МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2026
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2026
Proceedings of the Fifty-Fifth Spring Conference
of the Union of Bulgarian Mathematicians
Tryavna, Bulgaria, April 5–9, 2026

GABIDULIN CODES BASED POST-QUANTUM ENCRYPTION SCHEMES

Pierre Loidreau

Abstract

In this paper we make a historic survey of GPT-like encryption schemes, and show that there are new promising directions in the design of encryption schemes inspired from the pioneering works.

2020 Mathematics Subject Classification: 94A60, 94-02.

Key words: Gabidulin codes, McEliece cryptosystem.

1 Introduction. The principle of rank-metric code based cryptography relying on Gabidulin codes is over 30 years old. It dates back to the seminal GPT scheme [15], built upon distorting the so-called Gabidulin codes. The original intention of the authors was to propose an encryption scheme with a public-key size one order of magnitude smaller than that of the original McEliece cryptosystem [21].

Since 2017 and the call for standardisation of Post-Quantum resistant cryptography by NIST, this subject has become of tremendous interest. Unfortunately, the original scheme and all of its evolutions up to 2017 were severely broken, making it useless for cryptography.

The seminal weakness which has been again and again exploited is the fact that Gabidulin codes are almost *Galois stable*. For short, a Gabidulin code contains a huge ($(k-2)$-dimensional were k is the dimension) vector space which is invariant under the action of the Frobenius automorphism generating the Galois group. All the proposals have been carefully attacked in [24] and in [22], for essentially all the most recent evolutions up to 2017.

So was this the end of the story? Many could have thought that it was indeed impossible to repair it. However, a paper first published at ACCT in 2016, and then at PQCrypto 2017, proposed a new method to distort the structure of Gabidulin code, such that all the preceding attacks cannot be applied, [18, 19]. This idea uses an idea developed in the design of LRPC codes, that is to know the use of a rank multiplier [16]. It consists in taking the coefficients of the inverse of the right scrambler in a fixed secret subspace of sufficiently small dimension to keep polynomial-time decoding, and sufficiently large to break the stability of the Gabidulin code through the Frobenius action.

https://doi.org/10.55630/mem.2026.55.414-422

Up to now this approach has revealed to be resistant to all the attempted cryptanalysis and permits the design of public-keys within one and two orders of magnitude shorter than that of McEliece.

The goal of this paper is to present, the masking principle and some schemes using these properties together with briefly describing the most recent approaches supporting security claims around the schemes.

2 Preliminaries on the rank metric. Rank-metric cryptography relies on codes which are $\mathbb{F}_{q^m}$-linear, where $\mathbb{F}_{q^m}$ is the finite field with q^m elements, an extension of degree m over $\mathbb{F}_q$. In this context, the *rank* (or *weight*) of a vector $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_{q^m})^n$ denoted by $\mathrm{Rk}(\mathbf{a})$ is the dimension of the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ generated by the components of $\mathbf{a}$, *i.e.*

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

Gabidulin codes were first constructed by Delsarte as extremal object in a Bose–Mesner combinatorial algebra [12]. Some years later, Gabidulin presented an algebraic theory as well as a polynomial-time decoding algorithm [14]. These codes can be viewed as analogues of Reed–Solomon codes in the rank metric, where polynomials are replaced by linearized polynomials.

Definition 2.1. *Let integers $k \leq n \leq m$ and let $\mathbf{g} = (g_1, \ldots, g_m) \in (\mathbb{F}_{q^m})^n$ such that $Rk(\mathbf{g}) = n$. The k-dimensional Gabidulin code with support vector $\mathbf{g}$ denoted by $\mathcal{G}_k(\mathbf{g})$ is defined as*

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

where $[i] \stackrel{def}{=} q^i$, stands for the ith power of the Frobenius automorphism.

There are many different types of polynomial-time algorithms enabling to decode errors up to a rank of $\lfloor (n-k)/2 \rfloor$. In the rest of the paper we select any of them and define

$$\forall \mathbf{c} \in \mathcal{G}_k(\mathbf{g}), \mathbf{e} \in (\mathbb{F}_{q^m})^n, \begin{cases} \mathtt{Decode}(\mathbf{y} = \mathbf{c} + \mathbf{e}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{c}, \text{ if } \mathrm{Rk}(\mathbf{e}) \leq \lfloor (\mathtt{n} - \mathtt{k})/2 \rfloor \\ \mathtt{Decode}(\mathbf{y}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = *, \text{ else} \end{cases}$$

Finally, the following proposition shows that the dual of a Gabidulin code is a Gabidulin code.

Proposition 2.2 ([14])**.** *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 $\mathbb{F}_{q^m}$.*

Remark 2.3. *Note that Gabidulin codes are defined with the help of the Frobenius, but one obtains the same properties by replacing it by any other generator of the Galois group of $\mathbb{F}_{q^m}/\mathbb{F}_q$, see* [3].

3 Rise and fall of GPT code based-cryptography. To be employed in the design of encryption schemes, GPT cryptosystem must be an OW-CPA encryption scheme. OW stands for one-way and CPA for *chosen plaintext attack*. This simply means that without

the secret part which is the secret key, a given ciphertext cannot be inverted to recover the corresponding plaintext in a complexity which less than exponential in the plaintext size and depending on the required security level.

Let $\mathcal{G}_k(\mathbf{g})$ be a Gabidulin code over $(\mathbb{F}_{q^m})^n$ with generator matrix $\mathbf{G} = (g_j^{[i]})$. In [22], the authors show that all the proposed evolutions of original GPT can be synthetised under the following form:

- `KeyGen` — generation of the public key ($\mathbf{pk}$) and secret key ($\mathbf{sk}$) pair
  - Pick randomly a matrix $\mathbf{X} \in (\mathbb{F}_{q^m})^{k\times \ell}$, for some integer ℓ;
  - Pick randomly $\mathbf{S} \in GL_k(\mathbb{F}_{q^m})$;
  - Pick randomly $\mathbf{P} \in GL_n(\mathbb{F}_q)$;
  - Return $\mathbf{pk} = \mathbf{G}_{pub} = \mathbf{S}(\mathbf{X}|\mathbf{G})\mathbf{P}$ and $\mathbf{sk} = (\mathbf{S}, \mathbf{P})$.
- `Encrypt`($\mathbf{G}_{pub}$, $\mathbf{x}$, $t \leq \lfloor (n-k)/2 \rfloor$)
  - Pick randomly $\mathbf{e} \in (\mathbb{F}_{q^m})^n$ of rank t;
  - Compute $\mathbf{y} = \mathbf{x}\mathbf{G}_{pub} + \mathbf{e}$;
  - Return $\mathbf{y}$.
- `Decrypt`($\mathbf{y}$,$\mathbf{sk} = (\mathbf{S}, \mathbf{P})$):
  - Compute $\mathbf{yP} = \mathbf{xSG} + \mathbf{eP}$.
  - Remove the first ℓ coordinates of $\mathbf{yP} \mapsto \widehat{\mathbf{yP}}$
  - Now $\mathrm{Rk}(\widehat{\mathbf{eP}}) \leq \mathrm{Rk}(\mathbf{eP})$, and since $\mathbf{P} \in GL_n(\mathbb{F}_q)$ we have $\mathrm{Rk}(\mathbf{eP}) = \mathrm{Rk}(\mathbf{e})$ therefore
    $$\mathtt{Decode}(\widehat{\mathbf{yP}}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{xS}$$
  - Compute $\mathbf{xS} \overset{\mathbf{S^{-1}}}{\longmapsto} \mathbf{x}$
  - Return $\mathbf{x}$.

The security of encryption schemes using GPT like systems is related to the complexity of solving two different problems.

1. Distinguish the code generated by $\mathbf{G}_{pub}$ from random;
2. Decode $\mathbf{y}$ in the code generated by $\mathbf{G}_{pub}$. This problem is usually called Rank Syndrome Decoding problem (RSD).

The Rank Syndrome decoding problem is a generic problem, since it applies with sometimes some variants to the so-called rank-metric based cryptography.

It was first seriously considered in 1996 in [8], then some improvement was made in [23], then later improved in [17].

More recently, significant breakthroughs were done in the analysis of the problem in [6, 5]. Thus, it was necessary to reconsider all of the proposed parameters until now for a given security. However, in essence this implied a moderate increase of the parameters. Since the complexity studies are kind of *ad hoc*, it is hard to present a closed formula for

estimating this complexity. However, given parameters it is not very difficult to program estimations of the complexity.

Concerning GPT-like encryption schemes, the first problem appeared to be more serious. Indeed, let us denote by $\mathcal{C}_{pub}$ the code generated by $\mathbf{G}_{pub}$ and by $\mathcal{C}_{pub}^{[i]}$ the code obtained by elevating the codewords of $\mathcal{C}_{pub}$ to the ith power of the Frobenius automorphism. A generator of $\mathcal{C}_{pub}^{[i]}$ is

$$\mathbf{G}_{pub}^{[i]} = \mathbf{S}^{[i]}(\mathbf{X}^{[i]} \mid \mathbf{G}^{[i]})\mathbf{P},$$

where $[i]$ is applied coefficientwise on the matrix elements. Then the dimension of the intersection

$$\mathcal{C}_{pub}^{\perp} \cap \left(\mathcal{C}_{pub}^{[1]}\right)^{\perp} \cap \cdots \cap \left(\mathcal{C}_{pub}^{[i]}\right)^{\perp},$$

is at least the dimension of $\mathcal{G}_k(\mathbf{g})^{\perp} \cap \cdots \cap \left(\mathcal{G}_k(\mathbf{g})^{[i]}\right)^{\perp}$, that is at least $n-k-i-1$, due to the particular structure of the underlying Gabidulin code. If the codes were randomly chosen one would expect the dimension to be $\max(n-ik, 0)$. Hence one obtains a polynomial-time distinguisher for GPT cryptosystem. Even worse, if i is sufficiently large, we generally obtain

$$\mathcal{C}_{pub}^{\perp} \cap \cdots \cap \left(\mathcal{C}_{pub}^{[i]}\right)^{\perp} = \left(\mathcal{G}_k(\mathbf{g})^{\perp} \cap \cdots \cap \left(\mathcal{G}_k(\mathbf{g})^{[i]}\right)^{\perp}\right)\mathbf{P}.$$

And provided that the codes are non-trivial some elementary linear algebra operations enable to recover a polynomial-time decoder for $\mathcal{C}_pub$ with a large probability.

More elaborate forms of right scrambler were proposed, see for instance in [13, 25]. Unfortunately for the conceivers, the former point remains true. That is, $\mathbf{G}_{pub}$ can always be rewritten under the form

$$\mathbf{G}_{pub} = \mathbf{S}^*(\mathbf{X}^* \mid \mathbf{G}^*)\mathbf{P}^*, \tag{1}$$

where $\mathbf{P}^*$ has coefficients in $\mathbb{F}_q$, and $\mathbf{G}^*$ a generator matrix for a Gabidulin code of smaller length. This nice result comes from the paper [22].

4 Rank multipliers. Relaxing optimality on the code by scrambling the columns with a non-isometry of the metric is not new. This was done for Hamming metric in the case of GRS codes [4], by using an almost permutation matrix $\mathbf{P}$ and tolerating few rows and columns to have Hamming weight 2. This property was crucial to increase the Hamming weight of the errors that one could add, but not too much so as to be in the decoding region of the parent code. However this scheme and reparations was broken in [10], by designing a distinguisher on the Hamming weight of the rows of the scrambler.

We can also adapt similar transformations to the case of rank metric: let $\alpha_1, \ldots, \alpha_\lambda \in \mathbb{F}_{q^m}$, be $\mathbb{F}_q$-linearly independent. Let

$$\mathcal{V} = \langle \alpha_1, \ldots, \alpha_\lambda \rangle_{\mathbb{F}_q}$$

be the $\mathbb{F}_q$-linear subspace generated by $\alpha_1, \ldots, \alpha_\lambda$. Let $\mathbf{P} \in GL_n(\mathcal{V})$, be a $n \times n$-non singular matrix with coefficients taken in $\mathcal{V}$. Then

Proposition 4.1 (Rank multiplication)**.** *For all* $\mathbf{x} \in (\mathbb{F}_{q^m})^n$,

$$Rk(\mathbf{xP}) \leq \lambda Rk(\mathbf{x})$$

Proof. Consider $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathbb{F}_{q^m})^n$ of rank r. Let $\langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$ be generated by $(y_1, \ldots, y_r)$. Suppose $\mathcal{V} = \langle \alpha_1, \ldots, \alpha_\lambda \rangle$, then the components of $\mathbf{xP}$, belong to the $\mathbb{F}_q$-vector space generated by $(y_i \alpha_j)_{i,j}$. It has dimension at most λr. □

The concept of *rank multiplication* can be found in [16]. The paper also introduces the notion of *Low Rank Parity-Check* codes *a.k.a* LRPC codes for cryptographic purposes. This family of codes aims at being the equivalent of LDPC codes, but for rank metric.

An immediate corollary of the proposition is

Corollary 4.2. *Let* $\mathcal{C}$ *be a* $[n, k, d]_r$ *code over* $\mathbb{F}_{q^m}$*. Let* $\mathcal{V}$ *be a* λ*-dimensional subspace of* $\mathbb{F}_{q^m}$ *seen as an* $\mathbb{F}_q$*-vector space. And let* $\mathbf{P} \in M_n(\mathcal{V})$*. Then*

$$\mathcal{C}\mathbf{P}^{-1} \stackrel{def}{=} \{\mathbf{c}\mathbf{P}^{-1} \mid \mathbf{c} \in \mathcal{C}\}$$

has dimension k *and minimum rank distance* d'*, where* $d' \geq \lfloor d/\lambda \rfloor$*.*

Proof. Since $\mathbf{P}$ is invertible, $\mathcal{C}$ and $\mathcal{C}\mathbf{P}^{-1}$ have the same dimension. Concerning the minimum distance, suppose that $d' < d/\lambda$. Then let $\mathbf{c} \in \mathcal{C}\mathbf{P}^{-1} \neq \mathbf{0}$ with rank distance d'. By construction $\mathbf{cP} \in \mathcal{C}$. But from Proposition 4.1, $\mathrm{Rk}(\mathbf{cP}) \leq d'\lambda < d$, which implies that $\mathbf{cP} = \mathbf{0}$. Thus $\mathbf{c} = \mathbf{0}$, which contradicts the hypothesis. □

Now, with this notion of rank multiplication we are able to modify the GPT encryption scheme accordingly.

- `KeyGen` — generation of the public key ($\mathbf{pk}$) and secret key ($\mathbf{sk}$) pair
  - Pick randomly $\mathbf{S} \in GL_k(\mathbb{F}_{q^m})$;
  - Pick randomly $\mathcal{V} \subset \mathbb{F}_{q^m}$, $\mathbb{F}_q$-linear of dimension λ;
  - Pick randomly $\mathbf{P} \in GL_n(\mathcal{V})$;
  - Return $\mathbf{pk} = \mathbf{G}_{pub} = \mathbf{SGP}^{-1}$ and $\mathbf{sk} = (\mathbf{S}, \mathbf{P})$
- `Encrypt`($\mathbf{G}_{pub}$, $\mathbf{x}$, $t \leq \lfloor (n-k)/(2\lambda) \rfloor$)
  - Pick randomly $\mathbf{e} \in (\mathbb{F}_{q^m})^n$ of rank t;
  - Compute $\mathbf{y} = \mathbf{xG}_{pub} + \mathbf{e}$;
  - Return $\mathbf{y}$.
- `Decrypt`($\mathbf{y}$,$\mathbf{sk} = (\mathbf{S}, \mathbf{P})$):
  - Compute $\mathbf{yP} = \mathbf{xSG} + \mathbf{eP}$.
  - Now $\mathrm{Rk}(\mathbf{eP}) \leq \lambda \mathrm{Rk}(\mathbf{e}) \leq \lfloor (n-k)/2 \rfloor$, therefore

$$\mathtt{Decode}(\mathbf{yP}, \mathcal{G}_{\mathtt{k}}(\mathbf{g})) = \mathbf{xS}$$

– Compute $\mathbf{xS} \overset{\mathbf{S}^{-1}}{\longmapsto} \mathbf{x}$

– Return $\mathbf{x}$.

A Niederreiter form can be obtained similarly to the Niederreiter idea, enabling to reduce the public-key size and the ciphertext size without losing security.

The next question to investigate is how we dimension the encryption scheme for a given security. As stated in previous section there are two types of attacks to consider:

- Concerning the decoding of $\mathbf{y}$ in the code generated by $\mathbf{G}_{pub}$, the standard approach of [6, 5] is applied;
- The problem of distinguishing the public code from random, on which we will elaborate.

In 2019 it was shown in [9] that provided

$$\lambda(n-k+1) < n,$$

the public code can be polynomially distinguished from random, by simple linear algebra techniques. It is the so-called Coggia–Couvreur distinguisher.

In the other case however whenever $\lambda(n-k+1) \geq n$, we do have only attacks exponential in essence. A first basic analysis was presented in [19], and was further improved in [20] and finally, the most up-to-date attack is [7]. The most up-to-date complexity is thus

$$P(m,n,k)q^{(\lambda-1)m-\lambda n(1-R)R}$$

where $R = k/n$ is the rate of the code, and P is a degree 5 polynomial counting the complexity of linear algebra operations. Note, that since the systems are sparse we use the complexity given by Wiedemann's algorithm.

With all the latest improvements, the parameters for 128 bits of security are given by

$m = n$	k	λ	t	**pk**	**y**
128	20	3	18	34 kB	1.8 kB
128	42	3	7	58 kB	1.3 kB

For an equivalent security if one compares with the ClassicMcEliece NIST submission for an equivalent security, then the parameters are the following, [1]:

- **pk**: 260 kB;
- **y**: 0.13 kB.

So, concerning the public-key size the gain is between 5 and 8 times. Note that in this case the parameters are computed by considering the public-key under a systematic matrix form that is to know the size is $mk(n-k)/8$ kBytes.

5 Most recent evolutions. In this section we present two recent evolutions of the system which enable to consider a wider range of parameters, still with the intention to reduce the parameters by keeping the same security.

5.1 Direct generalisation. The first approach has been presented in 2009 in [13]. The idea is to combine the use of rank multipliers with Gabidulin, Rashwan and Honary approach. It consists in multiplying on the right by a matrix $\mathbf{Q} = (\mathbf{Q}_1|\mathbf{Q}_2)$, such that $\mathbf{Q}_2 \in \mathbb{F}_q^{n\times(n-\gamma)}$ has coefficients in the base field. With this modification, the public code can be decoded up to $\lfloor (n-k-\gamma)/(2\lambda)\rfloor$.

Coggia-Couvreur distinguisher can be extended accordingly and it happens that provided

$$\lambda(n-k+1)+\gamma < n,$$

the public code can be polynomially distinguished from a random code. Moreover, if one wants to generalize the attack in [7], then this adds a significant complexity, which becomes

$$P'(m,n,k)q^{(\lambda-1)m-\lambda[n(1-R)R-\gamma R]},$$

which is $q^{\lambda\gamma R}$ more complex than the original scheme.

Thanks to this generalisation, we obtain much more interesting parameters than for the original scheme. Namely one obtains the following figures:

m	n	k	λ	γ	t	**pk**	**y**
128	89	10	2	11	17	9.5 kB	0.94 kB

5.2 Multidimensional approach. A different type of approach was published in [2]. To sum up rather than decoding one ciphertext $\mathbf{y}$, we will consider ℓ such ciphertexts $\mathbf{y}_1,\ldots,\mathbf{y}_\ell$ with the property that the coefficients of the corresponding $\mathbf{e}_1,\ldots,\mathbf{e}_\ell$ lie all in the same t-dimensional vector-space. Roughly speaking, this reduces to decode in an ℓ-interleaved Gabidulin code for which there are polynomial-time algorithms decoding errors up to a rank of

$$\left\lfloor \frac{\ell}{\ell+1}(n-k)\right\rfloor.$$

This however changes the problems that we have to consider for security.

- The RSD problem is now replaced by the so-called RSL problem (Rank Syndrome Learning with errors). The latter problem consists to decode an increasing number ℓ of codewords corrupted by errors taken all in the same t dimensional vector-space. However, ℓ has to remain rather small. Namely, [11]
  - if $\ell \geq nt$, then the problem can be solved in probabilistic polynomial-time;
  - if $\ell \geq kt$, then the problem can be solved probabilistically in subexponential-time.

  This is the reason why one has to choose $\ell < kt$.
- The decoding algorithm is probabilistic with a failure probability p_f of

  $$p_f \approx 3.5q^{-m[\ell(n-k)-(\ell+1)\lambda t+1]}.$$

  This fact has to be taken into account when designing an encryption scheme.

This gives for a security of 128 bits:

m	n	k	λ	ℓ	t	**pk**	**y**	p_f
61	50	25	3	6	7	4.8 kB	1.2 kB	2^{-242}

6 Perspectives. In this paper we only considered evolutions of the use of Gabidulin codes to design encryption schemes based on the RSD, or RSL problems. However, one can use other types of codes such as QC-LRPC codes which are structured quasi-cyclic codes with a decoding algorithm. Concerning the problem of distinguishability relative to a random quasi-cyclic codes, this raises other types of concerns. Equally, since the decoder is in essence probabilistic, then there is a failure probability that has to be taken into account in security reductions.

Another potential perspective to improve parameters consists in using an extension of rank metric such as sum-rank metric. Such a proposal is made with the use of linearized Reed–Solomon codes.

REFERENCES.

[1] M. ALBRECHT, D. J. BERNSTEIN, T. CHOU, C. CID, J. GILCHER, T. LANGE, V. MARAM, I. von MAURICH, R. MIZOCZKI, R. NIEDERHAGEN, E. PERSICHETTI, K. PATERSON, C. PETERS, P. SCHWABE, N. SENDRIER, J. SZEFER, C. J. TJHAI, M. TOMLINSON, and WANG WEN. Classic McEliece (merger of Classic McEliece and NTS-KEM. `https://classic.mceliece.org`, October 2020. Third round finalist of the NIST post-quantum cryptography call.

[2] N. ARAGON, V. DYSERYN, PH. GABORIT, P. LOIDREAU, J. RENNER, and A. WACHTER-ZEH. LowMS: a new rank metric code-based KEM without ideal structure. *Des. Codes Cryptogr.*, 92(4):1075–1093, 2024.

[3] D. AUGOT, P. LOIDREAU, and G. ROBERT. Generalized Gabidulin codes over fields of any characteristic. *Des. Codes Cryptogr.*, 86(8):1807–1848, 2018.

[4] M. BALDI, M. BIANCHI, F. CHIARALUCE, J. ROSENTHAL, and D. SCHIPANI. Enhanced public key security for the McEliece cryptosystem. *J. Cryptology*, 29(1):1–27, 2016.

[5] M. BARDET, P. BRIAUD, M. BROS, PH. GABORIT, and J.-P. TILLICH. Revisiting algebraic attacks on minrank and on the rank decoding problem. *Des. Codes Cryptogr.*, 91(11):3671–3707, 2023.

[6] M. BARDET, M. BROS, D. CABARCAS, PH. GABORIT, R. PERLNER, D. SMITH-TONE, J.-P. TILLICH, and J. VERBEL. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In *Advances in Cryptology - ASIACRYPT 2020*, pages 507–536, 2020.

[7] P. BRIAUD and P. LOIDREAU. Cryptanalysis of Rank-Metric Schemes Based on Distorted Gabidulin Codes. In T. JOHANSSON and D. SMITH-TONE, editors, *Post-Quantum Cryptography 2023*, volume 14154 of *LNCS*, pages 38–56, 2023.

[8] F. CHABAUD and J. STERN. The cryptographic security of the syndrome decoding problem for rank distance codes. In *Advances in Cryptology - ASIACRYPT 1996*, volume 1163 of *LNCS*, pages 368–381, Kyongju, Korea. Springer, November 1996.

[9] 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.

[10] A. COUVREUR, A. OTMANI, J.-P. TILLICH, and V. GAUTHIER-UMAÑA. A polynomial-time attack on the BBCRS scheme. In J. KATZ, editor, *Public-Key Cryptography - PKC 2015*, volume 9020 of *LNCS*, pages 175–193. Springer, 2015.

[11] T. DEBRIS-ALAZARD and J.-P. TILLICH. Two attacks on rank metric code-based schemes: ranksign and an identity-based-encryption scheme. In *Advances in Cryptology - ASIACRYPT 2018*, volume 11272 of *LNCS*, pages 62–92, Brisbane, Australia. Springer, December 2018.

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

[13] E. GABIDULIN, H. RASHWAN, and B. HONARY. On improving security of GPT cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 1110–1114. IEEE, 2009.

[14] E. M. GABIDULIN. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[15] 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 LNCS, pages 482–489, Brighton, April 1991.

[16] PH. GABORIT, G. MURAT, O. RUATTA, and G. ZÉMOR. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. URL: `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`.
[17] PH. GABORIT, O. RUATTA, and J. SCHREK. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Information Theory*, 62(2):1006–1019, 2016.
[18] P. LOIDREAU. An evolution of GPT cryptosystem. In *Proceedings of the 15th Algebraic and Combinatorial Theory, Albena, Bulgaria*, pages 215–220, 2016.
[19] P. LOIDREAU. A new rank metric codes based encryption scheme. In *Post-Quantum Cryptography 2017*, volume 10346 of *LNCS*, pages 3–17. Springer, 2017.
[20] P. LOIDREAU. Analysis of a public-key encryption scheme based on distorted gabidulin codes. In *Twelfth International Workshop on Coding and Cryptography, WCC 2022*, 2022. URL: `https://www.wcc2022.uni-rostock.de`.
[21] R. J. MCELIECE. *A public-key system based on algebraic coding theory.* In DSN Progress Report 44. Jet Propulsion Lab, 1978, pages 114–116.
[22] A. OTMANI, H. TALÉ-KALACHI, and S. NDJEYA. Improved cryptanalysis of rank metric schemes based on Gabidulin codes. *Des. Codes Cryptogr.*, 86(9):1983–1996, 2018.
[23] A. V. OURIVSKI and T. JOHANSSON. New technique for decoding codes in the rank metric and its cryptography applications. English. *Problems of Information Transmission*, 38(3):237–246, 2002.
[24] R. OVERBECK. Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptology*, 21(2):280–301, 2008.
[25] H. RASHWAN, E. GABIDULIN, and B. HONARY. A smart approach for GPT cryptosystem based on rank codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2463–2467. IEEE, 2010.

Pierre Loidreau
DGA MI and IRMAR, CNRS
Université de Rennes, France
e-mail: `pierre.loidreau@univ-rennes.fr`

ПОСТКВАНТОВИ КРИПТОГРАФСКИ СХЕМИ, БАЗИРАНИ НА КОДОВЕТЕ НА ГАБИДУЛИН

Pierre Loidreau

Абстракт

В тази статия правим исторически обзор на шифрови схеми от типа GPT и показваме, че съществуват нови обещаващи направления при проектирането на шифрови схеми, вдъхновени от пионерските разработки.

Ключови думи: кодове на Габидулин, криптосистема на McEliece.