Engineering, p. 120. Springer, Heidelberg (2014). doi:10.1007/978-3-319-02556-8

[BBC08] Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the mceliece cryptosystem based on QC-LDPC codes. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 246–262. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85855-3_17

[BBC+16] Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: Enhanced public key security for the mceliece cryptosystem. J. Cryptol. **29**(1), 1–27 (2016)

[BC07] Baldi, M., Chiaraluce, F.: Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In: Proceedings of IEEE International Symposium on Information Theory - ISIT, pp. 2591–2595, Nice, France, June 2007

[BCD+16] Bardet, M., Chaulet, J., Dragoi, V., Otmani, A., Tillich, J.-P.: Cryptanalysis of the McEliece public key cryptosystem based on polar codes. In: Takagi, T. (ed.) PQCrypto 2016. LNCS, vol. 9606, pp. 118–143. Springer, Cham (2016). doi:10.1007/978-3-319-29360-8_9

[BCDR16] Bucerzan, D., Cayrel, P.-L., Dragoi, V., Richmond, T.: Improved timing attacks against the secret permutation in the mceliece PKC. Int. J. Comput. Commun. Control **12**(1), 7–25 (2016)

[BCS13] Bernstein, D.J., Chou, T., Schwabe, P.: McBits: fast constant-time code-based cryptography. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 250–272. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40349-1_15

[BDLO16] Bardet, M., Dragoi, V., Luque, J.-G., Otmani, A.: Weak keys for the quasi-cyclic MDPC public key encryption scheme. In: Pointcheval, D., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 2016. LNCS, vol. 9646, pp. 346–367. Springer, Cham (2016). doi:10.1007/978-3-319-31517-1_18

[BDOT16] Bardet, M., Dragoi, V., Otmani, A., Tillich, J.-P.: Algebraic properties of polar codes from a new polynomial formalism. In: IEEE International Symposium on Information Theory (ISIT 2016), Barcelona, Spain, 10–15 July 2016, pp. 230–234 (2016)

[BL05] Berger, T.P., Loidreau, P.: How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr. **35**(1), 63–79 (2005)

[BLP08] Bernstein, D.J., Lange, T., Peters, C.: Attacking and defending the McEliece cryptosystem. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 31–46. Springer, Heidelberg (2008). doi:10.1007/978-3-540-88403-3_3

[BLP10] Bernstein, D.J., Lange, T., Peters, C.: Wild McEliece. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 143–158. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19574-7_10

[BLP11] Bernstein, D.J., Lange, T., Peters, C.: Wild McEliece incognito. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 244–254. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25405-5_16

[BMvT78] Berlekamp, E., McEliece, R., van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory **24**(3), 384–386 (1978)

[BS08] Biswas, B., Sendrier, N.: McEliece cryptosystem implementation: theory and practice. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 47–62. Springer, Heidelberg (2008). doi:10.1007/978-3-540-88403-3_4

[CB13] Chizhov, I.V., Borodin, M.A.: The failure of McEliece PKC based on Reed-Muller codes. IACR Cryptology ePrint Archive, Report 2013/287 (2013). http://eprint.iacr.org/

[CB14] Chizhov, I.V., Borodin, M.A.: Effective attack on the McEliece cryptosystem based on Reed-Muller codes. Discr. Math. Appl. **24**(5), 273–280 (2014)

[CFS01] Courtois, N.T., Finiasz, M., Sendrier, N.: How to achieve a McEliece-based digital signature scheme. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 157–174. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_10

[CGG+14] Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.-P.: Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Des. Codes Cryptogr. **73**(2), 641–666 (2014)

[CHP12] Cayrel, P.-L., Hoffmann, G., Persichetti, E.: Efficient implementation of a CCA2-secure variant of mceliece using generalized srivastava codes. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 138–155. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30057-8_9

[CMCP14] Couvreur, A., Márquez-Corbella, I., Pellikaan, R.: A polynomial time attack against algebraic geometry code based public key cryptosystems. In: Proceedings of IEEE International Symposium on Information Theory (ISIT 2014), pp. 1446–1450, June 2014

[COT14a] Couvreur, A., Otmani, A., Tillich, J.-P.: New identities relating wild Goppa codes. Finite Fields Appl. **29**, 178–197 (2014)

[COT14b] Couvreur, A., Otmani, A., Tillich, J.-P.: Polynomial time attack on wild McEliece over quadratic extensions. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 17–39. Springer, Heidelberg (2014). doi:10.1007/978-3-642-55220-5_2

[CTS16] Canto Torres, R., Sendrier, N.: Analysis of information set decoding for a sub-linear error weight. In: Takagi, T. (ed.) PQCrypto 2016. LNCS, vol. 9606, pp. 144–161. Springer, Cham (2016). doi:10.1007/978-3-319-29360-8_10

[DCCR13] Dragoi, V., Cayrel, P.-L., Colombier, B., Richmond, T.: Polynomial structures in code-based cryptography. In: Paul, G., Vaudenay, S. (eds.) INDOCRYPT 2013. LNCS, vol. 8250, pp. 286–296. Springer, Cham (2013). doi:10.1007/978-3-319-03515-4_19

[DMN12] Döttling, N., Müller-Quade, J., Nascimento, A.C.A.: IND-CCA secure cryptography based on a variant of the LPN problem. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 485–503. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_30

[DV13] Duc, A., Vaudenay, S.: HELEN: a public-key cryptosystem based on the LPN and the decisional minimal distance problems. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 107–126. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38553-7_6

[FGO+13] Faugère, J.-C., Gauthier, V., Otmani, A., Perret, L., Tillich, J.-P.: A distinguisher for high rate McEliece cryptosystems. IEEE Trans. Inform. Theory **59**(10), 6830–6844 (2013)

[FM08] Faure, C., Minder, L.: Cryptanalysis of the McEliece cryptosystem over hyperelliptic curves. In: Proceedings of the Eleventh International Workshop on Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria, pp. 99–107, June 2008

[FOP+16] Faugère, J.-C., Otmani, A., Perret, L., de Portzamparc, F., Tillich, J.-P.: Folding alternant and Goppa Codes with non-trivial automorphism groups. IEEE Trans. Inform. Theory **62**(1), 184–198 (2016)

[Gab05] Gaborit, P.: Shorter keys for code based cryptography. In: Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005), Bergen, Norway, pp. 81–91, March 2005

[Gab08] Gabidulin, E.M.: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptogr. **48**(2), 171–177 (2008)

[Gal63] Gallager, R.G.: Low Density Parity Check Codes. M.I.T. Press, Cambridge (1963)

[GM13] Gueye, C.T., Mboup, E.H.M.: Secure cryptographic scheme based on modified Reed Muller codes. Int. J. Secur. Appl. **7**(3), 55–64 (2013)

[GMRZ13] Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography (WCC 2013), Bergen, Norway (2013). www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf

[GO01] Gabidulin, E.M., Ourivski, A.V.: Modified GPT PKC with right scrambler. Electron. Notes Discrete Math. **6**, 168–177 (2001)

[Gop70] Goppa, V.D.: A new class of linear correcting codes. Problemy Peredachi Informatsii **6**(3), 24–30 (1970)

[GP13] Gabidulin, E., Pilipchuk, N.: GPT cryptosystem for information network security. In: International Conference on Information Society (i-Society 2013), no. 8, pp. 21–25 (2013)

[GP14] Gabidulin, E., Pilipchuk, N.: Modified GPT cryptosystem for information network security. Int. J. Inf. Secur. Res. **4**(8), 937–946 (2014)

[GPT91] Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their application in cryptology. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 482–489. Springer, Heidelberg (1991). doi:10.1007/3-540-46416-6_41

[GRH09] Gabidulin, E., Rashwan, H., Honary, B.: On improving security of GPT cryptosystems. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 1110–1114. IEEE (2009)

[GRS16] Gaborit, P., Ruatta, O., Schrek, J.: On the complexity of the rank syndrome decoding problem. IEEE Trans. Inf. Theory **62**(2), 1006–1019 (2016)

[GZ16] Gaborit, P., Zémor, G.: On the hardness of the decoding and the minimum distance problems for rank codes. IEEE Trans. Inf. Theory **62**(12), 7245–7252 (2016)

[HMR15] Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J.: Extension of overbeck's attack for gabidulin based cryptosystems. CoRR, abs/1511.01549 (2015)

[HPS98] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). doi:10.1007/BFb0054868

[HSEA14] Hooshmand, R., Koochak Shooshtari, M., Eghlidos, T., Aref, M.R.: Reducing the key length of McEliece cryptosystem using polar codes. In: 2014 11th International ISC Conference on Information Security and Cryptology (ISCISC), pp. 104–108. IEEE (2014)

[HTMR16] Horlemann-Trautmann, A.-L., Marshall, K., Rosenthal, J.: Considerations for rank-based cryptosystems. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 2544–2548. IEEE (2016)

[HvMG13] Heyse, S., von Maurich, I., Güneysu, T.: Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 273–292. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40349-1_16

[ISR60] Solomon, G., Reed, I.S.: Polynomial codes over certain finite fields. J. Soc. Industr. Appl. Math. **8**(2), 300–304 (1960)

[JM96] Janwa, H., Moreno, O.: McEliece public key cryptosystems using algebraic-geometric codes. Des. Codes Cryptogr. **8**(3), 293–307 (1996)

[KKM+17] Kudekar, S., Kumar, S., Mondelli, M., Pfister, H.D., Sasoglu, E., Urbanke, R.: Reed-muller codes achieve capacity on erasure channels. IEEE Trans. Inf. Theory **PP**(99), 1 (2017)

[KMP14] Kiltz, E., Masny, D., Pietrzak, K.: Simple chosen-ciphertext security from low-noise LPN. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 1–18. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54631-0_1

[LDW94] Li, Y.X., Deng, R.H., Wang, X.M.: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans. Inform. Theory **40**(1), 271–273 (1994)

[LJ12] Löndahl, C., Johansson, T.: A new version of McEliece PKC based on convolutional codes. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 461–470. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34129-8_45

[Loi10] Loidreau, P.: Designing a rank metric based McEliece cryptosystem. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 142–152. Springer, Heidelberg (2010). doi:10.1007/978-3-642-12929-2_11

[LS01] Loidreau, P., Sendrier, N.: Weak keys in the McEliece public-key cryptosystem. IEEE Trans. Inform. Theory **47**(3), 1207–1211 (2001)

[LT13] Landais, G., Tillich, J.-P.: An efficient attack of a McEliece cryptosystem variant based on convolutional codes. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 102–117. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38616-9_7

[Mac99] MacKay, D.J.C.: Good error-correcting codes based on very sparse matrices. IEEE Trans. Inf. Theory **45**(2), 399–431 (1999)

[MB09] Misoczki, R., Barreto, P.S.L.M.: Compact McEliece keys from goppa codes. In: Jacobson, M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 376–392. Springer, Heidelberg (2009). doi:10.1007/978-3-642-05445-7_24

[McE78] McEliece, R.J.: A public-key system based on algebraic coding theory, pp. 114–116. Jet Propulsion Lab, DSN Progress Report 44 (1978)

[MCT16] Márquez-Corbella, I., Tillich, J.-P.: Using Reed-Solomon codes in the $(u|u+v)$ construction and an application to cryptography. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 930–934 (2016). arXiv:1601:08227

[Mit51] Mitani, N.: On the transmission of numbers in a sequential computer. National Convention of the Institute of Electrical Communication Engineers of Japan, November 1951

[MOG15] Maurich, I.V., Oder, T., Güneysu, T.: Implementing QC-MDPC McEliece encryption. ACM Trans. Embed. Comput. Syst. **14**(3), 44:1–44:27 (2015)

[MRAS00] Monico, C., Rosenthal, J., Shokrollahi, A.A.: Using low density parity check codes in the McEliece cryptosystem. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Sorrento, Italy, p. 215 (2000)

[MS86] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, 5th edn. North-Holland, Amsterdam (1986)

[MS07] Minder, L., Shokrollahi, A.: Cryptanalysis of the sidelnikov cryptosystem. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 347–360. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72540-4_20

[MTSB13] Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P.S.L.M.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 2069–2073 (2013)

[Mul54] Muller, D.E.: Application of boolean algebra to switching circuit design, to error detection. Trans. I.R.E. Prof. Group Electron. Comput. **EC-3**(3), 6–12 (1954)

[Nie86] Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Probl. Control Inf. Theory **15**(2), 159–166 (1986)

[OB09] Ouzan, S., Be'ery, Y.: Moderate-density parity-check codes. arXiv preprint (2009). arXiv:0911.3262

[OTD08] Otmani, A., Tillich, J.-P., Dallot, L.: Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes. In: Proceedings of First International Conference on Symbolic Computation and Cryptography, Beijing, China, 28–30 April 2008, pp. 69–81. LMIB Beihang University (2008)

[OTK15] Otmani, A., Kalachi, H.T.: Square code attack on a modified sidelnikov cryptosystem. In: El Hajji, S., Nitaj, A., Carlet, C., Souidi, E.M. (eds.) C2SI 2015. LNCS, vol. 9084, pp. 173–183. Springer, Cham (2015). doi:10.1007/978-3-319-18681-8_14

[OTKN16] Otmani, A., Talé-Kalachi, H., Ndjeya, S.: Improved cryptanalysis of rank metric schemes based on Gabidulin codes. CoRR, abs/1602.08549 (2016)

[Ove08] Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptol. **21**(2), 280–301 (2008)

[Per12] Persichetti, E.: Compact McEliece keys based on quasi-dyadic Srivastava codes. J. Math. Cryptol. **6**(2), 149–169 (2012)

[PR97] Petrank, E., Roth, R.: Is code equivalence easy to decide? IEEE Trans. Inform. Theory **43**(5), 1602–1604 (1997)

[Ree54] Reed, I.S.: A class of multiple-error-correcting codes and the decoding scheme. IRE Trans. IT **4**, 38–49 (1954)

[RGH10] Rashwan, H., Gabidulin, E., Honary, B.: A smart approach for GPT cryptosystem based on rank codes. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 2463–2467. IEEE (2010)

[RGH11] Rashwan, H., Gabidulin, E., Honary, B.: Security of the GPT cryptosystem and its applications to cryptography. Secur. Commun. Netw. **4**(8), 937–946 (2011)

[RSA78] Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)

[Sen94] Sendrier, N.: On the structure of a randomly permuted concatenated code. In: EUROCODE 1994, pp. 169–173 (1994)

[Sen98] Sendrier, N.: On the concatenated structure of a linear code. Appl. Algebra Eng. Commun. Comput. (AAECC) **9**(3), 221–242 (1998)

[Sen00] Sendrier, N.: Finding the permutation between equivalent linear codes: the support splitting algorithm. IEEE Trans. Inf. Theory **46**(4), 1193–1203 (2000)

[Sha48] Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)

[Sho94] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Goldwasser, S. (ed.) FOCS, pp. 124–134 (1994)

[Sid94] Sidelnikov, V.M.: A public-key cryptosytem based on Reed-Muller codes. Discr. Math. Appl. **4**(3), 191–207 (1994)

[SK14] Shrestha, S.R., Kim, Y.-S.: 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), pp. 368–372. IEEE (2014)

[SS92] Sidelnikov, V.M., Shestakov, S.O.: On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discr. Math. Appl. **1**(4), 439–444 (1992)

[SS96] Sipser, M., Spielman, D.A.: Expander codes. IEEE Trans. Inf. Theory **42**, 1710–1722 (1996)

[SSMS09] Shoufan, A., Strenzke, F., Molter, H.G., Stöttinger, M.: A timing attack against patterson algorithm in the McEliece PKC. In: Lee, D., Hong, S. (eds.) ICISC 2009. LNCS, vol. 5984, pp. 161–175. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14423-3_12

[STM+08] Strenzke, F., Tews, E., Molter, H.G., Overbeck, R., Shoufan, A.: Side channels in the McEliece PKC. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 216–229. Springer, Heidelberg (2008). doi:10.1007/978-3-540-88403-3_15

[Str10a] Strenzke, F.: A timing attack against the secret permutation in the McEliece PKC. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS, vol. 6061, pp. 95–107. Springer, Heidelberg (2010). doi:10.1007/978-3-642-12929-2_8

[Str10b] Strenzke, F.: A smart card implementation of the McEliece PKC. In: Samarati, P., Tunstall, M., Posegga, J., Markantonakis, K., Sauveron, D. (eds.) WISTP 2010. LNCS, vol. 6033, pp. 47–59. Springer, Heidelberg (2010). doi:10.1007/978-3-642-12368-9_4

[Str13] Strenzke, F.: Timing attacks against the syndrome inversion in code-based cryptosystems. In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, vol. 7932, pp. 217–230. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38616-9_15

[UG14] Urivskiy, A., Gabidulin, E.: On the equivalence of different variants of the GPT cryptosystem, no. 3, pp. 95–97. IEEE (2014)

[Wan16] Wang, Y.: Quantum resistant random linear code based public key encryption scheme rlce. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 2519–2523. IEEE (2016)

[Wie06a] Wieschebrink, C.: An attack on a modified niederreiter encryption scheme. In: Yung, M., Dodis, Y., Kiayias, A., Malkin, T. (eds.) PKC 2006. LNCS, vol. 3958, pp. 14–26. Springer, Heidelberg (2006). doi:10.1007/11745853_2

[Wie06b] Wieschebrink, C.: Two NP-complete problems in coding theory with an application in code based cryptography. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), pp. 1733–1737 (2006)

[Wie09] Wieschebrink, C.: Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. IACR Cryptology ePrint Archive, Report 2009/452 (2009)