

# POLYNOMIAL-TIME KEY RECOVERY ATTACK ON THE FAURE-LOIDREAU SCHEME BASED ON GABIDULIN CODES

PHILIPPE GABORIT, AYOUB OTMANI, AND HERVÉ TALÉ KALACHI

**ABSTRACT.** Encryption schemes based on the rank metric lead to small public key sizes of order of few thousands bytes which represents a very attractive feature compared to Hamming metric-based encryption schemes where public key sizes are of order of hundreds of thousands bytes even with additional structures like the cyclicity. The main tool for building public key encryption schemes in rank metric is the McEliece encryption setting used with the family of Gabidulin codes. Since the original scheme proposed in 1991 by Gabidulin, Paramonov and Tretjakov, many systems have been proposed based on different masking techniques for Gabidulin codes. Nevertheless, over the years most of these systems were attacked essentially by the use of an attack proposed by Overbeck.

In 2005 Faure and Loidreau designed a rank-metric encryption scheme which was not in the McEliece setting. The scheme is very efficient, with small public keys of size a few kiloBytes and with security closely related to the linearized polynomial reconstruction problem which corresponds to the decoding problem of Gabidulin codes. The structure of the scheme differs considerably from the classical McEliece setting and until our work, the scheme had never been attacked. We show in this article that for a range of parameters, this scheme is also vulnerable to a polynomial-time attack that recovers the private key by applying Overbeck's attack on an appropriate public code. As an example we break in a few seconds parameters with 80-bit security claim. Our work also shows that some parameters are not affected by our attack but at the cost of a lost of efficiency for the underlying schemes.

Post-quantum cryptography; Gabidulin code; Polynomial reconstruction; Faure-Loidreau scheme.

## 1. INTRODUCTION

**McEliece encryption setting.** Post-quantum cryptography aims at proposing schemes that resist to an hypothetical quantum computer. It represents more and more a serious alternative to classical cryptography based on the discrete logarithm problem and the factorization problem. McEliece opened the way to code-based cryptography by proposing the first post-quantum (public-key encryption) scheme [McE78]. The McEliece cryptosystem is in fact an encryption setting which relies on the hiding of particular class of decodable codes. The algorithmic assumption underlying the security is the difficulty of solving the closest vector problem with the Hamming metric for the particular class of masked decodable codes on which the scheme relies. Over the years many variants of the McEliece cryptosystem were proposed with different families of codes, and many were broken by recovering the structure of the masked codes. However the original family of codes, the binary Goppa codes, proposed by McEliece essentially remains unattacked. The resistance to structural attacks, which try to recover the structure of the masked codes, is the main potential weakness of this setting. For instance the highly structured Reed-Solomon codes are difficult to mask and most of McEliece variants relying on Reed-Solomon codes or variations on Reed-Solomon codes have been broken.

**Rank metric cryptography.** The McEliece cryptosystem setting is very versatile and only needs a decodable family of codes along with a particular masking technique of codes. Hence this approach

can also be used with another metric than the classical Hamming metric. An important metric emerging in cryptography is the rank metric which considers the ambient space  $\mathbb{F}^{ab}$  where  $\mathbb{F}$  is a (finite) field and  $a$  and  $b$  are positive integers, as the space of  $a \times b$  matrices so that we can associate the rank to any vector from  $\mathbb{F}^{ab}$ . By viewing any finite extension of finite fields  $\mathbb{F}/\mathbb{K}$  as a linear space over  $\mathbb{K}$  of dimension  $m > 1$  then for any positive integer  $n$ , the ambient space  $\mathbb{F}^n$  can also be viewed as the space of  $m \times n$  matrices. In [GPT91] Gabidulin, Paramonov and Tretjakov proposed the first rank-metric based encryption scheme. This scheme can be seen as an analog of the McEliece's one but based on the class of Gabidulin codes.

The main interest of the rank metric is that the time complexity of best known generic attacks for rank metric grows faster regarding the size of parameters, than for Hamming metric. In practice, without additional structure like cyclicity, it means that it is possible to obtain public key sizes for rank metric of only a few thousand bytes, when hundred of thousand bytes are needed for Hamming metric.

An important operation in the key generation of the GPT cryptosystem is the masking phase where the secret Gabidulin code  $\mathcal{G}$  undergoes a transformation to mask its inherent algebraic structure. This transformation is a probabilistic algorithm that adds some randomness to its input  $\mathcal{G}$ . Originally, the authors in [GPT91] proposed to use a *distortion* transformation that outputs (a generator matrix of) the code  $\mathcal{G} + \mathcal{R}$  where  $\mathcal{R}$  is random code with a prescribed dimension  $t_R$ . The presence of  $\mathcal{R}$  has however an impact: the sender has to add an error vector whose rank weight is  $t_{\text{pub}} = t - t_R$  where  $t$  is the error correction capability of the  $\mathcal{G}$ . Hence, roughly speaking, the hiding phase publishes a degraded code in terms of error correction.

Gabidulin codes are often seen as equivalent of Reed-Solomon codes because, like them, they are highly structured. That is the reason why their use in the GPT cryptosystem has been the subject to several attacks. Gibson was the first to prove the weakness of the system through a series of successful attacks [Gib95, Gib96]. Following these failures, the first works which modified the GPT scheme to avoid Gibson's attack were published in [GO01, GOHA03]. The idea is to hide further the structure of Gabidulin code by considering isometries for the rank metric. Consequently, a *right column scrambler*  $\mathbf{P}$  is introduced which is an invertible matrix with its entries in the base field  $\mathbb{F}_q$  while the ambient space of the Gabidulin code is  $\mathbb{F}_{q^m}^n$ . But Overbeck designed in [Ove05b, Ove05a, Ove08] a more general attack that dismantled all the existing modified GPT cryptosystems. His approach consists in applying an operator  $\Lambda_i$  which applies  $i$  times the Frobenius operation on the public generator matrix  $\mathbf{G}_{\text{pub}}$ . The dimension increases by 1 each time the Frobenius is applied. Therefore by taking  $i = n - k - 1$  the codimension becomes 1 if  $k$  is the rank of  $\mathbf{G}_{\text{pub}}$ . This phenomenon is a clearly distinguishing property of a Gabidulin code which cannot be encountered for instance with a random linear code where the dimension would increase by  $k$  for each use of the Frobenius operator.

Overbeck's attack uses crucially two important facts, namely the column scrambler matrix  $\mathbf{P}$  is defined on the base field  $\mathbb{F}_q$  and the codimension of  $\Lambda_{n-k-1}(\mathbf{G}_{\text{pub}})$  is equal to 1. Several works then proposed to resist to this attack either by taking special random codes  $\mathcal{R}$  so that the second property is not true as in [Loi10, RGH10], or by taking a column scrambler matrix defined over the extension field  $\mathbb{F}_{q^m}$  as in [Gab08, GRH09, RGH11].

But recently in [OTKN16] it was shown that even if the column scrambler is defined on the extension field as in [Gab08, GRH09, RGH11], by using precisely Overbeck's technique, it is still possible to recover very efficiently a secret Gabidulin code whose error correction  $t^*$  is certainly strictly less than the error correction of the secret original Gabidulin code but still strictly greater than the number of

added errors  $t_{\text{pub}}$ . In other words, an attacker is still able to decrypt any ciphertext and consequently, all schemes based on Gabidulin codes presented in [Gab08, GRH09, RGH11] are actually not secure.

**Faure-Loidreau’s approach.** Besides the McEliece setting used with Gabidulin codes, Faure and Loidreau proposed in [FL05] another approach for designing rank-metric encryption scheme based on Gabidulin codes. The scheme was supposed to be secure under the assumption that the problem of the *linearized polynomial reconstruction*<sup>1</sup> is intractable. This scheme follows the works done in [AF03, AFL03] where a public-key encryption scheme is defined that relies on the *polynomial reconstruction* problem which corresponds to the decoding problem of Reed-Solomon codes. The Polynomial Reconstruction (PR) consists in solving the following problem: *given two  $n$ -tuples  $(z_1, \dots, z_n)$  and  $(y_1, \dots, y_n)$  and parameters  $[n, k, w]$ , recover all polynomials  $P$  of degree less than  $k$  such that  $P(z_i) = y_i$  for at most  $w$  distinct indices  $i \in \{1, \dots, n\}$ .* The public key is then a noisy random codeword from a Reed-Solomon code where the (Hamming) weight of the error is greater than the decoding capability of the Reed-Solomon code. However the schemes have undergone polynomial-time attacks in [Cor03, Cor04, KY04]. The authors in [FL05] proposed an analog of Augot-Finiasz scheme but in the rank-metric context. The security of [FL05] is related to the difficulty of solving  $p$ -polynomial reconstruction corresponding actually to the decoding problem of a Gabidulin code beyond its error-correcting capability. After Overbeck’s attack, parameters proposed in [FL05] were updated in [Loi07, Chap. 7] in order to resist to it.

**Our results.** We show in this article that the Faure-Loidreau scheme is vulnerable to a structural polynomial-time attack that recovers the private key from the public key. Based in part on the security analysis given in [Loi07, Chap. 7], we show that by applying Overbeck’s attack on an appropriate public code an attacker can recover the private key very efficiently, only assuming a mild condition on the code, which was always true in all our experimentations.

Informally, the Faure-Loidreau encryption scheme considers three finite fields  $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{L}$ . The rank weight of vectors is computed over the field  $\mathbb{F}_q$ . The public key is then composed of a Gabidulin code of dimension  $k$  of length  $n$  defined by a matrix  $\mathbf{G} = (g_{i,j})$  with  $g_{i,j} \in \mathbb{F}_{q^m}^n$  and  $\mathbf{K} = \mathbf{x}\mathbf{G} + \mathbf{z}$  where  $\mathbf{x}$  is some vector in  $\mathbb{L}^k$  and  $\mathbf{z}$  is a vector of  $\mathbb{L}^n$  with (rank) weight  $w > \frac{1}{2}(n - k)$ . Both vectors  $\mathbf{x}$  and  $\mathbf{z}$  have to be kept secret but from attacker’s point of view the private key is *essentially*  $\mathbf{x}$  since  $\mathbf{z}$  can be deduced from it.

Our attack uses the Frobenius operator, introduced by Overbeck, which takes as input any vector space  $U \subseteq \mathbb{F}_{q^m}^n$  and integer  $i \geq 1$  in order to construct the vector space  $\Lambda_i(U)$  defined as

$$\Lambda_i(U) = U + U^q + \dots + U^{q^i}.$$

The first step of the attack considers a basis  $\gamma_1, \dots, \gamma_u$  of  $\mathbb{L}$  viewed as a vector space over  $\mathbb{F}_{q^m}$  of dimension  $u > 1$  and defines the vectors  $\mathbf{v}_i = \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{z})$ . Our main result shows that the system can be broken in polynomial time and can be stated as follows:

**Theorem 1.** *If the  $\mathbb{F}_{q^m}$ -vector space generated by  $\mathbf{v}_1, \dots, \mathbf{v}_u$  denoted by  $V$  satisfies the property*

$$\dim \Lambda_{n-w-k-1}(V) = w \tag{1}$$

*then the private key  $(\mathbf{x}, \mathbf{z})$  can be recovered from  $(\mathbf{G}, \mathbf{K})$  with  $O(n^3)$  operations in the field  $\mathbb{L}$ .*

Notice that if  $V$  behaves as random code then generally the condition (1) holds. We implemented our attack on parameters given in [FL05, Loi07] for 80-bit security, which were broken in a few seconds.

<sup>1</sup>In [FL05] the problem is termed as  $p$ -polynomial reconstruction problem.

A necessary condition for (1) to be true is to choose  $u(n - w - k) \geq w$  that is to say

$$w \leq \frac{u}{u+1}(n-k).$$

This was always the case for parameters proposed in [FL05, Loi07].

**Related work.** The attack presented in this paper is very similar to the approach proposed in [LO06] where the authors seek to decode several noisy codewords of a Gabidulin code. Let us assume that we received  $\ell$  words  $\mathbf{z}_1, \dots, \mathbf{z}_\ell$  from  $\mathbb{F}_{q^m}^n$  where each  $\mathbf{z}_i$  is written as  $z_i = \mathbf{c}_i + \mathbf{e}_i$  with  $\mathbf{c}_i$  belonging to a Gabidulin code  $\mathcal{C}$  of dimension  $k$  and length  $n$  over  $\mathbb{F}_{q^m}$  and the  $\mathbf{e}_i$ 's are vectors from  $\mathbb{F}_{q^m}^n$ . Let us denote by  $\mathbf{E}$  the matrix of size  $\ell \times n$  formed by the  $\mathbf{e}_i$ 's and let  $|\mathbf{E}|_q$  be the dimension of the  $\mathbb{F}_q$ -vector space generated by the columns of  $\mathbf{E}$ . The authors show that when  $|\mathbf{E}|_q \leq \frac{\ell}{\ell+1}(n-k)$  then Overbeck's technique recovers in  $O(n^3)$  operations the codewords  $\mathbf{c}_1, \dots, \mathbf{c}_\ell$ . It therefore provides a method that decodes a Gabidulin code beyond the classical error-correcting limit  $\frac{1}{2}(n-k)$ . This approach can be used here to attack the Faure-Loidreau scheme [FL05] because the vectors  $\mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_1 K), \dots, \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_u K)$  can be written as  $\mathbf{c}_1 + \mathbf{v}_1, \dots, \mathbf{c}_u + \mathbf{v}_u$  where  $\mathbf{c}_i = \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{x})\mathbf{G}$  belong to the Gabidulin generated by  $\mathbf{G}$  and the  $u \times n$  matrix  $\mathbf{V}$  formed by  $\mathbf{v}_1, \dots, \mathbf{v}_u$  satisfy  $|\mathbf{V}|_q = w$  which in turn has to verify  $w \leq \frac{u}{u+1}(n-k)$ .

**Organisation.** In Section 2 notation and important notions useful for our paper are given. Gabidulin codes are recalled in 3. In Section 4 we present the Faure-Loidreau scheme and in Section 5 we describe in full details our attack against it.

## 2. PRELIMINARIES

Vectors from  $\mathbb{F}^n$  where  $\mathbb{F}$  is a field are denoted by boldface letters as  $\mathbf{a} = (a_1, \dots, a_n)$ . The concatenation of two vectors  $\mathbf{u}$  and  $\mathbf{v}$  is denoted by  $(\mathbf{u} \mid \mathbf{v})$ . The set of matrices with entries in  $\mathbb{F}$  having  $m$  rows and  $n$  columns is denoted by  $\mathcal{M}_{m,n}(\mathbb{F})$  and the subset of  $n \times n$  invertible matrices form the general linear group denoted by  $\mathbf{GL}_n(\mathbb{F})$ . A *linear code*  $\mathcal{C}$  of length  $n$  over a field  $\mathbb{F}$  is a linear subspace of  $\mathbb{F}^n$ . An element of a code is called a *codeword* and a matrix whose rows form a basis is called a *generator matrix*. The *dual* of a code  $\mathcal{C} \subset \mathbb{F}^n$  is the linear space denoted by  $\mathcal{C}^\perp$  containing vectors  $\mathbf{z} \in \mathbb{F}^n$  such that:

$$\forall \mathbf{c} \in \mathcal{C}, \quad \langle \mathbf{c}, \mathbf{z} \rangle = \sum_{i=1}^n c_i z_i = 0.$$

Any generator matrix of  $\mathcal{C}^\perp$  is called a *parity-check* matrix of  $\mathcal{C}$ .

The finite field with  $q$  elements is denoted by  $\mathbb{F}_q$  where  $q$  is a power of a prime number  $p$ . The *trace operator* of  $\mathbb{F}_{q^m}$  over  $\mathbb{F}_q$  is the  $\mathbb{F}_q$ -linear map  $\mathbf{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$  defined for any  $x$  in  $\mathbb{F}_{q^m}$  by

$$\mathbf{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + \dots + x^{q^{m-1}}.$$

Let  $\mathfrak{B} = \{b_1, \dots, b_m\}$  be a basis of  $\mathbb{F}_{q^m}$  over  $\mathbb{F}_q$ . The *dual basis*, or also called the *trace orthogonal* basis of  $\mathfrak{B}$  is a basis  $\mathfrak{B}^* = \{b_1^*, \dots, b_m^*\}$  of  $\mathbb{F}_{q^m}$  over  $\mathbb{F}_q$  such that for any  $i$  and  $j$  in  $\{1, \dots, m\}$

$$\mathbf{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(b_i b_j^*) = \delta_{i,j}$$

where  $\delta_{i,i} = 1$  and  $\delta_{i,j} = 0$  when  $i \neq j$ . Note that there always exists a dual basis and furthermore it is possible to express any  $\alpha$  from  $\mathbb{F}_{q^m}$  as

$$\alpha = \sum_{i=1}^m \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha b_i^*) b_i. \quad (2)$$

Any univariate polynomial  $f \in \mathbb{F}_{q^m}[X]$  of the form  $f_0 + f_1 X^q + \dots + f_k X^{q^d}$  where  $0 \leq d < m$  is called a  $q$ -linearised polynomial and  $d$  is its  $q$ -degree.

Any map  $h : U \rightarrow V$  is naturally extended to vectors  $\mathbf{x} \in U^n$  by  $h(\mathbf{x}) = (h(\mathbf{x}_1), \dots, h(\mathbf{x}_n))$ . This applies in particular to the cases where  $h$  is a polynomial or is the Frobenius (and trace) operator. For any subsets  $U \subset \mathbb{F}^n$  and  $V \subset \mathbb{F}^n$  the notation  $U + V$  represents the set  $\{\mathbf{u} + \mathbf{v} \mid \mathbf{u} \in U \text{ and } \mathbf{v} \in V\}$ . For any subfield  $\mathbb{K} \subseteq \mathbb{F}$  and  $\mathbf{x}$  from  $\mathbb{F}^n$  the  $\mathbb{K}$ -vector space generated by  $\mathbf{x}$  is denoted by  $\mathbb{K}\mathbf{x}$ . For any  $U \subset \mathbb{F}^n$  and for any  $\mathbf{P} \in \text{GL}_n(\mathbb{K})$  the notation  $U\mathbf{P}$  is used to denote the set  $\{\mathbf{u}\mathbf{P} \mid \mathbf{u} \in U\}$ . For any subset  $V \subseteq \mathbb{F}_{q^m}^n$  and any integer  $i \geq 0$  we define  $V^{q^i}$  as the set of vectors  $\mathbf{v}^{q^i} = (v_1^{q^i}, \dots, v_n^{q^i})$  where  $\mathbf{v}$  describes  $V$ . Note that when  $V$  is a vector space then  $V^{q^i}$  is also a linear subspace of  $\mathbb{F}_{q^m}^n$ .

**Definition 2.** The *rank weight* of  $\mathbf{x} \in \mathbb{F}_{q^m}^n$  denoted by  $|\mathbf{x}|_q$  is the dimension of the  $\mathbb{F}_q$ -vector space generated by  $\{x_1, \dots, x_n\}$ , or equivalently

$$|\mathbf{x}|_q = \dim \sum_{i=1}^n \mathbb{F}_q x_i. \quad (3)$$

Note that for any  $\mathbf{x} \in \mathbb{F}^n$  with  $|\mathbf{x}|_q = w$  there exists  $\mathbf{P}$  in  $\text{GL}_n(\mathbb{F}_q)$  and  $\mathbf{x}^* \in \mathbb{F}_{q^m}^w$  such that  $\mathbf{x}\mathbf{P} = (\mathbf{x}^* \mid \mathbf{0})$  and  $|\mathbf{x}^*|_q = w$ .

Finally, an algorithm  $D : \mathbb{F}^n \rightarrow \mathcal{C}$  is said to decode  $t$  errors in a code  $\mathcal{C} \subset \mathbb{F}^n$  if for any  $\mathbf{c} \in \mathcal{C}$  and for any  $\mathbf{e} \in \mathbb{F}^n$  such that  $|\mathbf{e}|_q \leq t$  we have  $D(\mathbf{c} + \mathbf{e}) = \mathbf{c}$ . Generally, we call such a vector  $\mathbf{e}$  an *error vector*.

### 3. GABIDULIN CODES

We now introduce an important family of codes known for having an efficient decoding algorithm for the rank metric.

**Definition 3** (Gabidulin code). Let  $\mathbf{g}$  in  $\mathbb{F}_{q^m}^n$  such that  $|\mathbf{g}|_q = n$ . The Gabidulin code  $\mathcal{G}_k(\mathbf{g})$  of length  $n$  and dimension  $k$  is the  $\mathbb{F}_{q^m}$ -linear subspace of  $\mathbb{F}_{q^m}^n$  defined by

$$\mathcal{G}_k(\mathbf{g}) = \left\{ f(\mathbf{g}) \mid f = f_0 + f_1 X^q + \dots + f_k X^{q^{k-1}} \in \mathbb{F}_{q^m}[X] \right\}. \quad (4)$$

Equivalently, a generator matrix of  $\mathcal{G}_k(\mathbf{g})$  is given by  $\mathbf{G}$  where

$$\mathbf{G} = \begin{pmatrix} g_1 & \dots & g_n \\ g_1^q & \dots & g_n^q \\ \vdots & & \vdots \\ g_1^{q^{k-1}} & \dots & g_n^{q^{k-1}} \end{pmatrix}. \quad (5)$$

Gabidulin codes are known to possess a fast decoding algorithm that can decode errors of weight  $t$  provided that  $t \leq \lfloor \frac{1}{2}(n-k) \rfloor$ . Furthermore the dual of a Gabidulin code  $\mathcal{G}_k(\mathbf{g})$  is also a Gabidulin code (see for instance [Gab85, GPT91, Ber03]).

**Proposition 4.** *The dual of  $\mathcal{G}_k(\mathbf{g})$  is the Gabidulin code  $\mathcal{G}_{n-k}(\mathbf{h}^{q^{-(n-k-1)}})$  where  $\mathbf{h}$  belongs to  $\mathcal{G}_{n-1}(\mathbf{g})^\perp$  and  $|\mathbf{h}|_q = n$ .*

We also have the following proposition.

**Proposition 5.** *For any  $\mathbf{P}$  in  $\text{GL}_n(\mathbb{F}_q)$  and for any Gabidulin code  $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$  with  $|\mathbf{g}|_q = n$  then*

$$\mathcal{G}_k(\mathbf{g})\mathbf{P} = \mathcal{G}_k(\mathbf{g}\mathbf{P}). \quad (6)$$

*Proof.* The proof of this proposition comes directly from the fact that for any positive integer  $i$ , and for any  $\mathbf{P}$  in  $\text{GL}_n(\mathbb{F}_q)$ ,

$$(\mathbf{g}\mathbf{P})^{q^i} = \mathbf{g}^{q^i}\mathbf{P}$$

□

We gather important algebraic properties about Gabidulin codes in order to explain why many attacks occur when the underlying code is a Gabidulin code  $\mathcal{G}_k(\mathbf{g})$ . One key property is that Gabidulin codes can be easily distinguished from random linear codes. This singular behaviour has been precisely exploited by Overbeck [Ove05b, Ove05a, Ove08] to mount attacks. For that purpose we introduce the operator  $\Lambda_i$  defined for any linear vector subspace  $U \subseteq \mathbb{F}_{q^m}^n$  by

$$\Lambda_i(U) = U + U^q + \dots + U^{q^i}. \quad (7)$$

This operator can also be defined over matrices in an obvious manner. For instance a generator matrix of  $\mathcal{G}_k(\mathbf{g})$  is  $\Lambda_{k-1}(\mathbf{g})$ . This implies in particular the next proposition.

**Proposition 6.** *For any  $i \geq 0$ ,  $\Lambda_i(\mathcal{G}_k(\mathbf{g})) = \mathcal{G}_{k+i}(\mathbf{g})$  which implies in particular that*

$$\dim \Lambda_i(\mathcal{G}_k(\mathbf{g})) = \min\{k+i, n\}.$$

The importance of Proposition 6 becomes clear when we compare it to the case of random codes.

**Proposition 7.** *Let  $\mathcal{A} \subset \mathbb{F}_{q^m}^n$  be a code generated by a randomly drawn matrix from  $\mathcal{M}_{k,n}(\mathbb{F}_{q^m})$  then with a high probability*

$$\dim \Lambda_i(\mathcal{A}) = \min\{(i+1)k, n\} \quad (8)$$

*Remark 8.* Another way of understanding the previous proposition is to observe that if  $\mathcal{A}$  is random code then  $\dim \mathcal{A} \cap \mathcal{A}^q = 0$  whereas for Gabidulin codes we would obtain

$$\dim \mathcal{G}_k(\mathbf{g}) \cap \mathcal{G}_k(\mathbf{g})^q = k-2.$$

Thus there is property that can be computed in polynomial time such that it distinguishes between a Gabidulin code and a random code. This important fact has been used successfully in the cryptanalysis of several encryption schemes [COT14, CGG<sup>+</sup>14, OTK15].

## 4. FAURE-LOIDREAU ENCRYPTION SCHEME

**Key generation.** Throughout this step, besides the fields  $\mathbb{F}_q$  and  $\mathbb{F}_{q^m}$ , another field  $\mathbb{L}$  is considered where  $\mathbb{L}$  is the extension of  $\mathbb{F}_{q^m}$  of degree  $u > 1$ , and three integers  $k$ ,  $n$  and  $w$  such that  $u < k < n$  and

$$n - k > w > \left\lfloor \frac{n - k}{2} \right\rfloor. \quad (9)$$

- (1) Pick at random  $\mathbf{g} \in \mathbb{F}_{q^m}^n$  with  $|\mathbf{g}|_q = n$  and let  $\mathbf{G} \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$  be the generator matrix of  $\mathcal{G}_k(\mathbf{g}) \subset \mathbb{F}_{q^m}^n$  as in (5)
- (2) Pick at random  $\mathbf{x} \in \mathbb{L}^k$  such that  $\{x_{k-u+1}, \dots, x_k\}$  form a basis of  $\mathbb{L}$  over  $\mathbb{F}_{q^m}$
- (3) Generate randomly  $\mathbf{s} \in \mathbb{L}^w$  with  $|\mathbf{s}|_q = w$  and  $\mathbf{P} \in \mathbf{GL}_n(\mathbb{F}_q)$  and then compute  $\mathbf{z} \in \mathbb{L}^n$  defined as

$$\mathbf{z} = (\mathbf{s} \mid \mathbf{0}) \mathbf{P}^{-1}. \quad (10)$$

The private key is  $(\mathbf{x}, \mathbf{P})$  and the public key is  $(\mathbf{g}, k, \mathbf{K}, t_{\text{pub}})$  where

$$\mathbf{K} = \mathbf{x}\mathbf{G} + \mathbf{z} \quad \text{and} \quad t_{\text{pub}} = \left\lfloor \frac{n - w - k}{2} \right\rfloor. \quad (11)$$

**Encryption.** A plaintext here is a vector  $\mathbf{m} = (m_1, \dots, m_k)$  belonging to  $\mathbb{F}_{q^m}^k$  such that  $m_i = 0$  when  $i \in \{k - u + 1, \dots, k\}$ . To encrypt then  $\mathbf{m}$  one randomly generates  $\alpha \in \mathbb{L}$  and  $\mathbf{e} \in \mathbb{F}_{q^m}^n$  such that  $|\mathbf{e}|_q \leq t_{\text{pub}}$ . The ciphertext is the vector  $\mathbf{c} \in \mathbb{F}_{q^m}^n$  defined by

$$\mathbf{c} = \mathbf{m}\mathbf{G} + \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{K}) + \mathbf{e}. \quad (12)$$

**Decryption.** The receiver computes first  $\mathbf{c}\mathbf{P}$  that is to say

$$\mathbf{c}\mathbf{P} = \mathbf{m}\mathbf{G}\mathbf{P} + \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{x}\mathbf{G}\mathbf{P} + \alpha\mathbf{z}\mathbf{P}) + \mathbf{e}\mathbf{P} \quad (13)$$

$$= \left( \mathbf{m} + \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{x}) \right) \mathbf{G}\mathbf{P} + \left( \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{s}) \mid \mathbf{0} \right) + \mathbf{e}\mathbf{P} \quad (14)$$

Let  $\mathbf{G}'$  be the  $k \times (n - w)$  matrix obtained by removing the first  $w$  columns of  $\mathbf{G}\mathbf{P}$  and let  $\mathbf{e}'$  and  $\mathbf{c}'$  be respectively the restriction of  $\mathbf{e}\mathbf{P}$  and  $\mathbf{c}\mathbf{P}$  to the last  $n - w$  coordinates. We then have

$$\mathbf{c}' = \left( \mathbf{m} + \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{x}) \right) \mathbf{G}' + \mathbf{e}'. \quad (15)$$

Using the fact that  $\mathbf{G}'$  generates a Gabidulin code of length  $n - w$  and dimension  $k < n - w$  and since  $|\mathbf{e}'|_q \leq |\mathbf{e}|_q \leq \lfloor \frac{1}{2}(n - w - k) \rfloor$ , it is possible to recover  $\mathbf{m}' = \mathbf{m} + \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{x})$  by applying a decoding algorithm. Since by construction  $\mathbf{m} \in \mathbb{F}_{q^m}^k$  is chosen so that  $m_i = 0$  when  $i \in \{k - u + 1, \dots, k\}$  then by choosing a dual basis  $\{x_{k-u+1}^*, \dots, x_k^*\}$  of  $\{x_{k-u+1}, \dots, x_k\}$  the value of  $\alpha$  can be computed as the following

$$\sum_{i=k-u+1}^k m'_i x_i^* = \sum_{i=k-u+1}^k \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha x_i) x_i^* = \alpha.$$

Once  $\alpha$  is recovered, the plaintext  $\mathbf{m}$  is then equal to  $\mathbf{m}' - \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\alpha\mathbf{x})$ .

5. POLYNOMIAL-TIME KEY RECOVERY ATTACK WHEN  $w \leq \frac{u}{u+1}(n-k)$ 

In this section, we show that it is possible to recover an alternative private key from the public data  $\mathbf{K}$  and  $\mathbf{G}$  when the condition  $w \leq \frac{u}{u+1}(n-k)$  holds. We start by remarking that if an attacker  $\mathbb{A}$  is able to find a matrix  $\mathbf{T} \in \mathbf{GL}_n(\mathbb{F}_q)$  and  $\mathbf{z}^* \in \mathbb{L}^w$  such that

$$\mathbf{z}\mathbf{T} = (\mathbf{z}^* \mid \mathbf{0}) \text{ and } |\mathbf{z}^*|_q = w$$

then  $\mathbb{A}$  can fully recover  $\mathbf{x} \in \mathbb{L}^k$  by solving only the last  $n-w$  equations of the following linear system (see Algorithm 1 for more details)

$$\mathbf{K}\mathbf{T} = \mathbf{x}\mathbf{G}\mathbf{T} + (\mathbf{z}^* \mid \mathbf{0}). \quad (16)$$

In the sequel, we describe a way to obtain  $\mathbf{x}$  by finding such a matrix  $\mathbf{T}$ . The first step is to consider a basis  $\gamma_1, \dots, \gamma_u$  of  $\mathbb{L}$  viewed as a vector space over  $\mathbb{F}_{q^m}$  of dimension  $u > 1$ . For any  $i \in \{1, \dots, u\}$  we set  $\mathbf{K}_i = \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{K})$ . Lastly, let  $\mathcal{C}_{\text{pub}} \subset \mathbb{F}_{q^m}^n$  be the (public) code generated by  $\mathbf{K}_1, \dots, \mathbf{K}_u$  and  $\mathcal{G}_k(\mathbf{g})$ , that is to say

$$\mathcal{C}_{\text{pub}} = \mathcal{G}_k(\mathbf{g}) + \sum_{i=1}^u \mathbb{F}_{q^m} \mathbf{K}_i. \quad (17)$$

*Remark 9.*  $\mathcal{C}_{\text{pub}}$  is defined by the generator matrix  $\mathbf{G}_{\text{pub}}$  where

$$\mathbf{G}_{\text{pub}} = \begin{pmatrix} \mathbf{G} \\ \mathbf{K}_1 \\ \vdots \\ \mathbf{K}_u \end{pmatrix} \quad (18)$$

For all  $i \in \{1, \dots, u\}$  let us set  $\mathbf{v}_i = \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{z})$  and  $\mathbf{b}_i = (\mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{s}) \mid \mathbf{0}) \in \mathbb{F}_{q^m}^n$ . By construction, we also have the equality

$$\mathbf{v}_i \mathbf{P} = \mathbf{b}_i. \quad (19)$$

**Lemma 10.** *Let us define  $\mathcal{B} = \sum_{i=1}^m \mathbb{F}_{q^m} \mathbf{b}_i$  then we have*

$$\mathcal{C}_{\text{pub}} \mathbf{P} = \mathcal{G}_k(\mathbf{g}\mathbf{P}) + \mathcal{B}.$$

*Proof.* Set  $\mathbf{x}_i = \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{x}) \in \mathbb{F}_{q^m}^k$ . It is sufficient to use Proposition 5 and to observe that

$$\begin{aligned} \mathbf{K}_i \mathbf{P} &= \mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{x}) \mathbf{G}\mathbf{P} + (\mathbf{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{s}) \mid \mathbf{0}) \\ &= \mathbf{x}_i \mathbf{G}\mathbf{P} + \mathbf{b}_i \end{aligned}$$

□

**Proposition 11.** *Let  $f = n - w - k - 1$  and assume that  $\dim \Lambda_f(\mathcal{B}) = w$ . The code  $\Lambda_f(\mathcal{C}_{\text{pub}})^\perp$  is then of dimension 1 generated by  $(\mathbf{0} \mid \mathbf{h}) \mathbf{P}^T$  where  $\mathbf{h} \in \mathbb{F}_{q^m}^{n-w}$  and  $|\mathbf{h}|_q = n - w$ .*

Furthermore, for any  $\tilde{\mathbf{h}} \in \Lambda_f(\mathcal{C}_{\text{pub}})^\perp$  with  $\tilde{\mathbf{h}} \neq \mathbf{0}$  and for any  $\mathbf{T} \in \mathbf{GL}_n(\mathbb{F}_q)$  such that

$$\tilde{\mathbf{h}}(\mathbf{T}^{-1})^T = (\mathbf{0} \mid \mathbf{h}') \quad (20)$$

where  $\mathbf{h}' \in \mathbb{F}_{q^m}^{n-w}$ , there exists  $\mathbf{z}^* \in \mathbb{F}_{q^m}^w$  with  $|\mathbf{z}^*|_q = w$  such that  $\mathbf{z}\mathbf{T} = (\mathbf{z}^* \mid \mathbf{0})$ .

*Proof.* Let us decompose  $\mathbf{G}\mathbf{P}$  as  $(\mathbf{L} \mid \mathbf{R})$  where  $\mathbf{L} \in \mathcal{M}_{k,w}(\mathbb{F}_{q^m})$  and  $\mathbf{R} \in \mathcal{M}_{k,n-w}(\mathbb{F}_{q^m})$ . Let  $\mathbf{B} \in \mathcal{M}_{u,w}(\mathbb{F}_{q^m})$  be the matrix where the  $i$ -th row is composed by the  $w$  first components of  $\mathbf{b}_i$ . Note that  $\mathbf{G}_{\text{pub}}\mathbf{P}$  where  $\mathbf{G}_{\text{pub}}$  is defined as in (18) is a generator matrix of  $\mathcal{C}_{\text{pub}}\mathbf{P}$ , and the following equality holds

$$\mathbf{G}_{\text{pub}}\mathbf{P} = \begin{pmatrix} \mathbf{L} & \mathbf{R} \\ \mathbf{B} & \mathbf{0} \end{pmatrix}. \quad (21)$$

Hence  $\Lambda_f(\mathbf{G}_{\text{pub}}\mathbf{P}) = \Lambda_f(\mathbf{G}_{\text{pub}})\mathbf{P}$  is a generator matrix of the code  $\Lambda_f(\mathcal{C}_{\text{pub}}\mathbf{P}) = \Lambda_f(\mathcal{C}_{\text{pub}})\mathbf{P}$  which satisfies the equality

$$\Lambda_f(\mathbf{G}_{\text{pub}})\mathbf{P} = \begin{pmatrix} \Lambda_f(\mathbf{L}) & \Lambda_f(\mathbf{R}) \\ \Lambda_f(\mathbf{B}) & \mathbf{0} \end{pmatrix}.$$

The fact that  $\mathbf{R}$  generates an  $(n-w, k)$ -Gabidulin code implies that

$$\text{rank}(\Lambda_f(\mathbf{R})) = k + f = n - w - 1.$$

Consequently, there exists  $\mathbf{h} \in \mathbb{F}_{q^m}^{n-w}$  with  $|\mathbf{h}|_q = n - w$  that satisfies  $\Lambda_f(\mathbf{R})\mathbf{h}^T = \mathbf{0}$ . Furthermore, the equality  $\dim \Lambda_f(\mathcal{B}) = \Lambda_f(\mathbf{B})$  holds which implies that

$$\dim \Lambda_f(\mathcal{C}_{\text{pub}})\mathbf{P} = \text{rank}(\Lambda_f(\mathbf{B})) + \text{rank}(\Lambda_f(\mathbf{R})) = k + f + w = n - 1.$$

This means that  $(\mathbf{0} \mid \mathbf{h})$  generates actually the full space  $(\Lambda_f(\mathcal{C}_{\text{pub}})\mathbf{P})^\perp$  which is equivalent to say  $(\mathbf{0} \mid \mathbf{h})\mathbf{P}^T$  generates  $\Lambda_f(\mathcal{C}_{\text{pub}})^\perp$ .

For the second part of the proposition, let  $\tilde{\mathbf{h}}$  be any element from  $\Lambda_f(\mathcal{C}_{\text{pub}})^\perp$  with  $\tilde{\mathbf{h}} \neq \mathbf{0}$  and let  $\mathbf{T}$  be in  $\mathbf{GL}_n(\mathbb{F}_q)$  such that (20) holds for some  $\mathbf{h}'$  in  $\mathbb{F}_q^{n-w}$ . There exists an element  $\alpha$  in  $\mathbb{F}_{q^m}$  such that  $\tilde{\mathbf{h}} = (\mathbf{0} \mid \alpha\mathbf{h})\mathbf{P}^T$ . Consider matrices  $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3$  and  $\mathbf{A}_4$  such that  $\mathbf{A}_1 \in \mathcal{M}_{w,w}(\mathbb{F}_q)$  and  $\mathbf{A}_4 \in \mathcal{M}_{(n-w),(n-w)}(\mathbb{F}_q)$  so that we have

$$\mathbf{T}^{-1}\mathbf{P} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{A}_2 \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix}.$$

We have then the following equalities

$$(\mathbf{0} \mid \mathbf{h}') = \tilde{\mathbf{h}}(\mathbf{T}^{-1})^T = (\mathbf{0} \mid \alpha\mathbf{h})\mathbf{P}^T(\mathbf{T}^{-1})^T = (\mathbf{0} \mid \alpha\mathbf{h})(\mathbf{T}^{-1}\mathbf{P})^T \quad (22)$$

It follows from (22) that  $\mathbf{h}\mathbf{A}_2^T = \mathbf{0}$  and hence  $\mathbf{A}_2 = \mathbf{0}$  since  $|\mathbf{h}|_q = n - w$ . So we can write

$$\mathbf{T}^{-1}\mathbf{P} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{0} \\ \mathbf{A}_3 & \mathbf{A}_4 \end{pmatrix}.$$

We deduce that  $\mathbf{P}^{-1}\mathbf{T} = \begin{pmatrix} \mathbf{A}_1^{-1} & \mathbf{0} \\ -\mathbf{A}_4^{-1}\mathbf{A}_3\mathbf{A}_1^{-1} & \mathbf{A}_4^{-1} \end{pmatrix} = \begin{pmatrix} \mathbf{A}' & \mathbf{0} \\ \mathbf{C}' & \mathbf{D}' \end{pmatrix}$  and consequently, we get

$$\mathbf{z}\mathbf{T} = (\mathbf{s} \mid \mathbf{0})\mathbf{P}^{-1}\mathbf{T} = (\mathbf{s} \mid \mathbf{0}) \begin{pmatrix} \mathbf{A}' & \mathbf{0} \\ \mathbf{C}' & \mathbf{D}' \end{pmatrix} = (\mathbf{s}\mathbf{A}' \mid \mathbf{0}).$$

So by letting  $\mathbf{z}^* = \mathbf{s}\mathbf{A}' = \mathbf{s}\mathbf{A}_1^{-1}$  we have proved the proposition.  $\square$

Proposition 11 shows that an equivalent key can be found in polynomial time by simply using a non zero element of  $\Lambda_f(\mathcal{C}_{\text{pub}})^\perp$ . We now prove our main result stated in the introduction which shows the weakness of the system.

**Theorem 1.** *If the  $\mathbb{F}_{q^m}$ -vector space generated by  $\mathbf{v}_1, \dots, \mathbf{v}_u$  denoted by  $V$  satisfies the property*

$$\dim \Lambda_{n-w-k-1}(V) = w$$

*then the private key  $(\mathbf{x}, \mathbf{z})$  can be recovered from  $(\mathbf{G}, \mathbf{K})$  with  $O(n^3)$  operations in the field  $\mathbb{L}$*

*Proof.* Firstly, note that from (19) we know that  $V\mathbf{P} = \mathcal{B}$ . Algorithm 1 gives the full description of the attack and provides a proof of Theorem 1. Indeed, the attack consists in picking any codeword  $\tilde{\mathbf{h}}$  from  $\Lambda_{n-w-k-1}(\mathcal{C}_{\text{pub}})^\perp$  and then, by Gaussian elimination, we transform  $\tilde{\mathbf{h}}$  so that there exists  $\mathbf{T} \in \text{GL}_n(\mathbb{F}_q)$  for which we have

$$\tilde{\mathbf{h}}(\mathbf{T}^{-1})^T = (\mathbf{0} \mid \mathbf{h}')$$

where  $\mathbf{h}' \in \mathbb{F}_q^{n-w}$ . From Proposition 11 we know that  $\mathbf{T}$  is an equivalent key that will give an equality of the form (16), and therefore it is possible by solving a linear system to find  $\mathbf{x}$ . Lastly, the time complexity comes from the fact the operations involved are essentially Gaussian eliminations over square matrices with  $n$  columns and entries in  $\mathbb{L}$ .  $\square$

An important assumption for the success of the attack is that  $\dim \Lambda_{n-w-k-1}(\mathcal{C}_{\text{pub}})^\perp = 1$  which was always true in all our experimentations. This assumption is true if and only if the equality  $\dim \Lambda_{n-w-k-1}(\mathcal{B}) = w$  holds, which implies to have  $u(n-w-k) \geq w$ , or equivalently

$$w \leq \frac{u}{u+1}(n-k). \quad (23)$$

Assuming that  $\mathcal{B}$  behaves as a random code then  $\dim \Lambda_{n-w-k-1}(\mathcal{B}) = w$  would hold with high probability as long as (23) is true. The parameters proposed in [Loi07] satisfy (23). Furthermore, the analysis given in [Loi07] implies to take  $u \geq 3$ . We implemented the attack with Magma V2.21-6 and the secret key  $\mathbf{x}$  was found in less than 1 second confirming the efficiency of the approach.

*Remark 2.* Let us observe that taking  $w > \frac{u}{u+1}(n-k)$  implies for  $t_{\text{pub}}$  to be very small since we have

$$t_{\text{pub}} \leq \frac{1}{2}(n-w-k) < \frac{1}{2} \left( \frac{n-k}{u+1} \right). \quad (24)$$

For instance, with parameters proposed in [Loi07] we would have  $t_{\text{pub}} \leq 3$ . Consequently the values of  $n, k$  and  $m$  have to be changed so that general decoding attacks fail [GRS16]. Let us notice that this situation is quite similar to the counter-measures proposed in [RGH10, Loi10] to resist to Overbeck's attack. But the strength of this reparation deserves a thorough analysis.

TABLE 1. Bound on  $w$  with parameters taken from [Loi07] ( $m = n$ ).

$n$	$k$	$u$	$w$	$\frac{u}{u+1}(n-k)$
56	28	3	16	21
54	32	4	13	17

**Algorithm 1** Key recovery of Faure-Loidreau scheme where the public key is  $(\mathbf{G}, \mathbf{K})$ 


---

```

1:  $\{\gamma_1, \dots, \gamma_u\} \leftarrow$  arbitrary basis of  $\mathbb{L}$  viewed as a linear space over  $\mathbb{F}_{q^m}$ 
2: for all  $1 \leq i \leq u$  do
3:    $K_i \leftarrow \text{Tr}_{\mathbb{L}/\mathbb{F}_{q^m}}(\gamma_i \mathbf{K})$ 
4: end for
5: Let  $\mathcal{C}_{\text{pub}} \subset \mathbb{F}_{q^m}^n$  be the code generated by  $\mathbf{G}_{\text{pub}}$   $\triangleright \mathbf{G}_{\text{pub}}$  is defined as in (18)
6: if  $\dim \Lambda_{n-w-k-1}(\mathcal{C}_{\text{pub}})^\perp = 1$  then
7:   Pick at random  $\mathbf{h} \in \Lambda_{n-w-k-1}(\mathcal{C}_{\text{pub}})^\perp$ 
8:   Compute  $\mathbf{T} \in \text{GL}_n(\mathbb{F}_q)$  and  $\mathbf{h}' \in \mathbb{F}_{q^m}^{n-w}$  such that
      
$$\tilde{\mathbf{h}}(\mathbf{T}^{-1})^T = (\mathbf{0} \mid \mathbf{h}')$$

9:    $\mathbf{K}^* \leftarrow \mathbf{K}\mathbf{T}$   $\triangleright \mathbf{K}^* = (\mathbf{K}_1^*, \dots, \mathbf{K}_n^*) \in \mathbb{L}^n$ 
10:   $\mathbf{G}^* \leftarrow \mathbf{G}\mathbf{T}$   $\triangleright \mathbf{G}^* = (g_{i,j}^*) \in \mathcal{M}_{k,n}(\mathbb{F}_{q^m})$ 
11:  Solve the linear system where  $(X_1, \dots, X_k)$  are the unknowns
      
$$(\mathcal{L}) : \begin{cases} \mathbf{K}_{w+1}^* &= g_{1,w+1}^* X_1 + \dots + g_{k,w+1}^* X_k \\ &\vdots \\ \mathbf{K}_n^* &= g_{1,n}^* X_1 + \dots + g_{k,n}^* X_k \end{cases}$$

12:   $\mathbf{z} \leftarrow \mathbf{K} - \mathbf{x}\mathbf{G}$  where  $\mathbf{x}$  is the unique solution of  $(\mathcal{L})$ 
13: end if
14: return  $(\mathbf{x}, \mathbf{z})$ 

```

---

## 6. CONCLUSION

Faure and Loidreau proposed a rank-metric encryption scheme based on Gabidulin codes related to the problem of the linearized polynomial reconstruction. We showed that the scheme is vulnerable to a polynomial-time key recovery attack by using Overbeck's techniques applied on an appropriate public code.

Our attack assumes that parameters are chosen so that  $w \leq \frac{u}{u+1}(n-k)$  which was always the case in [FL05, Loi07]. We have also seen that taking  $w > \frac{u}{u+1}(n-k)$  implies to choose  $t_{\text{pub}} < \frac{1}{2} \left( \frac{n-k}{u+1} \right)$  which exposes further the system to general decoding attacks like [GRS16]. Hence it imposes to increase the key sizes and consequently reduces the practicability of the scheme while offering no assurance that the scheme is still secure. The best choice from a designer's point of view would be to take  $u$  as small as possible but a thorough analysis has to be undertaken in light of the connections with the reparations proposed in [RGH10, Loi10]. This point is left as an open question in our paper and breaking this kind of parameters would lead arguably to a cryptanalysis of [RGH10, Loi10], and to an algorithm that decodes Gabidulin codes beyond the bound  $\frac{u}{u+1}(n-k)$ .

## 7. ACKNOWLEDGEMENTS

The authors would like to thank Pierre Loidreau for helpful discussions and for bringing reference [LO06] to our attention.

## REFERENCES

- [AF03] Daniel Augot and Matthieu Finiasz. A public key encryption scheme based on the polynomial reconstruction problem. In *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Comput. Sci.*, pages 229–240. Springer, 2003.
- [AFL03] Daniel Augot, Matthieu Finiasz, and Pierre Loidreau. Using the trace operator to repair the polynomial reconstruction based cryptosystem presented at eurocrypt 2003. *IACR Cryptology ePrint Archive*, 2003:209, 2003.
- [Ber03] Thierry P. Berger. Isometries for rank distance and permutation group of gabidulin codes. *IEEE Trans. Inform. Theory*, 49(11):3016–3019, 2003.
- [CGG<sup>+</sup>14] Alain Couvreur, Philippe Gaborit, Valérie Gauthier-Umaña, Ayoub Otmani, and Jean-Pierre Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Des. Codes Cryptogr.*, 73(2):641–666, 2014.
- [Cor03] Jean-Sébastien Coron. Cryptanalysis of the repaired public-key encryption scheme based on the polynomial reconstruction problem. *IACR Cryptology ePrint Archive*, 2003:219, 2003.
- [Cor04] Jean-Sébastien Coron. Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem. In *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, pages 14–27, 2004.
- [COT14] Alain Couvreur, Ayoub Otmani, and Jean-Pierre Tillich. Polynomial time attack on wild McEliece over quadratic extensions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Comput. Sci.*, pages 17–39. Springer Berlin Heidelberg, 2014.
- [FL05] Cédric Faure and Pierre Loidreau. A new public-key cryptosystem based on the problem of reconstructing  $p$ -polynomials. In *Coding and Cryptography, International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005. Revised Selected Papers*, pages 304–315, 2005.
- [Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.
- [Gab08] Ernst M. Gabidulin. Attacks and counter-attacks on the GPT public key cryptosystem. *Des. Codes Cryptogr.*, 48(2):171–177, 2008.
- [Gib95] Keith Gibson. Severely denting the Gabidulin version of the McEliece public key cryptosystem. *Des. Codes Cryptogr.*, 6(1):37–45, 1995.
- [Gib96] Keith Gibson. The security of the Gabidulin public key cryptosystem. In Ueli Maurer, editor, *Advances in Cryptology - EUROCRYPT '96*, volume 1070 of *Lecture Notes in Comput. Sci.*, pages 212–223. Springer, 1996.
- [GO01] Ernst M. Gabidulin and Alexei V. Ourivski. Modified GPT PKC with right scrambler. *Electron. Notes Discrete Math.*, 6:168–177, 2001.
- [GOHA03] Ernst M. Gabidulin, Alexei V. Ourivski, Bahram Honary, and Bassem Ammar. Reducible rank codes and their applications to cryptography. *IEEE Trans. Inform. Theory*, 49(12):3289–3293, 2003.
- [GPT91] Ernst 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.
- [GRH09] Ernst Gabidulin, Haitam Rashwan, and Bahram Honary. On improving security of GPT cryptosystems. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 1110–1114. IEEE, 2009.
- [GRS16] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Information Theory*, 62(2):1006–1019, 2016.
- [KY04] Aggelos Kiayias and Moti Yung. Cryptanalyzing the polynomial-reconstruction based public-key system under optimal parameter choice. In *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, pages 401–416, 2004.
- [LO06] Pierre Loidreau and Raphael Overbeck. Decoding rank errors beyond the error-correction capability. In *Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-10*, pages 168–190, 2006.
- [Loi07] Pierre Loidreau. *Rank metric and cryptography*. Accreditation to supervise research, Université Pierre et Marie Curie - Paris VI, January 2007.
- [Loi10] Pierre Loidreau. Designing a rank metric based McEliece cryptosystem. In Nicolas Sendrier, editor, *Post-Quantum Cryptography 2010*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 142–152. Springer, 2010.

- [McE78] Robert J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.
- [OTK15] Ayoub Otmani and Hervé Talé-Kalachi. Square code attack on a modified Sidelnikov cryptosystem. In Said El Hajji, Abderrahmane Nitaj, Claude Carlet, and El Mamoun Souidi, editors, *Codes, Cryptology, and Information Security - First International Conference, C2SI 2015, Rabat, Morocco, May 26-28, 2015, Proceedings - In Honor of Thierry Berger*, volume 9084 of *Lecture Notes in Computer Science*, pages 173–183. Springer, 2015.
- [OTKN16] Ayoub Otmani, Hervé Talé-Kalachi, and Sélestin Ndjeya. Improved cryptanalysis of rank metric schemes based on Gabidulin codes. *CoRR*, abs/1602.08549, 2016.
- [Ove05a] Raphael Overbeck. Extending Gibson’s attacks on the GPT cryptosystem. In Oyvind Ytrehus, editor, *WCC 2005*, volume 3969 of *Lecture Notes in Comput. Sci.*, pages 178–188. Springer, 2005.
- [Ove05b] Raphael Overbeck. A new structural attack for GPT and variants. In *Mycrypt*, volume 3715 of *Lecture Notes in Comput. Sci.*, pages 50–63, 2005.
- [Ove08] Raphael Overbeck. Structural attacks for public key cryptosystems based on Gabidulin codes. *J. Cryptology*, 21(2):280–301, 2008.
- [RGH10] Haitam Rashwan, Ernst Gabidulin, and Bahram Honary. A smart approach for GPT cryptosystem based on rank codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2463–2467. IEEE, 2010.
- [RGH11] Haitam Rashwan, Ernst Gabidulin, and Bahram Honary. Security of the GPT cryptosystem and its applications to cryptography. *Security and Communication Networks*, 4(8):937–946, 2011.

PHILIPPE GABORIT IS WITH XLIM-DMI, UNIVERSITÉ DE LIMOGES, 123, AVENUE ALBERT THOMAS, F-87060, LIMOGES CEDEX, FRANCE.

*E-mail address:* gaborit@unilim.fr

AYOUB OTMANI AND HERVÉ TALÉ KALACHI ARE WITH THE UNIVERSITY OF ROUEN, UFR DES SCIENCES ET DES TECHNIQUES, BP 12, AVENUE DE L’UNIVERSITÉ, F-76801 SAINT-ÉTIENNE-DU-ROUVRAY CEDEX, FRANCE.

*E-mail address:* ayoub.otmani@univ-rouen.fr

HERVÉ TALÉ KALACHI IS WITH THE UNIVERSITY OF YAOUNDE I, DEPARTMENT OF MATHEMATICS, ERAL, CAMEROON.

*E-mail address:* hervekalachi@gmail.com