On a Rank-Metric Code-Based Cryptosystem with Small Key Size

Julian Renner, *Student Member, IEEE,* Sven Puchinger, *Member, IEEE,* Antonia Wachter-Zeh, *Member, IEEE*

Abstract

A repair of the Faure–Loidreau (FL) public-key code-based cryptosystem is proposed. The FL cryptosystem is based on the hardness of list decoding Gabidulin codes which are special rank-metric codes. We prove that the recent structural attack on the system by Gaborit *et al.* is equivalent to decoding an interleaved Gabidulin code. Since all known polynomial-time decoders for these codes fail for a large constructive class of error patterns, we are able to construct public keys that resist the attack. It is also shown that all other known attacks fail for our repair and parameter choices. Compared to other code-based cryptosystems, we obtain significantly smaller key sizes for the same security level.

Index Terms

code-based cryptography, rank-metric codes, interleaving, Gabidulin codes

I. Introduction

Public-key cryptography is the foundation for establishing secure communication between multiple parties. Traditional public-key algorithms such as RSA are based on the hardness of factoring large numbers or the discrete logarithm problem, but can be attacked in polynomial time once a capable quantum computer exists. Code-based public-key cryptosystems are considered to be post-quantum secure, but compared to RSA their main drawback are significantly larger key sizes.

The Faure–Loidreau (FL) code-based cryptosystem [2], [3] is based on the problem of reconstructing linearized polynomials and can be seen as linearized equivalent of the (broken) Augot–Finiasz cryptosystem [4]. While the Augot–Finiasz cryptosystem is closely connected to (list) decoding Reed–Solomon codes, the FL cryptosystem is connected to (list) decoding Gabidulin codes, a special class of rank-metric codes [5].

The main drawback of code-based cryptography compared to systems based on the factorization (e.g., RSA) or the discrete logarithm problem (e.g., the Diffie–Hellman key exchange) are large key sizes. In contrast to McEliece or Niederreiter-type cryptosystems, where the public key is a *matrix*, in the FL system, the key is only a *vector*, resulting in a much smaller key. At the time when the FL cryptosystem was designed, it was only *conjectured* that Gabidulin codes cannot be list decoded efficiently. As this was *proven* recently for many families of Gabidulin codes [6], [7], the FL system is a very promising post-quantum secure public-key cryptosystem.

However, there are attacks on the FL cryptosystem: syndrome decoding [8], an Overbeck-like attack [9] which can be avoided by choosing the parameters in a certain way (cf. [3]) and, more severe, the recent attack by Gaborit, Otmani and Talé Kalachi [10] which leaves no secure set of parameters of the system.

The main contributions of this paper are as follows. Firstly, a new coding-theoretic interpretation of the FL system is given and an alternative decryption algorithm is proposed. Secondly, it is shown that the public key can be seen as corrupted codeword of an *interleaved Gabidulin code*. Further, it is proven that the failure condition of the attack by Gaborit *et al.* [10] on the public key is equivalent to the failure condition of decoding the public key as an interleaved Gabidulin code to obtain the private key. Thirdly, a repair of the FL system is proposed. By choosing the public key in a way that the corresponding interleaved decoder is guaranteed to fail, the system is secured against the attack in [10]. We also prove that the repaired system resists all other known attacks.

The structure of this paper is as follows. In Section II, the notation is introduced and definitions are given. In Section III, the original FL system is shown and its complexity is analyzed. A new interpretation of the ciphertext and the public key is shown in Section IV. In Section V, the attack by Gaborit *et al.* [10] is recalled and its equivalence to decoding the public key as an interleaved Gabidulin is proven. Based on this proof, a repair of the system is proposed in Section VI and a security analysis of the repair is given in Section VII. In Section VIII, example parameters for security levels of 80, 128, 256 bit are proposed and compared to those of McEliece-like systems based on Goppa codes, Gabidulin codes, QC-MDPC codes and DC-LRPC codes. Conclusions are given in Section IX.

J. Renner, S. Puchinger, and A. Wachter-Zeh are with the Institute for Communications Engineering, Technical University of Munich (TUM), Germany, e-mail: {julian.renner, sven.puchinger, antonia.wachter-zeh}@tum.de.

This paper was presented in part at the IEEE International Symposium on Information Theory, 2018 [1]. J. Renner's and A. Wachter-Zeh's work was supported by the TUM—Institute for Advanced Study, funded by the German Excellence Initiative and European Union Seventh Framework Programme under Grant Agreement No. 291763. This work was partly done while S. Puchinger was with Ulm University.

II. Preliminaries

A. Notation

Let q be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_{q^m}$ its extension field of order q^m. We use $\mathbb{F}_q^{m\times n}$ to denote the set of all $m \times n$ matrices over $\mathbb{F}_q$ and $\mathbb{F}_{q^m}^n = \mathbb{F}_{q^m}^{1\times n}$ for the set of all row vectors of length n over $\mathbb{F}_{q^m}$. Further, we use another field extension $\mathbb{F}_{q^{mu}}$ with $u > 1$. Thus, $\mathbb{F}_q \subseteq \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^{mu}}$.

For a field $\mathbb{F}$, the vector space that is spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_l \in \mathbb{F}^n$ is denoted by

$$\langle \mathbf{v}_1, \ldots, \mathbf{v}_l \rangle_{\mathbb{F}} = \left\{ \sum_{i=1}^{l} a_i \mathbf{v}_i \ : \ a_i \in \mathbb{F} \right\}.$$

Denote the set of integers $[a, b] = \{i : a \leq i \leq b\}$. Rows and columns of $m \times n$-matrices are indexed by $1, \ldots, m$ and $1, \ldots, n$, where $A_{i,j}$ is the element in the i-th row and j-th column of the matrix $\mathbf{A}$. Further,

$$\mathbf{A}_{[a,b]} := \begin{pmatrix} A_{1,a} & \ldots & A_{1,b} \\ \vdots & \ddots & \vdots \\ A_{m,a} & \ldots & A_{m,b} \end{pmatrix}.$$

By $\mathrm{rank}_q(\mathbf{A})$ and $\mathrm{rank}_{q^m}(\mathbf{A})$, we denote the rank of a matrix $\mathbf{A}$ over $\mathbb{F}_q$, respectively $\mathbb{F}_{q^m}$. Let $(\gamma_1, \gamma_2, \ldots, \gamma_u)$ be an ordered basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$. By utilizing the vector space isomorphism $\mathbb{F}_{q^{mu}} \cong \mathbb{F}_{q^m}^u$, we can relate each vector $\mathbf{a} \in \mathbb{F}_{q^{mu}}^n$ to a matrix $\mathbf{A} \in \mathbb{F}_{q^m}^{u\times n}$ according to

$$\begin{aligned} \mathrm{ext}_{\boldsymbol{\gamma}} : \mathbb{F}_{q^m}^n &\to \mathbb{F}_q^{m\times n} \\ \mathbf{a} = (a_1, \ldots, a_n) &\mapsto \mathbf{A} = \begin{pmatrix} A_{1,1} & \ldots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \ldots & A_{m,n} \end{pmatrix}, \end{aligned}$$

where $\boldsymbol{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_u)$ and

$$a_j = \sum_{i=1}^{m} A_{i,j}\gamma_i, \quad \forall j \in [1, n].$$

The trace operator of a vector $\mathbf{a} \in \mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is defined by

$$\begin{aligned} \mathrm{Tr}_{q^m/q} : \mathbb{F}_{q^m}^n &\to \mathbb{F}_q^n \\ \mathbf{a} = (a_1, \ldots, a_n) &\mapsto \left(\sum_{i=0}^{m-1} a_1^{q^i}, \ldots, \sum_{i=0}^{m-1} a_n^{q^i} \right). \end{aligned}$$

A dual basis $(\gamma_1^*, \gamma_2^*, \ldots, \gamma_u^*)$ to $(\gamma_1, \gamma_2, \ldots, \gamma_u)$ is a basis that fulfills

$$\mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \gamma_j^*) = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ else} \end{cases},$$

where $i, j \in [1, u]$. Note that a dual basis always exists.

Denote by $\mathcal{M}_{s,q}(\mathbf{a}) \in \mathbb{F}_{q^m}^{s\times n}$ the $s \times n$ Moore matrix for a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_{q^m}^n$, i.e.,

$$\mathcal{M}_{s,q}(\mathbf{a}) = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1^q & a_2^q & \ldots & a_n^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{s-1}} & a_2^{q^{s-1}} & \ldots & a_n^{q^{s-1}} \end{pmatrix}.$$

If $a_1, a_2, \ldots, a_n \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$, then $\mathrm{rank}_{q^m}(\mathcal{M}_{s,q}(\mathbf{a})) = \min\{s, n\}$, cf. [11, Lemma 3.15]. This definition can also be extended to matrices by

$$\mathcal{M}_{s,q}(\mathbf{A}) = \begin{pmatrix} A_{1,1} & A_{1,2} & \ldots & A_{1,n} \\ A_{2,1} & A_{2,2} & \ldots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{l,1} & A_{l,2} & \ldots & A_{l,n} \\ A_{1,1}^q & A_{1,2}^q & \ldots & A_{1,n}^q \\ A_{2,1}^q & A_{2,2}^q & \ldots & A_{2,n}^q \\ \vdots & \vdots & \ddots & \vdots \\ A_{l,1}^{q^{s-1}} & A_{l,2}^{q^{s-1}} & \ldots & A_{l,n}^{q^{s-1}} \end{pmatrix},$$

where $\mathbf{A} \in \mathbb{F}_{q^m}^{l \times n}$.

The Gaussian binomial coefficients are denoted by

$$\begin{bmatrix} s \\ r \end{bmatrix}_q := \begin{cases} \frac{(1-q^s)(1-q^{s-1})\ldots(1-q^{s-r+1})}{(1-q)(1-q^2)\ldots(1-q^r)} & \text{for } r \leq s \\ 0 & \text{for } r > s, \end{cases}$$

where s and r are non-negative integers.

B. Rank-Metric Codes and Gabidulin Codes

The *rank norm* $\mathrm{rank}_q(\mathbf{a})$ is the rank of the matrix representation $\mathbf{A} \in \mathbb{F}_q^{m \times n}$ over $\mathbb{F}_q$. The rank distance between $\mathbf{a}$ and $\mathbf{b}$ is the rank of the difference of the two matrix representations, i.e.,

$$d_{\mathsf{R}}(\mathbf{a}, \mathbf{b}) := \mathrm{rank}_q(\mathbf{a} - \mathbf{b}) = \mathrm{rank}_q(\mathbf{A} - \mathbf{B}).$$

An $[n, k, d]_q^{\mathsf{R}}$ code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is a linear rank-metric code, i.e., it is a linear subspace of $\mathbb{F}_{q^m}^n$ of dimension k and minimum rank distance

$$d := \min_{\substack{\mathbf{a},\mathbf{b} \in \mathcal{C} \\ \mathbf{a} \neq \mathbf{b}}} \left\{ d_{\mathsf{R}}(\mathbf{a}, \mathbf{b}) = \mathrm{rank}_q(\mathbf{a} - \mathbf{b}) \right\}.$$

For linear codes with $n \leq m$, the Singleton-like upper bound [5], [12] implies that $d \leq n - k + 1$. If $d = n - k + 1$, the code is called a *maximum rank distance* (MRD) code.

Gabidulin codes [5] are a special class of rank-metric codes and can be defined by their generator matrices.

Definition 1 (Gabidulin Code [5]) *A linear $\mathcal{G}(n, k)$ code over $\mathbb{F}_{q^m}$ of length $n \leq m$ and dimension k is defined by its $k \times n$ generator matrix*

$$\mathbf{G}_{\mathcal{G}} = \mathcal{M}_{k,q}(g_1, g_2, \ldots, g_n),$$

where $\mathbf{g} = (g_1, g_2, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ and $\mathrm{rank}_q(\mathbf{g}) = n$.

In [5], it is shown that Gabidulin codes are MRD codes, i.e., $d = n - k + 1$.

For a short description on decoding of Gabidulin codes, denote by $\mathbf{C}_{\mathcal{G}} \in \mathbb{F}_q^{m \times n}$ the transmitted codeword (i.e., the matrix representation of $\mathbf{c}_{\mathcal{G}} \in \mathbb{F}_{q^m}^n$) of a $\mathcal{G}(n, k)$ code that is corrupted by an additive error $\mathbf{E} \in \mathbb{F}_q^{m \times n}$. At the receiver side, only the received matrix $\mathbf{R} \in \mathbb{F}_q^{m \times n}$, where $\mathbf{R} = \mathbf{C}_{\mathcal{G}} + \mathbf{E}$, is known. The channel might provide additional side information in the form of erasures:

- ϱ row erasures (in [13] called "deviations") and
- γ column erasures (in [13] called "erasures"),

such that the received matrix can be decomposed into

$$\mathbf{R} = \mathbf{C}_{\mathcal{G}} + \underbrace{\mathbf{A}^{(R)}\mathbf{B}^{(R)} + \mathbf{A}^{(C)}\mathbf{B}^{(C)} + \mathbf{E}}_{=\mathbf{E}_{\text{total}}}, \tag{1}$$

where $\mathbf{A}^{(R)} \in \mathbb{F}_q^{m \times \varrho}$, $\mathbf{B}^{(R)} \in \mathbb{F}_q^{\varrho \times n}$, $\mathbf{A}^{(C)} \in \mathbb{F}_q^{m \times \gamma}$, $\mathbf{B}^{(C)} \in \mathbb{F}_q^{\gamma \times n}$ are full-rank matrices, respectively, and $\mathbf{E}^{(E)} \in \mathbb{F}_q^{m \times n}$ is a matrix of rank t. The decoder knows $\mathbf{R}$ and additionally $\mathbf{A}^{(R)}$ and $\mathbf{B}^{(C)}$. Further, t denotes the number of errors without side information. The rank-metric error-erasure decoding algorithms from [13]–[15] can then reconstruct $\mathbf{c}_{\mathcal{G}} \in \mathcal{G}(n, k)$ with asymptotic complexity $\mathcal{O}(n^2)$ operations over $\mathbb{F}_{q^m}$, or in sub-quadratic complexity using the fast operations described in [16], [17], if

$$2t + \varrho + \gamma \leq d - 1 = n - k \tag{2}$$

is fulfilled.

Table I
SUMMARY OF THE PARAMETERS

Name	Use	Restriction
q	small field size	prime power
m	extension degree	$1 \leq m$
n	code length	$n \leq m$
k	code dimension	$k < n$
u	extension degree	$2 \leq u < k$
w	error weight in public key	$\max\left\{n-k-\frac{k-u}{u-1}, \left\lfloor \frac{n-k}{2} \right\rfloor + 1\right\} \leq w < \frac{u}{u+2}(n-k)$
t_{pub}	error weight in ciphertext	$t_{\mathsf{pub}} = \left\lfloor \frac{n-k-w}{2} \right\rfloor$

C. Decoding Rank Errors Beyond Half the Minimum Distance

Interleaved Gabidulin Codes are a code class for which efficient decoders are known that are able to correct errors or rank larger than $\lfloor \frac{d-1}{2} \rfloor$.

Definition 2 (Interleaved Gabidulin Codes [18]) *A linear (vertically, homogeneous) interleaved Gabidulin code $\mathcal{IG}(u; n, k)$ over $\mathbb{F}_{q^m}$ of length $n \leq m$, dimension $k \leq n$, and interleaving order u is defined by*

$$\mathcal{IG}(u; n, k) := \left\{ \begin{pmatrix} \mathbf{c}_{\mathcal{G}}^{(1)} \\ \mathbf{c}_{\mathcal{G}}^{(2)} \\ \vdots \\ \mathbf{c}_{\mathcal{G}}^{(u)} \end{pmatrix} : \mathbf{c}_{\mathcal{G}}^{(i)} \in \mathcal{G}(n,k), \forall i \in [1,u] \right\}.$$

When considering random errors of rank weight t, the code $\mathcal{IG}(u; n, k)$ can be decoded uniquely with high probability up to $t \leq \lfloor \frac{u}{u+1}(n-k) \rfloor$ errors[1], cf. [15], [18], [19]. However, it is well-known that there are many error patterns for which the known efficient decoders fail. In fact, we can explicitly construct a large class of such errors, see Lemma 6 in Section V-B.

III. THE ORIGINAL FAURE–LOIDREAU SYSTEM

In this section, the algorithms of the original FL cryptosystem are recalled and the main assumption on which the security of the system is based are explained.

A. Parameters

Let $q, m, n, k, u, w, t_{\mathsf{pub}}$ be positive integers that fulfill the restrictions given in Table I. In the following, we consider the three finite fields $\mathbb{F}_q$, $\mathbb{F}_{q^m}$, and $\mathbb{F}_{q^{mu}}$, which are extension fields of each other, respectively:

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^{mu}}.$$

B. Key Generation

The original FL key generation is shown in Algorithm 1.

Algorithm 1: Key Generation

Input: Parameters q, m, n, k, u, w as in Table I
Output: Private key $(\mathbf{x}, \mathbf{P})$, public key $(\mathbf{g}, k, \mathbf{k}_{\mathsf{pub}}, t_{\mathsf{pub}})$

Choose $\mathbf{g} \in \mathbb{F}_{q^m}^n$ at random with $\mathrm{rank}_q(\mathbf{g}) = n$
Choose $\mathbf{x} \in \mathbb{F}_{q^{mu}}^k$ at random such that $\{x_{k-u+1}, \ldots, x_k\}$ forms a basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$
Choose $\mathbf{s} \in \mathbb{F}_{q^{mu}}^w$ with $\mathrm{rank}_q(\mathbf{s}) = w$
Choose an invertible matrix $\mathbf{P} \in \mathbb{F}_q^{n \times n}$ at random
$\mathbf{G}_{\mathcal{G}} \leftarrow \mathcal{M}_{k,q}(\mathbf{g})$
$\mathbf{z} \leftarrow (\mathbf{s} \mid \mathbf{0}) \cdot \mathbf{P}^{-1}$
$\mathbf{k}_{\mathsf{pub}} \leftarrow \mathbf{x} \cdot \mathbf{G}_{\mathcal{G}} + \mathbf{z}$
$t_{\mathsf{pub}} \leftarrow \left\lfloor \frac{n-w-k}{2} \right\rfloor$
return $(\mathbf{x}, \mathbf{P})$, $(\mathbf{g}, k, \mathbf{k}_{\mathsf{pub}}, t_{\mathsf{pub}})$

[1]In this setting, an error of weight t is a $u \times n$ matrix of $\mathbb{F}_q$-rank t. Note that this means that the tall $(um) \times n$-matrix obtained by expanding the matrix component-wise over $\mathbb{F}_q$ has rank t.

C. Encryption

The encryption scheme is given in Algorithm 2.

Algorithm 2: Encryption

Input: Plaintext $\mathbf{m} = (m_1, \ldots, m_{k-u}, 0, \ldots, 0) \in \mathbb{F}_{q^m}^k$, public key $(\mathbf{g}, k, \mathbf{k}_{\mathsf{pub}}, t_{\mathsf{pub}})$
Output: Ciphertext $\mathbf{c}$

1 Choose $\alpha \in \mathbb{F}_{q^{mu}} \setminus \{0\}$ at random
2 Choose $\mathbf{e} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{rank}_q(\mathbf{e}) = t_{\mathsf{pub}}$ at random
3 $\mathbf{G}_{\mathcal{G}} \leftarrow \mathcal{M}_{k,q}(\mathbf{g})$
4 **return** $\mathbf{c} \leftarrow \mathbf{m} \cdot \mathbf{G}_{\mathcal{G}} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{k}_{\mathsf{pub}}) + \mathbf{e}$.

D. Decryption

The decryption method is shown in Algorithm 3.

Algorithm 3: Decryption

Input: Ciphertext $\mathbf{c}$, private key $(\mathbf{x}, \mathbf{P})$
Output: Plaintext $\mathbf{m}$

1 $\mathbf{c}' \leftarrow \mathbf{c}\mathbf{P}_{[w+1,n]}$
2 $\mathcal{G}' \leftarrow$ Gabidulin code generated by $\mathbf{G}_{\mathcal{G}}\mathbf{P}_{[w+1,n]}$
3 $\mathbf{m}' \leftarrow$ decode $\mathbf{c}'$ in $\mathcal{G}'$
4 $\alpha \leftarrow \sum_{i=k-u+1}^{k} m'_i x_i^*$
5 **return** $\mathbf{m} \leftarrow \mathbf{m}' - \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x})$

Theorem 1 (Correctness [2]) *Algorithm 3 returns the correct plaintext* $\mathbf{m}$.

Proof: Line 1 computes

$$\mathbf{c}\mathbf{P} = (\mathbf{m} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x}))\mathbf{G}_{\mathcal{G}}\mathbf{P} + (\mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{s})|\mathbf{0}) + \mathbf{e}\mathbf{P},$$

whose last $n - w$ columns are given by

$$\mathbf{c}' = (\mathbf{m} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x}))\mathbf{G}' + \mathbf{e}',$$

where $\mathbf{G}' := \mathbf{G}_{\mathcal{G}}\mathbf{P}_{[w+1,n]} \in \mathbb{F}_{q^m}^{k \times (n-w)}$ and $\mathbf{e}' := \mathbf{e}\mathbf{P}_{[w+1,n]}$. By decoding in $\mathcal{G}'$, we thus obtain the vector

$$\mathbf{m}' = \mathbf{m} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x}).$$

Since the last u positions of the plaintext $\mathbf{m}$ are zero (i.e., $m_i = 0$ for $i = k - u + 1, \ldots, k$), we get $\alpha = \sum_{i=k-u+1}^{k} m'_i x_i^*$, where $\{x_{k-u+1}^*, \ldots, x_k^*\}$ is a dual basis to $\{x_{k-u+1}, \ldots, x_k\}$. The latter observation is technical to prove. As we know α and $\mathbf{x}$, we can therefore compute the plaintext $\mathbf{m}$. ∎

E. Complexity

It is essential for a cryptosystem that key generation, encryption, and decryption can be implemented fast. The following results were not known when the original FL system was proposed, but have a major impact on its efficiency.

The complexity of key generation and encryption is dominated by the cost of encoding in a Gabidulin code (Line 7 of Algorithm 1 and Line 4 of Algorithm 2).[2] The asymptotically fastest-known algorithms [16], [17] for this require

- $O^{\sim}(n^{\min\{\frac{\theta+1}{2}, 1.635\}})$ operations in $\mathbb{F}_{q^m}$ in general and
- $O^{\sim}(n)$ operations in $\mathbb{F}_{q^m}$ if the entries of $\mathbf{g}$ form a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$,

where θ is the matrix multiplication exponent and $O^{\sim}$ means that $\log$ factors are neglected.

The bottleneck of decryption is (error-erasure-) decoding in a Gabidulin code (Line 3 of Algorithm 3, see also Section IV-A below), where the asymptotically fastest algorithm costs

$$O^{\sim}\left(n^{\min\{\frac{\theta+1}{2}, 1.635\}}\right)$$

operations in $\mathbb{F}_{q^m}$ [16], [17].

For small lengths n, the algorithms in [20]–[22], which have quadratic complexity over $\mathbb{F}_{q^m}$ (or cubic complexity over $\mathbb{F}_q$), might be faster than the mentioned algorithms due to smaller hidden constants in the O-notation.

[2]Note that since $\mathbf{x}$ and $\mathbf{z}$ have coefficients in the large field $\mathbb{F}_{q^{mu}}$, this line can be realized as encoding and corruption of u messages over $\mathbb{F}_{q^m}$ with the generator matrix $\mathbf{G}_{\mathcal{G}} \in \mathbb{F}_{q^m}^{k \times n}$ (see also Section IV-B below).

F. Assumption of the FL System

The security of the system is based on the assumption that it is computationally infeasible to retrieve any part of the private key $(\mathbf{x}, \mathbf{P})$ given the public key and the ciphertext. As soon as the attacker knows one part of it, he is able to find an alternative private key efficiently. E.g., if the vector $\mathbf{x}$ is known, one can compute $\mathbf{z} = \mathbf{k}_{\mathsf{pub}} - \mathbf{x}\mathbf{G}_{\mathcal{G}}$ and an invertible matrix $\hat{\mathbf{P}} \in \mathbb{F}_q^{n\times n}$ such that $\mathbf{z}\hat{\mathbf{P}} = (\hat{\mathbf{s}} \mid \mathbf{0})$. Then, the attacker simply applies the decryption algorithm using $(\mathbf{x}, \hat{\mathbf{P}})$ as private key to retrieve the plaintext from the ciphertext.

IV. Coding-Theoretic Interpretation of the Original Faure–Loidreau System

We present two coding-theoretic interpretations of the Faure–Loidreau system, which—to the best of our knowledge—have not been observed before.

A. Decryption as Error-Erasure Decoding

Lemma 2 *Fix a basis γ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then, the matrix representation of the ciphertext can be written in the form*

$$\operatorname{ext}_\gamma(\mathbf{c}) = \mathbf{C}_{\mathcal{G}} + \mathbf{A}^{(C)}\mathbf{B}^{(C)} + \mathbf{E}, \tag{3}$$

where

$$\mathbf{C}_{\mathcal{G}} = \operatorname{ext}_\gamma([\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})] \cdot \mathbf{G}_{\mathcal{G}}) \in \mathbb{F}_q^{m\times n}$$

is unknown and a codeword of a Gabidulin code,

$$\mathbf{A}^{(C)} = \operatorname{ext}_\gamma(\operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{s})) \in \mathbb{F}_q^{m\times w}$$

is unknown,

$$\mathbf{B}^{(C)} = (\mathbf{P}^{-1})_{[1,\dots,w]} \in \mathbb{F}_q^{w\times n}$$

is known and

$$\mathbf{E} = \operatorname{ext}_\gamma(\mathbf{e}) \in \mathbb{F}_q^{m\times n}$$

is unknown.

Proof: Due to the $\mathbb{F}_{q^m}$-linearity of the trace map $\operatorname{Tr}_{q^{mu}/q^m}$ and the fact that the entries of the matrices $\mathbf{G}_{\mathcal{G}}$ and $\mathbf{P}^{-1}$ are in $\mathbb{F}_{q^m}$, we can write the ciphertext as follows.

$$\begin{aligned}
\mathbf{c} &= \mathbf{m}\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{k}_{\mathsf{pub}}) + \mathbf{e} \\
&= \mathbf{m}\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x}\mathbf{G}_{\mathcal{G}} + \alpha\mathbf{z}) + \mathbf{e} \\
&= \left[\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})\right]\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{z}) + \mathbf{e} \\
&= \left[\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})\right]\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha(\mathbf{s} \mid \mathbf{0})\mathbf{P}^{-1}) + \mathbf{e} \\
&= \left[\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})\right]\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{s}(\mathbf{P}^{-1})_{[1,w]}) + \mathbf{e} \\
&= \left[\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})\right]\mathbf{G}_{\mathcal{G}} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{s})(\mathbf{P}^{-1})_{[1,w]} + \mathbf{e}.
\end{aligned}$$

Since the entries of $(\mathbf{P}^{-1})_{[1,\dots,w]}$ are in $\mathbb{F}_q$, the expansion of the ciphertext into the $\mathbb{F}_q$-basis γ of $\mathbb{F}_{q^m}$ can be written as in (3) above. ∎

Theorem 3 *The message vector $\mathbf{m}$ can be reconstructed by the error-erasure decoders in [13]–[15] (as well as their speed-up in [16], [17]) and Steps 4 and 5 of Algorithm 3.*

Proof: As seen in Lemma 2, we can decompose the matrix representation of the ciphertext into a codeword plus an error that is partially known. In fact, the decomposition is of the form as in (1) (see Section II-B), so $\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})$ can be reconstructed by the error-erasure decoders in [13]–[15] since the decoding condition (2) reads as

$$w + 2\operatorname{rank}_q(\mathbf{E}) = w + 2t_{\mathsf{pub}} \le n - k$$

in this case and is fulfilled by Table I.

The message $\mathbf{m}$ can then be recovered from $\mathbf{m} + \operatorname{Tr}_{q^{mu}/q^m}(\alpha\mathbf{x})$ using the same steps as in Algorithm 3. ∎

Theorem 3 leads to the following observation. The ciphertext is a codeword plus an error of rank weight $w + t_{\mathsf{pub}}$, which is beyond the unique decoding radius. The legitimate receiver can only decrypt since she knows the (w-dimensional) row space of a part of the error. Although the attacker knows the code, she cannot recover the message since she has no further knowledge about the structure of the error. Note the difference to the code-based McEliece cryptosystem, where the security relies on the

fact that an attacker does not know the structure of the code. We will turn this observation into an exponential-time message attack in Section VII-C, which we will consider in our parameter choice.

Furthermore, the procedure implied by Theorem 3 might have a practical advantage compared to the original decryption algorithm. The code $\mathcal{G}'$ used for decoding in Algorithm 3 depends on the private key. In Theorem 3, the code is given by $\mathbf{g}$, which is public and in fact does not need to be chosen randomly in the key generation.[3] Depending on the used algorithm and type of implementation (e.g., in hardware), it can be advantageous in terms of complexity or implementation size if the code is fixed.

B. Public Key as Corrupted Interleaved Codeword

Our second observation is that the public key $\mathbf{k}_{\mathsf{pub}}$ of the cryptosystem is a corrupted codeword of an interleaved Gabidulin code. To our knowledge, this connection between the public key and interleaved Gabidulin codes has not been known before. This interpretation is central to this paper and will be used in Section V-B to derive a modification of the public key that is not vulnerable against the attacks described in Section V.

Theorem 4 *Fix a basis γ of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$. Let γ^* be a dual basis to γ and write $\mathbf{k}_{\mathsf{pub}} = \sum_{i=1}^{u} \mathbf{k}_{\mathsf{pub}}^{(i)} \gamma_i^*$. Then,*

$$\begin{pmatrix} \mathbf{k}_{\mathsf{pub}}^{(1)} \\ \mathbf{k}_{\mathsf{pub}}^{(2)} \\ \vdots \\ \mathbf{k}_{\mathsf{pub}}^{(u)} \end{pmatrix} = \begin{pmatrix} \mathbf{c}_{\mathcal{G}}^{(1)} \\ \mathbf{c}_{\mathcal{G}}^{(2)} \\ \vdots \\ \mathbf{c}_{\mathcal{G}}^{(u)} \end{pmatrix} + \begin{pmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \\ \vdots \\ \mathbf{z}_u \end{pmatrix}, \tag{4}$$

where the $\mathbf{c}_{\mathcal{G}}^{(i)} \in \mathbb{F}_{q^m}^n$ are codewords of the Gabidulin code $\mathcal{G}(n,k)$ with generator matrix $\mathbf{G}_{\mathcal{G}}$ and the $\mathbf{z}_i \in \mathbb{F}_{q^m}^n$ are obtained from the vector $\mathbf{z} \in \mathbb{F}_{q^{mu}}^n$ by $\mathbf{z} = \sum_{i=1}^{u} \mathbf{z}_i \gamma_i^*$.

Proof: Recall the definition of the public key

$$\mathbf{k}_{\mathsf{pub}} = \mathbf{x} \cdot \mathbf{G}_{\mathcal{G}} + \mathbf{z},$$

where $\mathbf{x} \in \mathbb{F}_{q^{mu}}^k$, $\mathbf{G}_{\mathcal{G}} \in \mathbb{F}_{q^m}^{k \times n}$ is the generator matrix of a $\mathcal{G}(n,k)$ code, and $\mathbf{z} \in \mathbb{F}_{q^{mu}}^n$ with $\mathrm{rank}_q(\mathbf{z}) = w$. Let $\mathbf{x} = \sum_{i=1}^{u} \mathbf{x}_i \gamma_i^*$, where the $\mathbf{x}_i$ have coefficients in $\mathbb{F}_{q^m}$.

Then, we obtain the following representation of the public key $\mathbf{k}_{\mathsf{pub}}$ as a $u \times n$ matrix in $\mathbb{F}_{q^m}$

$$\begin{pmatrix} \mathbf{k}_{\mathsf{pub}}^{(1)} \\ \mathbf{k}_{\mathsf{pub}}^{(2)} \\ \vdots \\ \mathbf{k}_{\mathsf{pub}}^{(u)} \end{pmatrix} = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_u \end{pmatrix} \cdot \mathbf{G}_{\mathcal{G}} + \begin{pmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \\ \vdots \\ \mathbf{z}_u \end{pmatrix} = \begin{pmatrix} \mathbf{x}_1 \cdot \mathbf{G}_{\mathcal{G}} \\ \mathbf{x}_2 \cdot \mathbf{G}_{\mathcal{G}} \\ \vdots \\ \mathbf{x}_u \cdot \mathbf{G}_{\mathcal{G}} \end{pmatrix} + \begin{pmatrix} \mathbf{z}_1 \\ \mathbf{z}_2 \\ \vdots \\ \mathbf{z}_u \end{pmatrix}.$$

Since $\mathbf{x}_i \cdot \mathbf{G}_{\mathcal{G}}$ is a codeword of a $\mathcal{G}(n,k)$ code, $\forall i \in [1,u]$, the matrix representation of $\mathbf{k}_{\mathsf{pub}}$ can be seen as a codeword from an $\mathcal{IG}(u;n,k)$ code, corrupted by an error. ∎

Note that the error $(\mathbf{z}_1^\top, \ldots, \mathbf{z}_u^\top)^\top$ in (4) has $\mathbb{F}_q$-rank at most w due to the structure of $\mathbf{z} = (\mathbf{s} \mid \mathbf{0})\mathbf{P}^{-1}$.

V. Efficient Structural Attacks

Among all known attacks on the original FL cryptosystem, there are only two that are considered to be efficient. These two structural attacks on the original FL system provide an alternative private key in polynomial time and are shown in this section. The first one was proposed by Gaborit, Otmani and Talé Kalachi in [10], whereas the second is new and is derived. Further, it is proven that the failure conditions of both attacks are equivalent.

A. GOT Attack

The attack shown in Algorithm 4 was proposed by Gaborit, Otmani, and Talé Kalachi in [10, Algo. 1]. It determines an (alternative) private key that can be used in Algorithm 3 and it is herein referred to as GOT Attack.

[3]Note that we described the key generation as in [2], where $\mathbf{g}$ is chosen at random, but this is not necessary for the security of the system.

Algorithm 4: GOT Attack

Input: Public key $(\mathbf{g}, k, \mathbf{k}_{\mathsf{pub}}, t_{\mathsf{pub}})$
Output: Private key $(\mathbf{x}, \mathbf{P})$

Choose $\gamma_1, \ldots, \gamma_u$ to be a basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$

$\mathbf{k}_{\mathsf{pub}}^{(i)} \leftarrow \mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \mathbf{k}_{\mathsf{pub}})$ for all $i = 1, \ldots, u$

$\mathbf{G}_{\mathcal{G}} \leftarrow \mathcal{M}_{k,q}(\mathbf{g})$

Pick at random a non-zero vector $\tilde{\mathbf{h}} \in \mathbb{F}_{q^m}^n$ such that

$$\mathcal{M}_{n-w-k,q}\left(\begin{pmatrix}\mathbf{G}_{\mathcal{G}}\\ \mathbf{k}_{\mathsf{pub}}^{(1)}\\ \vdots \\ \mathbf{k}_{\mathsf{pub}}^{(u)}\end{pmatrix}\right)\tilde{\mathbf{h}}^{\mathrm{T}} = \mathbf{0}.$$

Choose $\mathbf{P} \in \mathbb{F}_q^{n\times n}$ and $\mathbf{h}' \in \mathbb{F}_{q^m}^{n-w}$ such that $\tilde{\mathbf{h}}\left(\mathbf{P}^{-1}\right)^{\mathrm{T}} = (\ \mathbf{0} \mid \mathbf{h}')$

Choose $\mathbf{x}$ such that $\mathbf{x}\mathbf{G}_{\mathcal{G}}\mathbf{P}' = \mathbf{k}_{\mathsf{pub}}\mathbf{P}'$, where $\mathbf{P}' = \mathbf{P}_{[w+1,n]} \in \mathbb{F}_q^{n\times(n-w)}$

return $(\mathbf{x}, \mathbf{P})$

The key recovery shown in Algorithm 4 on the FL system succeeds under the conditions of the following theorem.

Theorem 5 (GOT Attack [10, Thm. 1]) *Let $\gamma_1, \ldots, \gamma_u \in \mathbb{F}_{q^{mu}}$ be a basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$ and let $\mathbf{z}_i = \mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \mathbf{z})$, for $i = 1, \ldots u$.*

If the matrix $\mathbf{Z} \in \mathbb{F}_{q^m}^{u\times n}$ with $\mathbf{z}_1, \ldots, \mathbf{z}_u$ as rows, satisfies

$$\mathrm{rank}_{q^m}(\mathcal{M}_{n-k-w,q}(\mathbf{Z})) = w,$$

then $(\mathbf{x}, \mathbf{z})$ can be recovered from $\mathbf{G}_{\mathcal{G}}, \mathbf{k}_{\mathsf{pub}}$ with $\mathcal{O}(n^3)$ operations in $\mathbb{F}_{q^{mu}}$.

If the key is generated as described in Section III-B, the GOT attack breaks the FL system with high probability.

B. Interleaved Decoding Attack

The second attack is based on the observation in Section IV-B that the public key $\mathbf{k}_{\mathsf{pub}}$ is a corrupted interleaved codeword. We will refer to it in the following as *Interleaved Decoding attack*. The idea is to decode $\mathbf{k}_{\mathsf{pub}}$ in an interleaved Gabidulin code. Since $w \leq \frac{u}{u+1}(n-k)$, such a decoder will return $\mathbf{x}$ with high probability, but fail in certain cases.

Lemma 6 (Interleaved Decoding [18], [19], [22, p. 64]) *Let $\mathbf{c}_i = \mathbf{x}_i \cdot \mathbf{G}_{\mathcal{G}}$. All known[4] efficient decoders for $\mathcal{IG}(u; n, k)$ codes fail to correct an error $\mathbf{z} \in \mathbb{F}_{q^{mu}}^n$ with $\mathbf{z} = \sum_{i=1}^{u} \mathbf{z}_i \gamma_i^*$ and $\mathrm{rank}_q(\mathbf{z}) = w$ if*

$$\mathrm{rank}_{q^m}\begin{pmatrix}\mathcal{M}_{n-w-1,q}(\mathbf{g})\\ \mathcal{M}_{n-k-w,q}(\mathbf{c}_1 + \mathbf{z}_1)\\ \mathcal{M}_{n-k-w,q}(\mathbf{c}_2 + \mathbf{z}_2)\\ \vdots \\ \mathcal{M}_{n-k-w,q}(\mathbf{c}_u + \mathbf{z}_u)\end{pmatrix} < n-1.$$

Since $\mathrm{rank}_{q^m}(\mathcal{M}_{n-w-1,q}(\mathbf{g})) = n-w-1$, the interleaved decoder fails if

$$\mathrm{rank}_{q^m}\left(\tilde{\mathbf{Z}}\right) := \varphi < w, \tag{5}$$

where

$$\tilde{\mathbf{Z}} = \begin{pmatrix}\mathcal{M}_{n-k-w,q}(\mathbf{z}_1)\\ \mathcal{M}_{n-k-w,q}(\mathbf{z}_2)\\ \vdots \\ \mathcal{M}_{n-k-w,q}(\mathbf{z}_u)\end{pmatrix}. \tag{6}$$

[4]i.e., the algorithms in [18], [19], and [22, p. 64].

C. Equivalence of GOT Attack's and Interleaved Decoding Attack's Failure Conditions

In the following theorem, we prove that the failure condition of the GOT Attack is equivalent to the condition that decoding $\mathbf{k}_{\mathsf{pub}}$ in an interleaved Gabidulin code fails.

Theorem 7 *The GOT Attack from [10] fails if and only if the Interleaved Decoding Attack from Section V-B fails. In particular, it fails if* (5) *holds.*

Proof: Rewrite the matrix from Theorem 5 as

$$\mathcal{M}_{n-w-k,q}\left(\mathbf{Z}\right) = \begin{pmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_u \\ \mathbf{z}_1^q \\ \vdots \\ \mathbf{z}_u^q \\ \vdots \\ \mathbf{z}_1^{q^{n-w-k-1}} \\ \vdots \\ \mathbf{z}_u^{q^{n-w-k-1}} \end{pmatrix} \tag{7}$$

and the matrix from equation (6) as

$$\tilde{\mathbf{Z}} = \begin{pmatrix} \mathbf{z}_1 \\ \vdots \\ \mathbf{z}_1^{q^{n-w-k-1}} \\ \mathbf{z}_2 \\ \vdots \\ \mathbf{z}_2^{q^{n-w-k-1}} \\ \vdots \\ \mathbf{z}_u \\ \vdots \\ \mathbf{z}_u^{q^{n-w-k-1}} \end{pmatrix}. \tag{8}$$

Since the matrix in (7) and in (8) only differ in row permutations, they are row-space equivalent, implying that they have the same rank. Further, the rank of the matrix in (8) cannot become larger than w (since any vector in the right kernel of this matrix has rank weight at least $n-w$ [23, Algorithm 3.2.1]). Thus, the failures of Theorem 5 and Lemma 6 are equivalent. ■

VI. Reparation of the FL System

To repair the FL system, we introduce a new key generation algorithm that is based on choosing $\mathbf{z} = \sum_{i=1}^{u} \mathbf{z}_i \gamma_i^*$ in a way that $\varphi < w$. In this case, an interleaved decoder, see (5), and therefore also the GOT attack [10] fail, see Theorem 7.

Theorem 8 *Let* $\dim(\langle \mathbf{z}_1, \ldots, \mathbf{z}_u \rangle_{\mathbb{F}_{q^m}}) = \zeta$. *Then*

$$\varphi \leq \min\{\zeta(n-k-w), w\}. \tag{9}$$

Proof: The dimension of $\langle \mathbf{z}_1, \ldots, \mathbf{z}_u \rangle_{\mathbb{F}_{q^m}}$ implies that at most $\zeta(n-k-w)$ rows of $\tilde{\mathbf{Z}}$ are linearly independent over $\mathbb{F}_{q^m}$, meaning that $\varphi \leq \zeta(n-k-w)$.

The definition of $\mathbf{z} = (\mathbf{s} \mid \mathbf{0}) \cdot \mathbf{P}^{-1}$ leads to

$$
\begin{aligned}
\varphi &= \operatorname{rank}_{q^m}(\tilde{\mathbf{Z}}) \\
&= \operatorname{rank}_{q^m}\left(\left(\begin{array}{c|c} \mathcal{M}_{n-k-w,q}(\mathbf{s}_1) & \mathbf{0} \\ \vdots & \vdots \\ \mathcal{M}_{n-k-w,q}(\mathbf{s}_u) & \mathbf{0} \end{array}\right)\mathbf{P}^{-1}\right) \\
&= \operatorname{rank}_{q^m}\begin{pmatrix} \mathcal{M}_{n-k-w,q}(\mathbf{s}_1) \\ \vdots \\ \mathcal{M}_{n-k-w,q}(\mathbf{s}_u) \end{pmatrix} \\
&\leq w,
\end{aligned}
$$

where the last inequality holds since $\mathbf{s}_1, \ldots, \mathbf{s}_u$ are vectors of length w. ■

We therefore propose the following modification to Line 3 of the **Key Generation**.

3 Choose $\zeta < \frac{w}{n-k-w}$ *and generate* $\mathbf{s}_1, \ldots, \mathbf{s}_u \in \mathbb{F}_{q^m}^w$ *at random such that* $\dim(\langle \mathbf{s}_1, \ldots, \mathbf{s}_u \rangle_{\mathbb{F}_{q^m}}) = \zeta$ *and* $\operatorname{rank}_q\left(\sum_{i=1}^u \mathbf{s}_i \gamma_i^*\right) = w$. *Compute* $\mathbf{s} = \sum_{i=1}^u \mathbf{s}_i \gamma_i^*$.

Clearly, we restrict the choice of $\mathbf{z}$ in Line 3 of the Key Generation algorithm but we will see that there are still enough possibilities for $\mathbf{z}$ to preserve a high security level.

A SageMath v8.4 [24] implementation of the FL system including the proposed repair can be downloaded from https://bitbucket.org/julianrenner/repaired_fl. It should be noted that the purpose of the source code is to clarify the shown algorithms but not to provide a secure and efficient implementation.

VII. Security Analysis of the Repair

In this section, we summarize the most efficient attacks on the FL system and we show that the restriction on $\mathbf{z}$ from (6) does not pose a problem in terms of the security level. Furthermore, we show that choosing $\zeta = 1$ provides the largest security level.

A. Brute-Force the Vector $\mathbf{z}$ Attack

As shown in Section III-F, knowing $\mathbf{z}$ is sufficient to be able to decrypt the ciphertext. Thus, one possible attack is to try all possible choices of $\mathbf{z}$. We count the number of such choices using the following result. In [23, Lemma 3.13], the number of $a \times b$ matrices of rank c over $\mathbb{F}_q$ is given by

$$
M_{a,b,c} := \prod_{i=0}^{c-1} \frac{(q^a - q^i)(q^b - q^i)}{q^c - q^i}.
$$

Together with the constructive argument in [25, Section IV.B], we obtain the following bounds on $M_{a,b,c}$:

$$
q^{c(a+b-c-1)} \leq M_{a,b,c} \leq \gamma_c \cdot q^{c(a+b-c)}, \tag{10}
$$

where $\gamma_c := \prod_{i=0}^{c-1} \frac{1}{1-q^{i-c}} \leq 0.288^{-1} \leq 3.48$.

In the general case $\zeta < \frac{w}{n-k-w}$, the number of Moore matrices as in (6) and such that $\operatorname{rank}_q(\mathbf{z}) = w$ is given from the *failure probability* of an interleaved Gabidulin decoder, cf. [19]. The number of such matrices therefore equals

$$
|\{\mathbf{z} \in \mathbb{F}_{q^{mu}}^n \ : \ \operatorname{rank}_q(\mathbf{z}) = w\}| \cdot P_f \geq q^{w(mu+n-w-1)} \cdot P_f,
$$

where the inequality is due to (10). However, a *lower* bound on the failure probability is not known. As an approximation, we can use $P_f \approx q^{-m}$ and therefore the number of such matrices is at least $q^{w(mu+n-w-1)-m}$.

The number of vectors $\mathbf{s}_1 \in \mathbb{F}_{q^m}^w$ with $\operatorname{rank}_q(\mathbf{s}_1) = w$ is at least $q^{w(m+n-w-1)}$ by (10). Thus, for $\zeta = 1$, the number of vectors $\mathbf{s} \in \mathbb{F}_{q^{mu}}^w$ is greater or equal to $q^{w(m+n-w-1)}q^{m(u-1)}$. Since there are at least q^{n^2-n} full-rank matrices $\mathbf{P} \in \mathbb{F}_q^{n \times n}$, the number of possible vectors $\mathbf{z}$ in Line 3 of Algorithm 1 is lower-bounded by

$$
\mathrm{WF}_{\mathbf{z}} = q^{w(m+n-w-1)+m(u-1)+n^2-n}.
$$

Since $u < n \leq m$, this is always larger than the work factor $\mathrm{WF}_\alpha = q^{mu}$ of brute-forcing α and thus, trying all possible $\mathbf{z}$ does not reduce the security of the system.

B. Interleaved Decoding Attack

As described in Section V-B, an attacker can apply an interleaved decoder on $\mathbf{k}_{\mathsf{pub}}$ to retrieve an alternative private key.

The crucial point in the interleaved decoding algorithm is solving a linear system of equations based on the syndromes with $w+1$ unknowns and φ linearly independent equations which is equivalent to finding the kernel of the matrix in (6), cf. [22, Section 4.1]. For $\zeta \geq \frac{w}{n-k-w}$, the dimension of the solution space is one and all solutions are valid for the remaining decoding steps. For $\zeta < \frac{w}{n-k-w}$, the dimension of the solution space is $w+1-\varphi$ but the valid solutions form only a one-dimensional subspace of the solution space. One can search in the solution space for a valid solution which requires on average

$$\frac{(q^m)^{w+1-\varphi}}{q^m} = q^{m(w-\varphi)}$$

trails.

The size of the solution space is maximized for the smallest-possible value of φ, i.e., $\varphi = n-k-w$. In this case, search through the solution space has a work factor of

$$\mathrm{WF}_{\mathrm{ILD}} = q^{m(2w-n+k)}.$$

Since the size of the solution space is maximal for $\varphi = n-k-w$, the repair from Section VI with the explicit parameter value $\zeta = 1$ is the most secure choice *in this sense*. However, we keep the choice of ζ free for the case that an attack is found which utilizes the pair-wise linear dependence of the $\mathbf{z}_i$.

Besides the interleaved decoding algorithms in [18], [19], and [22, p. 64], there is an interpolation-based decoding algorithm [22, Section 4.3 (page 72)]. This interpolation-based algorithm can be interpreted both as a list decoder with exponential worst-case and average list size or as a probabilistic unique decoder.

It is mentioned in [22, Section 4.3.2] that the probabilistic unique interpolation-based decoder fails if and only if the decoding algorithms in [18], [19], [22, p. 64] fail.

In case of the list decoder, there are two known results on the list size:

- [22, Lemma 4.5] states that the maximal list size of the decoder (and thus the work factor of the resulting attack) is at most
$$\mathrm{WF}_{\text{list, public key}} \leq q^{m(u-1)k}. \tag{11}$$
- [22, Lemma 4.6] states that the average list size is relatively small, assuming that the received word is uniformly distributed at random in $\mathbb{F}_{q^m}^{u \times n}$. This assumption is not satisfied in our case. Since there is a dependency of decoding failure of the probabilistic unique decoder and the list size of the list decoder, we conjecture that the average list size is close to the worst case since the error is chosen such that unique decoding always fails.

C. (List) Decoding on the Ciphertext Attack

As we have seen in Section IV-A, the ciphertext of the (repaired) FL system is a codeword of a Gabidulin code, corrupted by an error of rank weight at most $\tau = w + t_{\mathsf{pub}}$. Hence, an attacker can try to decode the ciphertext directly. Since τ is always greater than the unique decoding radius $\left\lfloor \frac{n-k}{2} \right\rfloor$ of the Gabidulin code, this would require the existence of an efficient (list) decoding algorithm up to radius τ.

However, such an algorithm has not been found, yet. It was even shown in [6], [7] that for some classes of Gabidulin codes (of rate $\geq \frac{1}{5}$) such an algorithm cannot exist. Note that the latter result was not yet known when the FL cryptosystem was proposed.

For instance, for a Gabidulin code with parameters $n \mid m$ and $\gcd(n, n-\tau) \geq 2$, there is a received word such that there are at least

$$\mathcal{L}_{\mathbf{c},\mathrm{worst}} \geq \max\left\{ \frac{\left[\frac{n/g}{(n-\tau)/g}\right]_{q^g}}{q^{n(\tau/g-1)}} \;:\; g \geq 2,\, g \mid \gcd(n, n-\tau) \right\} \tag{12}$$

codewords in rank distance at most τ to it.

Note that the list size $\mathcal{L}_{\mathbf{c},\mathrm{worst}}$ is a lower bound on the *worst-case* work factor of the attack. Although it does not imply any statement about the average list size/average work factor, it gives us an estimate in which order of magnitude the work factor of such an attack can be. We ensured that the value of $\mathcal{L}_{\mathbf{c},\mathrm{worst}}$ is sufficiently large in our example parameters in Section VIII.

On the other hand, it implies that there is no polynomial-time list decoding algorithm for arbitrary Gabidulin codes beyond the unique decoding radius (such as the Guruswami–Sudan algorithm for Reed–Solomon codes). Hence, an efficient attack can always be counteracted by a suitable parameter choice.

D. Syndrome Decoding Attack

The ciphertext can be interpreted as a codeword from a code of dimension k (see [2]), generated by the generator matrix

$$\begin{pmatrix} \mathcal{M}_{k-u,q}\left(\mathbf{g}\right) \\ \mathrm{Tr}_{q^{um}/q^m}(\gamma_1 \mathbf{k}_{\mathsf{pub}}) \\ \vdots \\ \mathrm{Tr}_{q^{um}/q^m}(\gamma_u \mathbf{k}_{\mathsf{pub}}) \end{pmatrix}.$$

Since the structure of this code only permits decoding like a random rank-metric code, it can be decoded with the syndrome decoding attack from [26] whose complexity is in the order of

$$\mathrm{WF}_{\mathrm{SD}} = (n-k)^3 m^3 q^{t_{\mathsf{pub}}\lceil \frac{(k+1)m}{n} \rceil - m}.$$

E. Linearization Attack

In [2], a message attack was proposed which succeeds for some parameters with high probability in polynomial time.

Lemma 9 (Linearization Attack [2]) *Let* $\mathbf{k}_{\mathsf{pub}}^{(i)} = \mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \mathbf{k}_{\mathsf{pub}})$ *for* $i = 1, \ldots, u$ *and*

$$\mathbf{M} = \begin{pmatrix} \mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{c}\right) \\ -\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{k}_{\mathsf{pub}}^{(1)}\right) \\ \vdots \\ -\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{k}_{\mathsf{pub}}^{(u)}\right) \\ -\mathcal{M}_{k+t_{\mathsf{pub}}-u,q}\left(\mathbf{g}\right) \end{pmatrix}. \tag{13}$$

Then, the encrypted message $\mathbf{m}$ *can be efficiently recovered if the left kernel of* $\mathbf{M}$ *has dimension* $\dim(\ker(\mathbf{M})) = 1$.

If $(u+2)t_{\mathsf{pub}} + k > n$, then $\mathbf{M}$ has at least two more rows than columns and we have $\dim(\ker(\mathbf{M})) > 1$. If $\mathbf{k}_{\mathsf{pub}}$ is random and $(u+2)t_{\mathsf{pub}} + k \leq n$, the attack is efficient with high probability [2].

Lemma 10 *Let* $\mathbf{M}$ *be as in* (13)*. Then,*

$$\mathrm{rank}_{q^m}(\mathbf{M}) \leq \min\{\varphi + k + 2t_{\mathsf{pub}} - u, n\}.$$

Proof: We can write

$$\begin{aligned} \mathbf{k}_{\mathsf{pub}}^{(i)} &= \mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \mathbf{k}_{\mathsf{pub}}) \\ &= \mathrm{Tr}_{q^{mu}/q^m}(\gamma_i \mathbf{x}) \cdot \mathcal{M}_{k,q}\left(\mathbf{g}\right) + \mathbf{z}_i, \end{aligned}$$

so by elementary row operations, we can transform $\mathbf{M}$ into

$$\mathbf{M}' = \begin{pmatrix} \mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{c}\right) \\ -\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{z}_1\right) \\ \vdots \\ -\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{z}_u\right) \\ -\mathcal{M}_{k+t_{\mathsf{pub}}-u,q}\left(\mathbf{g}\right) \end{pmatrix}.$$

Due to $w + 2t_{\mathsf{pub}} < n - k$, the matrix $\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{z}_i\right)$ is a sub-matrix of $\mathcal{M}_{n-k-w,q}\left(\mathbf{z}_i\right)$, so

$$\begin{aligned} &\mathrm{rank}_{q^m}(\mathbf{M}) = \mathrm{rank}_{q^m}(\mathbf{M}') \\ &\leq \varphi + \mathrm{rank}_{q^m}(\mathcal{M}_{t_{\mathsf{pub}}+1,q}\left(\mathbf{c}\right)) + \mathrm{rank}_{q^m}(\mathcal{M}_{k+t_{\mathsf{pub}}-u,q}\left(\mathbf{g}\right)) \\ &= \varphi + k + 2t_{\mathsf{pub}} - u. \end{aligned}$$

Further, since the number of columns of $\mathbf{M}$ is equal to n,

$$\mathrm{rank}_{q^m}(\mathbf{M}) \leq n.$$

■

The linearization attack is inefficient if the rank of $\mathbf{M}$ is smaller than its number of rows, which implies the following, stronger version of the original statement in [2].

Theorem 11 *If $t_{\mathsf{pub}} > \frac{n-k}{u+2}$ or $\varphi < u(t_{\mathsf{pub}}+1)$, the linearization attack in [2] is inefficient and its work factor is*

$$WF_{\mathrm{Lin}} = q^{m\cdot\max\{ut_{\mathsf{pub}}+u+1-\varphi,(u+2)t_{\mathsf{pub}}+k+1-n\}}.$$

The first condition in Corollary 11 is again fulfilled by the choice of w in Table I. The second one reads $t_{\mathsf{pub}} > \frac{\varphi}{u}+1$, and for any valid φ, there are choices of w such that t_{pub} fulfills this inequality for any $u > 1$.

F. Algebraic Attacks

Faure and Loidreau [2] also described two message attacks of exponential worst-case complexity. The first one is based on computing gcds of polynomials of degrees

$$q^{m(u-1)}\frac{q^{t_{\mathsf{pub}}+1}-1}{q-1} =: \mathrm{WF}_{\mathrm{Alg}}. \tag{14}$$

Since computing the gcd of two polynomials can be implemented in quasi-linear time in the polynomials' degree, (14) gives an estimate on the work factor of this attack. The second algebraic attack is based on finding Gröbner bases of a system of $n_{\mathrm{p}} = \binom{n}{k+2t_{\mathsf{pub}}-u+1}$ many polynomials of degree approximately $d_{\mathrm{p}} = \frac{q^{t_{\mathsf{pub}}+1}-1}{q-1}$. The attack is only efficient for small code parameters, cf. [2, Sec. 5.3]. Since the average-case complexity of Gröbner bases algorithms is hard to estimate, we cannot directly relate n_{p} and d_{p} to the attack's work factor. Faure and Loidreau choose the code parameters such that $n_{\mathrm{p}} \approx 2^{32}$ and $d_{\mathrm{p}} = 127$ and claim that the attack is inefficient for these values. Our example parameters in Section VIII result in at least these values.

G. Overbeck-like Attack

The key attack described in [3, Ch. 7, Sec. 2.1] is based on a similar principle as Overbeck uses to attack the McEliece cryptosystem based on rank-metric codes [9]. The attack from [3, Ch. 7, Sec. 2.1] cannot be applied if

$$w \geq n-k-\frac{k-u}{u-1}.$$

H. Moving to Another Close Error Attack

The following attack by Rosenkilde [27] tries to move the vector $\mathbf{z}$ (which we have chosen such that the interleaved decoder fails) on a close vector for which the interleaved decoder for $\mathbf{k}_{\mathsf{pub}}$ does not fail. Therefore, a vector $\mathbf{y} \in \mathbb{F}_{q^m}^{u\times n}$ is needed such that for $\mathbf{z}' := \mathbf{z}+\mathbf{y}$ it holds that $\mathrm{rank}_q(\mathbf{z}') \leq w$ and that the rank of the matrix from (6) over $\mathbb{F}_{q^m}$ is at least w.

Rosenkilde suggested to find such a vector by guessing $2w-n+k$ independent vectors from $\mathbb{F}_q^n$ which are in the $\mathbb{F}_q$-row space of $\mathbf{z}$, put them as the first rows of a matrix in $\mathbb{F}_q^{um\times n}$ (the remaining rows are zeros) and use its mapping to a matrix in $\mathbb{F}_{q^m}^{u\times n}$ as matrix $\mathbf{y}$. That way, $\mathbf{z}'$ is in the row space of $\mathbf{z}$ and $\mathrm{rank}_q(\mathbf{z}') \leq w$ is guaranteed. Further, the rank of the matrix from (6) over $\mathbb{F}_{q^m}$ is increased to w with high probability.

The complexity of this attack is dominated by the complexity of finding $2w-n+k$ independent vectors from $\mathbb{F}_q^n$ which are in the $\mathbb{F}_q$-row space of $\mathbf{z}$, i.e.:

$$\mathrm{WF}_{\mathrm{MCE}} = q^{(2w-n+k)(n-w)}.$$

I. Brute-Force the Parameter α Attack

An attacker can brute-force α, which has a complexity of

$$\mathrm{WF}_{\alpha} = q^{mu}.$$

By knowing α, he just needs to apply an efficient decoding algorithm on $\tilde{\mathbf{c}} = \mathbf{c} - \mathrm{Tr}_{q^{mu}/q^m}(\alpha\mathbf{k}_{\mathsf{pub}})$ to retrieve the secret message.

VIII. Analysis of the repaired system

In this section, we recall the conditions on the choice of the parameters such that all known attacks are inefficient and summarize their work factors. Furthermore, we give specific parameters and compare the FL system to other code-based cryptosystems.

Table II
SUMMARY OF THE DISCUSSED ATTACKS' WORK FACTORS

Name of the attack	Work factor	Reference
Brute-force $\mathbf{z}$	$\mathrm{WF}_{\mathbf{z}} = q^{w(m+n-w-1)+m(u-1)+n^2-n}$	Section VII-A
Interleaved Decoding	$\mathrm{WF}_{\mathrm{ILD}} = q^{m(2w-n+k)}$	Section VII-B
Syndrome Decoding	$\mathrm{WF}_{\mathrm{SD}} = (n-k)^3 m^3 q^{t_{\mathsf{pub}}\lceil \frac{(k+1)m}{n} \rceil - m}$	Section VII-D, using [26]
Linearization	$\mathrm{WF}_{\mathrm{Lin}} = q^{m\cdot\max\{ut_{\mathsf{pub}}+u+1-\varphi,(u+2)t_{\mathsf{pub}}+k+1-n\}}$	First in [2], cf. Section VII-E
Algebraic	$\mathrm{WF}_{\mathrm{Alg}} = q^{m(u-1)\,\frac{q^{t_{\mathsf{pub}}+1}-1}{q-1}}$	First in [2], cf. Section VII-F
Moving to Another Close Error	$\mathrm{WF}_{\mathrm{MCE}} = q^{(2w-n+k)(n-w)}$	First in [27], cf. Section VII-H
Brute-force α	$\mathrm{WF}_{\alpha} = q^{mu}$	Section VII-I

Table III
COMPARISON OF THE MCELIECE (BASED ON GOPPA CODES), THE LOIDREAU, THE REPAIRED FL, THE QC-MDPC AND THE DC-LRPC CRYPTOSYSTEMS

Method	q	u	k	n	m	w	τ	t_{Loi}	λ	Security level	Rate	Key size
McEliece	2		1436	1876	11		41			80.04	0.77	78.98 KB
Loidreau	2		32	50	50			3	3	80.93	0.64	3.60 KB
Repaired FL	2	3	31	61	61	16				90.00	0.46	1.86 KB
QC-MDPC	2		4801	9602						80.00	0.50	0.60 KB
DC-LRPC	2		37	74	41					80.00	0.50	0.19 KB
McEliece	2		2482	3262	12		66			128.02	0.76	242.00 KB
Loidreau	2		40	64	96			4	3	139.75	0.63	11.52 KB
Repaired FL	2	3	31	62	62	17				131.99	0.45	1.92 KB
QC-MDPC	2		9857	19714						128.00	0.50	1.23 KB
DC-LRPC	2		47	94	47					128.00	0.50	0.30 KB
McEliece	2		5318	7008	13		133			257.47	0.76	1123.43 KB
Loidreau	2		80	120	128			4	5	261.00	0.67	51.20 KB
Repaired FL	2	4	48	83	83	21				256.99	0.53	4.31 KB
QC-MDPC	2		32771	65542						256.00	0.50	4.10 KB

A. Summary of the Work Factors

In the following, we choose the parameters q, m, n, k, u, w, and t_{pub} as in Table I. Recall that this choice of w prevents the Overbeck-like attack (Section VII-G) and results in an exponential work factor of the linearization attack (Section VII-E). Furthermore, we choose $\zeta = 1$ to maximize the work factor of searching the exponentially-large output of the interleaved decoding attack (Section VII-B). Note that the latter attack returns an exponentially-large output if and only if of the GOT [10] attack fails, cf. Theorem 7.

The resulting considered work factors are summarized in Table II. In addition to these work factors, we have considered the following additional requirements:

- The work factor of the second algebraic attack in [2] (cf. Section VII-F) is unknown. Hence, we choose the code parameters such that the resulting non-linear system of equations occurring in the attack consists of more than $n_{\mathrm{p}} \approx 2^{32}$ many polynomials of degree at least $d_{\mathrm{p}} = 127$. This is the same choice as in [2].
- Since there is no efficient list decoder for Gabidulin codes, the work factor of the list-decoding ciphertext attack in Section VII-C is not known. However, we do have a lower bound on the worst-case work factor for some codes, given by the maximal list size $\mathcal{L}_{\mathbf{c},\mathrm{worst}}$ in (12). In all examples for which the bound holds, we chose the parameters such that $\log_2(\mathcal{L}_{\mathbf{c},\mathrm{worst}})$ is much larger than the claimed security level.

B. Parameters and Key Sizes

To evaluate the performance of the repaired FL cryptosystem, we compare it to McEliece's cryptosystem based on Goppa codes using list decoding [28], Loidreau's new rank-metric code-based encryption scheme [29], [30], the QC-MDPC cryptosystem [31] and the DC-LRPC based system [32].

The most efficient attack on McEliece has a work factor (cf. [28]) of

$$\mathrm{WF}_{\mathrm{ME}} = \min\left\{ \frac{1}{2}\binom{n}{\tau}\binom{n-k}{\tau-p}^{-1}\binom{k}{p}^{-1/2} : 0 \le p \le \min\{\tau, k\} \right\}$$

operations, where τ is the binary Johnson bound.

The work factor of Loidreau's system [29], [30] is

$$\mathrm{WF}_{\mathrm{Loi}} = m^3 q^{(t_{\mathrm{Loi}}-1)\lfloor (k\cdot\min(m,n))/n \rfloor},$$

operations, where $t_{\mathrm{Loi}} \cdot \lambda = \left\lfloor \frac{n-k}{2} \right\rfloor$.

In Table III, parameters for expected work factors of around 2^{80}, 2^{128} and 2^{256} are shown. Further, both the required key sizes and the achieved rates are given, where the rate states the ratio of length of the secret message to the length of the ciphertext. The shown work factors of the repaired FL system stem from the number of operations required by the most efficient attack which is the Moving to Another Close Error Attack for 2^{80} and the Algebraic Attack for 2^{128} and 2^{256}. We observe that in all cases McEliece has the highest rate followed by Loidreau, repaired FL, QC-MDPC and DC-LRPC. The results further show that repaired FL requires much smaller key sizes compared to Loidreau and McEliece, it has similar key sizes as QC-MDPC and it is in this sense only worse compared to the system based on DC-LRPC codes[5]. Since public-key cryptosystems are mostly used for encrypting small data packages (usually they are used to exchange the private key of a symmetric cryptosystem), small key sizes are usually more important than high code rates.

IX. Conclusion

In this paper, new coding-theoretic interpretations of the Faure–Loidreau system were given. It was shown that the ciphertext is a corrupted codeword of a Gabidulin code, where to an unauthorized receiver, the error weight is too large to be correctable. The authorized user knows the row space of a part of the error and is thus able to correct the error.

Further, it was derived that a part of the public key can be seen as a corrupted codeword of an interleaved Gabidulin code and that in the original FL system, an interleaved Gabidulin decoder can efficiently recover the private key from this part of the public key with high probability. It was proven that the condition that interleaved Gabidulin decoders fail is equal to the condition that the severe attack by Gaborit, Otmani and Talé Kalachi fails.

Based on the latter interpretation, a repair was proposed that modifies the key generation algorithm such that interleaved Gabidulin decoders fail which in turn implies that the attack by Gaborit *et al.* fails.

A security analysis was conducted and it was shown that the security level is not decreased with respect to all other known attacks by the proposed repair.

Parameters for security levels of 80, 128, 256 bit where presented and compared to McEliece-like systems based on Goppa codes, Gabidulin codes, QC-MPDC codes and DC-LRPC codes. It was observed that the repaired FL system has smaller key sizes compared the systems based on Goppa codes and Gabidulin codes, similar key sizes as the system based on QC-MDPC codes but larger key sizes than DC-LRPC based system. However, while both the QC-MDPC and DC-LRPC scheme give no guarantee that the ciphertext can be decrypted as decoding these codes might fail, the repaired FL system guarantees decryption. Hence, the repaired FL cryptosystem has advantages compared to the other mentioned systems and should be considered as an alternative of small key size.

Acknowledgment

We would like to thank Johan Rosenkilde for proposing the "moving to a close error" attack. Also, we are thankful to Michael Schelling for his observation that decryption of the FL system can be seen as error-erasure decoding. Further, we thank Pierre Loidreau for his valuable comments on a previous version of this paper.

References

[1] A. Wachter-Zeh, S. Puchinger, and J. Renner, "Repairing the faure-loidreau public-key cryptosystem," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 2426–2430.

[2] C. Faure and P. Loidreau, "A new public-key cryptosystem based on the problem of reconstructing p-polynomials," in *Coding and Cryptography*. Springer, 2006, pp. 304–315.

[3] P. Loidreau, "Métrique rang et cryptographie (in French)," Mémoire d'habilitation à diriger des recherches, Université Pierre et Marie Curie, Paris 6, Sep 2007.

[4] D. Augot and M. Finiasz, "A public key encryption scheme based on the polynomial reconstruction problem," *LNCS: Revised selected papers of EUROCRYPT 2003*, vol. 2656, pp. 229–249, 2003.

[5] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Inf. Transm.*, vol. 21, no. 1, pp. 3–16, 1985.

[6] A. Wachter-Zeh, "Bounds on list decoding of rank-metric codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7268–7277, Nov. 2013.

[7] N. Raviv and A. Wachter-Zeh, "Some Gabidulin codes cannot be list decoded efficiently at any radius," *IEEE Trans. Inform. Theory*, vol. 62, no. 4, pp. 1605–1615, Apr. 2016.

[8] P. Gaborit, O. Ruatta, and J. Schrek, "On the complexity of the rank syndrome decoding problem," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, pp. 1006–1019, Feb 2016.

[9] R. Overbeck, "A new structural attack for GPT and variants," *LNCS: MYCRYPT*, vol. 3715, p. 50–63, 2005.

[10] P. Gaborit, A. Otmani, and H. Talé Kalachi, "Polynomial-time key recovery attack on the faure–loidreau scheme based on gabidulin codes," *Des. Codes Cryptogr.*, vol. 86, no. 7, pp. 1391–1403, Jul 2018.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Oct. 1996.

[5] Since no parameters for a security level of 256 bit were provided in [32], Table III doesn't include the LRPC system for this security level.

[12] P. Delsarte, "Bilinear forms over a finite field with applications to coding theory," *J. Comb. Theory Ser. A*, vol. 25, no. 3, pp. 226–241, Nov. 1978.
[13] D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3951–3967, Sep. 2008.
[14] E. M. Gabidulin and N. I. Pilipchuk, "Error and erasure correcting algorithms for rank codes," *Des. Codes Cryptogr.*, vol. 49, no. 1-3, pp. 105–122, Dec. 2008.
[15] A. Wachter-Zeh and A. Zeh, "List and unique error-erasure decoding of interleaved gabidulin codes with interpolation techniques," *Des. Codes Cryptogr.*, vol. 73, no. 2, pp. 547–570, Nov. 2014.
[16] S. Puchinger and A. Wachter-Zeh, "Sub-quadratic decoding of gabidulin codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 2554–2558.
[17] S. Puchinger and A. Wachter-Zeh, "Fast operations on linearized polynomials and their applications in coding theory," *J. Symb. Comp*, vol. 89, pp. 194–215, Dec. 2018.
[18] P. Loidreau and R. Overbeck, "Decoding rank errors beyond the error correcting capability," in *Int. Workshop Alg. Combin. Coding Theory (ACCT)*, Sep. 2006.
[19] V. R. Sidorenko, L. Jiang, and M. Bossert, "Skew-feedback shift-register synthesis and decoding interleaved Gabidulin codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 621–632, Feb. 2011.
[20] M. Gadouleau and Z. Yan, "Complexity of decoding gabidulin codes," in *IEEE Annual Conf. Inform. Science and Syst.*, 2008, pp. 1081–1085.
[21] D. Silva and F. R. Kschischang, "Fast encoding and decoding of gabidulin codes," in *IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2009, pp. 2858–2862.
[22] A. Wachter-Zeh, "Decoding of block and convolutional codes in rank metric," Ph.D. dissertation, Ulm University and University of Rennes 1, Ulm, Germany and Rennes, France, Oct. 2013.
[23] R. Overbeck, "Public key cryptography based on coding theory," Ph.D. dissertation, TU Darmstadt, Darmstadt, Germany, 2007.
[24] W. A. Stein *et al.*, SageMath Software, http://www.sagemath.org.
[25] E. M. Gabidulin, A. V. Ourivski, B. Honary, and B. Ammar, "Reducible rank codes and their applications to cryptography," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3289–3293, 2003.
[26] N. Aragon, P. Gaborit, A. Hauteville, and J.-P. Tillich, "A new algorithm for solving the rank syndrome decoding problem," in *IEEE Int. Symp. Inf. Theory (ISIT)*, June 2018, pp. 2421–2425.
[27] J. S. H. Rosenkilde, Personal Communication, 2018.
[28] M. Barbier and P. S. L. M. Barreto, "Key reduction of McEliece's cryptosystem using list decoding," in *IEEE Int. Symp. Inform. Theory (ISIT)*, July 2011, pp. 2681–2685.
[29] P. Loidreau, "An evolution of GPT cryptosystem," in *Int. Workshop Alg. Combin. Coding Theory (ACCT)*, 2016.
[30] ——, "A new rank metric codes based encryption scheme," in *8th Int. Conf. on Post-Quantum Cryptography (PQCrypto)*, 2017.
[31] R. Misoczki, J. P. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *IEEE Int. Symp. Inform. Theory (ISIT)*, July 2013, pp. 2069–2073.
[32] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in *Int. Workshop Coding Cryptogr. (WCC)*, Apr. 2013, pp. 168–180.