# Low Rank Parity Check codes and their application to cryptography

Philippe Gaborit[1], Gaetan Murat[1], Olivier Ruatta[1] and Gilles Zémor[2]

[1] Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas
87060 Limoges Cedex, France.
gaborit,murat,ruatta@unilim.fr
[2] Université Bordeaux I, A2X,
351 cours de la Libération
33400 Talence Cedex, France.
gilles.zemor@math.u-bordeaux.fr

**Abstract.** In this paper we introduce a new family of rank metric codes: the Low Rank Parity Check codes for which we propose an efficient probabilistic decoding algorithm. This family of codes can be seen as the equivalent of classical LDPC codes for the rank metric. We then propose to use these codes for cryptography in the McEliece encryption setting. At the difference of previous encryption algorithms based on rank metric -especially based on Gabidulin codes -, the codes we use have a very poor structure. Our cryptosystem can be seen as an equivalent to the NTRU cryptosystem [15] (and also to the more recent MDPC[22] cryptosystem) in a rank metric context. Overall our system permits to achieve a very low public key of 1517 bits for a security of $2^{80}$, moreover our system is very fast with a complexity of decryption of order $2^{17}$ operations in the base field, and with a decryption failure which can be made arbitrarily small.

**Keys words: Public key cryptosystem, rank metric**

## 1 Introduction

The rank metric was introduced by Gabidulin in 1985 in [8], along with the Gabidulin codes which are an equivalent of the Reed-Solomon codes for the rank metric. Since then, rank metric codes have been used in many applications: for coding theory and space-time codes and also for cryptography. Until now the main tool for rank based cryptography was based on masking the Gabidulin codes [10] in different ways and using the McEliece (or Niederreiter) setting with these codes. Meanwhile most of the systems were broken by using structural attacks which used the particular structure of the Gabidulin codes ([26], [6], [2], [18],[9]). A similar situation exists in the Hamming case for which all cryptosystems based on the Reed-Solomon have been broken for the same reason: the Reed-Solomon are so structured that their structure is difficult to mask and there is always structural information leaking.

Since the introduction of code-based cryptography by McEliece in 1978, the different cryptosystems, proposed in the Hamming distance setting, were based on masking a special family of decodable codes, like Goppa, Reed-Muller of Reed-Solomon codes. The strong structure of these codes usually implies a large size of public key. Now in 1996 and 1997, two lattice-based cryptosystems were proposed independently: the NTRU [15] and the GGH [14] cryptosystems which can be seen as a cryptosystems in a McEliece setting but for the Euclidean distance. Notice that lattice based cryptography is no more than code-based cryptography with q-ary codes but with the Euclidean distance rather than the Hamming distance. Both NTRU and GGH cryptosystems are based on the same idea: knowing a *random* basis of small weight vectors permits to obtain an efficient decoding algorithm suitable for cryptography. Moreover the NTRU cryptosysem (which can be seen as an optimized case of the GGH cryptosystem [20]) introduced for the first time the idea to use double-circulant matrices in order to decrease the size of the public key, this idea was made possible because of the randomness of the small dual basis. At last we remark that for 15 years the NTRU cryptosystem has

not been really attacked on its double-circulant structure, indeed the best attacks still remain general LLL attacks on lattice.

In a classical cryptographic Hamming context, the first author [11] introduced in 2005 the idea to use quasi-cyclic codes to decrease the size of the public, meanwhile the idea to add a quasi-cyclic structure on an already structured family of codes introduces too much structure and the system was broken [24]. This idea was then used with other families of quasi-cyclic (or quasi-dyadic) structured codes like Goppa quasi-dyadic [21] or quasi-cyclic alternant codes [1], these systems lead to much smaller keys, but eventually they were attacked in [5] and even though the idea remains valid, the cryptanalysis of [5] showed that this the idea of quasi-cyclic or quasi-dyadic structured codes could not lead to secure public key of a few thousand bits, but rather to secure keys of a few tenth thousand bits.

More recently new proposal were made in the spirit of the original NTRU schems with Hamming distance, first by the the use of quasi-cyclic LDPC codes, then with MDPC codes in [22]. The last family of codes permits to obtain the same type of feature than the NTRU cryptosystem: a very compact key (of 4800b) and a security based on decoding by a random dual matrix with small weight.

**Our contribution** In this paper we built anew on the NTRU setting but in a rank metric context. We introduce the Low Rank Parity Check codes (an equivalent of the LDPC codes for Hamming distance) for which we propose an efficient probabilistic decoding algorithm. We then use these codes in a quasi-cyclic form and obtain a cryptosystem with public key three times smaller than the MDPC codes (1517 bits), moreover our system is more than 100 times faster than [22] (in term of number of operations).

The paper is organized as follows: Section 2 gives background on rank metric codes and cryptography, Section 3 consider results on subspaces, Section 4 defines the LRPC codes, Section 5 gives a decoding algorithm and at last Secction 6 and 7 consider the cryptographic application of these codes.

## 2 Background on rank metric codes and cryptography

### 2.1 Definitions and notation

**Notation :**
Let $q$ be a power of a prime $p$, $m$ an integer and let $V_n$ be a $n$ dimensional vector space over the finite field $\mathrm{GF}(q^m) = F_{q^m}$. Let $\beta = (\beta_1, \ldots, \beta_m)$ be a basis of $F_{q^m}$ over $F_q$.
Let $\mathcal{F}_i$ be the map from $F_{q^m}$ to $F_q$ where $\mathcal{F}_i(x)$ is the $i$-th coordinate of $x$ in the basis $\beta$.
To any $v = (v_1, \ldots, v_n)$ in $V_n$ we associate the matrix $\overline{v} \in \mathcal{M}_{m,n}(F_q)$ in which $\overline{v}_{i,j} = \mathcal{F}_i(v_j)$.
The rank weight of a vector $v$ can be defined as the rank of the associated matrix $\overline{v}$. If we name this value $\mathrm{rank}(v)$ we can have a distance between two vectors $x, y$ using the formula $\mathrm{rd}(x, y) = \mathrm{rank}(x - y)$. We refer to [19] for more details on codes for the rank distance.

A rank code $C$ of length $n$ and dimension $k$ over $F_{q^m}$ is a subspace of dimension $k$ of $F_{q^m}$ embedded with its rank metric. The minimum rank distance of the code $C$ is the minimum rank of non-zero vectors of the code.

**Definition 1.** *Let $x = (x_1, x_2, \cdots, x_n) \in F_{q^m}^n$ be a vector of rank $r$. We denote $E$ the $F_q$-sub vector space of $F_{q^m}$ generated by $x_1, x_2, \cdots, x_n$. The vector space $E$ is called the* **support** *of $x$.*

*Remark 1.* The notion of support of a code word for Hamming distance and the one introduced in definition 1 are different even if they share a common principle. Indeed, in both case, giving a low weight syndrome associated to $x$, once the support is known one only have to solve a linear system in both case.

*Remark 2.* For any code, the action of the general linear group does not change the weight of the words. In the case a rank metric code, this action does not change the supports of the word also. Also an interesting remark is that in

the case of Hamming distance over $F_q$ increasing the value of $q$ permits to increase the minimum distance of a code but does not change the type of support (it is always a binomial coefficient with the same length) when for rank metric increasing the base field $F_q$ increases in a strong the size of the support (ie: the number of bases which can be found by the Gaussian binomial).

**Notation 1** *In the text below, $\mathcal{C}$ is a rank metric code of length $n$ and dimension $k$ over $F_{q^m}$. The matrix $G$ denotes a $k \times n$ generator matrix of $\mathcal{C}$ and $H$ one of its parity check matrix.*

### 2.2 Cryptography and rank codes

The main problem used for rank codes in the cryptographic context is the generalization of the classical syndrome decoding problem with Hamming distance in the case of rank metric:

**Syndrome decoding problem for the rank distance(RSD)** Let $H$ be a $((n-k) \times n)$ matrix over $F_{q^m}$ with $k \leq n$, $i \in F_{q^m}^k$ and $r$ an integer. The problem is to find $s$ such that $\text{rank}(s) = r$ and $Hs^t = i$.

In that case it is not proven that the problem is NP-hard, but this problem is very close to the syndrome decoding problem which is NP-hard, moreover the problem can be seen as a structured version of the MinRank problem which is also NP-hard (the RSD problem can be attacked as a MinRank problem but in practice the attack do not work since there are too many unknowns [4]). Moreover the problem has been studied for more than 20 years and the best attacks are exponential, so that the problem is generally believed to be hard.

The first non-trivial attack on the problem was proposed by Chabaud and Stern [3] in 1996, then in 2002 Ourivski and Johannson [25] improved the previous attack and proposed a new attack, meanwhile these two attacks did not take account of the value of $m$ in the exponent. Very recently the two previous attacks were generalized in [13] (and used to break some reparations of the GPT cryposystems) moreover an algebraic new setting was also proposed.

The new complexity for the best known attacks are now in our context: $(n-k)^3 m^3 q^{(r-1)\lfloor \frac{(k+1)m}{n} \rfloor})$ for the generalization of previous attacks including $m$ in the exponential factor and $q^{r\lceil \frac{r(k+1)-(n+1)}{r} \rceil})$ a lower bound for the hybrid attack using Groebner basis of [13]. Notice that there are other possible attacks with Groebner basis (Kipnis-Shamir or attacks by minors) but they are not relevant in our context (see [13] for more details), except the attacks of [17] which can be more efficient than [13] in the case where $q$ is high.

## 3 Some results on the product of two subspaces

Before introducing the LRPC codes we need to introduce some results on the product of two subspaces, we only cite the main result here, all the proofs are presented in the appendix:

**Definition 2.** *Let $A$ and $B$ be two $F_q$-subspaces of $F_{q^m}$ of dimensions $\alpha$ and $\beta$, generated respectively by $\{A_1, \cdots, A_\alpha\}$ and $\{B_1, \cdots, B_\beta\}$ all $A_i$ and $B_j$ in $F_{q^m}$, we denote by $\langle A.B \rangle$ the product space generated by the set $\{a.b, a \in A, b \in B\}$.*

The product space $\langle A.B \rangle$ is obviously generated by the set $\{A_1.B_1, \cdots, A_1.B_\beta, \cdots, A_\alpha.B_1, \cdots, A_\alpha.B_\beta\}$ and its dimension is bounded above by $\alpha\beta$.

A question of interest in our case is the probability that the dimension is not maximal when $\alpha$ and $\beta$ are relatively small. We suppose $\alpha\beta < m$ and we investigate the typical dimension of the product subspace $\langle AB \rangle$.

Let $A$ and $B$ be random $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^m$ of dimensions $\alpha$ and $\beta$ respectively. We suppose $\alpha\beta < m$ and we investigate the typical dimension of the subspace $\langle AB \rangle$.

We rely on the following observation:

**Lemma 1.** *Let $A'$ and $B$ be two subspaces of $\mathbb{F}_q^m$ of dimensions $\alpha'$ and $\beta$ such that $\dim\langle A'B\rangle = \alpha'\beta$. Let $A = A' + \langle a\rangle$ where $a$ is a uniformly chosen random element of $\mathbb{F}_q^m$. Then*

$$\mathbb{P}\left(\dim\langle AB\rangle < \alpha'\beta + \beta\right) \leq \frac{q^{\alpha'\beta+\beta}}{q^m}.$$

**Proposition 1.** *Let $B$ be a fixed subspace and suppose we construct a random subspace $A$ by choosing $\alpha$ independent (in the sense of probability) random vectors of $\mathbb{F}_q^m$ and letting $A$ be the subspace generated by these $\alpha$ random vectors. We have that $\dim\langle AB\rangle = \alpha\beta$ with probability at least $1 - \alpha\frac{q^{\alpha\beta}}{q^m}$.*

Let $B$ be a fixed subspace of $\mathbb{F}_q^m$ containing 1 and let $\langle B^2\rangle$ be the subspace generated by all products of elements of $B$. Let $\beta_2 = \dim\langle B^2\rangle$. Let $A$ be a random subspace of $\mathbb{F}_q^m$ of dimension $\alpha$. By the Proposition we have that $\dim\langle AB^2\rangle = \alpha\beta_2$ with probability at least $1 - \alpha\frac{q^{\alpha\beta_2}}{q^m}$. **Remark:** we have $\beta_2 \leq \beta(\beta+1)/2$.

**Lemma 2.** *Suppose $\dim\langle AB^2\rangle = \alpha\beta_2$. Let $e \in \langle AB\rangle$ with $e \notin A$. Suppose $eB \subset \langle AB\rangle$. Then there exists $x \in B$, $x \notin \mathbb{F}_q$, such that $xB \subset B$.*

**Proposition 2.** *Suppose $m$ is prime. Let $A$ and $B$ be random subspaces of dimensions $\alpha$ and $\beta$ respectively. Let $(b_i)$ be a basis of $B$ and let $S = \langle AB\rangle$. Then with probability at least $1 - \alpha\frac{q^{\alpha\beta(\beta+1)/2}}{q^m}$ we have that $\bigcap_i b_i^{-1}S = A$.*

**Proposition 3.** *Let $B$ be a subspace of dimension $\beta$ containing 1 such that $\dim B + Bb^{-1} = 2\beta - 1$ for some $b \in B$. Let $A$ be a randomly chosen subspace of dimension $\alpha$. With probability at least $1 - \alpha\frac{q^{\alpha(2\beta-1)}}{q^m}$ we have that $\langle AB\rangle \cap \langle AB\rangle b^{-1} = A$*

*Remark 3.* It is interesting to remark that in practice the probability for which an upper bound is given in Proposition 2 and 3, decreases much more faster to 0. Indeed when the degree of the extension $m$ increases by one (for $m$ greater than $rd$), the probability that $\bigcap_i b_i^{-1}S \neq A$ is divided by a factor at least $q^{r-1}$. This means that in practice the previous upper bound is rather bad, and that one can consider that as soon as $m$ is greater than $rd$ by 8 or more (and increasing) the probability is far below $2^{-30}$. It will be the case when one will choose parmaters in the last section.

## 4 Low Rank Parity Check Codes

The idea of these codes is to generalize the classical LDPC codes approach for Hamming distance to the rank metric. There is a natural analogy between low density matrices and matrices with low rank.

**Definition 3.** *A Low Rank Parity Check (LRPC) code of rank $d$, length $n$ and dimension $k$ over $F_{q^m}$ is a code such that the code has a parity check $(n-k)\times n$ matrix such that the sub-vector space of $F_{q^m}$ generated by its coefficients $h_{ij}$ is at dimension at most $d$. We call this dimension the weight of $H$. Denoting $F$ the sub-vector space of $F_{q^m}$ generated by the coefficients $h_{ij}$ of $H$, we denote $F_1, F_2, \cdots, F_d$ one of its basis.*

In practice it means that for any $1 \leq i \leq k, 1 \leq j \leq n$, there exist $h_{ijk} \in F_q$ such that $h_{ij} = \sum_{k=1}^{d} h_{ijk}F_k$. One can also define a special sub-class of LRPC codes:

**Definition 4.** *A Quasi-Cyclic Low Rank Parity Check (QC-LRPC) code of rank $d$, is a quasi-cyclic code such that the code has a parity check quasi-cyclic $H$ of low weight $d$.*

**Remark:** Of particular interest is the case of double circulant LRPC codes (DC-LRPC) of rank $d$, which are codes with parity check matrix $H$, a double-circulant matrix (concatenation of two cyclic matrices) of weight $d$.

In the following we will also be interested by a special matrix $A_H^r$ which permits to decode the LRPC codes in a very efficient way.

**Definition 5.** *Let $H := (h_{ij})$ be a parity check matrix $(n-k) \times n$ of low weight $d$ over $\mathbb{F}_{q^m}$, such that all $h_{ij}$ belong to $F = \{F_1, \ldots, F_d\}$, then for all $1 \leq i \leq n-k, 1 \leq j \leq n$, $h_{ij} = \sum_{k=1}^{d} h_{ijk} F_k$, for $h_{ijk} \in F_q$. Assume that we have an error of low rank, say $r$, such that there is a basis $E_1, .., E_r$ of the sub-vector space of $F_{q^m}$ where the coefficients of the error lie. We will construct a matrix $A_H^r$ depending on $F$ and $r$ but not directly of a special basis of the error space. In fact, the following construction can be viewed as unfolding over $F_q$ the matrix $H$ on a "symbolic" basis of the product of the space $F$ and the space $E$ of the coefficient of the error . The considered matrix is a $nr \times (n-k)rd$ matrix $A_H^r = (a_{ij})$ by setting all $a_{ij} = 0$ and then write:*

$$a_{wr+v+1+urd, j+vn} = h_{ljw},$$

$$\text{for } 0 \leq u \leq n-k-1,\ 0 \leq v \leq r-1,\ 1 \leq j \leq n \text{ and } 0 \leq w \leq d-1.$$

The matrix $A_H^r$ corresponds to a formal rewriting of the system $H.e^t = s$, where $e = (e_1, \ldots, e_n)$ with $e_i \in E =< E_1, \ldots, E_r >$ and $e_i = \sum_{i=1}^{n} e_{ij} E_j$. Notice that the matrix $A_H^r$ does not depend on the subspace $F$ since all is written symbolically.

All $s_i$ can be written in the formal basis $\{F_1E_1, F_1E_2, ..., F_1E_r, F_2E_1, ..., F_dE_r\}$ over $F_q$. Then the matrix $A_H^r$ is such that:

$$A_H^r.(e_{11}, e_{21}, ..., e_{n1}, e_{12}, e_{22}, ..., e_{n2}, ..., e_{r1}, ..., e_{rn})^t = (s_1, ..., s_{n-k})^t$$

where each $s_i$ is written in the formal product basis $\{F_1E_1, F_1E_2, ..., F_1E_r, F_2E_1, ..., F_dE_r\}$ with the same order of coordinates (and therefore $(s_1, ..., s_{n-k})$ is considered as a vector in $F_q$ of length $(n-k).rd$.

For instance, the first row of $A_H^r$ consists on the impact of the error vector $e$ on the first row of $H(h_{11}, \ldots, h_{1n})$ on the symbolic basis element $F_1E_1$. Since the $e_{ij}$ are ordered in the previous given order, the first row of $A_H^r$ only deals with the projection of $h_{1j}$ on the basis element $F_1$, therefore the $h_{1j1} (\in F_q)$. Now since one considers for the first row of $A_H^r$ the impact on $F_1E_1$, the first n coordinates $a_{1j}$ of the first row of $A_H^r$ are $a_{1j} = h_{1j1}$ for $1 \leq j \leq n$ and the remaining coordinates are $a_{1j} = 0$ for $n+1 \leq j \leq nr$, since they involve $E_2, E_3, \ldots$.

Now if one takes random values of coordinates for low rank $H$, it is easy to find matrices $A_H^r$ of maximal rank $nr$.

**Definition 6.** *In the following we denote by $A_H$ a $nr \times nr$ invertible submatrix of $A_H^r$, and we denote by $D_H = A_H^{-1}$ a decoding matrix of $H$.*

**Remark** The matrix $D_H$ permits to recover directly the $nr$ values $e_{ij}$ from $nr$ positions of the $s_i$ written in product basis by a simple multiplication.

## 5 Decoding algorithm for LRPC codes

### 5.1 General idea

The general idea of the algorithm is to use the fact that the weight of the parity check matrix is small, the idea is that the space generated by the coordinates of syndrome $< s_1, \ldots, s_{n_k} >$ permits to recover the whole product space $P =< E.F >$ of the support of the error and of the known small basis of $H$. Knowing the *whole* space $P$ and the space $F$ permits to recover $E$. Then , knowing the support $E$ of the error $e$, it is easy to recover the exact value of each coordinate by solving a linear system. This approach is very similar to the classical decoding procedure of BCH codes for instance, where one recovers the error-locator polynomial, which gives the support of the error , and then the value of the error coordinates.

### 5.2 A general decoding algorithm

Consider a $[n,k]$ LRPC code $C$ of low weight $d$ over $F_{q^m}$, with generator matrix $G$ and dual $(n-k)\times n$ matrix $H$, such that all the coordinates $h_{ij}$ of $H$ belong to a space $F$ of rank $d$ with basis $\{F_1,\cdots,F_d\}$ and suppose that as in the previous section $H$ is chosen such that there exists an invertible associated decoding matrix $D_H$.

Suppose the received word to be $y=xG+e$ for $x$ and $e$ in $(F_{q^m})^n$, and where $e(e_1,\cdots,e_n)$ is the error vector of rank $r$, which means that for any $1\leq i\leq n$, $e_i\in E$, a vector space of dimension $r$ with basis (say) $\{E_1,\ldots,E_r\}$.

We have the following general decoding algorithm, this algorithm has a probability of failure that we will consider in the next subsection, we give general parameters at the end of the section for which the algorithm works.

1. **Syndrome space computation**
   Compute the syndrome vector $H.y^t=s(s_1,\cdots,s_{n-k})$ and the syndrome space $S=<s_1,\cdots,s_{n-k}>$.
2. **Recovering the support $E$ of the error**
   Define $S_i=F_i^{-1}S$, the subspace where all generators of $S$ are multiplied by $F_i^{-1}$. Compute the support of the error $E=S_1\cap S_2\cap\cdots\cap S_d$, and compute a basis $\{E_1,E_2,\cdots,E_r\}$ of $E$.
3. **Recovering the error vector $e$**
   Write $e_i(1\leq i\leq n)$ in the error support as $e_i=\sum_{i=1}^{n}e_{ij}E_j$, solve the system $H.e^t=s$, where the equations $H.e^t$ and the syndrome coordinates $s_i$ are written as elements of the product space $P=<E.F>$ in the basis $\{F_1E_1,\cdots,F_1E_r,\cdots,F_dE_1,\cdots,F_dE_r\}$. The system has $nr$ unknowns (the $e_{ij}$) in $F_q$ and $(n-k).rd$ equations from the syndrome.
4. **Recovering the message $x$**
   Recover $x$ from the system $xG=y-e$.

**Fig. 1.** Algorithm 1:a general decoding algorithm for LRPC codes

### 5.3 Correctness of the algorithm

We prove the correctness of the algorithm in the ideal case when dimension$(<E.F>)=rd, dimension(S)=rd$ and dimension $(S_1\cap S_2\cap\cdots\cap S_d)=r$, we will see in the next subsection that this is the general case.

**step 1**:The first step of the algorithm is obvious.

**step 2**:now we want to prove that $E\subset S_1\cap S_2\cap\cdots\cap S_d$. We defined $S_i=F_i^{-1}S=\{F_i^{-1}x, x\in S\}$, now since by hypothesis $S$ is *exactly* the product space $E.F=\{a.b|a\in E,b\in F\}$, we have $F_i.E_j\in S,\forall 1\leq j\leq r$, hence $E_j\in S_i$, and therefore $E\subset S_i$, and hence $E$ is contained in $S_1\cap S_2\cap\cdots\cap S_d$, now by hypothesis dimension$(S_1\cap S_2\cap\cdots\cap S_d)$=dimension(E) and hence $E=S_1\cap S_2\cap\cdots\cap S_d$.

**step 3**: once the support $E$ of the error of $x$ is known, one can write $x=\sum_{1\leq i\leq n,1\leq j\leq r}e_{ij}E_j$, for $e_{ij}\in F_q$ and solve the linear system $H.x^t=s$ in the $nr$ unknown $e_{ij}$. The system has $nr$ unknown in $F_q$ and $(n-k).m$ equations in $F_q$ coming from the $n-k$ syndrome equations in $F_{q^m}$. The parameter $r$ is chosen such that $r\geq\frac{(n-k)m}{n}$. Notice moreover that one can consider the product space $<E.F>$ for a formal $F$ so that in that case the system equations are uniquely related to the matrix $H$. Hence $H$ can be chosen such that a decoding matrix $D_H$ exists and permits to solve the system by a simple multiplication by $D_H$ of the set of $s_i$ written in the product space basis.

### 5.4 Probability of failure

We now consider the different possibility of failure, there three cases to consider. The case dimension($< E.F >$) $= rd$ corresponds to Prop. 1 of Section 3, the case $E = S_1 \cap S_2 \cap \cdots \cap S_d$ corresponds to Prop. 2 of the same section. In both cases the probability can be made exponentially small depending on parameters, especially when in practice the upper bound given are really large compared to experimental results.

The last case is the case $dimension(S) = rd$. We have the following easy proposition:

**Proposition 4.** *The probability that the $n-k$ syndromes does not generate the product space $P =< E.F >$ is less than $q^{1+(n-k)-rd}$.*

*Proof.* By construction all $s_i$ belong to the product space $P$ and since the error is taken randomly the $s_i$ can be seen as random elements of $P$, now if one considers a set of $(n-k)$ random elements of space of dimension $rd$ (with $n-k \geq rd$) the probability that this set does not generate the whole space is roughly given by $q^{-(1+(n-k)-rd)}$ - the probability that a random $[rd, n-k] = [rd, rd+(n-k)-rd]$ matrix over $F_q$ not be invertible.

Therefore the previous discussion shows that depending on the parameters the probability of failure of the previous algorithm can be made arbitrarily small and that the main probability we have to consider in fact is the probability given by Proposition 4, which is not an upper bound but what happens in practice.

### 5.5 Complexity of decoding

The most costly step of the algorithm are step 2) et step 3). The cost of step 2) is the cost of the intersection of vector spaces which has cost $4r^2d^2m$ operations in the base field (this operation can also be done in a very elegant way with $q$-polynomials [23]). Now the cost of step 3) is the cost of solving the system $H.e^t = s$ when the support $E$ of the error is known, if one proceeds naively there are $nr$ unknowns (the $e_{ij}$) and the cost of matrix inversion in $n^3r^3$, now one can use the formal decoding matrix $D_H$ of the previous section and simply recover the $(e_{ij})$ by multiplying by $D_H$ the $nr$ positions (written in the product basis of $\langle E.F \rangle$) of $s_1, .., s_{n-k}$ associated to the matrix $D_H$ of definition 6. Therefore the cost of the inversion becomes only the cost of a matrix multiplication: $n^2r^2$. Remark that the matrix $D_H$ can be precomputed and stocked or even reconstructed column by column from random hash values - in that case one fixes $D_H$ and one derives $H$.

### 5.6 A general theorem

If we sum up the results of the different subsection one obtains the following general theorem:

**Theorem 1.** *Let $H$ be a $(n-k) \times n$ dual matrix of a LRPC codes with low rank $d \geq 2$ over $F_{q^m}$, then algorithm 1 decodes a random error $e$ of low rank $r$ such that $rd \leq n-k$, with failure probability $q^{-(n-k+1-rd)}$ and complexity $r^2(4d^2m + n^2)$.*

*Proof.* This theorem is a direct result from previous subsection.

*Remark 4.* In term of pure decoding capacity the LRPC codes are less intersting than Gabidulin codes, since they hardly decode up to $(n-k)/2$ and moreover the algorithm is probabilistic, but they are perfectlu fitted for cryptography.

## 6 Application to cryptography: the LRPC cryptosystem

In the following we propose a new cryptosystem in the spirit of NTRU and the more recent MDPC system.

### 6.1 The LRPC cryptosystem

For our new cryptosystem we use the McEliece cryptographic setting, the Niederreiter setting could also be used but less semantic security is known for this setting.

Let us consider $C$ a LRPC code with a $(n-k) \times n$ parity check matrix $H$. We consider $H$ to be either a LRPC codes or double circulant LRPC codes (DC-LRPC) $\frac{n}{2} \times n$ of rank $d$, such that the code corrects error of rank $r$. We hide the matrix $H$ with a random invertible matrix $R$, in the case of double circulant codes the matrix $S$ is random circulant $\frac{n}{2} \times \frac{n}{2}$. Figure 2 presents the LRPC cryptosytem.

1. **Key creation** Choose a random LRPC code over $F_{q^m}$ of low rank $d$ with support $F$ and parity check $(n-k) \times n$ matrix $H$, generator matrix $G$ and decoding matrix $D_H$ which correct errors of rank $r$ (as in previous section). And a random invertible $(n-k) \times (n-k)$ matrix $R$
   • **Secret key**: the low rank matrix $H$, the masking matrix $R$
   • **Public key**: the matrix $G' = RG$
2. **Encryption**
   Translate the information vector $M$ into a word $x$, choose a random error $e$ of rank $r$ on $F_{q^m}$. The encryption of $M$ is $c = xG' + e$.
3. **Decryption**
   Compute syndrome $s = H.c^t$ and recover the error vector $e$ then $xR$ and $x$.

**Fig. 2.** The LRPC cryptosystem

*Remark 5.* The cryptosystem can be adpated in the case of DC-LRPC codes, in that case the matrix $G'$ can be written $G' = (A^{-1}B^t|I)$ were $A$ and $B$ are two circulant matrices of low rank $d$ for the same space $F$.

• General parameters of the LRPC cryptosystem:

1. Size of public key (bits): LRPC: $(n-k)(n-k)mLog(q)$ / DC-LRPC: $\frac{nm}{2}Log(q)$
2. Size of secret key (bits): a random vector can used to recover the different parameters
3. Size of message: LRPC: $(n-k)mLog(q)$ / DC-LRPC: $\frac{nm}{2}Log(q)$
4. Encryption rate: LRPC: $\frac{r(m+n)}{(n-k)m}$ / DC-LRPC: $\frac{2r(m+n)}{nm}$
5. Complexity of encryption: LRPC:(n-k)(n-k)mr op. in $F_q$ / DC-LRPC:$\frac{n^2mr}{4}$ op. in $F_q$
6. Complexity of decryption: $r^2(n^2+4d^2m)$ op. in $F_q$
7. Complexity of the best usual attack: Support attack: $O((n-k)^3m^3q^{(r-1)\lfloor\frac{(k+1)m}{n}\rfloor})$ / algebraic attacks (Grobner basis) - lower bound: $q^{r\lceil\frac{r(k+1)-(n+1)}{r}\rceil}$) and heuristic results of [17]

*Remark 6.* in the case of DC-LRPC , since the matrix is double-circulant the complexity of encryption can be optimized.

*Remark 7.* We choose to present a McEliece setting, in that case the size of the message is greater than for the Niederreiter setting but more can be proven for semantic security.

We made a non-optimized implementation in Magma which confirmed our results.

## 7 Security of the LRPC cryptosystem

### 7.1 Semantic security

The problem on which relies the security of our system is the following:

**The LRPC problem**: *Given a public matrix $G'$ it is difficult to recover low weight vector of rank weight $d$ in the dual code.*

**Discussion on the problem** The problem considered here is the adaptation of the NTRU problem and the MDPC problem but in rank metric. Notice that clearly the matrix used are not random, meanwhile this special structure could not be used for attacks for NTRU over 15 years. Also for MDPC the same situation arises.

Now in term of semantic security the approach developed for the MDPC cryptosystem in [22] on the indistingability to random codes can be adapted in a context of rank metric, moreover particular the CCA-2 conversion of K. Kobara and H. Imai [16]. can also be adapted to rank metric but this discussion goes well beyond this extended abstract.

Also concerning decryption failure it is possible to use the approach of E. Fujisaki and T. Okamoto [7] which permits that no information is given in case of decryption failure (the same approach was proposed for NTRU and MDPC).

### 7.2 Practical security

We review the different attacks:

• Message attack:in that case the attacker tries to recover directly the message M by trying to recover $e$ of rank $r$ with classical attacks on a random code.

• Attack on the secret key: the attacker tries to recover a codeword of rank $d$ in $H$. Notice that classical attacks first recover the support of a small weight word, in that case all the rows of $H$ have the same support and the fact that there are $n/2$ cyclic vector does not seem to be helpful.

• Spurious key attack: as in the NTRU case (see [15]) this attack corresponds to finding small word vectors in $H$ with rank slightly greater than $d$, and to use them for decoding. Although theoritically possible this attack is not doable in practice since the fact that $H$ contains small weight vectors implies indeed that many words of weight $2d$ exist. We do not go into details in this extended but as for MDPC codes [22], when the weight increases the complexity of the attacks grows faster than the number of small weight vectors, so that this attacks - as for NTRU and MDPC- does not work in practice.

Overall no structural attacks seem to appear in that case. Notice that this system is the exact adaptation of the NTRU and GGH frame in the case of rank distance. In particular, the double circulant case with $A^{-1}B$) corresponds to this case and no attack was found.

## 8 Examples of parameters and comparison to MDPC

### 8.1 Examples of parameters

We give three examples of parameters for the DC-LPRC case: an example with security $2^{80}$ which optimizes the size of the public key at $1500b$ with a decryption probability of $2^{-22}$, an example with security $2^{128}$, and at last an example with decryption failure probability of $2^{-80}$. In the table 'failure' stands for 'decryption failure', 'decryp. comp.' is the cost of the decryption in number of operations in $F_q$, the last two columns give the cost of the best known attacks : support attack and algebraic attacks (see [13]). We give parameters for different level of security, but also for different decryption failure, in particular it is possible to reach a $2^{-80}$ easily at the cost of doubling the size

of the key. Notice that the parameters are very versatile. Although no special attack is known for non prime number we choose to consider prime numbers in general.

| n | k | m | q | d | r | failure ($Log_2$) | public key(bits) | decryp. comp. ($Log_2$) | Support Att. ($Log_2$) | Algeb. att.($Log_2$) |
|---|---|---|---|---|---|---|---|---|---|---|
| 74 | 37 | 41 | 2 | 4 | 4 | -22 | 1517 | 17 | 84 | 80 |
| 94 | 47 | 47 | 2 | 5 | 5 | -23 | 2397 | 19 | 128 | 145 |
| 68 | 34 | 23 | $2^4$ | 4 | 4 | -80 | 3128 | 17 | 153 | 100 |

### 8.2 Comparison to MDPC

The system we propose compares well to the MDPC cryptosystem on three features: 1) the size of key can be three times smaller, 2) the system is much faster (at least a speed up of 100) - the complexity of MDPC is in $\lambda w^2 r$ for $w$ close to 90 and $r$ around 5000) and at last 3) it is easier to control the decryption probability failure and to decrease it to $2^{-80}$ rather than $2^{-23}$ at a cost of simply doubling parameters.

## 9 Conclusion

In this paper, as the recent MDPC paper [22] we generalize the NTRU [15] approach in a coding context but with the rank metric. To do so we introduced a new type of codes, the LRPC codes, for which we propose an efficient decoding algorithm. Overall as it is often the case for rank metric codes, the obtained results compare well to Hamming distance cryptosystem since the known attacks increase in difficulty . Moreover when rank metric cryptosystem have a strong history of broken system because of structural attacks based on recovering the Gabidulin code structure, the cryptosystem we propose is the first rank-metric based cryptosystem with a poor random structure and which is not based on Gabidulin codes. It is hence interesting to remark that this type of structure was never really attacked in the case of lattices as it seems the case for the MDPC cryptosystem. Of course the cryptosystem needs more scrutiny from the communauty but it seems like a very interesting system for the future.

## References


1. Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, Ayoub Otmani: Reducing Key Length of the McEliece Cryptosystem. AFRICACRYPT 2009: 77-97
2. Thierry P. Berger, Pierre Loidreau: Designing an Efficient and Secure Public-Key Cryptosystem Based on Reducible Rank Codes. INDOCRYPT 2004: 218-229
3. Florent Chabaud, Jacques Stern: The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes. ASIACRYPT 1996: 368-381
4. J.-C. Faugère, F. Levy-dit-Vehel, L. Perret. Cryptanalysis of MinRank. In *CRYPTO 2008*, LNCS 5157, pages 280–296. Springer Verlag, 2008.
5. Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Jean-Pierre Tillich: Algebraic Cryptanalysis of McEliece Variants with Compact Keys. EUROCRYPT 2010: 279-298
6. Cédric Faure, Pierre Loidreau: A New Public-Key Cryptosystem Based on the Problem of Reconstructing p-Polynomials. WCC 2005: 304-315
7. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology – CRYPTO'1999, volume 1666 of Lecture Notes in Computer Science, pages 537–554, Gold Coast, Australia, 1999. Springer.
8. Ernst M. Gabidulin, Theory of Codes with Maximum Rank Distance, Probl. Peredachi Inf, (21), pp. 3-16 (1985).
9. Ernst M. Gabidulin: Attacks and counter-attacks on the GPT public key cryptosystem. Des. Codes Cryptography 48(2): 171-177 (2008)
10. Ernst M. Gabidulin, A. V. Paramonov, O. V. Tretjakov: Ideals over a Non-Commutative Ring and thier Applications in Cryptology. EUROCRYPT 1991: 482-489

11. P. Gaborit, Shorter keys for code based cryptography P Gaborit Proceedings of the 2005 International Workshop on Coding and Cryptography
12. Philippe Gaborit, Julien Schrek, Gilles Zémor: Full Cryptanalysis of the Chen Identification Protocol. PQCrypto 2011: 35-50
13. P. Gaborit, O. Ruatta and J. Schrek, On the complexity of the rank syndrome decoding problem, eprint
14. Oded Goldreich, Shafi Goldwasser, Shai Halevi: Public-Key Cryptosystems from Lattice Reduction Problems. CRYPTO 1997: 112-131
15. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman: NTRU: A Ring-Based Public Key Cryptosystem. ANTS 1998: 267-288
16. K. Kobara and H. Imai. Semantically secure mceliece public-key cryptosystems -conversions for mceliece pkc -. In K. Kim, editor, Public Key Cryptography, volume 1992 of Lecture Notes in Computer Science, pages 19–35. Springer Berlin / Heidelberg, 2001. 10.1007/3-540-44586-2-2.
17. F. Levy-dit-Vehel and L. Perret, Algebraic decoding of rank metric codes, proceedings of YACC06.
18. Pierre Loidreau: Designing a Rank Metric Based McEliece Cryptosystem. PQCrypto 2010: 142-152
19. P. Loidreau, Properties of codes in rank metric, http://arxiv.org/abs/cs/0610057
20. Daniele Micciancio, Oded Regev, Lattice-based Cryptography Book chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008
21. Rafael Misoczki, Paulo S. L. M. Barreto: Compact McEliece Keys from Goppa Codes. Selected Areas in Cryptography 2009: 376-392
22. Rafael Misoczki and Jean-Pierre Tillich and Nicolas Sendrier and Paulo S. L. M. Barreto, MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes Cryptology ePrint Archive: Report 2012/409
23. O. Ore, On a special class of polynomials, Trans. American Math. Soc. (1933)
24. Ayoub Otmani, Jean-Pierre Tillich, Léonard Dallot: Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes. Mathematics in Computer Science 3(2): 129-140 (2010)
25. Ourivski, A. V. and Johansson, T., New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications,Probl. Inf. Transm.(38), 237–246 (2002)
26. Raphael Overbeck: Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes. J. Cryptology 21(2): 280-301 (2008)

## APPENDIX

In this appendix we give the proofs of the results of Section 3:

Let $A$ and $B$ be random $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^m$ of dimensions $\alpha$ and $\beta$ respectively. We suppose $\alpha\beta < m$ and we investigate the typical dimension of the subspace $\langle AB\rangle$.

We rely on the following observation:

**Lemma 3.** *Let $A'$ and $B$ be two subspaces of $\mathbb{F}_q^m$ of dimensions $\alpha'$ and $\beta$ such that $\dim\langle A'B\rangle = \alpha'\beta$. Let $A = A' + \langle a\rangle$ where $a$ is a uniformly chosen random element of $\mathbb{F}_q^m$. Then*

$$\mathbb{P}\left(\dim\langle AB\rangle < \alpha'\beta + \beta\right) \leq \frac{q^{\alpha'\beta+\beta}}{q^m}.$$

*Proof.* We have $\dim\langle AB\rangle < \alpha'\beta + \beta$ if and only if the subspace $aB$ has a non-zero intersection with $\langle A'B\rangle$. Now,

$$\mathbb{P}\left(\dim\langle A'B\rangle \cap aB \neq \{0\}\right) \leq \sum_{b\in B, b\neq 0} \mathbb{P}\left(ab \in \langle A'B\rangle\right) \tag{1}$$

$$\leq (|B|-1)\frac{q^{\alpha'\beta}}{q^m} \tag{2}$$

since for any fixed $a \neq 0$, we have that $ab$ is uniformly distributed in $\mathbb{F}_q^m$. Writing $|B| - 1 \leq |B| = q^\beta$ we have the result.

**Proposition 5.** *Let $B$ be a fixed subspace and suppose we construct a random subspace $A$ by choosing $\alpha$ independent (in the sense of probability) random vectors of $\mathbb{F}_q^m$ and letting $A$ be the subspace generated by these $\alpha$ random vectors. We have that*

$$\dim\langle AB\rangle = \alpha\beta$$

*with probability at least*

$$1 - \alpha\frac{q^{\alpha\beta}}{q^m}.$$

*Proof.* Apply the Lemma $\alpha$ times, starting with a random subspace $A' \subset A$ of dimension 1, and adding a new element to $A'$ until we obtain $A$.

Let $B$ be a fixed subspace of $\mathbb{F}_q^m$ containing 1 and let $\langle B^2\rangle$ be the subspace generated by all products of elements of $B$. Let $\beta_2 = \dim\langle B^2\rangle$. Let $A$ be a random subspace of $\mathbb{F}_q^m$ of dimension $\alpha$. By the Proposition we have that

$$\dim\langle AB^2\rangle = \alpha\beta_2$$

with probability at least

$$1 - \alpha\frac{q^{\alpha\beta_2}}{q^m}.$$

**Remark:** we have $\beta_2 \leq \beta(\beta+1)/2$.

**Lemma 4.** *Suppose $\dim\langle AB^2\rangle = \alpha\beta_2$. Let $e \in \langle AB\rangle$ with $e \notin A$. Suppose $eB \subset \langle AB\rangle$. Then there exists $x \in B$, $x \notin \mathbb{F}_q$, such that $xB \subset B$.*

*Proof.* Let $(a_i)$ be a basis of $A$. We have

$$e = \sum_i \lambda_i a_i b_i$$

with $\lambda_i \in \mathbb{F}_q$ for all $i$ and $b_j \notin \mathbb{F}_q$ and $\lambda_j \neq 0$ for some $j$, otherwise $e \in A$ contrary to our assumption. Let $b$ be any element of $B$. By our hypothesis we have $eb \in \langle AB \rangle$, meaning

$$\sum_i \lambda_i a_i b_i b = \sum_i \mu_i a_i b'_i$$

with $b'_i \in B$. Now the maximality of the dimension of $\langle AB^2 \rangle$ implies that

$$\lambda_j a_j b_j b = \mu_j a_j b'_j$$

from which we deduce $b_j b \in B$. Since this holds for arbitrary $b \in B$, we have $b_j B \subset B$.

**Proposition 6.** *Suppose $m$ is prime. Let $A$ and $B$ be random subspaces of dimensions $\alpha$ and $\beta$ respectively. Let $(b_i)$ be a basis of $B$ and let $S = \langle AB \rangle$. Then with probability at least*

$$1 - \alpha \frac{q^{\alpha\beta(\beta+1)/2}}{q^m}$$

*we have that*

$$\bigcap_i b_i^{-1} S = A.$$

*Proof.* If not, there exists a subspace $E \supsetneq A$, such that $\langle EB \rangle = \langle AB \rangle$. By the remark before Lemma 4 we have that with probability at least

$$1 - \alpha \frac{q^{\alpha\beta(\beta+1)/2}}{q^m}$$

the conditions of Lemma 4 hold. But then there is $x \notin \mathbb{F}_q$ such that $xB \subset B$. But this implies that $\mathbb{F}_q(x)B \subset B$. But $m$ prime implies that there is no intermediate field between $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, hence $\mathbb{F}_{q^m} \subset B$, a contradiction.

*A better bound* Our goal is to show that with a large probability, when $A$ and $B$ are randomly chosen with sufficiently small dimension, then with probability close to 1 we have that:

$$\bigcap_{b \in B} \langle AB \rangle b^{-1} = A.$$

Without loss of generality we can suppose that $1 \in B$. We shall show that for a random $b \in B$, we have

$$\langle AB \rangle \cap \langle AB \rangle b^{-1} = A$$

with probability close to 1.

**Lemma 5.** *Let $B_1$ be a subspace of dimension $\beta_1$. Let $b$ be a uniformly distributed random element of $\mathbb{F}_q^m$. Then the probability that $b \in B_1 + B_1 b^{-1}$ is at most:*

$$\frac{2q^{2\beta_1}}{q^m}.$$

*Proof.* This event can only happen if $b$ is a root of an equation of the form

$$x^2 - b_1 x - b'_1 = 0.$$

There are at most $|B_1|^2 = q^{2\beta_1}$ such equations, and each one of the has at most two roots.

Let $B_1$ be any vector space containing 1 and of dimension $\beta_1$. Let $b$ be a random element uniformly distributed in $\mathbb{F}_q^m$ and set $B = B_1 + \langle b \rangle$. Denote $\beta = \dim B = \beta_1 + 1$ (with probability $1 - q^{\beta_1}/q^m$). Since $b^{-1}$ is also uniformly distributed, we have that $B_1 \cap B_1 b^{-1} \neq \{0\}$ with probability at most

$$(|B_1| - 1)\frac{|B_1|}{q^m} \leq \frac{q^{2\beta_1}}{q^m}.$$

Therefore with probability at least

$$1 - \frac{q^{2\beta_1}}{q^m}$$

we have that

$$\dim(B_1 + B_1 b^{-1}) = 2\beta_1.$$

Now applying Lemma 5 we obtain:

**Lemma 6.** *With probability at least*

$$1 - \frac{3q^{2\beta_1}}{q^m}$$

*we have that*

$$\dim(B + Bb^{-1}) = 2\beta - 1.$$

**Proposition 7.** *Let $B$ be a subspace of dimension $\beta$ containing 1 such that $\dim B + Bb^{-1} = 2\beta - 1$ for some $b \in B$. Let $A$ be a randomly chosen subspace of dimension $\alpha$. With probability at least*

$$1 - \alpha\frac{q^{\alpha(2\beta-1)}}{q^m}$$

*we have that*

$$\langle AB \rangle \cap \langle AB \rangle b^{-1} = A$$

*Proof.* By Proposition 5 we have that with probability at least

$$1 - \alpha\frac{q^{\alpha(2\beta-1)}}{q^m}$$

$$\dim\langle A(B + Bb^{-1})\rangle = \alpha(2\beta - 1) = 2\alpha\beta - \alpha.$$

On the other hand, we have that

$$\begin{aligned} \dim\langle A(B + Bb^{-1})\rangle &= \dim\langle AB\rangle + \dim\langle ABb^{-1}\rangle - \dim(\langle AB\rangle \cap \langle ABb^{-1}\rangle) && (3)\\ &= 2\alpha\beta - \dim(\langle AB\rangle \cap \langle ABb^{-1}\rangle) && (4) \end{aligned}$$

hence

$$\dim(\langle AB\rangle \cap \langle ABb^{-1}\rangle) = \alpha.$$

But this proves the result since $A \subset \langle AB\rangle \cap \langle ABb^{-1}\rangle$ and $\dim A = \alpha$.