On the security of a Loidreau's rank metric code based encryption scheme

Daniel Coggia[1,2] and Alain Couvreur[2,3]

[1] DGA
[2] INRIA,
[3] LIX, CNRS UMR 7161, École polytechnique,
91128 Palaiseau Cedex, France.
daniel.coggia@inria.fr, alain.couvreur@inria.fr

Abstract. We present a polynomial time attack of a rank metric code based encryption scheme due to Loidreau for some parameters.

Key words. Rank metric codes, Gabidulin codes, code based cryptography, cryptanalysis.

Introduction

To instantiate McEliece encryption scheme, one needs a family of codes with random looking generator matrices and an efficient decoding algorithm. If the original proposal due to McEliece himself [12] relies on classical Goppa codes endowed with the Hamming metric, one can actually consider codes endowed with any other metric. The use of $\mathbb{F}_{q^m}$–linear rank metric codes, first suggested by Gabidulin *et. al.* [7] is of particular interest, since the $\mathbb{F}_{q^m}$–linearity permits a very "compact" representation of the code and hence permits to design a public key encryption scheme with rather short keys compared to the original McEliece proposal.

Compared to the Hamming metric world, only few families of codes with efficient decoding algorithms are known in rank metric. Basically, the McEliece scheme has been instantiated with two general families of rank metric codes, namely Gabidulin codes [5,6] and LRPC codes [8].

In [11], Loidreau proposed the use of codes which can somehow be regarded as an intermediary version between Gabdiulin codes and LRPC codes. These codes are obtained by right multiplying a Gabidulin code with an invertible matrix whose entries are in $\mathbb{F}_{q^m}$ and span an $\mathbb{F}_q$–subspace of small dimension λ. This approach can be regarded as a "rank metric" counterpart of BBCRS scheme [1] in Hamming metric.

In the present article, we explain why the case $\lambda = 2$ and $\dim \mathscr{C}_{\text{pub}} \geqslant n/2$ is weak and describe a key recovery attack in this situation.

Note. The material of the present article has been communicated to Pierre Loidreau in april 2016. The article [11] is subsequent to this discussion and proposes parameters which avoid the attack described in the present article.

1 Prerequisites

1.1 Rank metric codes

In this article m, n denote positive integers and q a prime power. A *code of dimension k* is an $\mathbb{F}_{q^m}$–subspace of $\mathbb{F}_{q^m}^n$ whose dimension as an $\mathbb{F}_{q^m}$–vector space is k. Given a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, the *rank weight* or *rank* of $\boldsymbol{x}$, denoted as $|\boldsymbol{x}|_{\mathrm{R}}$ is the dimension of the $\mathbb{F}_q$–vector sub-space of $\mathbb{F}_{q^m}$ spanned by the entries of $\boldsymbol{x}$. The *support* of a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, denoted $\mathsf{supp}(\boldsymbol{x})$ is the $\mathbb{F}_q$–vector space spanned by the entries of $\boldsymbol{x}$. Hence the rank of $\boldsymbol{x}$ is nothing but the dimension of its support. The *rank distance* or *distance* of two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is defined as

$$d_{\mathrm{R}}(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} |\boldsymbol{x} - \boldsymbol{y}|_{\mathrm{R}}.$$

Given a code $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$, the *minimum distance* of $\mathscr{C}$ is defined as

$$\mathrm{d}_{\min}(\mathscr{C}) \stackrel{\text{def}}{=} \min_{\boldsymbol{x} \in \mathscr{C} \setminus \{0\}} \{|\boldsymbol{x}|_{\mathrm{R}}\}.$$

1.2 q–polynomials and Gabidulin codes

A *q–polynomial* or a *linear polynomial* is an $\mathbb{F}_{q^m}$–linear combination of monomials $X, X^q, X^{q^2}, \ldots, X^{q^s}, \ldots$ Such a polynomial induces a function $\mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$ which is $\mathbb{F}_q$–linear. The *q–degree* of a q–polynomial P, denoted by $\deg_q(P)$ is the integer s such that the degree of P is q^s. In short:

$$P = \sum_{i=0}^{\deg_q P} p_i X^{q^i}, \ p_i \in \mathbb{F}_{q^m}, \ p_{\deg_q P} \neq 0.$$

The following very classical result is crucial in what follows.

Proposition 1. *Let $P \in \mathbb{F}_{q^m}[X]$ be a q–polynomial. Then, the set of roots of P in $\mathbb{F}_{q^m}$ is an $\mathbb{F}_q$–vector space of dimension less than or equal to $\deg_q P$.*

The space of q–polynomials is denoted by $\mathcal{L}$ and, given a positive integer s, the space of q–polynomials of degree less than s is denoted by

$$\mathcal{L}_{<s} \stackrel{\text{def}}{=} \left\{P \in \mathcal{L} \mid \deg_q P < s\right\}.$$

Given positive integers k, n with $k \leqslant n \leqslant m$ and an n–tuple $\boldsymbol{a} = (a_1, \ldots, a_n)$ of $\mathbb{F}_q$–linearly independent elements of $\mathbb{F}_{q^m}$, the *Gabidulin code* $\mathcal{G}_k(\boldsymbol{a})$ is defined as

$$\mathcal{G}_k(\boldsymbol{a}) \stackrel{\text{def}}{=} \{(f(a_1), \ldots, f(a_n)) \mid f \in \mathcal{L}_{<k}\}.$$

Such codes are known to have minimum distance $n - k + 1$ and to benefit from a decoding algorithm correcting up to half the minimum distance (see [9]).

The n–tuple $\boldsymbol{a}$ is referred to as the *support* of the code. Note that the support is not unique as shown by the following lemma which will be useful for our attack.

Lemma 1. *Let* $\alpha \in \mathbb{F}_{q^m}$. *Then* $\mathcal{G}_k(\boldsymbol{a}) = \mathcal{G}_k(\alpha\boldsymbol{a})$.

1.3 The component-wise Frobenius map

In what follows, we will frequently apply the component-wise Frobenius map or its iterates to vectors or codes. Hence, we introduce the following notation. Given a vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ and a nonnegative integer s, we denote by $\boldsymbol{v}^{[s]}$ the vector:

$$\boldsymbol{v}^{[s]} \stackrel{\text{def}}{=} (v_1^{q^s}, \ldots, v_n^{q^s}).$$

Similarly, given a code $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ and a positive integer s, the code $\mathscr{C}^{[s]}$ denotes the code

$$\mathscr{C}^{[s]} \stackrel{\text{def}}{=} \{\boldsymbol{c}^{[s]} \mid \boldsymbol{c} \in \mathscr{C}\}.$$

1.4 Overbeck's distinguisher

In [13], Overbeck proposes a general framework to break cryptosystems based on Gabidulin codes. The core of his attack is that a simple operation permits to distinguish Gabidulin codes from random ones. Indeed, given a random code $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ of dimension $k < n/2$, the expected dimension of the code $\mathscr{C} + \mathscr{C}^{[1]}$ equals $2k$ and, equivalently $\mathscr{C} \cap \mathscr{C}^{[1]}$ is likely to be equal to 0. More generally, we have the following statement.

Proposition 2. *If $\mathscr{C}_{rand}$ is a code of length n and dimension k chosen uniformly at random, then for a nonnegative integer a and for a positive integer $s < k$, we have*

$$\mathbb{P}\left(\dim_{\mathbb{F}_{q^m}} \mathscr{C}_{rand}+\mathscr{C}_{rand}{}^{[1]}+\cdots+\mathscr{C}_{rand}{}^{[s]} \leqslant \min(n,(s+1)k)-a\right) = O(q^{-ma}).$$

On the other hand, for a Gabidulin code, the behaviour with respect to such operations is completely different as explained in the following statement.

Proposition 3. *Let $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ be a word of rank n, $k \leqslant n$ and s be an integer. Then,*

$$\mathcal{G}_k(\boldsymbol{a}) \cap \mathcal{G}_k(\boldsymbol{a})^{[1]} = \mathcal{G}_{k-1}(\boldsymbol{a}^{[1]});$$
$$\mathcal{G}_k(\boldsymbol{a}) + \cdots + \mathcal{G}_k(\boldsymbol{a})^{[s]} = \mathcal{G}_{k+s}(\boldsymbol{a}).$$

2 Loidreau's scheme

In order to mask the structure of Gabidulin codes and to resist to Overbeck's attack, Loidreau suggested in [11] the following construction. Denote by $\boldsymbol{G}$ a random generator matrix of a Gabidulin code $\mathcal{G}_k(\boldsymbol{a})$. Fix an integer $\lambda \leqslant m$ and an $\mathbb{F}_q$–vector subspace $\mathcal{V}$ of $\mathbb{F}_{q^m}$ of dimension λ. Let $\boldsymbol{P} \in \mathbf{GL}(n, \mathbb{F}_{q^m})$ whose entries are all in $\mathcal{V}$. Then, let

$$\boldsymbol{G}_{\text{pub}} \stackrel{\text{def}}{=} \boldsymbol{G}\boldsymbol{P}^{-1}.$$

We have the following encryption scheme.

Public key: The pair $(\boldsymbol{G}_{\text{pub}}, t)$ where $t \stackrel{\text{def}}{=} \lfloor \frac{n-k}{2\lambda} \rfloor$.
Secret key: The pair $(\boldsymbol{a}, \boldsymbol{P})$.
Encryption: Given a plaintext $\boldsymbol{m} \in \mathbb{F}_{q^m}^k$, choose a uniformly random vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of rank weight t. The ciphertext is

$$\boldsymbol{c} \stackrel{\text{def}}{=} \boldsymbol{m}\boldsymbol{G}_{\text{pub}} + \boldsymbol{e}.$$

Decryption: Compute,

$$\boldsymbol{c}\boldsymbol{P} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}\boldsymbol{P}.$$

Since the entries of $\boldsymbol{P}$ are all in $\mathcal{V}$ then, the entries of $\boldsymbol{e}\boldsymbol{P}$ are in the product space $\mathsf{supp}(\boldsymbol{e}) \cdot \mathcal{V} \stackrel{\text{def}}{=} \langle uv \mid u \in \mathsf{supp}(\boldsymbol{e}),\ v \in \mathcal{V}\rangle_{\mathbb{F}_q}$. The dimension of this space is bounded from above by $t\lambda \leqslant \frac{n-k}{2}$. Therefore, using a classical decoding algorithm for Gabidulin codes, one can recover $\boldsymbol{m}$.

3 A distinguisher when $\lambda = 2$

3.1 Context

The goal of this section is to establish a distinguisher for Loidreau's cryptosystem instantiated with $\lambda = 2$ and a public code $\mathscr{C}_{\mathrm{pub}}$ of dimension $k \geqslant \frac{n}{2}$. Similarly to Overbeck's attack, this distinguisher reposes on Propositions 2 and 3.

Similarly to the attacks of BBCRS system [3,4], it is more convenient to work on the dual of the public code because of the following lemmas.

Lemma 2 ([10, Page 52]). *The code $\mathcal{G}_k(\boldsymbol{a})^\perp$ is a Gabidulin code $\mathcal{G}_{n-k}(\boldsymbol{b})$ for some $\boldsymbol{b} \in \mathbb{F}_{q^m}^n$ of rank n.*

Lemma 3 ([4, Lemma 1]). *Any full-rank generator matrix $\boldsymbol{H}_{\mathrm{pub}}$ of $\mathscr{C}_{pub}^\perp$ can be decomposed as $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{H}_{\mathrm{sec}}\boldsymbol{P}^T$ where $\boldsymbol{H}_{\mathrm{sec}}$ is a parity–check of the Gabidulin code $\mathcal{G}_k(\boldsymbol{a})$.*

The convenient aspect of the previous lemma is that the matrix $\boldsymbol{P}$ has its entries in a small vector space, while its inverse has not.

3.2 The case $\lambda = 2$

We suppose in this section that the vector space $\mathcal{V} \subseteq \mathbb{F}_{q^m}^n$ in which the matrix $\boldsymbol{P}$ has all its entries has dimension 2:

$$\lambda = \dim_{\mathbb{F}_q} \mathcal{V} = 2.$$

Note that, w.l.o.g, one can suppose that $1 \in \mathcal{V}$. Indeed, if $\mathcal{V}$ is spanned over $\mathbb{F}_q$ by $\alpha, \beta \in \mathbb{F}_{q^m} \setminus \{0\}$, then one can replace $\boldsymbol{H}_{\mathrm{sec}}$ by $\boldsymbol{H}'_{\mathrm{sec}} = \alpha \boldsymbol{H}_{\mathrm{sec}}$ which spans the **same code** and $\boldsymbol{P}' = \alpha^{-1}\boldsymbol{P}$ has entries in $\mathcal{V}' = \mathbf{Span}\{1, \alpha^{-1}\beta\}$ and $\boldsymbol{H}_{\mathrm{pub}} = \boldsymbol{H}'_{\mathrm{sec}}\boldsymbol{P}'^T$.

Thus, from now on, we suppose that $\mathcal{V} = \mathbf{Span}\{1, \gamma\}$ for some $\gamma \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$. Consequently, $\boldsymbol{P}^T$ can be decomposed as

$$\boldsymbol{P}^T = \boldsymbol{P}_0 + \gamma \boldsymbol{P}_1,$$

where $\boldsymbol{P}_0, \boldsymbol{P}_1$ are square matrices with entries in $\mathbb{F}_q$. For convenience, we suppose from now on that $\boldsymbol{P}_0$ and $\boldsymbol{P}_1$ are both invertible. Note that this actually holds with a high probability. If one of these matrices was not invertible, then the attack could probably be performed after minor adjustments.

We have seen that $\mathscr{C}_{\mathrm{sec}}^\perp = \mathcal{G}_{n-k}(\boldsymbol{a})$ for some $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ with $|\boldsymbol{a}|_{\mathrm{R}} = n$. We define

$$\boldsymbol{g} \stackrel{\mathrm{def}}{=} \boldsymbol{a}\boldsymbol{P}_0 \quad \text{and} \quad \boldsymbol{h} \stackrel{\mathrm{def}}{=} \boldsymbol{a}\boldsymbol{P}_1.$$

Lemma 4. *The code* $\mathscr{C}_{pub}^{\perp}$ *is spanned by*

$$\boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]} + \gamma \boldsymbol{h}^{[1]}, \dots, \boldsymbol{g}^{[n-k-1]} + \gamma \boldsymbol{h}^{[n-k-1]}.$$

We can now state a crucial result.

Theorem 1. *The dual of the public code satisfies:*

$$\dim_{\mathbb{F}_{q^m}} \mathscr{C}_{pub}^{\perp} + {\mathscr{C}_{pub}^{\perp}}^{[1]} + {\mathscr{C}_{pub}^{\perp}}^{[2]} \leqslant 2 \dim_{\mathbb{F}_{q^m}} \mathscr{C}_{pub}^{\perp} + 2.$$

As a conclusion, thanks to Proposition 2, we deduce that $\mathscr{C}_{\text{pub}}^{\perp}$ is distinguishable in polynomial time from a random code as soon as $2k-2 > n$.

4 The attack

In this section, we derive an attack from the distinguisher defined in Section 3. In what follows, we suppose that $\lambda = 2$ and the public code has rate larger than 1/2 so that the distinguisher introduced in Section 3 works on it. Recall that $\mathscr{C}_{\text{pub}}^{\perp} = \mathcal{G}_{n-k}(\boldsymbol{a})\boldsymbol{P}$ for some $\boldsymbol{a} \in \mathbb{F}_{q^m}^n$ whose entries are $\mathbb{F}_q$–independent and $\boldsymbol{P}$ is of the form $\boldsymbol{P}_0 + \gamma \boldsymbol{P}_1$ for $\boldsymbol{P}_0, \boldsymbol{P}_1 \in \mathcal{M}_n(\mathbb{F}_q)$ and $\gamma \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$. Finally recall that

$$\boldsymbol{g} \stackrel{\text{def}}{=} \boldsymbol{a}\boldsymbol{P}_0 \qquad \text{and} \qquad \boldsymbol{h} \stackrel{\text{def}}{=} \boldsymbol{a}\boldsymbol{P}_1.$$

In addition, we make the following assumptions:

(1) $\boldsymbol{P}_0, \boldsymbol{P}_1 \in \mathbf{GL}(n, \mathbb{F}_q)$;
(2) γ is not contained in any subfield of $\mathbb{F}_{q^m}$;
(3) $\dim \mathscr{C}_{\text{pub}}^{\perp} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[1]} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[2]} = 2(n-k) + 2$.

Assumption (1) has already been discussed in § 3.2. Assumption (2) is reasonable in order to prevent against possible attacks based on an exhaustive search of γ. Finally, Assumption (3) is what typically happens according to our experiments using Magma [2].

The aim of the attack is to recover the triple $(\gamma, \boldsymbol{g}, \boldsymbol{h})$, or more precisely, to recover a triple $(\gamma', \boldsymbol{g}', \boldsymbol{h}')$ such that

$$\mathscr{C}_{\text{pub}}^{\perp} = \langle \boldsymbol{g}'^{[i]} + \gamma' \boldsymbol{h}'^{[i]} \mid i = 0, \dots, n-k-1 \rangle. \tag{1}$$

Actually, the triple $(\gamma, \boldsymbol{g}, \boldsymbol{h})$ is far from being unique and any other triple satisfying (1) permits to decrypt messages (see further § 4.3). Let us describe an action of $\mathbf{PGL}(2, \mathbb{F}_q)$ on such triples.

Proposition 4. *Let* $a, b, c, d \in \mathbb{F}_q$ *such that* $ad - bc \neq 0$ *and* $\delta \in \mathbb{F}_{q^m}$ *such that* $\gamma = \frac{a\delta + b}{c\delta + d}$*. Then, the triple* $(\delta, d\boldsymbol{g} + b\boldsymbol{h}, c\boldsymbol{g} + a\boldsymbol{h})$ *satisfies (1).*

4.1 Step 1: using the distinguisher to compute some subcodes

As shown in the proof of Theorem 1, $\mathscr{C}_{\text{pub}}^{\perp} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[1]}$ is spanned by:

$$\boldsymbol{g} + \gamma \boldsymbol{h} \quad \text{and} \quad \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]}, \dots, \boldsymbol{g}^{[t]}, \boldsymbol{h}^{[t]} \quad \text{and} \quad \boldsymbol{g}^{[t+1]} + \gamma^q \boldsymbol{h}^{[t+1]},$$

where $t \stackrel{\text{def}}{=} n - k - 1$. Then, by iterating intersections

$$(\mathscr{C}_{\text{pub}}^{\perp} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[1]}) \cap ({\mathscr{C}_{\text{pub}}^{\perp}}^{[1]} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[2]}) \cap \dots \cap ({\mathscr{C}_{\text{pub}}^{\perp}}^{[t]} + {\mathscr{C}_{\text{pub}}^{\perp}}^{[t+1]}),$$

we obtain the code spanned by

$$\boldsymbol{g}^{[t]} + \gamma^{q^t} \boldsymbol{h}^{[t]} \quad \text{and} \quad \boldsymbol{g}^{[t+1]} + \gamma^q \boldsymbol{h}^{[t+1]}.$$

Notice that Assumption (3) permits to prove that this intersection has exactly dimension 2. Applying the inverse of the t–th Frobenius, we get the code spanned by

$$\boldsymbol{g} + \gamma \boldsymbol{h} \quad \text{and} \quad \boldsymbol{g}^{[1]} + \gamma^{q^{1-t}} \boldsymbol{h}^{[1]}.$$

Note that $t = n - k - 1 < n \leqslant m$. Hence $\gamma^{q^{1-t}} \neq \gamma^q$ because of Assumption (2). Next, one can compute

$$\mathscr{C}_{\text{pub}}^{\perp} \cap \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]} + \gamma^{q^{1-t}} \boldsymbol{h}^{[1]} \rangle = \langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle \tag{2}$$

and

$$\begin{aligned} \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]} + \gamma^{q^{1-t}} \boldsymbol{h}^{[1]} \rangle + \langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle^{[1]} & \\ = \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]} + \gamma^{q^{1-t}} \boldsymbol{h}^{[1]}, \boldsymbol{g}^{[1]} + \gamma^q \boldsymbol{h}^{[1]} \rangle & \\ = \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]} \rangle. & \end{aligned}$$

Similarly, we compute the intersection with ${\mathscr{C}_{\text{pub}}^{\perp}}^{[-1]} \stackrel{\text{def}}{=} {\mathscr{C}_{\text{pub}}^{\perp}}^{[m-1]}$ and get

$${\mathscr{C}_{\text{pub}}^{\perp}}^{[-1]} \cap \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g}^{[1]}, \boldsymbol{h}^{[1]} \rangle = \langle \boldsymbol{g}^{[1]} + \gamma^{q^{m-1}} \boldsymbol{h}^{[1]} \rangle. \tag{3}$$

Applying the inverse Frobenius to the last code, we get $\langle \boldsymbol{g} + \gamma^{q^{m-2}} \boldsymbol{h} \rangle$. Since, from (2), we also know $\langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle$, one can compute

$$\langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle + \langle \boldsymbol{g}^{[1]} + \gamma^{q^{m-1}} \boldsymbol{h}^{[1]} \rangle^{[-1]} = \langle \boldsymbol{g} + \gamma \boldsymbol{h}, \boldsymbol{g} + \gamma^{q^{m-2}} \boldsymbol{h} \rangle = \langle \boldsymbol{g}, \boldsymbol{h} \rangle. \tag{4}$$

Next, for any $i \in \{1, \dots, t\}$ one can compute

$${\mathscr{C}_{\text{pub}}}^{\perp} \cap \langle \boldsymbol{g}, \boldsymbol{h} \rangle^{[i]} = \langle \boldsymbol{g}^{[i]} + \gamma \boldsymbol{h}^{[i]} \rangle.$$

By applying the i–th inverse Frobenius to the previous result, we obtain the space $\langle \boldsymbol{g} + \gamma^{q^{-i}} \boldsymbol{h} \rangle$ for any $i \in \{1, \dots, t\}$. In summary, we know the spaces

$$\langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle, \langle \boldsymbol{g} + \gamma^{q^{-1}} \boldsymbol{h} \rangle, \dots, \langle \boldsymbol{g} + \gamma^{q^{-t}} \boldsymbol{h} \rangle.$$

In addition, from Lemma 1, the vector $\boldsymbol{g}$ is determined up to some multiplicative constant. Therefore, one can choose an arbitrary element of $\langle \boldsymbol{g} + \gamma \boldsymbol{h} \rangle$ and suppose that this element is $\boldsymbol{g} + \gamma \boldsymbol{h}$.

4.2 Step 2. Finding γ

In summary, the vector $\boldsymbol{g} + \gamma \boldsymbol{h}$ and the spaces $\langle \boldsymbol{g} + \gamma^{q^i} \boldsymbol{h} \rangle$ for any $i \in \{-1, \dots, -t\}$ are known. To compute γ, we will use the following lemma.

Lemma 5. *For $i, j \in \{1, \dots, t\}$, $i \neq j$, there exists a unique pair $(\boldsymbol{u}_{ij}, \boldsymbol{v}_{ij}) \in \langle \boldsymbol{g} + \gamma^{q^{-i}} \boldsymbol{h} \rangle \times \langle \boldsymbol{g} + \gamma^{q^{-j}} \boldsymbol{h} \rangle$ such that $\boldsymbol{u}_{ij} + \boldsymbol{v}_{ij} = \boldsymbol{g} + \gamma \boldsymbol{h}$.*

The pairs of vectors $(\boldsymbol{u}_{ij}, \boldsymbol{v}_{ij})$ can be easily computed. Thus, from now on, we suppose we know them. In addition, despite γ, $\boldsymbol{g} + \gamma^{q^{-i}} \boldsymbol{h}$ and $\boldsymbol{g} + \gamma^{q^{-j}} \boldsymbol{h}$ are unknown, a calculation permits to show that $\boldsymbol{u}_{ij}, \boldsymbol{v}_{ij}$ have the following expressions.

$$\boldsymbol{u}_{ij} = \frac{\gamma^{q^{-j}} - \gamma}{\gamma^{q^{-j}} - \gamma^{q^{-i}}} \cdot (\boldsymbol{g} + \gamma^{q^{-i}} \boldsymbol{h}) \quad \text{and} \quad \boldsymbol{v}_{ij} = \frac{\gamma - \gamma^{q^{-i}}}{\gamma^{q^{-j}} - \gamma^{q^{-i}}} \cdot (\boldsymbol{g} + \gamma^{q^{-j}} \boldsymbol{h}). \quad (5)$$

Consider the vectors $\boldsymbol{u}_{12}$ and $\boldsymbol{u}_{13}$. They are collinear since, from (5), they are both multiples of $\boldsymbol{g} + \gamma^{q^{-1}} \boldsymbol{h}$. Therefore, one can compute the scalar α such that $\boldsymbol{u}_{12} = \alpha \cdot \boldsymbol{u}_{13}$. From (5) we deduce that γ satisfies the following relation.

$$\frac{\gamma^{q^{-2}} - \gamma}{\gamma^{q^{-2}} - \gamma^{q^{-1}}} = \alpha \cdot \frac{\gamma^{q^{-2}} - \gamma}{\gamma^{q^{-2}} - \gamma^{q^{-1}}}. \quad (6)$$

Or equivalently, γ is a root of the polynomial

$$Q_\gamma(X) \stackrel{\text{def}}{=} (X^q - X^{q^3})(X - X^{q^2}) - \alpha^{q^3} (X - X^{q^3})(X^q - X^{q^2}).$$

One can easily check that $(X^q - X)^{q+1}$ divides Q_γ and we set

$$P_\gamma(X) \stackrel{\text{def}}{=} \frac{Q_\gamma}{(X^q - X)^{q+1}}.$$

The element γ we look for is a root of P_γ but actually, the forthcoming Proposition 5 provides the description of the other roots. We first need a technical Lemma.

Lemma 6. *Let* $a, b, c, d \in \mathbb{F}_q$*, let* i, j *be two nonnegative integers and set* $A(X) = X^{q^i} - X^{q^j} \in \mathbb{F}_q[X]$*. Then,*

$$A\left(\frac{aX+b}{cX+d}\right) = \frac{ad-bc}{(cX+d)^{q^i+q^j}} \cdot A(X).$$

Proposition 5. *The set of roots of* P_γ *equals the orbit of* γ *under the action of* $\mathbf{PGL}(2, \mathbb{F}_q)$*. Equivalently, any root of* P_γ *is of the form* $\frac{a\gamma+b}{c\gamma+d}$ *for* $a, b, c, d \in \mathbb{F}_q$ *such that* $ad - bc \neq 0$*.*

Thanks to Propositions 4 and 5, we deduce that choosing an arbitrary root γ' of P_γ provides a candidate for γ and there remains to compute $\boldsymbol{g}', \boldsymbol{h}'$ providing our triple. The triple can be deduced from the knowledge of $\boldsymbol{g} + \gamma \boldsymbol{h} = \boldsymbol{g}' + \gamma' \boldsymbol{h}'$ and the computation of $\boldsymbol{g}' + \gamma'^{q^{-1}} \boldsymbol{h}'$ which can be proved to satisfy

$$\boldsymbol{g}' + \gamma'^{q^{-1}} \boldsymbol{h}' = \frac{\gamma'^{q^{-2}} - \gamma'^{q^{-1}}}{\gamma'^{-2} - \gamma'} \boldsymbol{u}_{12}.$$

4.3 End of the attack

Given the pair $\boldsymbol{g}', \boldsymbol{h}'$, compute the matrix $\boldsymbol{Q} \in \mathbf{GL}(n, \mathbb{F}_q)$ such that $\boldsymbol{h}' = \boldsymbol{g}'\boldsymbol{Q}$. Then,

$$\mathscr{C}_{\text{pub}}^{\perp} = \mathcal{G}_{n-k}(\boldsymbol{g}') \cdot (\boldsymbol{I}_n + \gamma' \boldsymbol{Q})$$

and this representation of the dual provides all the elements necessary to decode, that is to decrypt any ciphertext.

Conclusion

We provided a distinguisher *à la Overbeck* for the public keys of Loidreau's scheme when $\lambda = 2$ and the public code has rate $R_{\text{pub}} \geqslant \frac{1}{2}$. From this distinguisher, we are able to derive a polynomial time key recovery attack. This attack can probably be extended to other values of λ when the public code rate satisfies $R_{\text{pub}} \geqslant 1 - \frac{1}{\lambda}$. Therefore, such parameters should be avoided in Loidreau's scheme.

5 Acknowledgements

The second author was funded by French ANR projects ANR-15-CE39-0013 *Manta* and ANR-17-CE39-0007 CBCrypt.

References

1. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: Enhanced public key security for the McEliece cryptosystem. J. Cryptology **29**(1), 1–27 (2016). https://doi.org/10.1007/s00145-014-9187-8, `http://dx.doi.org/10.1007/s00145-014-9187-8`
2. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: The user language. J. Symbolic Comput. **24**(3/4), 235–265 (1997)
3. Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Otmani, A., Tillich, J.P.: Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. Des. Codes Cryptogr. **73**(2), 641–666 (2014)
4. Couvreur, A., Otmani, A., Tillich, J.P., Gauthier-Umaña, V.: A polynomial-time attack on the BBCRS scheme. In: Katz, J. (ed.) Public-Key Cryptography - PKC 2015. LNCS, vol. 9020, pp. 175–193. Springer (2015)
5. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. J. Comb. Theory, Ser. A **25**(3), 226–241 (1978)
6. Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)
7. Gabidulin, E.M., Paramonov, A.V., Tretjakov, O.V.: Ideals over a non-commutative ring and their applications to cryptography. In: Advances in Cryptology - EUROCRYPT'91. pp. 482–489. No. 547 in LNCS, Brighton (Apr 1991)
8. Gaborit, P., Murat, G., Ruatta, O., Zémor, G.: Low rank parity check codes and their application to cryptography. In: Proceedings of the Workshop on Coding and Cryptography WCC'2013. Bergen, Norway (2013), available on `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`
9. Loidreau, P.: A Welch–Berlekamp like algorithm for decoding Gabidulin codes. In: Ytrehus, Ø. (ed.) Coding and Cryptography. pp. 36–45. Springer Berlin Heidelberg, Berlin, Heidelberg (2006)
10. Loidreau, P.: Rank metric and cryptography. Accreditation to supervise research, Université Pierre et Marie Curie - Paris VI (Jan 2007), `https://tel.archives-ouvertes.fr/tel-00200407`
11. Loidreau, P.: A new rank metric codes based encryption scheme. In: International Workshop on Post-Quantum Cryptography. pp. 3–17. Springer (2017)
12. McEliece, R.J.: A Public-Key System Based on Algebraic Coding Theory, pp. 114–116. Jet Propulsion Lab (1978), dSN Progress Report 44
13. Overbeck, R.: Structural attacks for public key cryptosystems based on Gabidulin codes. J. Cryptology **21**(2), 280–301 (2008)