Designing a rank metric based McEliece cryptosystem

Pierre Loidreau

DGA and IRMAR, Université de Rennes 1
Pierre.Loidreau@univ-rennes1.fr

keywords:

Abstract. In this paper we describe the rank metric based McEliece type cryptosystems which where first introduced by Gabidulin, Paramonov and Tretjakov in the 90's. Then we explain the principle of Overbeck's attack is so efficient on these types of systems. Finally we show how to choose the parameters so that the public-key size remain relatively small (typically less than 20 000 bits), with a good security against structural and decoding attacks.

1 Introduction

Code based public-key cryptosystem form an interesting alternative to public-key cryptosystems based on coding theory. Their principle was first stated by McEliece in the early days of public-key cryptography, [20]. These systems have some nice properties such as

- they are very fast in encryption and decryption compared to number theory based systems,
- there are no algorithms working on quantum computers that would enable to decrease the complexity of the attacks contrarily to number theory based cryptosystems,
- the related complexity problem have been widely investigated since Shannon's seminal paper more than 60 years ago.

The main drawback which made them unpractical in the 70's and 80's is that the public-key size is too large to be implemented on limited resource devices, typically several hundreds of thousands of bits. Therefore one of the great challenges designing of code based cryptosystems is to find a way to reduce the public-key size, sufficiently to be implemented on cheap devices.

Since 20 years several proposals were made in that sense. Basically two directions have been considered. The first one consists of exploiting the algebraic structure of families of codes to diminish the key-size. For instance using of Goppa codes with a non-trivial automorphism group as the family of codes, [18], hiding the structure of codes by taking subcodes of generalised Reed-Solomon codes [5], and more recently the using quasi-cyclic codes [14], or dyadic Goppa

codes [21]. However attacks against some of these systems show that the structure of the codes introduces structural weaknesses in the public-key [17, 3, 23].

The second direction which is the heart of this paper consists of using rank metric rather than Hamming metric, a metric in which the decoding problems have the reputation to be more complex. This idea was first used by Gabidulin, Paramonov and Tretjakov in 1991, who proposed a public-key cryptosystem based on a family of codes published by Gabidulin correcting rank errors, [13]. In the seminal paper, they proposed to use public-keys as low as 5 000 bits. During the 90's, different modifications of the system were published, see [5, 12, 25, 26, 4] especially after the design of structural attacks by Gibson [15, 16] which lead to increasing the key size, however these kind of systems survived until Overbeck designed a somehow devastating attack exploiting fully the structure of the underlying family of codes, [30].

Until now the question was to know if cryptosystems based on rank metric can be made resistant to Overbeck's attack or not, by keeping a public-key size reasonably small compared to the counterpart in Hamming metric. A first step in the analysis of the problem consists in fully understanding the principle on which is based Overbeck's attack, that is to know, the relative stability of the codes under the action of the Frobenius automorphism of the codes. In a second step, we establish results and relations between parameters so that the attack does not work.

In a first part we recall some essential properties of rank metric and of Gabidulin codes. In a second part we design an attack on the system. This attack uses the same structural flaw as Overbeck's attack, and has the same working domain. From the study of the working domain of the attack, a conceiver can deduce parameters to secure the cryptosystem.

2 Background on rank metric and Gabidulin codes

In this section we briefly recall the definition of rank metric and Gabidulin codes, which form the heart of rank metric based cryptosystems. We will use only fields of characteristic 2 but all these results can be extended to fields of any prime characteristic.

2.1 Rank metric

Let $GF(2^m)$ be the finite field with 2^m elements and let $(\beta_1, \ldots, \beta_m)$ be a basis of $GF(2^m)$ over $GF(2)$.

Définition 1 ([9])
Let $\mathbf{x} = (x_1, \ldots, x_n) \in GF(2^m)^n$. *The rank of* $\mathbf{x}$ *in* $GF(2)$ *is the rank of the matrix* $\mathbf{X} = (x_{ij})$, *where* $x_j = \sum_{i=1}^{m} x_{ij}\beta_i$. *It is written* $\mathrm{Rg}(\mathbf{x})$.

The rank of a vector is a norm, independent of the chosen basis $(\beta_1, \ldots, \beta_m)$, and if $\mathcal{C}$ is a linear code, the minimum rank distance of $\mathcal{C}$ is naturally defined by

$$d \stackrel{def}{=} \min_{\mathbf{c} \in \mathcal{C}^*} (\mathrm{Rg}(\mathbf{c}))$$

Let $\mathcal{C}$ be a code, $\mathbf{y}$ be a vector and t be an integer, the complexity problem **Bounded decoding** for codes in rank metric can be defined as:

Bounded decoding$(\mathbf{y}, \mathcal{C}, t)$
Find if exists $\mathbf{c} \in \mathcal{C}$ *and* $\mathbf{e} \in GF(2^m)^n$ *with* $\mathrm{Rg}(\mathbf{e}) \leq t$ *such that* $\mathbf{y} = \mathbf{c} + \mathbf{e}$.

If d denotes the minimum rank distance of $\mathcal{C}$, k its dimension, and in the case where $t \leq (d-1)/2$, this problem has either one or zero solution. In the case where there is exactly one solution, the best algorithms to find the solution are probabilistic algorithms due to Ourivski and Johannson and have average work factor, which are based on the principle of finding codewords of the smallest rank in a linear code, [27]:

- Basis enumeration algorithm: $W_{\text{bases}} \approx (k+t)^3 2^{(t-1)(m-t)+2}$.
- Coordinate enumeration algorithm: $W_{\text{coord}} \approx (k+t)^3 t^3 2^{(t-1)(k+1)}$.

If we consider the same problem on the same parameters but in Hamming metric, solving the problem is considerably less difficult, [7, 1]. This is the reason why McEliece types rank metric based cryptosystems can theoretically employ public-keys of much smaller size than for Hamming metric based cryptosystems.

2.2 Gabidulin codes

Let $\mathbf{g} = (g_1, \ldots, g_n) \in GF(2^m)$ linearly independent over $GF(2)$. Let

$$\mathbf{G} = \begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}, \tag{1}$$

where $[i] \stackrel{def}{=} 2^i$ is the ith power of the Frobenius automorphism of $GF(2^m)/GF(2)$.

Définition 2 ([9])
The Gabidulin code $Gab_k(\mathbf{g})$ *over* $GF(2^m)$ *of dimension* k *and generator vector* $\mathbf{g}$ *is the code generated by* $\mathbf{G}$.

The error-correcting capability of $Gab_k(\mathbf{g})$ is $\lfloor (n-k)/2 \rfloor$. There are very efficient decoding algorithms for Gabidulin codes up to the rank error correcting capability [9, 10, 32, 31, 19].

3 McEliece type cryptosystems based on rank metric

In this section we first describe the original GPT cryptosystem, published in 1991, by Gabidulin, Paramonov and Tretjakov, [13]. Other versions where later published like the one by Ourivski and Gabidulin, using a right scrambler which is a linear isometry of rank metric [25]. It is immediate to see that this version is a generalisation of the initial proposition. Therefore we will only present this version of the cryptosystem.

3.1 The original system

Parameters

- The field $GF(2^m)$
- An integer t_1

Key generation The *private key* is composed with

- $\mathbf{S}$, a $k \times k$ non-singular matrix with coefficients in $GF(2^m)$.
- $\mathbf{G}$, a $k \times n$ matrix over $GF(2^m)$ generating a Gabidulin code of generator vector $\mathbf{g} = (g_1, \ldots, g_n)$ under the canonical form given in (1). Hence we can correct up to rank $t = \lfloor (n-k)/2 \rfloor$ errors.
- $\mathbf{Z}$, a $k \times t_1$ matrix with coefficients in $GF(2^m)$.
- $\mathbf{T}$, a $(n+t_1) \times (n+t_1)$ non-singular matrix with coefficients in $GF(2)$. The matrix $\mathbf{T}$ is a *linear isometry* of rank metric [2].

The public-key is thus the $k \times (n+t_1)$ matrix

$$\mathbf{G}_{\text{pub}} = \mathbf{S}(\mathbf{G} \mid \underbrace{\mathbf{Z}}_{t_1 \ cols})\mathbf{T} \tag{2}$$

The encryption procedure is exactly the same as for the original McEliece cryptosystem:

Encryption Let $\mathbf{x} \in GF(2^m)^k$ be the information vector that must be encrypted. The ciphertext $\mathbf{y}$ is

$$\mathbf{y} = \mathbf{x}\mathbf{G}_{\text{pub}} + \mathbf{e}$$

where $\mathbf{e}$ is a vector of rank $\leq t = \lfloor (n-k)/2 \rfloor$

The decryption procedure is:

Decryption Let $\mathbf{y}$ be the received ciphertext, we have

$$\mathbf{y} = \mathbf{x}\mathbf{G}_{\text{pub}} + \mathbf{e},$$

where $\text{Rg}(\mathbf{e}) \leq t$. Then the receiver computes

$$\mathbf{y}\mathbf{T}^{-1} = \mathbf{x}(\mathbf{G} \mid \mathbf{Z}) + \mathbf{e}\mathbf{T}^{-1},$$

and removes the last t_1 positions of $\mathbf{y}\mathbf{T}^{-1}$. Finally he decodes in the Gabidulin code of generator matrix $\mathbf{G}$.

The security of the cryptosystem relies on the following two assumptions:

- The code generated by $\mathbf{G}_{\text{pub}}$ behaves randomly.
- Solving **Bounded decoding**$(\mathbf{y}, \mathcal{C}, t)$, where $\mathcal{C}$ is a random code of length n, dimension k over $GF(2^m)$ is difficult

As shown in section 2.1, the second assumption is satisfied provided the parameters are sufficiently large. The first assumption however is more problematic, since the previous cryptosystems based on scrambled Gabidulin codes have until now been severely attacked.

3.2 Structural attacks

One of the main problem in designing rank metric based cryptosystems is that there is only known family of codes with a fast decoding algorithm, the family of Gabidulin codes. Therefore all rank metric based cryptosystems have to rely on codes derived from Gabidulin codes (scrambled codes, subfield subcode for instance). Moreover, it is impossible to use Gabidulin codes without scrambling the structure as it was shown by Gabidulin (case where $t_1 = 0$). Namely in that case there exists an attack recovering a decoder for the public-code in polynomial time. This attack is an analog of Sidel'nikov-Shestakov attack in the case where Generalised Reed-Solomon codes are used in the Hamming metric based McEliece cryptosystem.

Moreover, different attacks have shown that the scrambling matrix $\mathbf{Z}$ had to be very carefully chosen. The first person to attack structurally the initial parameters was Gibson [15, 16], who exploited some properties of Gabidulin codes. After these attacks some new parameters, as well as modifications of the system were proposed to render Gibson attacks inefficient, [12, 25]. More recently Overbeck used Gibson's attacks as black boxes against the new versions of the system, [29]. But the most powerful attack until now using fully the structure of the codes was still proposed by Overbeck who cryptanalysed almost all versions of McEliece type cryptosystems based Gabidulin codes, [28, 30]. To prevent the attack from succeeding, the parameters should be so much increased that the interest of rank metric systems decreases compared to Hamming based systems.

The success of this approach is that Overbeck fully exploits the large structure of Gabidulin codes, that is that the intersection of a k–dimensional Gabidulin code and the Gabidulin code on which the Frobenius automorphism acts is a $k-1$–dimensional Gabidulin code, namely it:

$$Gab_k(\mathbf{g}) \cap Gab_k(\mathbf{g})^{[1]} = Gab_{k-1}(\mathbf{g}^{[1]})$$

To show how to design cryptosystems which are resistant to Overbeck's attacks, and still with very reasonable key sizes, we first need to present an attack whose efficiency is comparable to that of Overbeck's. The heart of the attack is described in proposition 1, which is not in Overbeck's work.

The public key is given by the matrix $\mathbf{G}_{\text{pub}}$ from equation (2). Let us recall that $\mathbf{G}^{[i]}$ is the matrix derived from $\mathbf{G}$, by elevating each component to the ith power of the Frobenius automorphism, that is to the power 2^i.

If all the components of $\mathbf{G}_{\text{pub}}$ are elevated to the powers $[1], [2], \ldots, [n-k-1]$, we obtain

$$\underbrace{\begin{pmatrix} \mathbf{G}_{\text{pub}} \\ \mathbf{G}_{\text{pub}}^{[1]} \\ \vdots \\ \mathbf{G}_{\text{pub}}^{[n-k-1]} \end{pmatrix}}_{\mathcal{G}_{\text{pub}}} = \underbrace{\begin{pmatrix} \mathbf{S} & 0 & \cdots & 0 \\ 0 & \mathbf{S}^{[1]} & \ddots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & \cdots & & \mathbf{S}^{[n-k-1]} \end{pmatrix}}_{\mathcal{S}} \underbrace{\left(\begin{array}{c|c} \mathbf{G} & \mathbf{Z} \\ \mathbf{G}^{[1]} & \mathbf{Z}^{[1]} \\ \vdots & \vdots \\ \mathbf{G}^{[n-k-1]} & \mathbf{Z}^{[n-k-1]} \end{array}\right)}_{(\mathcal{G} \mid \mathcal{Z})} \mathbf{T}, \quad (3)$$

where

- $\mathcal{G}_{\text{pub}}$ is a $k(n-k) \times n$ matrix of rank $n-1$, thanks to the properties of Gabidulin codes.
- Since $\mathbf{S}$ is non-singular, so is $\mathcal{S}$.
- Since $\mathbf{T}$ has coefficients in the base field $GF(2)$, for all i, $\mathbf{T}^{[i]} = \mathbf{T}$, and $\mathbf{T}$ has rank $n + t_1$.
- $\mathcal{Z}$ is a $k(n-k) \times t_1$ matrix of rank $s \leq \min(k(n-k), t_1)$.

Since we want to optimise the public-key size in the design of the system it is reasonable to suppose that t_1 is much less than $k(n-k)$. In that case, if $\mathbf{Z}$ is chosen randomly, then $\mathcal{Z}$ has very probably rank t_1. This implies that $\mathcal{G}_{\text{pub}}$ is very probably of rank $n + t_1 - 1$. Hence its right kernel has rank 1. This leads to the following proposition which shows that in the cases where the right kernel is one dimensional, a decoder form the public-code can be recovered in polynomial-time.

Proposition 1
If the right kernel $\ker_r(\mathcal{G}_{\text{pub}})$ *of* $\mathcal{G}_{\text{pub}}$ *has dimension* 1*, then*

- *There exists a vector* $\mathbf{h}$ *of rank* n *over* $GF(2)$ *such that*

$$\ker(\mathcal{G}_{\text{pub}}) = \{\ \mathbf{T}^{-1}(\alpha\mathbf{h} \mid \mathbf{0})^T \mid \alpha \in GF(2^m)\}.$$

- *Let* $\mathbf{y} \in \ker(\mathcal{G}_{\text{pub}})$*, then every matrix* $\mathbf{Q}$ *of size* $(n+t_1) \times (n+t_1)$ *and with coefficients in* $GF(2)$ *such that* $\mathbf{Qy} = (\mathbf{x} \mid \mathbf{0})^T$*, is non-singular and satisfies*

$$\mathbf{TQ}^{-1} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{D} \end{pmatrix},$$

where $\mathbf{A}$ *is an* $n \times n$ *non-singular matrix, and* $\mathbf{D}$ *is an* $t_1 \times t_1$ *non-singular matrix. Such a matrix* $\mathbf{Q}$ *can be determined in polynomial-time.*

Proof

- Since the right kernel of $\mathcal{G}_{\text{pub}}$ has dimension 1 the kernel of $(\mathcal{G} \mid \mathcal{Z})$ is of the form $(\alpha\mathbf{h} \mid \mathbf{0})$ where $\mathbf{h}$ generates the right kernel of $\mathcal{G}$. But $\mathcal{G}$ generates a $n-1$–dimensional Gabidulin code whose *dual* is a 1–dimensional Gabidulin code with generator vector $\mathbf{h}$. This implies in particular that $\mathbf{h}$ has rank n over $GF(2)$.

– Let $\mathbf{y} \in \ker(\mathcal{G}_{\text{pub}})$. From the structure of the kernel describe in the preceding item, we have $\mathbf{y} = \mathbf{T}^{-1}(\alpha\mathbf{h} \mid \mathbf{0})^T$. Suppose we have determined a binary non-singular matrix $\mathbf{Q}$ such that

$$\mathbf{Qy} = (\mathbf{x} \mid \mathbf{0})^T = \mathbf{QT}^{-1}(\alpha\mathbf{h} \mid \mathbf{0})^T.$$

If we split $\mathbf{QT}^{-1}$ into four blocks such that

$$\mathbf{QT}^{-1} = \begin{pmatrix} \mathbf{A}' & \mathbf{B}' \\ \mathbf{C}' & \mathbf{D}' \end{pmatrix},$$

then we have $\mathbf{C}'\mathbf{h}^T = \mathbf{0}$. Therefore for all $i = 1, \ldots t_1$, $\mathbf{c}_i\mathbf{h}^T = 0$ where $\mathbf{c}_i$ is the ith row of $\mathbf{C}'$. Since the components of $\mathbf{C}'$ are in $GF(2)$ and since $\mathbf{h}$ has rank n over $GF(2)$, we have that $\alpha\mathbf{h}$ has also rank n over $GF(q)$ and for all $i = 1, \ldots, t_1$ we have $\mathbf{c}_i = \mathbf{0}$. Moreover, since $\mathbf{Q}$ is non-singular, the inverse $(\mathbf{QT}^{-1})^{-1} = \mathbf{TQ}^{-1}$ is also upper-triangular by blocks.

Given $\mathbf{y} \in \ker(\mathcal{G}_{\text{pub}})$ we determine a non-singular matrix $\mathbf{Q}$ by:

1. Solving the equation$\mathbf{Q}_2\mathbf{y}^T = \mathbf{0}$ where $\mathbf{Q}_2$ is a $t_1 \times (n + t_1)$ matrix of rank t_1.
2. Determining a matrix $\mathbf{Q}_1$ such that

$$\mathbf{Q} \stackrel{def}{=} \begin{pmatrix} \mathbf{Q}_1 \\ \mathbf{Q}_2 \end{pmatrix},$$

is invertible

Since $\mathbf{y}$ has rank n over $GF(2)$ the matrix $\mathbf{Y}$ obtained by expanding the components of $\mathbf{y}$ over a basis of $GF(2^m)/GF(2)$ has size $m \times (n + t_1)$ and rank n. Hence the right kernel of $\mathbf{Y}$ has dimension t_1. Finding $\mathbf{Q}_2$ consists thus in finding a bases of the right kernel of $\mathbf{Y}$, since we have to solve $\mathbf{YQ}_2^T = 0$. This can be done in polynomial time.

■

Now whenever the right kernel $\ker_r(\mathcal{G}_{\text{pub}})$ has rank 1, by applying the previous proposition, we can find a matrix $\mathbf{Q}$ satisfying

$$\mathbf{G}_{\text{pub}}\mathbf{Q}^{-1} = \mathbf{S}(\mathbf{GA} \mid \mathbf{Z}').$$

Since $\mathbf{A}$ is non-singular and has components in the base field $GF(2)$, the matrix $\mathbf{G}' = \mathbf{GA}$ generates $Gab_k(\mathbf{gA})$. If we denote by $\mathbf{G}_1$ the n first columns of $\mathbf{G}_{\text{pub}}\mathbf{Q}^{-1}$, the attacker has to solve the equation

$$\mathbf{G}_1 = \mathbf{SG}',$$

that is $\mathbf{G}_1$ is a randomly chosen generator matrix of $Gab_k(\mathbf{gA})$. This can be done in polynomial time [11]. The matrix $\mathbf{S}$ thus determined is unique.

We have just proved the following proposition

Proposition 2

If the right kernel of $\mathcal{G}_{\text{pub}}$ *given by the equation* (3) *has dimension* 1, *an attacker can recover in polynomial-time matrices* $\mathbf{Q}, \mathbf{S}$ *and* $\mathbf{Z}$ *such that*

$$\mathbf{G}_{\text{pub}}\mathbf{Q}^{-1} = \mathbf{S}(\mathbf{G}' \mid \mathbf{Z}'),$$

where

- $\mathbf{Q}$ *is a* $(n + t_1) \times (n + t_1)$ *matrix with coefficients in* $GF(2)$,
- $\mathbf{S}$ *is a* $k \times k$ *non-singular matrix*
- $\mathbf{G}'$ *generates a* k*-dimensional Gabidulin code,*
- $\mathbf{Z}'$ *is a* $k \times t_1$ *matrix.*

4 Which parameters for a rank metric based cryptosystem

From previous section, the parameters of the system must be chosen so that the dimension of the right kernel of $\mathcal{G}_{pub}$ is greater than 1, and even sufficiently large to avoid enumeration so that an attacker fall by chance on a vector of the dual of the Gabidulin code by selecting a vector randomly in the kernel.

The following corollary gives us information to choose the parameters of the system so that we cannot apply the previous attack.

4.1 Design criteria

Corollary 1 *Let* $\mathbf{G}_{\text{pub}} = \mathbf{S}(\mathbf{G} \mid \mathbf{Z})\mathbf{T}$ *of size* $k \times (n + t_1)$. *If there is an integer* ℓ *such that*

$$1 \leq \text{Rg}(\mathbf{Z}) \leq \frac{t_1 - \ell}{n - k},$$

then the dimension of $\ker_r(\mathcal{G}_{\text{pub}})$ *is greater or equal to* $1 + \ell$.

Proof

If $s = \text{Rg}(\mathbf{Z})$, then $\text{Rg}(\mathcal{Z}) \leq s(n - k)$. Hence $\text{Rg}(\mathcal{G}_{\text{pub}}) \leq s(n - k) + n - 1$. Then if $s(n - k) \leq t_1 - \ell$, the right kernel of $\mathcal{G}_{\text{pub}}$ has dimension $\geq 1 + \ell$.
■

Therefore to prevent attacks based on the principle described in previous section, it suffices to choose $\ell \geq 1$ and the distortion matrix $\mathbf{Z}$ such that

$$\text{Rg}(\mathbf{Z}) \leq \frac{t_1 - \ell}{n - k},$$

which implies $t_1 > (n - k)$.

Now here are the criteria that have to be taken into account in the design of the cryptosystem:

- First note that the dimension of $\ker_r(\mathcal{G}_{pub})$ must be large enough to avoid enumerations since the vector $\mathbf{h}$ discussed in proposition 1
- Second, the best decoding attack has to be of sufficient complexity. We take as references the complexities given in section 2.1
- Third we try to obtain the smallest possible size for these systems

4.2 Proposition of parameters

Suppose that we want to reach a security of 2^{80} binary operations for the system. In table 1 we propose two sets of parameters, involving a Gabidulin code correcting rank 6 errors over $GF(2^{24})^{24}$. We can easily show that the complexity of the decoding attacks is larger than 2^{80}

- In the first proposal $\ker_r(\mathcal{G}_{pub})$ has dimension 5 over $GF(2^{24})$
- In the second proposal $\ker_r(\mathcal{G}_{pub})$ has also dimension 4 over $GF(2^{24})$

This implies that an attack consisting in enumerating the right kernel and testing all vectors candidates for being $\mathbf{h}$ will take on average $(2^{120}-1)/(2^{24}-1) \approx 2^{96}$ tries.

The last column shows how it is possible to improve the transmission rate of the system by using a modification proposed in [4]. It increases the transmission rate by

$$\frac{(m+n-t)t-r}{m(n+t_1)},$$

where r is the number of selected random bits.

$m=n$	k	s	t_1	Key size	Decoding	k/n	Improv. BeLoi2004
24	12	3	40	14 976bits	$> 2^{83}$	19%	30%
24	12	4	52	18 432bits	$> 2^{83}$	15,8%	24,3%

Table 1. Proposed parameters

5 Conclusion and perspectives

In this paper we have shown how to choose parameters be to design rank metric based cryptosystems. The resulting proposals are public-key cryptosystems with public-keys of very reasonable sizes compared to the original McEliece cryptosystem.

The performances of the systems in encryption and decryption have to be compared to Hamming metric based cryptosystems, but this is another story.

References

1. A. Barg. *Handbook of Coding Theory, Vol. 1*, chapter 7, pages 649–754. North–Holland, 1998.
2. T. P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Transactions on Information Theory*, 49(11):3016–3019, November 2003.

3. T. P. Berger, P. L. Cayrel, P. Gaborit, and A. Otmani. Reducing key-length of the McEliece cryptosystem. In *Progress in Cryptology - Africacrypt 2009*, volume 5580 of *LNCS*, pages 77–97, 2009.
4. T. P. Berger and P. Loidreau. Designing an efficient and secure public-key cryptosystem based on reducible rank codes. In *Proceedings of INDOCRYPT 2004*, 2004.
5. T. P. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35:63–79, 2005.
6. E. R. Berlekamp, R. J. McEliece, and H. C. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3), May 1978.
7. A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.
8. N. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based signature scheme. In C. Boyd, editor, *Advances in Cryptology - ASIACRYPT'2001*, number 2248 in LNCS, pages 151–174. Springer, 2001.
9. E. M. Gabidulin. Theory of codes with maximal rank distance. *Problems of Information Transmission*, 21:1–12, July 1985.
10. E. M. Gabidulin. A fast matrix decoding algorithm for rank-error correcting codes. In G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, editors, *Algebraic coding*, volume 573 of *LNCS*, pages 126–133. Springer, 1991.
11. E. M. Gabidulin. Public-key cryptosystems based on linear codes over large alphabets: efficiency and weakness. In P. G. Farrell, editor, *Codes and Cyphers*, pages 17–31. Formara Limited, Southend-on-sea, Essex, 1995.
12. E. M. Gabidulin and A. V. Ourivski. Modified GPT PKC with right scrambler. In D. Augot and C. Carlet, editors, *Proceedings of the 2nd International workshop on Coding and Cryptography, WCC 2001*, pages 233–242, 2001. ISBN Number : 2-761-1179-3.
13. E .M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT'91*, volume 547 of *LNCS*, pages 482–489. Springer, 1991.
14. P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of WCC 2005*, 2005.
15. J. K. Gibson. Severely denting the Gabidulin version of the McEliece public-key cryptosystem. *Designs, Codes and Cryptography*, 6:37–45, 1995.
16. J. K. Gibson. The security of the Gabidulin public-key cryptosystem. In U. Maurer, editor, *EUROCRYPT'96*, pages 212–223, 1996.
17. K. Kobara and H. Imai. On the one-wayness against chosen-plaintext attacks of the Loidreau's modified McEliece PKC. *IEEE Transactions on Information Theory*, 49(12):3160–3168, December 2003.
18. P. Loidreau. Strengthening McEliece public-key cryptosystem. In T. Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000*, LNCS. IACR, Springer, December 2000.
19. P. Loidreau. A Welch-Berlekamp like algorithm for decoding Gabidulin codes. In Ø. Ytrehus, editor, *Coding and Cryptography - WCC 2005, 4th International workshop on Coding and Cryptography, Revised Selected Papers*, number 3969 in LNCS, pages 36–45. Springer, 2006.

20. R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Technical report, Jet Propulsion Lab. DSN Progress Report, 1978.
21. R. Misoczki and P. Barreto. Compact McEliece keys from goppa codes. In *Selected areas in cryptography, 16th International Workshop, SAC 2009*, number 5867 in LNCS, page 2009.
22. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159 – 166, 1986.
23. A. Otmani, J. P. Tillich, and L. Dallot. Cryptanalysis of two mceliece cryptosystems based on quasi-cyclic codes. *Mathematics in Computer Science*. to appear.
24. A. V. Ourivski. Recovering a parent code for subcodes of maximal rank distance codes. In D. Augot, P. Charpin, and G. Kabatianski, editors, *Proceedings of the 3rd International workshop on Coding and Cryptography, WCC 2003*, pages 357–363, 2003. ISBN Number : 2-7261-1205-6.
25. A. V. Ourivski and E. M. Gabidulin. Column scrambler for the GPT cryptosystem. *Discrete Applied Mathematics*, 128(1):207–221, May 2003. Special issue of the second International Workshop on Coding and Cryptography (WCC2001).
26. A. V. Ourivski, E. M. Gabidulin, B. Honary, and B. Ammar. Reducible rank codes and their applications to cryptography. *IEEE Transactions on Information Theory*, 49(12):3289–3293, December 2003.
27. A. V. Ourivski and T. Johannson. New technique for decoding codes in the rank metric and its cryptography applications. *Problems of Information Transmission*, 38(3):237–246, September 2002.
28. R. Overbeck. A new structural attack for GPT and variants. In E. Dawson and S. Vaudenay, editors, *Proceedings of MyCrypt 2005*, volume 3715 of *LNCS*, pages 50–63. Springer, 2005.
29. R. Overbeck. Extending Gibson's attacks on the GPT cryptosystem. In Ø Ytrehus, editor, *Coding and Cryptography - WCC 2005, 4th International workshop on Coding and Cryptography*, number 3969, pages 178–188. Springer, 2006.
30. R. Overbeck. Structural attacks for public-key cryptosystems based on gabidulin codes. *Journal of Cryptology*, 21(2):280–301, 2008.
31. G. Richter and S. Plass. Fast decoding of rank-codes with rank errors and column erasures. In *2004 IEEE International Symposium on Information Theory, ISIT'04*, 2004.
32. R. M. Roth. Maximum-Rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, March 1991.
33. N. Sendrier. Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs, 2001.
34. A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Transactions on Information Theory*, 43(6):1757–1766, November 1997.