# Weak Keys in the Faure–Loidreau Cryptosystem

Thomas Jerkovits and Hannes Bartz

Institute of Communication and Navigation
Deutsches Zentrum für Luft- und Raumfahrt (DLR), D-82234 Wessling, Germany
{thomas.jerkovits,hannes.bartz}@dlr.de

**Abstract.** Some types of weak keys in the Faure–Loidreau (FL) cryptosystem are presented. We show that from such weak keys the private key can be reconstructed with a computational effort that is substantially lower than the security level ($\approx 2^{25}$ operations for 80-bit security). The proposed key-recovery attack is based on ideas of generalized minimum distance (GMD) decoding for rank-metric codes.

**Keywords:** code-based cryptography, rank-metric codes, interleaving, Gabidulin codes, generalized minimum distance (GMD) decoding, post-quantum cryptography, Faure–Loidreau

## 1 Introduction

Most current public-key cryptosystems like Rivest, Shamir and Adleman (RSA) [1] rely on hard mathematical problems such as prime factorization problem or the discrete logarithm problem. In 1999, Shor presented an algorithm for quantum computers that is able to solve the prime factorization problem and the discrete logarithm problem in polynomial time [2]. Thus, assuming that quantum computer of sufficient scale can be built one day, current cryptosystems like RSA can be broken in polynomial time rendering most of todays communication systems insecure. Current post-quantum secure public-key cryptosystems, i.e. systems that are resilient against attacks on quantum computers, suffer from large public keys compared to RSA, that means typically several hundreds of thousands of bits [3]. For example, the first code-based cryptosystem by McEliece [4] uses as a public key an obfuscated generator matrix of a linear block code, which results in a key size that is quadratic in the length of the code.

In 2006, Faure and Loidreau proposed a cryptosystem [5] that is based on the problem of reconstructing linearized polynomials. The Faure–Loidreau (FL) cryptosystem is the rank-metric equivalent of the Augot–Finiasz cryptosystem [6] and admits very small public keys for a given security level ($\approx 2KB$ for 80-bit security). In 2018, Gaborit et al. showed, that the private key in the FL cryptosystem can be recovered in polynomial time from the public key with high probability. In [7] it was shown, that the attack from [8] is equivalent to the problem of list decoding interleaved Gabidulin codes [9]. In other words, the private key is a noisy codeword of an interleaved Gabidulin code with error weight chosen slightly larger then the unique decoding radius. Such noisy codewords

can be recovered with a high probability by applying list decoding. That means the size of the list returned by the decoder is one with high probability. Whenever the list size is larger than one, the decoder fails. This kind of decoding is called probabilist unique decoding. By restricting to error patterns that make the probabilistic unique decoder of an interleaved Gabidulin decoder fail, the FL cryptosystem can be repaired [7].

In this paper, we consider a new method to recover the private key from the public key in the FL cryptosystem that uses properties that are *not* related to the previous key-recovery attacks in [7, 8]. The method uses ideas from generalized minimum distance (GMD) decoding [10] which improves decoding by trading errors for erasures and also was applied for rank-metric codes [10, 11]. This allows to recover private keys from some weak public keys with a computational complexity that is substantially below the security level of the cryptosystem. We characterize some types of weak keys and show that the key-recovery attack is feasible for the parameters suggested in [5, 7].

## 2 Preliminaries

Let $q$ be a power of a prime and denote by $\mathbb{F}_q$ a finite field of order $q$ and by $\mathbb{F}_{q^m}$ the extension field of $\mathbb{F}_q$ of degree $m$. For an integer $u > 1$, we define an extension field $\mathbb{F}_{q^{mu}}$ of $\mathbb{F}_{q^m}$ such that $\mathbb{F}_q \subset \mathbb{F}_{q^m} \subset \mathbb{F}_{q^{mu}}$. By $\mathcal{B} = (\beta_1, \beta_2, \ldots, \beta_u)$ we denote an ordered basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$.

We denote the set of all $m \times n$ matrices over $\mathbb{F}_q$ by $\mathbb{F}_q^{m\times n}$ and define $\mathbb{F}_q^n \stackrel{\text{def}}{=} \mathbb{F}_q^{1\times n}$. Matrices and vectors are denoted by bold uppercase and lowercase letters such as $\mathbf{A}$ and $\mathbf{a}$, respectively. The Hamming weight $w_{\mathrm{H}}(\mathbf{a})$ of a vector $\mathbf{a}$ is defined as the number of nonzero entries in $\mathbf{a}$.

Under a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ there is a bijective mapping between any vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ and a corresponding matrix $\mathbf{A} \in \mathbb{F}_q^{m\times n}$. The rank $\mathrm{rk}_q(\mathbf{a})$ of a vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ is defined as the rank of the corresponding matrix $\mathbf{A} \in \mathbb{F}_q^{m\times n}$ such that $\mathrm{rk}_q(\mathbf{a}) \stackrel{\text{def}}{=} \mathrm{rk}_q(\mathbf{A})$. The field trace of any $a \in \mathbb{F}_{q^{mu}}$ to $\mathbb{F}_{q^m}$ is denoted by $\mathrm{Tr}_{q^{mu}/q^m}(a)$. We use $\mathrm{Tr}_{q^{mu}/q^m}(\mathbf{a})$ to denote the element-wise field trace of a vector $\mathbf{a} \in \mathbb{F}_{q^{mu}}^n$.

For a given vector $\mathbf{a} \in \mathbb{F}_{q^m}^n$ and integer $r$, the *Moore* matrix is defined as

$$\mathbf{M}_r(\mathbf{a}) \stackrel{\text{def}}{=} \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1^{[1]} & a_2^{[1]} & \ldots & a_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{[r-1]} & a_2^{[r-1]} & \ldots & a_n^{[r-1]} \end{pmatrix}$$

where $[i] \stackrel{\text{def}}{=} q^i$ denotes the $i$-th Frobenius power.

### 2.1 Gabidulin Codes

The rank distance $d_{\mathrm{R}}$ between two matrices $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{m \times n}$ with corresponding vectors $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^n$ is defined as

$$d_{\mathrm{R}}\left(\mathbf{A}, \mathbf{B}\right) = d_{\mathrm{R}}\left(\mathbf{a}, \mathbf{b}\right) \stackrel{\text{def}}{=} \mathrm{rk}_q(\mathbf{A} - \mathbf{B}) = \mathrm{rk}_q(\mathbf{a} - \mathbf{b}).$$

A linear rank-metric code of length $n \leq m$ and dimension $k$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m \times n}$. The minimum rank distance $d_{\mathrm{R}}$ of a rank-metric code of length $n$ and dimension $k$ is upper bounded by the Singleton-like bound (see [12])

$$d_{\mathrm{R}} \leq n - k + 1. \tag{1}$$

Codes that fulfill the Singleton-like bound in (1) with equality are called maximum rank distance (MRD) codes [12]. Gabidulin codes are a special class of rank-metric codes and fulfill (1) with equality, i.e. have minimum distance $d_{\mathrm{R}} = n - k + 1$, and thus are MRD codes. A Gabidulin [12] code $\mathrm{Gab}[n, k]$ of length $n$ and dimension $k$ over $\mathbb{F}_{q^m}$ is defined by the $\mathbb{F}_{q^m}$-linear row space of the generator matrix

$$\mathbf{G} = \mathbf{M}_k(\mathbf{g})$$

with $\mathbf{g} \in \mathbb{F}_{q^m}^n$ and $\mathrm{rk}_q(\mathbf{g}) = n$.

A rank error channel takes a matrix $\mathbf{X} \in \mathbb{F}_q^{m \times n}$ as an input and outputs a matrix $\mathbf{Y} \in \mathbb{F}_q^{m \times n}$ such that

$$\mathbf{Y} = \mathbf{X} + \mathbf{E}$$

where the error matrix $\mathbf{E} \in \mathbb{F}_q^{m \times n}$ has rank $\mathrm{rk}_q(\mathbf{E}) = t$.

Besides $t$ rank errors, the transmitted matrix may be corrupted by row- or column erasures [13]. A matrix $\mathbf{X} \in \mathbb{F}_q^{m \times n}$ is corrupted by $\rho$ row erasures and $\epsilon$ column erasures if $\rho$ rows and $\epsilon$ columns are erased (i.e. set to zero). There exist efficient error erasure correcting decoders for Gabidulin codes that can correct $t$ rank errors, $\epsilon$ column erasures and $\rho$ row erasures up to

$$2t + \rho + \epsilon \leq n - k \tag{2}$$

requiring $\mathcal{O}(n^2)$ operations in $\mathbb{F}_{q^m}$ (see [14–16]). Note that $\epsilon$ column erasures in the matrix $\mathbf{X} \in \mathbb{F}_q$ correspond to $\epsilon$ symbol erasures in the corresponding vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$.

### 2.2 Interleaved Gabidulin Codes

A homogeneous interleaved Gabidulin code $\mathrm{IGab}[u; n, k]$ of length $n$, interleaving order $u$ and component code dimension $k$ over $\mathbb{F}_{q^m}$ is defined as the $u$-fold Cartesian product of a (component) Gabidulin code $\mathrm{Gab}[n, k]$, i.e.

$$\mathrm{IGab}[u; n, k] \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} \mathbf{c}^{(1)} \\ \mathbf{c}^{(2)} \\ \vdots \\ \mathbf{c}^{(u)} \end{pmatrix} : \mathbf{c}^{(j)} \in \mathrm{Gab}[n, k], \forall j = 1, \ldots, u \right\}.$$

An interleaved Gabidulin code IGab$[u; n, k]$ can correct rank errors up to

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

with high probability (see e.g. [9, 17, 18]). Note, that interleaving improves the decoding radius for rank errors but does not improve the decoding radius for row and column erasures.

Under a fixed basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$ a $u$-interleaved Gabidulin code IGab$[u; n, k]$ over $\mathbb{F}_{q^m}$ can be represented as the $\mathbb{F}_{q^{mu}}$-linear row space of the generator matrix $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$ of Gab$[n, k]$.

## 3 Key-Recovery Attacks on the Faure–Loidreau Cryptosystem

In the following a brief description of the FL cryptosystem is given. The encryption and decryption process are described in the Appendix. Let $w$ be an integer that satisfies

$$\left\lfloor \frac{n-k}{2} \right\rfloor < w < n-k.$$

### 3.1 Key-Generation

1. Choose $\mathbf{g} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(\mathbf{g}) = n$ at random and denote by $\mathbf{G} = \mathbf{M}_k(\mathbf{g})$ the generator matrix of the corresponding Gabidulin code Gab$[n, k]$.
2. Choose a vector $\mathbf{x} \in \mathbb{F}_{q^{mu}}^k$ such that the last $u$ positions of $\mathbf{x}$ are $\mathbb{F}_{q^m}$-linearly independent at random.
3. Choose $\mathbf{s} = (s_1 \ s_2 \ \ldots \ s_w) \in \mathbb{F}_{q^{mu}}^w$ such that $\mathrm{rk}_q(\mathbf{s}) = w$ at random.
4. Choose a random invertible matrix $\mathbf{P} \in \mathbb{F}_q^{n \times n}$ and compute

$$\mathbf{z} = (\,\mathbf{s} \,|\, \mathbf{0}\,)\,\mathbf{P}^{-1}. \tag{3}$$

**Private key:** $(\mathbf{P}, \mathbf{z}, \mathbf{x})$

**Public key:** $(\mathbf{g}, k, \mathbf{k}_{\mathrm{pub}}, t_{\mathrm{pub}})$ where

$$\mathbf{k}_{\mathrm{pub}} = \mathbf{x}\mathbf{G} + \mathbf{z} \tag{4}$$

and

$$t_{\mathrm{pub}} = \left\lfloor \frac{n-k-w}{2} \right\rfloor. \tag{5}$$

### 3.2 Key-Recovery Attacks on the Faure–Laudreau Cryptosystem

Gaborit, Otmani and Kalachi showed that an alternative private key $\mathbf{k}'_{\mathrm{pub}}$ can be recovered in polynomial time from the public key $\mathbf{k}_{\mathrm{pub}}$ and $\mathbf{G}$ with high probability if

$$w \leq \frac{u}{u+1}(n-k) \tag{6}$$

holds [8]. The attack cannot be prevented by adjusting the parameters, e.g. by choosing $w > \frac{u}{u+1}(n-k)$, since $w$ reduces $t_{\text{pub}}$ (see (5)) such that decoding attacks become feasible.

Consider the public key $\mathbf{k}_{\text{pub}}$ from (4) where $\mathbf{x} \in \mathbb{F}_{q^{mu}}^k$ and $\mathbf{z} \in \mathbb{F}_{q^{mu}}^n$ with $\text{rk}_q(\mathbf{z}) = w$. By defining $\mathbf{k}_{\text{pub}} = \sum_{i=1}^u \mathbf{k}_{\text{pub}}^{(i)} \beta_i$, $\mathbf{z} = \sum_{i=1}^u \mathbf{z}^{(i)} \beta_i$ and $\mathbf{x} = \sum_{i=1}^u \mathbf{x}^{(i)} \beta_i$ we can express the public key as

$$\begin{pmatrix} \mathbf{k}_{\text{pub}}^{(1)} \\ \mathbf{k}_{\text{pub}}^{(2)} \\ \vdots \\ \mathbf{k}_{\text{pub}}^{(u)} \end{pmatrix} = \begin{pmatrix} \mathbf{x}^{(1)}\mathbf{G} \\ \mathbf{x}^{(2)}\mathbf{G} \\ \vdots \\ \mathbf{x}^{(u)}\mathbf{G} \end{pmatrix} + \begin{pmatrix} \mathbf{z}^{(1)} \\ \mathbf{z}^{(2)} \\ \vdots \\ \mathbf{z}^{(u)} \end{pmatrix} \tag{7}$$

where $\mathbf{x}^{(j)} \in \mathbb{F}_{q^m}^k$ and $\mathbf{k}_{\text{pub}}^{(j)}, \mathbf{z}^{(j)} \in \mathbb{F}_{q^m}^n$ with $\text{rk}_q(\mathbf{z}^{(j)}) \leq w$ for all $j = 1, \ldots, u$. Note, that the public key in (7) is a codeword of an interleaved Gabidulin code $\text{IGab}[u; n, k]$ over $\mathbb{F}_{q^m}$ that is corrupted by an error of rank $w$.

Recently, Wachter-Zeh et al. showed that the key-recovery attack from [8] is equivalent to the decoding problem of an interleaved Gabidulin code [7, Thm. 3], i.e. to the problem of recovering $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(u)}$ and $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(u)}$ from (7). Hence, an attacker can reconstruct an alternative private key by running an interleaved decoder on the public key $\mathbf{k}_{\text{pub}}$, which is possible since the generator matrix $\mathbf{G}$ of the component codes is public.

This observation provides an explicit repair of the FL system by choosing the error vectors $\mathbf{z}^{(j)}$ for $j = 1, \ldots, u$ in the key generation step (see Section 3.1) such that a probabilistic unique interleaved Gabidulin decoder fails although $w$ satisfies (6). The most secure choice for $\mathbf{z}$ in (7) is such that $\mathbf{z}^{(1)} = \mathbf{z}^{(2)} = \cdots = \mathbf{z}^{(u)}$ with $\text{rk}_q(\mathbf{z}^{(j)}) = w$ for all $j = 1, \ldots, u$. The number of keys is still large enough by restricting to error vectors of this form [7]. Hence, the cryptosystem can be repaired by constructing the component error vectors of $\mathbf{z}$ in (3) as

$$\mathbf{z}^{(j)} = (\mathbf{s}^{(1)} | \mathbf{0}) \mathbf{P}^{-1} \qquad \forall j = 1, \ldots, u$$

with $\mathbf{s}^{(1)} \in \mathbb{F}_{q^m}^w$ and $\text{rk}_q(\mathbf{s}^{(1)}) = w$. The parameters of the repaired FL system as in [7] are given in Table 1.

## 4 A GMD-based Key-Recovery Attack

In this section we present a new attack on the repaired FL cryptosystem that allows to recover the private key of some weak public keys efficiently. The attack is based on the principle of GMD decoding [10]. The general idea of GMD decoding is to incorporate soft information (e.g. from the communication channel) in the bounded minimum distance (BMD) decoding process by erasing the most unreliable positions. This results in an improved error correction performance, since a BMD decoder can correct twice more erasures than errors. The principle of GMD decoding can be extended to rank-metric codes [11], where rank errors

can be traded for row and column erasures (see (2)). An erasure in the case of rank-metric codes can occur either row and/or column wise in the corresponding codeword matrix. That means the entries in one or more rows and/or columns are erased but the positions of the rows and columns are known.

Although an attacker is not provided with soft information about the error vector $\mathbf{z}$ that obfuscates the private information about the public key (4), we show that a GMD-based key-recovery attack that exploits the improved correction capability for row and column erasures is feasible for some error patterns $\mathbf{z}$, even if all possible combinations of row and column erasure positions need to be considered. The knowledge of $\mathbf{z}$ allows to recover $\mathbf{x}$ by computing

$$\mathbf{x} = (\mathbf{k}_{\text{pub}} - \mathbf{z})\mathbf{G}^{\dagger}$$

where $\mathbf{G}^{\dagger}$ is the right inverse of the generator matrix $\mathbf{G}$. Hence, an alternative private key $(\tilde{\mathbf{P}}, \mathbf{x}, \mathbf{z})$ can be obtained by computing an invertible matrix $\tilde{\mathbf{P}} \in \mathbb{F}_q^{n\times n}$ satisfying

$$\mathbf{z}\mathbf{P} = \left(\tilde{\mathbf{s}}^{(1)} | \mathbf{0}\right)$$

with $\tilde{\mathbf{s}}^{(1)} \in \mathbb{F}_{q^m}^{w}$ and $\text{rk}_q(\tilde{\mathbf{s}}^{(1)}) = w$. Since one $\mathbf{z}^{(j)}$ in (7) is sufficient to recover the whole error vector $\mathbf{z}$ in the repaired FL system, we focus on the first row of the expanded public key in (7), i.e.

$$\mathbf{k}_{\text{pub}}^{(1)} = \mathbf{x}^{(1)}\mathbf{G} + \mathbf{z}^{(1)} \quad \text{with } \text{rk}_q(\mathbf{z}^{(1)}) = w.$$

A straightforward decoding approach using a BMD Gabidulin decoder for the code $\text{Gab}[n, k]$ with generator matrix $\mathbf{G}$ will fail since $w = \text{rk}_q\left(\mathbf{z}^{(1)}\right)$ is chosen such that $w > (n-k)/2$. We define the excess of the error rank $w$ over the unique decoding radius as

$$\xi \stackrel{\text{def}}{=} w - \frac{n-k}{2}. \tag{8}$$

Recall, that for Gabidulin codes there exist algorithms [13,14,16] that can correct $\delta = \epsilon + \rho$ row and column erasures and errors of rank $w$ up to (see (2))

$$2w + \delta \leq n - k.$$

By artificially imposing $\delta$ row and column erasures on $\mathbf{k}_{\text{pub}}^{(1)}$ and thus on the error vector $\mathbf{z}^{(1)}$, one obtains a new error vector $\mathbf{z'}^{(1)}$ with $w' \stackrel{\text{def}}{=} \text{rk}_q\left(\mathbf{z'}^{(1)}\right) \leq w$. Thus, an error and row/column erasure decoder can successfully decode if

$$2w' + \delta \leq n - k. \tag{9}$$

Using (8), (9) and the fact that $w - \delta \leq w' \leq w$, we obtain[1]

$$2\xi \leq \delta \leq n - k. \tag{10}$$

[1] Note, that by definition $2\xi$ is always an integer (see (8)).

Let $\mathsf{Dec}_{\mathbf{G}}(\cdot)$ denote an efficient error erasure decoding algorithm for the Gabidulin code $\mathrm{Gab}[n,k]$ characterized by the generator matrix $\mathbf{G}$ that returns an estimate $\hat{\mathbf{x}}^{(1)}\mathbf{G}$ of the "transmitted" codeword $\mathbf{x}^{(1)}\mathbf{G} \in \mathrm{Gab}[n,k]$.

We define the set $\mathcal{I}_\delta$ of row and column erasure patterns as

$$\mathcal{I}_\delta \stackrel{\text{def}}{=} \{(\mathbf{a},\mathbf{b}) : \mathbf{a} \in \mathbb{F}_2^m, \mathbf{b} \in \mathbb{F}_2^n \text{ with } \mathrm{w}_H(\mathbf{a}) + \mathrm{w}_H(\mathbf{b}) = \delta\}$$

where the nonzero entries in $\mathbf{a}$ and $\mathbf{b}$ indicate the row and column erasure positions and $\mathrm{w}_H(\cdot)$ denotes the Hamming weight of a binary vector.

For any matrix $\mathbf{Y} \in \mathbb{F}_q^{m\times n}$ let $\mathcal{E}_{(\mathbf{a},\mathbf{b})}(\mathbf{Y})$ denote the row and column erasure operator that returns the matrix $\mathbf{Y} \in \mathbb{F}_q^{m\times n}$ where the rows and columns are erased (i.e. set to zero) according to the erasure pattern $(\mathbf{a},\mathbf{b})$. We may also use the operator $\mathcal{E}_{(\mathbf{a},\mathbf{b})}(\mathbf{y})$ on the corresponding vector $\mathbf{y} \in \mathbb{F}_{q^m}^n$. Algorithm 1 summarizes the proposed GMD-based key-recovery attack.

**Algorithm 1:** A GMD-based Key-Recovery Attack

**Input** : $\mathbf{k}_{\text{pub}}^{(1)}, \mathbf{G}, w, \mathcal{I}_\delta, N_{\max}$

**Output:** $\hat{\mathbf{x}}^{(1)}, \hat{\mathbf{z}}^{(1)}$ with $\mathrm{rk}_q(\hat{\mathbf{z}}^{(1)}) = w$ s.t. $\hat{\mathbf{x}}^{(1)}\mathbf{G} + \hat{\mathbf{z}}^{(1)} = \mathbf{k}_{\text{pub}}^{(1)}$ or "failure"

```
1  foreach i ∈ [1, N_max] do
2      foreach δ ∈ [2ξ, n − k] do
3          Pick an erasure pattern (a, b) uniformly at random from I_δ
4          ĉ^(1) ← Dec_G( E_(a,b)(k_pub) )
5          if ĉ^(1) ≠ ∅ then
6              x̂^(1) ← ĉ^(1) G^†
7              z^(1) ← k_pub^(1) − x̂^(1) G
8              if rk_q z^(1) = w then
9                  return x^(1), z^(1)
10 return "failure"
```

In some cases the rank $w$ of the error $\mathbf{z}^{(1)}$ is not reduced enough by the $\delta$ artificial row and column erasures on $\mathbf{k}_{\text{pub}}^{(1)}$ such that (9) is not satisfied. In this case we either get a miscorrection (i.e. decoder returns an estimate $\hat{\mathbf{c}}^{(1)} \neq \mathbf{c}^{(1)}$) or a decoding failure ($\mathsf{Dec}_{\mathbf{G}}(\cdot) = \emptyset$). Line 8 detects miscorrections that lead to codewords $\hat{\mathbf{c}}^{(1)}$ that are not at rank distance $w$ from $\mathbf{k}_{\text{pub}}$.[2]

The worst-case computational complexity of the attack in Algorithm 1 is on the order of $|\mathcal{I}_\delta|\mathcal{O}(n^2)$ operations in $\mathbb{F}_{q^m}$. The codes considered for the FL cryptosystem are rather short (see Table 1). That means it is computationally

[2] There may be estimates $\hat{\mathbf{c}}^{(1)}$ at rank distance $w$ from $\mathbf{k}_{\text{pub}}$ such that $\hat{\mathbf{c}}^{(1)} \neq \mathbf{c}^{(1)}$. However, this event is very unlikely since $\xi$ is very small for the considered parameters (see Table 1) and was not observed in our simulations.

affordable to iterate through all possible erasure patterns with $\delta$ row and column erasures which are satisfying (10). Algorithm 1 can be parallalized to improve the runtime of the attack.

We say that the attack in Algorithm 1 is successful if the algorithm outputs $\hat{\mathbf{x}}^{(1)}, \hat{\mathbf{z}}^{(1)}$ (not "failure"). This means, that there exists an erasure pattern incorporating $\delta$ row and column erasures such that (9) is satisfied.

## 5 Classification of Weak Keys

In this section we classify some types of weak keys, in particular the corresponding error vectors $\mathbf{z}^{(1)}$, that are vulnerable against the key-recovery attack in Algorithm 1.

Let the invertible matrix $\mathbf{P}^{-1} \in \mathbb{F}_q^{n \times n}$ in (3) be partitioned such that

$$\mathbf{P}^{-1} = \begin{pmatrix} \mathbf{P}_1 \\ \mathbf{P}_2 \end{pmatrix}$$

with matrices $\mathbf{P}_1 \in \mathbb{F}_q^{w \times n}$ and $\mathbf{P}_2 \in \mathbb{F}_q^{(n-w) \times n}$ having full rank. Then by (3) we have that

$$\mathbf{z}^{(1)} = \mathbf{s}^{(1)} \mathbf{P}_1. \tag{11}$$

Since $\mathbf{P}_1$ is of full rank we can decompose it as

$$\mathbf{P}_1 = \mathbf{A} \cdot [\mathbf{I}_{w \times w} \,|\, \mathbf{Q}] \cdot \mathbf{B} \tag{12}$$

where $\mathbf{A} \in \mathbb{F}_q^{w \times w}$ is of full rank and $\mathbf{B} \in \mathbb{F}_q^{n \times n}$ is a permutation matrix.

In the following we restrict to column erasure attacks only (i.e. $\delta = \epsilon$) and describe weak keys by the structure of $\mathbf{Q}$. The decomposition in (12) of $\mathbf{P}_1$ is in general not unique. By "weak keys" we refer to error vectors $\mathbf{z}^{(1)}$ of the form (11) for which there exists a decomposition (12) of $\mathbf{P}_1$ with $\mathbf{Q}$ having a structure as described in the following subsections. Note, that by writing (11) over $\mathbb{F}_q$ we get similar arguments for row erasures on the rows of the corresponding matrix $\mathbf{S}^{(1)}$ of the vector $\mathbf{s}^{(1)}$.

### 5.1 Rank Equal to Hamming Weight Error Patterns

The rank of $\mathbf{z}^{(1)}$ is equal to its Hamming weight, i.e. $\mathrm{rk}_q(\mathbf{z}^{(1)}) = \mathrm{w}_H(\mathbf{z})$, if $\mathbf{Q}$ in (12) is the allzero matrix ($\mathbf{Q} = \mathbf{0}$). A necessary condition for the success of Algorithm 1 is that the erasure pattern for the column erasures at a certain iteration is chosen such that (9) holds. Let us denote by $S_{\epsilon,1}$ such an event for a specific number of column erasures $\epsilon$ given that the error vector $\mathbf{z}^{(1)}$ has rank equal to its Hamming weight. For this special case we can compute the success probability as

$$\Pr(S_{\epsilon,1}) = \frac{\sum_{i=\lceil \xi + \epsilon/2 \rceil}^{\min(\epsilon, w)} \binom{w}{i} \binom{n-w}{\epsilon - i}}{\binom{n}{\epsilon}} \tag{13}$$

where the denominator is the number of all possible column erasure patterns for a given $\epsilon$ and the numerator is the sum of the number of events for which $i$ many errors are traded for erasures. The maximum number of errors that can be traded for erasures is $\min(\epsilon, w)$. The minimum amount of errors that need to be traded for erasures such that (9) holds is $\lceil \xi + \epsilon/2 \rceil$, which we obtain by inserting the relation $w' = w - i$ into (9) and using the definition of $\xi$ from (8). The probability $\Pr(S_{\epsilon,1})$ for the 80-bit security parameters proposed in [7] is shown in Figure 1.

### 5.2 $\eta$-Weak Error Patterns

The weakness of the keys described by an allzero matrix $\mathbf{Q}$ comes from the fact that whenever one of the $w$ nonzero entries in $\mathbf{z}$ is hit by an erasure the rank of $\mathbf{z}$ is reduced by one. The number of these events is considerably high (see numerator of (13)), even for error patterns that can be decomposed as in (12) with a matrix $\mathbf{Q}$ having a certain amount of allzero rows. Let $\eta$ denote the fraction of allzero rows in $\mathbf{Q}$, i.e. $\eta = N_0/w$, where $N_0$ is the number of allzero rows in $\mathbf{Q}$. Clearly, for $\eta = 1$ we have that $\mathrm{w}_H(\mathbf{z}^{(1)}) = \mathrm{rk}_q(\mathbf{z}^{(1)})$. The success probability of Algorithm 1 for keys with $\eta < 1$, which we refer to as $\eta$-weak error patterns, depends on the remaining nonzero entries of $\mathbf{Q}$.

Based on (13) we derive a lower bound on the success probability by assuming that only the positions in $\mathbf{z}^{(1)}$ that are related to the allzero rows of $\mathbf{Q}$ are the cause for the rank reduction of $\mathbf{z}$. Let $S_{\epsilon,\eta}$ denote the event that in a certain iteration of Algorithm 1 an erasure pattern with $\epsilon$ columns erasures such that (9) holds is picked, given that $\mathbf{z}^{(1)}$ is an $\eta$-weak error pattern. The probability of $S_{\epsilon,\eta}$ can be lower bounded by

$$\Pr(S_{\epsilon,\eta}) \geq P(\epsilon,\eta) \stackrel{\text{def}}{=} \frac{\sum_{i=\lceil \xi+\epsilon/2 \rceil}^{\min(\epsilon, w\eta)} \binom{w\eta}{i} \binom{n-w\eta}{\epsilon-i}}{\binom{n}{\epsilon}} \tag{14}$$

that is the cumulative sum of a hypergeometric distribution.

The tightness of the lower bound $P(\epsilon, \eta)$ in (14) is validated by simulations for different $\eta$-weak error patterns $\mathbf{z}^{(1)}$ for the 80-bit security parameters from [7]. The simulation results are illustrated in Figure 1. The success rates for the smallest possible $\eta$ for different security levels are given in Table 1.

### 5.3 Further Weak Error Patterns

Simulation results show that there exist further error patterns that are different from the previously characterized patterns and can be recovered by Algorithm 1. In particular, another class of weak keys is characterized by matrices $\mathbf{Q}$ with $\mathrm{rk}_q(\mathbf{Q}) \ll \min(w, n-w)$. Figure 2 shows the simulations results of the success rate over $\epsilon$ for matrices $\mathbf{Q}$ with $\mathrm{rk}_q \mathbf{Q} = 1$ and $\mathrm{rk}_q \mathbf{Q} = 2$ that do not correspond to $\eta$ error patterns with $\eta > 0$.

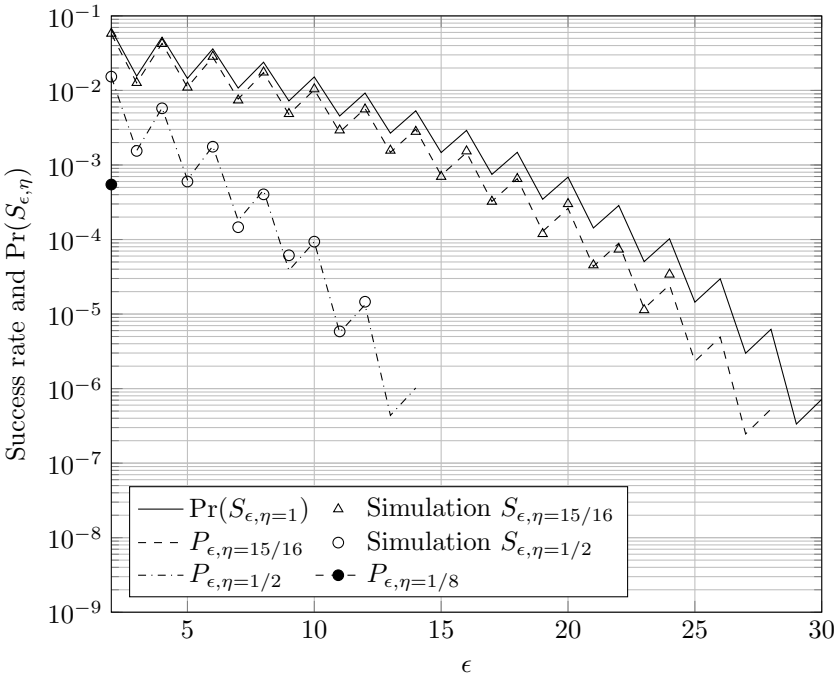


**Fig. 1.** Conditional success rate and success probability of a column erasure attack according to Algorithm 1 for $\eta$-weak error patterns with different values of $\eta$ using the parameters proposed in [7] for the 80-bit security level. For each value of $\eta$ and $\epsilon$ the simulation results were obtained by Monte Carlo Simulations running $2 \cdot 10^6$ iterations and choosing in every iteration a random $\eta$-weak error pattern $\mathbf{z}^{(1)}$ with $\mathrm{rk}_q(\mathbf{z}^{(1)}) = w$ and $\mathbf{Q}$ having $w\eta$ allzero rows.

**Table 1.** Parameters for the repaired FL cryptosystem in [7] and the corresponding probabilities for $\eta$-weak error patterns with $\eta = 2\xi/w$ and a column erasure attack with $\epsilon = 2\xi$ column erasures.

| Security Level | $q$ | $m$ | $u$ | $n$ | $k$ | $w$ | Key Size | $\xi$ | $\log_2(\Pr(S_{2\xi,2\xi/w}))$ |
|---|---|---|---|---|---|---|---|---|---|
| 80-bit | 2 | 61 | 3 | 61 | 31 | 16 | 1.86 KB | 1 | -10.82 |
| 128-bit | 2 | 63 | 3 | 63 | 31 | 18 | 1.98 KB | 2 | -19.16 |
| 256-bit | 2 | 82 | 4 | 82 | 48 | 20 | 4.20 KB | 3 | -28.36 |

## 6 Conclusions

A new key-recovery attack on the Faure–Loidreau (FL) system was presented. The attack uses ideas from generalized minimum distance (GMD) decoding of rank-metric codes to recover private keys from some weak public keys. Some families of weak keys were classified and analyzed.

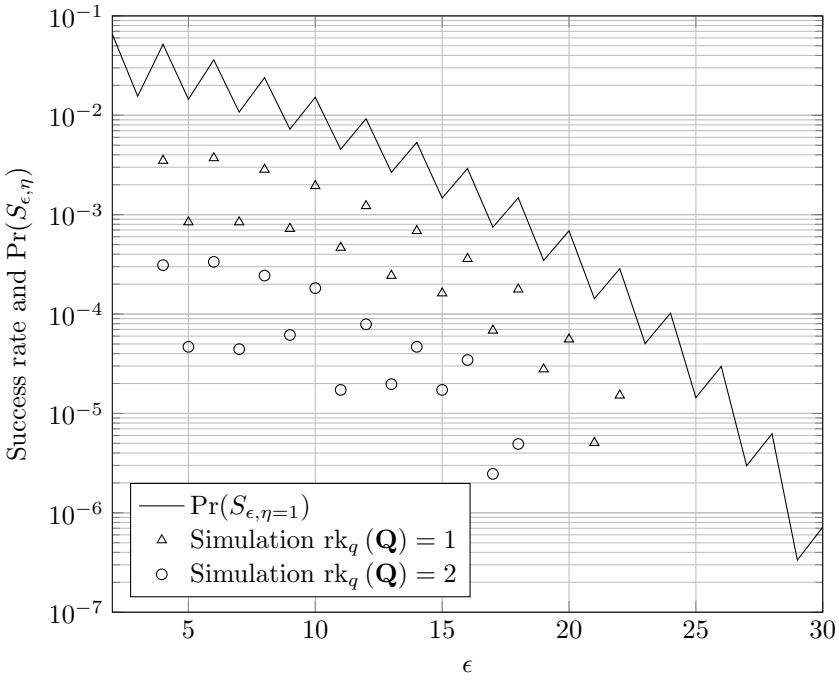


**Fig. 2.** Conditional success rate and success probability of a column erasure attack according to Algorithm 1 for weak keys with $\mathbf{Q}$ of low rank and having no allzero rows. The parameters proposed in [7] for the 80-bit security level are used. For each value of $\epsilon$ the simulation results were obtained by Monte Carlo simulations runing $2 \cdot 10^6$ iterations and choosing in every iteration a random error vector $\mathbf{z}^{(1)}$ with $\mathrm{rk}_q(\mathbf{z}^{(1)}) = w$ and $\mathrm{rk}_q(\mathbf{Q}) \in \{1, 2\}$. The probability of success $\Pr(S_{\epsilon,\eta=1})$ for error patterns with Hamming weight equal to their rank weight is plotted as a reference.

We showed, that for the current parameters, the private keys of some weak public keys can be recovered with an effort which is substantially lower than the security level of the cryptosystem. The classification of all weak keys that are vulnerable to the attack presented in this paper is still an open problem and subject to further research. That means we require that by generating a random public key as proposed in the FL cryptosystem the probability of picking a weak key that is affected by the attack is within the proposed security level.

## References

1. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

2. P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.
3. P. Loidreau, "Designing a rank metric based mceliece cryptosystem," in *Post-Quantum Cryptography*, N. Sendrier, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 142–152.
4. R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Codes," *Deep Space Network Progress Report*, vol. 44, pp. 114–116, 1978.
5. 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.
6. D. Augot and M. Finiasz, "A Public Key Encryption Scheme based on the Polynomial Reconstruction Problem," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2003, pp. 229–240.
7. A. Wachter-Zeh, S. Puchinger, and J. Renner, "Repairing the Faure-Loidreau Public-Key Cryptosystem," in *IEEE Int. Symp. Inform. Theory (ISIT)*, Jun 2018.
8. P. Gaborit, A. Otmani, and H. T. Kalachi, "Polynomial-time Key Recovery Attack on the Faure–Loidreau Scheme based on Gabidulin codes," *Designs, Codes and Cryptography*, vol. 86, no. 7, pp. 1391–1403, 2018.
9. P. Loidreau and R. Overbeck, "Decoding Rank Errors Beyond the Error Correcting Capability," in *International Workshop on Algebraic and Combinatorial Coding Theory (ACCT)*, Sep. 2006, pp. 186–190.
10. G. Forney, "Generalized Minimum Distance Decoding," *IEEE Transactions on Information Theory*, vol. 12, no. 2, pp. 125–131, 1966.
11. M. Bossert, E. Costa, E. Gabidulin, E. Schulz, and M. Weckerle, "Verfahren und Kommunikationsvorrichtung zum Dekodieren von mit einem Rang-Code codierten Daten ," EU Patent EP20 040 104 458, 2003.
12. E. M. Gabidulin, "Theory of Codes with Maximum Rank Distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.
13. E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Rank Errors and Rank Erasures Correction," in *4th International Colloquium on Coding Theory*, 1991.
14. G. Richter and S. Plass, "Error and Erasure Decoding of Rank-Codes with a Modified Berlekamp-Massey Algorithm," in *International ITG Conference on Systems, Communications and Coding 2004 (SCC)*, 2004.
15. E. M. Gabidulin and N. I. Pilipchuk, "Error and Erasure Correcting Algorithms for Rank Codes," *Designs, codes and Cryptography*, vol. 49, no. 1-3, pp. 105–122, 2008.
16. D. Silva, "Error Control for Network Coding," Ph.D. dissertation, 2009.
17. V. Sidorenko, L. Jiang, and M. Bossert, "Skew-feedback shift-register synthesis and decoding interleaved gabidulin codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 621–632, Feb 2011.
18. A. Wachter-Zeh and A. Zeh, "List and unique error-erasure decoding of interleaved gabidulin codes with interpolation techniques," *Des. Codes Cryptography*, vol. 73, no. 2, pp. 547–570, Nov. 2014. [Online]. Available: http://dx.doi.org/10.1007/s10623-014-9953-5

# A Appendix

## A.1 Encryption

Let $\mathbf{m} = (m_1\ m_2\ \ldots\ m_{k-u}\,|\,0\ \ldots\ 0) \in \mathbb{F}_{q^m}^k$ be the plaintext.

1. Choose an element $\alpha \in \mathbb{F}_{q^{mu}}$ at random.
2. Choose $\mathbf{e} \in \mathbb{F}_{q^m}^n$ with $\mathrm{rk}_q(\mathbf{e}) \leq t_{\mathrm{pub}}$ at random.
3. Compute the ciphertext $\mathbf{c} \in \mathbb{F}_{q^m}^n$ as

$$\mathbf{c} = \mathbf{mG} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{k}_{\mathrm{pub}}) + \mathbf{e}.$$

## A.2 Decryption

1. Compute

$$\mathbf{cP} = \mathbf{mGP} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{k}_{\mathrm{pub}})\mathbf{P} + \mathbf{eP}.$$

   Due to the $\mathbb{F}_{q^m}$-linearity of the trace we have

$$\mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{k}_{\mathrm{pub}})\mathbf{P} = \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x})\mathbf{GP} + (\mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{s})\,|\,\mathbf{0})$$

   and get

$$\mathbf{cP} = (\mathbf{m} + \mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{x}))\mathbf{GP} + (\mathrm{Tr}_{q^{mu}/q^m}(\alpha \mathbf{s})\,|\,\mathbf{0}) + \mathbf{eP}.$$

2. Define $\mathbf{G}'_P$ as the last $n-w$ columns of the product $\mathbf{GP}$ and let $\mathbf{c}'$ and $\mathbf{e}'$ be the last $n-w$ positions of $\mathbf{c}$ and $\mathbf{eP}$, respectively. Then we have that

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

   with $\mathrm{rk}_q(\mathbf{e}') \leq t_{\mathrm{pub}} = \left\lfloor \frac{n-k-w}{2} \right\rfloor$.
   Since $\mathbf{G}'_P$ is a generator matrix of $\mathrm{Gab}[n-w, k]$ we can decode to remove $\mathbf{e}'$ and get

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

3. Since $\mathbf{m} = (m_1\ m_2\ \ldots\ m_{k-u}\,|\,\underbrace{0\ \ldots\ 0}_{u})$ we have that the last $u$ positions of $\mathbf{m}'$ are

$$m'_i = \mathrm{Tr}_{q^{mu}/q^m}(\alpha x_i), \qquad \forall i = k-u+1, \ldots, k.$$

   Since $\mathcal{X} \stackrel{\mathrm{def}}{=} (x_{k-u+1}, \ldots, x_k)$ forms an ordered basis of $\mathbb{F}_{q^{mu}}$ over $\mathbb{F}_{q^m}$ we can compute $\alpha$ as

$$\alpha = \sum_{i=k-u+1}^{k} \mathrm{Tr}_{q^{mu}/q^m}(\alpha x_i) x_i^{\perp} = \sum_{i=k-u+1}^{k} m'_i x_i^{\perp},$$

   where $\mathcal{X}^{\perp} \stackrel{\mathrm{def}}{=} (x_{k-u+1}^{\perp}, \ldots, x_k^{\perp})$ denotes the dual basis of $\mathcal{X}$. Finally, we can recover the plaintext as

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