Analysis of a Public-Key Encryption Scheme based on distorted Gabidulin codes

Pierre Loidreau

DGA MI and Univ Rennes, CNRS, IRMAR
UMR 6625, F-35000 Rennes, France
pierre.loidreau@univ-rennes1.fr**

Abstract. We proove a conjecture on the complexity of a structural attack on the One-Way Public-Key Encryption scheme (OW-PKE) based on Gabidulin codes distorted by a small dimensional vector space. This work was presented at PQCrypto 2017. We show that the complexity to recover a polynomial-time decoder for the public code essentially depends on the secret vector space which is used to distort the structure of a Gabidulin codes. This is a straightforward extension of Gabidulin's idea that one can find in the seminal paper introducing GPT systems. By taking into account the recent improvements on the decoding of rank errors we propose sets of parameters ensuring fixed security levels for the OW-PKE.

1 Introduction

A McEliece type OW-PKE based on Gabidulin codes was proposed in [Loi17]. It mimics the orignal McEliece type OW-PKE. Compared to modern PKE and especially to those proposed at the NIST post-quantum standardization process it has three main advantages.

- Decryption is deterministic. This makes it easier to handle as an IND-CCA version than Lattice based schemes and MDPC codes based schemes.
- Key size is between one and two orders of magnitude smaller than other Hamming metric based cryptosystem. It favourably compares to unstructured lattice-based PKEs such as `FrodoKEM`.
- The ciphertext is small compared to unstructured lattice based OW-PKE's and compares favourably with structured lattices.

On the other its security analysis is not yet sufficiently stabilized. The security of the scheme relies on two paradigms:

- The complexity of distinguishing the public code from random.
- The complexity of decoding a random code in rank metric.

The latter problem is a hard problem in the complexity class ZPP [GZ15]. Significant progresses were made in the computational complexity which makes necessary to reconsider the parameters of the original scheme [BBC+20].

Concerning the former problem, the public code is a Gabidulin code distorted with a non-singular matrix with coefficients in a small subvector space of the ambient field. A conjecture was claimed in [Loi17] concerning the complexity of solving the problem, for parameters not impacted by the attack in [CC20]. In the paper we proove the conjecture and provide a more accurate evaluation of the complexity.

From the results of that [BBC+20] and from that analysis we propose new parameters sets for the OW-PKE.

First part we recall some background on rank metric and Gabidulin codes. In a second part we detail the design of the OW-PKE. In a third part we show that a way to construct a

** This work was partially supported by the French government "Investissements d'Avenir" program ANR-11-LABX-0020-01

polynomial-time decryption algorithm is to solve an underdetermined linear system. Then we show that taking into account constraints on the small dimensional vector subspace this system can be rewritten as a bilinear system. It is sufficient to specialize some variables to obtain an underdetermined system giving a solution enabling to decrypt. Finally we propose new parameters for given security targets.

2 Background on Gabidulin codes and on rank metric

Definition 1 (Rank of a vector). *Let q be the power of a prime. Let $\mathbb{F}_{q^m}$ be the finite field with q^m elements and $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$. Then the rank of $\mathbf{a}$ denoted by $Rk(\mathbf{a})$ is the dimension of the $\mathbb{F}_q$-dimensional vector subspace of $\mathbb{F}_{q^m}$ generated by the components of $\mathbf{a}$,* i.e.

$$Rk(\mathbf{a}) \stackrel{def}{=} \dim\langle a_1, \ldots, a_n\rangle_{\mathbb{F}_q}$$

As extremal object in Bose-Mesner algebra Gabidulin codes were first constructed by Delsarte. Some years later Gabidulin presented an algebraic theory as well as a polynomial-time decoding algorithm [Del78,Gab85].

Definition 2. *Let $\mathbb{F}_{q^m}$ be the finite field with q^m elements, $k \leq n \leq m$, and $\mathbf{g} = (g_1, \ldots, g_m) \in \mathbb{F}_{q^m}^n$ be a vector of rank n. Then the k-dimensional Gabidulin code with support vector $\mathbf{g}$ denoted by $\mathcal{G}_k(\mathbf{g})$ is*

$$\mathcal{G}_k(\mathbf{g}) = \left\{ \mathbf{x} \left(g_j^{[i]}\right)_{i=0,j=1}^{k-1,n} \mid \mathbf{x} \in \mathbb{F}_{q^m}^k \right\},$$

where $[i] \stackrel{def}{=} q^i$

This proposition establishes that the dual of a Gabidulin code is a Gabidulin code. Namely,

Proposition 1 ([Gab85]) *Let $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$, then there exists $\mathbf{h} \in \mathbb{F}_{q^m}^n$ of rank n such that $\mathcal{G}_{n-k}(\mathbf{h}) = \mathcal{G}_k(\mathbf{g})^\perp$ for the usual scalar product in $\mathbb{F}_{q^m}$*

3 Structure of the encryption scheme

Originally it was proposed for $q = 2$, but it can be declined for any q power of a prime. Let $\mathcal{M}_{m,n}(\mathcal{A})$, the set of $n \times m$-matrices with coefficients in $\mathcal{A}$ and $GL_n(\mathbb{F}_{q^m})$, the group of non-singular $n \times n$-matrices over $\mathbb{F}_{q^m}$.
The parameters of OW-PKE are:

- integers $k \leq n \leq m$ and $\lambda < \lfloor (n-k)/2 \rfloor$;
- a finite field $\mathbb{F}_{q^m}$.

By formalizing the scheme described in [Loi17], we have the three different standard procedures:

`KeyGen()`

1. Construct a k-dimensional Gabidulin code $\mathcal{G} \subset \mathbb{F}_{q^m}^n$.
2. Pick $\mathbf{G}$ random in the set of generator matrices for $\mathcal{G}$. A usual way to do it is to choose a matrix under canonical form, say $\left(g_j^{[i]}\right)_{i=0,j=1}^{k-1,n}$, then multiply on the left by a randomly chosen matrix in $GL_k(\mathbb{F}_{q^m})$.
3. Pick $\mathcal{V} \subset \mathbb{F}_{q^m}$ a randomly chosen λ-dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$.
4. Pick $\mathbf{P}$ randomly in $GL_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_{n,n}(\mathcal{V})$.
5. **return** $\mathbf{G}_{pub} = \mathbf{G}\mathbf{P}^{-1}$, and $\mathbf{sk} = (\mathbf{G}, \mathbf{P})$.

Suppose that $\mathbf{p} \in \mathbb{F}_{2^m}^k$ is the plaintext to be encrypted.

`Encrypt(p,`$\mathbf{G}_{pub}$`)`
1. Pick $\mathbf{e} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{Rk}(\mathbf{e}) \leq \lfloor (n-k)/2\lambda \rfloor$.
2. **return** $\mathbf{c} = \mathbf{p} \cdot \mathbf{G}_{pub} + \mathbf{e}$.

`Decrypt(c,sk)`
- **return** `Decode(`$\mathbf{c} \cdot \mathbf{P}$`,`$\mathbf{G}$`)`.

where `Decode(`$*$`,`$\mathbf{G}$`)` stands for any decoding algorithm for a Gabidulin code with generator matrix $\mathbf{G}$ decoding up to the error-correcting capability $\lfloor (n-k)/2 \rfloor$.
The public-key is $\mathbf{G}_{pub} = \mathbf{G}\mathbf{P}^{-1}$, where $\mathbf{G} \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ is a randomly chosen generator matrix of $\mathcal{G}$. We denote by $\mathcal{C}_{pub}$ the code generated by $\mathbf{G}_{pub}$.
The security of the scheme is related to the difficulty of solving the two following problems:
1. Distinguish the public-code $\mathcal{C}_{pub} = \langle \mathbf{G}_{pub} \rangle$ from a random code.
2. Solve the Rank Bounded Distance Decoding problem for a randomly generated code with the parameters of the scheme. This corresponds to be able to decode errors of rank $\lfloor (n-k)/(2\lambda) \rfloor$ in a k-dimensional code of length n with components in $\mathbb{F}_{q^m}$.

Our work addresses the security of the former problem. We proove that by enumerating $\lambda - 1$ dimensional vector subspaces of $\mathbb{F}_{2^m}$ we recover a polynomial-time decoder for $\mathcal{C}_{pub}$ on the given parameters. This naturally distinguishes $\mathcal{C}_{pub}$ from a random code.
The idea that we develop here is a natural extension of an original idea by Gabidulin, Paramonov and Tretjakov in [GPT91]. They showed that masking a Gabidulin code with a non-singular matrix $\mathbf{P}$ in the base field did not work. Namely, a decoder can be recovered in polynomial-time. In our setting, their approach corresponds to choosing a vector space $\mathcal{V}$ with $\lambda = 1$. For this parameter we have trivially the polynomial-time algorithm. Indeed, this corresponds to directly solving an overdetermined linear system with at least one solution.
More than this our work shows that the Gabidulin code itself can just be set as a parameter (this means that the matrix $\mathbf{G}$ generating $\mathcal{G}$ can be know to everyone) without loosing security. This would lead to a simplification of the key-generation procedure which could be rewritten under the form

`KeyGen()`
- Pick $\mathcal{V} \subset \mathbb{F}_{q^m}$ a randomly chosen λ-dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$.
- Pick $\mathbf{P}$ randomly in $GL_n(\mathbb{F}_{q^m}) \cap \mathcal{M}_{n,n}(\mathcal{V})$.
- **return** $\mathbf{G}_{pub} = \mathbf{pk} = \mathbf{G}\mathbf{P}^{-1}$, and $\mathbf{sk} = \mathbf{P}$.

4 Solving a linear system

Let $r \stackrel{def}{=} n - k$. To clarify the situation we denote with a hat the datas that are known to an attacker. From the knowledge of $\mathcal{C}_{pub}$, an attacker can construct a parity-check matrix, say $\widehat{\mathbf{H}}_{pub} \in \mathcal{M}_{r,n}(\mathbb{F}_{q^m})$.
From proposition 1, there exists $\mathbf{h} \in \mathbb{F}_{q^m}^n$ such that $\mathbf{H} = (\mathbf{h}^{[i]})_{i=0}^{r-1}$ is a parity-chek matrix for $\mathcal{G}$. There exists $\mathbf{S} \in GL_r(\mathbb{F}_{q^m})$, such that

$$\mathbf{S}\widehat{\mathbf{H}}_{pub} = \mathbf{H}\mathbf{P}^t, \tag{1}$$

Namely, $\mathbf{H}\mathbf{P}^t\mathbf{G}_{pub}^t = \mathbf{H}\mathbf{P}^t(\mathbf{P}^t)^{-1}\mathbf{G}^t = \mathbf{H}\mathbf{G}^t = \mathbf{0}$. Therefore $\mathbf{H}\mathbf{P}^t$ is a parity-check matrix for $\mathcal{C}_{pub}$. And any parity-check matrix can be obtained by a basis transformation induced by a non-singular matrix $\mathbf{S}$.
Without loss of generalities we fix $\alpha \in \mathbb{F}_{q^m}$ a normal element. Then

$$\mathcal{A} = \{\alpha^{[i]},\ i = 0, \ldots, m-1\}$$

is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let us define the matrix $\widehat{\mathbf{H}}_{norm} = (\alpha^{[i+j-2]})_{i=1,j=1}^{r,m}$. A straightforward proposition is

Proposition 2 *Let* $\mathbf{H} = (\mathbf{h}^{[i]})_{i=0}^{r-1}$ *be a parity check matrix for* $\mathcal{G}$ *under canonical form, there exists a* q*-ary matrix* $\mathbf{M} \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ *of rank* n *such that*

$$\mathbf{H} = \widehat{\mathbf{H}}_{norm}\mathbf{M}.$$

Proof. Let $\mathbf{h} = (h_1, \ldots, h_n)$ be the first row of $\mathbf{H}$. Then the ith column of $\mathbf{M}$ corresponds to the m-dimensional q-ary vector formed by the coordinates of h_i on the basis $\mathcal{A}$. Moreover, by construction of Gabidulin codes, $\mathbf{h}$ has maximum rank $n \leq m$, therefore, $\mathbf{M}$ has full rank. □

Now equation (1) can be rewritten as

$$\mathbf{S}\widehat{\mathbf{H}}_{pub} = \widehat{\mathbf{H}}_{norm}\underbrace{\mathbf{M}\mathbf{P}^t}_{\mathbf{T}}. \tag{2}$$

Since $\mathbf{M}$ is a q-ary matrix of full rank n and $\mathbf{P} \in GL_n(\mathcal{V})$, we have that $\mathbf{T} \in \mathcal{V}^{m\times n}$ has full rank n.
The following proposition shows that designing a polynomial-time decryption algorithm is tantamount to solving a constrained linear system.

Proposition 3 *Let* $r = n - k$ *and* $\widehat{\mathbf{H}}_{pub}$ *be a parity-check matrix for* $\mathcal{C}_{pub}$*. Let* $\alpha \in \mathbb{F}_{q^m}$ *be a normal element and* $\widehat{\mathbf{H}}_{norm} = (\alpha^{[i+j-2]})_{i=1,j=1}^{r,m}$*. Let* $\mathbf{V} \in \mathcal{M}_{r\times r}(\mathbb{F}_{q^m})$*, and* $\mathbf{W} \in \mathcal{M}_{m\times n}(\mathcal{W})$ *of rank* n *where* $\mathcal{W}$ *is an* $\mathbb{F}_q$*-vector subspace of* $\mathbb{F}_{q^m}$ *of dimension* $\leq \lambda$*, such that*

$$\mathbf{V}\widehat{\mathbf{H}}_{pub} = \widehat{\mathbf{H}}_{norm}\mathbf{W}. \tag{3}$$

Then any ciphertext can be decrypted in polynomial time.

Proof. Recall that a ciphertext is $\mathbf{c} = \mathbf{p}\cdot\mathbf{G}_{pub} + \mathbf{e} \in \mathbb{F}_{q^m}^n$, where $\mathrm{Rk}(\mathbf{e}) = \lfloor (n-k)/(2\lambda)\rfloor$. Thus $\widehat{\mathbf{H}}_{pub}\mathbf{c}^t = \widehat{\mathbf{H}}_{pub}\mathbf{e}^t$ and

$$\mathbf{V}\widehat{\mathbf{H}}_{pub}\mathbf{e}^t = \widehat{\mathbf{H}}_{norm}\underbrace{\mathbf{W}\mathbf{e}^t}_{\mathbf{e}'^t}$$

Since $\mathcal{W}$ is $\leq \lambda$-dimensional, this implies that and $\mathrm{Rk}(\mathbf{e}') \leq \lambda\mathrm{Rk}(\mathbf{e}) \leq \lfloor (n-k)/2\rfloor$. Therefore by decoding in the public Gabidulin code with parity-check matrix $\widehat{\mathbf{H}}_{norm}$, one recovers $\mathbf{e}'^t = \mathbf{W}\mathbf{e}^t$. Since $\mathbf{W}$ has rank $n \leq m$, $\mathbf{e} \mapsto \mathbf{W}^t\mathbf{e}$ is one-to-one and $\mathbf{e}$ can be uniquely recovered. The vector $\mathbf{p}$ such that $\mathbf{p}\cdot\mathbf{G}_{pub} = \mathbf{c} - \mathbf{e}$ can also be uniquely recovered. □

From proposition 3, to design a decryption algorithm – implying thus a distinguisher of the public code – it is *sufficient* to solve the linear system (3), with

- $r^2 + mn$ unknowns over $\mathbb{F}_{q^m}$. These are the coefficients $\mathbf{V}$ and $\mathbf{W}$,
- rn equations.

An attack would be thus to enumerate the solutions to the linear system. However, is over $\mathbb{F}_{q^m}$ and and the solution space is of dimension at least $r^2+(m-r)n$. Therefore, an attacker could enumerate the solutions and test the corresponding matrices $\mathbf{W}$ solution to check if their coefficients lie in some small dimensional $\mathbb{F}_q$-vector subspace of $\mathbb{F}_{q^m}$. Even if one takes into account that their maybe multiple possibilities (we do not know exactly how many), this effort lies beyond the capacities of any computer even for moderate parameters.
Moreover, this approach does not use the fact that we *a priori* know that $\mathbf{M}$ has coefficients in a small dimensional space. This additional information is used in the next section to improve the attack consisting in solving the linear system.

5 Rewriting the system

Let us consider system (3). We search for a matrix $\mathbf{W}$ whose components lie in a λ-dimensional vector space $\mathcal{W}$. Let $\mu_1, \ldots, \mu_\lambda$ be an $\mathbb{F}_q$-basis of $\mathcal{W}$. Since μ_1 is non-zero we can factorize and rewrite

$$\mathbf{W} = \mu_1 \widetilde{\mathbf{W}}$$

Solving (3) is equivalent to solve

$$\underbrace{(\mu_1^{-1}\mathbf{V})}_{\tilde{\mathbf{V}}} \widehat{\mathbf{H}}_{pub} = \widehat{\mathbf{H}}_{norm} \widetilde{\mathbf{W}}. \tag{4}$$

where the coefficients of $\widetilde{\mathbf{W}}$ are now in a λ-dimensional vectorspace

$$\widetilde{\mathcal{W}} = \langle 1, \mu_2, \ldots, \mu_\lambda \rangle_{\mathbb{F}_q}$$

Therefore, without loss of generality we assume that the first element μ_1 of the basis is known equal to 1. Now let $\widetilde{\mathbf{W}} = (w_{ij})$. For $i = 1, \ldots, m$ and $j = 1, \ldots, n$ we write the element w_{ij} on the basis $1, \mu_2, \ldots, \mu_\lambda$ and obtain

$$w_{ij} = \sum_{\ell=1}^{\lambda} b_{ij}^{(\ell)} \mu_\ell, \quad b_{ij}^{(\ell)} \in \mathbb{F}_q \tag{5}$$

Let us fix an arbitrary basis $\widehat{\mathcal{B}}$ of $\mathbb{F}_{2^m}/\mathbb{F}_2$. For any element $a \in \mathbb{F}_{q^m}$ we denote by $\boldsymbol{a}$ the m-dimensional vector of its coordinates over $\mathcal{B}$. And for any $\mu \in \mathbb{F}_{2^m}$ we denote by $\mathbf{M}_\mu$ the q-ary matrix of the multiplication by μ in the basis $\widehat{\mathcal{B}}$. That is

$$\forall a,\ \mu \in \mathbb{F}_{q^m} \text{ if } b \stackrel{def}{=} \mu a \text{ then } \boldsymbol{b} = \mathbf{M}_\mu \boldsymbol{a}$$

From now on if we state $\widetilde{\mathbf{V}} = (v_{ij})$, $\widehat{\mathbf{H}}_{pub} = (\widehat{h}_{ij})$, and $\widehat{\mathbf{H}}_{norm} = (\alpha^{[i+j-2]})$, system (4) can be rewritten under the form

$$\forall \begin{cases} i \in \{1, \ldots, r\} \\ j \in \{1, \ldots, n\} \end{cases}, \quad \sum_{u=1}^{r} \mathbf{M}_{\widehat{h}_{uj}} \boldsymbol{v_{iu}} = \sum_{u=1}^{m} \mathbf{M}_{\alpha^{[i+u-2]}} \boldsymbol{w_{uj}}$$

Formula (5) induces the following vectorial decomposition $\boldsymbol{w_{uj}} = \sum_{\ell=1}^{\lambda} b_{uj}^{(\ell)} \boldsymbol{\mu_\ell}$. Therefore

$$\forall \begin{cases} i \in \{1, \ldots, r\} \\ j \in \{1, \ldots, n\} \end{cases}, \quad \sum_{u=1}^{r} \mathbf{M}_{\widehat{h}_{uj}} \boldsymbol{v_{iu}} = \sum_{u=1,\ell=1}^{m,\lambda} b_{uj}^{(\ell)} \mathbf{M}_{\alpha^{[i+u-2]}} \boldsymbol{\mu_\ell} \tag{6}$$

6 Specializing variables

Now, system (6) has become a bilinear system where the unknowns are $\boldsymbol{v_{iu}}$, $b_{uj}^{(\ell)}$ and $\boldsymbol{\mu_\ell}$. An approach to solve it is to specialize the variables $\boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_\lambda$. They form the q-ary representations of the elements $\mu_2, \ldots, \mu_\lambda$ in the basis $\widehat{\mathcal{B}}$. System (6) thus becomes a linear system

- with rnm equations,
- with $(\lambda n + r^2)m$ unknowns.

Under the assumption that the matrix of the system looks like *random*, provided $rn > \lambda n + r^2$ it has a unique non-zero solution (1-dimensional vector space over $\mathbb{F}_q$) with high probability. For practical cryptographic applications we are always in this situation. The complexity of solving the system is thus divided into two parts

- Enumerating the variables $\boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_\lambda$. The enumeration space has size $q^{m(\lambda-1)}$.

– Solving the linear system. This costs at least a Gaussian elimination on the matrix. The complexity is estimated to be $((\lambda n + r^2)m)^\omega$ arithmetical operations in $\mathbb{F}_q$, where ω is the linear algebra constant. For practical applications it is commonly admitted that $\omega = 2.81$.

The complexity of linear algebra can be improved. First, there is no need to consider all the unknowns and equations to specialize the μ_i's. A subsystem suffices: Let $j_0 \leq n$ be the smallest integer such that

$$rj_0 \geq \lambda j_0 + r^2.$$

That is $j_0 = \lceil r^2/(r-\lambda) \rceil$. By truncating the system after the j_0 equation, we obtain

$$\forall \begin{cases} i \in \{1, \ldots, r\} \\ j \in \{1, \ldots, j_0\} \end{cases}, \quad \sum_{u=1}^{r} \mathbf{M}_{\widehat{h}_{uj}} \boldsymbol{v_{iu}} = \sum_{u=1,\ell=1}^{m,\lambda} b_{uj}^{(\ell)} \mathbf{M}_{\alpha^{[i+u-2]}} \boldsymbol{\mu_\ell} \tag{7}$$

This system is overdetermined. This gives a complexity for the linear algebra part of $((\lambda j_0 + r^2)m)^\omega$ arithmetical operations in $\mathbb{F}_q$.

We can even go one step further in reducing the complexity by noticing that the matrix of the system is sparse. Namely, the equations have weight $m(r+\lambda)$. If the system were random, the weight of one equation should be on average $\approx m(r^2 + \lambda j_0)$. This enables to then apply Wiedemann's algorithm [Wie86]. We lower bound the complexity by considering the cost of inverting a sparse square matrix of size $m(\lambda j_0 + r^2)$ corresponding to the number of unknowns with a number of non-zero coefficients roughly equal to $m^2(r+\lambda)(\lambda j_0 + r^2)$. An estimation of this lower bound is

$$m^3(r+\lambda)(\lambda j_0 + r^2)^2 \approx (mr^2)^3 \frac{r+\lambda}{(r-\lambda)^2} > m^3 r^5$$

q-ary operations.
Since $r = n - k$, we estimate a lower bound on the complexity of solving the system to be

$$m^3(n-k)^5 2^{m(\lambda-1)}$$

q-ary operations.

7 Updated parameters proposals

We update the parametres proposed in [Loi17]. In that case we have $q = 2$. We take into account both the updated evaluation for the decoding of a random code in rank metric, [BBC+20], the parameters induced by the existence of the Coggia-Couvreur attack [CC20], and the security analysis of this paper.

$m = n$	k	λ	t	PK size	CT size	Decoding.	K. Rec.
128	20	3	18	34.5 kBytes	1.8 kBytes	$\approx 2^{180}$	2^{311}
128	44	3	14	58 kBytes	1.3 kBytes	$\approx 2^{275}$	2^{308}

Table 1: Updated parameters for the OW-PKE of [Loi17]. $q = 2$. *Decoding* stands for the complexity of the best decoding algorithms among all existing, including [BBC+20] and *K. Rec.* stands for the algorithm proposed in this paper

For an equal security level, these parameters compare very favourably with LWE based submissions and with unstructured code based submissions in Hamming metric.

References

[BBC+20] M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. A. Perlner, D. Smith-Tone, J.-P. Tillich, and J. A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *ASIACRYPT 2020*, volume 12491 of *LNCS*, pages 507–536. Springer, 2020.

[CC20] D. Coggia and A. Couvreur. On the security of a Loidreau rank metric code based encryption scheme. *Des. Codes Cryptogr.*, 88(9):1941–1957, 2020.

[Del78] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Comb. Theory, Ser. A*, 25(3):226–241, 1978.

[Gab85] E. M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inf. Transm.*, 21(1):3–16, 1985.

[GPT91] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT'91*, number 547 in Lecture Notes in Comput. Sci., pages 482–489, Brighton, April 1991.

[GZ15] P. Gaborit and G. Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Inform. Theory*, 62(12):7245–7252, 2015.

[Loi17] P. Loidreau. A new rank metric codes based encryption scheme. In *PQCrypto 2017*, volume 10346 of *Lecture Notes in Computer Science*, pages 3–17. Springer, 2017.

[Wie86] D. H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inform. Theory*, page 54, 1986.