A polynomial attack on a NIST proposal: RankSign, a code-based signature in rank metric

Thomas Debris-Alazard [*†] Jean-Pierre Tillich [†]

April 7, 2018

Abstract

RankSign is a code-based signature scheme proposed to the NIST competition for post-quantum cryptography [AGH$^+$17]. It is based on the rank metric and enjoys remarkably small key sizes, about 10KBytes for an intended level of security of 128 bits. It is also one of the fundamental blocks used in the rank metric identity based encryption scheme [GHPT17]. Unfortunately we will show that all the parameters proposed for this scheme in [AGH$^+$17] can be broken by an algebraic attack that exploits the fact that the augmented LRPC codes used in this scheme have very low weight codewords.

1 Introduction

It is a long standing open problem to build an efficient and secure signature scheme based on the hardness of decoding a linear code which could compete in all respects with DSA or RSA. Such schemes could indeed give a quantum resistant signature for replacing in practice the aforementioned signature schemes that are well known to be broken by quantum computers. A first partial answer to this question was given in [CFS01]. It consisted in adapting the Niederreiter scheme [Nie86] for this purpose. This requires a linear code for which there exists an efficient decoding algorithm for a non-negligible set of inputs. This means that if $\mathbf{H}$ is an $r \times n$ parity-check matrix of the code, there exists for a non-negligible set of elements $\mathbf{s}$ in $\{0,1\}^r$ an efficient way to find a word $\mathbf{e}$ in $\{0,1\}^n$ of smallest Hamming weight such that $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$.

The authors of [CFS01] noticed that very high rate Goppa codes are able to fulfill this task, and their scheme can indeed be considered as the first step towards a solution of the aforementioned problem. However, the poor scaling of the key size when security has to be increased prevents this scheme to be a completely satisfying answer to this issue.

There has been some exciting progress in this area for another metric, namely the rank metric [GRSZ14]. A code-based signature scheme whose security relies on decoding codes with respect to the rank metric has been proposed there. It is called RankSign. Strictly speaking, the rank metric consists in viewing an element in $\mathbb{F}_q^N$ (when N is a product $N = m \times n$) as an $m \times n$ matrix over $\mathbb{F}_q$ and the rank distance between two elements $\mathbf{x}$ and $\mathbf{y}$ is defined as the rank of the matrix $\mathbf{x} - \mathbf{y}$. This depends of course on how N is viewed as a product of two elements. Decoding in this metric is known to be an NP hard problem [BFS99, Cou01]. In

[*] Sorbonne Universités, UPMC Univ Paris 06, France

[†] Inria, SECRET Project, 2 Rue Simone Iff 75012 Paris Cedex

the particular case of [GRSZ14], the codes which are considered are not $\mathbb{F}_q$-linear but, as is customary in the setting of rank metric based cryptography, $\mathbb{F}_{q^m}$-linear. This allows to reduce the key size by a factor of m when compared to the $\mathbb{F}_q$-linear setting (for more details see the paragraph at the end of Section 2).

Decoding such codes for the rank metric is not known to be NP-hard anymore. There is however a randomized reduction of this problem to decode an $\mathbb{F}_q$-linear code for the Hamming metric [GZ16] when the degree m of the extension field is sufficiently big. This situation is in some sense reminiscent to the current thread in cryptography based on codes or on lattices where structured codes (for instance quasi-cyclic codes) or structured lattices (corresponding to an additional ring structure) are taken. In the case at hand, there is however a randomized reduction to an NP complete problem. Furthermore, RankSign comes with a security proof showing that there is no leakage coming from signing many times and enjoys remarkably small key sizes: it is about 10KBytes for 128 bits of security for the parameters proposed in the NIST submission[AGH$^+$17]. It also proved to be a fundamental building block in the identity based encryption scheme based on the rank metric suggested in [GHPT17].

Unfortunately we will show here that all the parameters proposed in [GRSZ14, AGH$^+$17] can be broken by a suitable algebraic attack. The problem is actually deeper than that, because we will show in the full-version of this paper that the attack is actually polynomial in nature and can not really be thwarted by changing the parameters. The attack builds upon the following observations

- The RankSign scheme is based on augmented LRPC codes;
- To have an efficient signature scheme, the parameters of the augmented LRPC codes have to be chosen very carefully;
- For the whole range of admissible parameters, it turns out rather unexpectedly that these augmented LRPC codes have very low-weight codewords. This can be proved by subspace product considerations;
- These low-weight codewords can be recovered by algebraic techniques and reveal enough of the secret trapdoor used in the scheme to be able to sign like a legitimate user.

2 Generalities on rank metric and $\mathbb{F}_{q^m}$-linear codes

2.1 Definitions and notation

We provide here some notation and definitions that will be used throughout the paper.

Vector notation. Vectors will be written using bold lower-case letters, e.g. $\mathbf{x}$. The ith component of $\mathbf{x}$ will be denoted by x_i. Vectors are in row notation. Matrices will be written as bold capital letters, e.g. $\mathbf{X}$, and the i-th column of a matrix $\mathbf{X}$ is denoted $\mathbf{X}_i$. The rank of a matrix $\mathbf{X}$ will be simply denoted by $|\mathbf{X}|$.

Field notation. Let q be a power of a prime number. We will denote by $\mathbb{F}_q$ the finite field of cardinality q.

Coding theory notation. A linear code $\mathscr{C}$ over a finite field $\mathbb{F}_q$ of length n and dimension k is a subspace of the vector space $\mathbb{F}_q^n$ of dimension k. We say that it has parameters $[n, k]$

or that it is an $[n,k]$-code. A generator matrix $\mathbf{G}$ for it is a $k \times n$ matrix over $\mathbb{F}_q$ that is such that

$$\mathscr{C} = \{\mathbf{uG} : \mathbf{u} \in \mathbb{F}_q^k\}.$$

In other words, the rows of $\mathbf{G}$ form a basis of $\mathscr{C}$. A parity-check matrix $\mathbf{H}$ for it is a full-rank $(n-k) \times n$ matrix over $\mathbb{F}_q$ such that

$$\mathscr{C} = \{\mathbf{c} \in \mathbb{F}_q^n : \mathbf{H}\mathbf{c}^{\intercal} = 0\}.$$

In other words, $\mathscr{C}$ is the null space of $\mathbf{H}$.
Rank metric codes basically consist in viewing codewords as matrices. More precisely, when N is the product of two numbers m and n, $N = mn$ we will equip the vector space $\mathbb{F}_q^N$ with the rank metric by viewing its elements as matrices over $\mathbb{F}_q^{m \times n}$, i.e.

$$d(\mathbf{X}, \mathbf{Y}) = |\mathbf{X} - \mathbf{Y}|.$$

An $[m \times n, K]$ *matrix code* of dimension K over $\mathbb{F}_q^{m \times n}$ is a subspace of $\mathbb{F}_q^{m \times n}$ of dimension K. Such a code is equipped in a natural way with the rank metric. There is a particular subclass of matrix codes that has the nice property to be specified much more compactly than a generic matrix code. It consists in taking a linear code over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ of length n. Such a code can be viewed as a matrix code consisting of matrices in $\mathbb{F}_q^{m \times n}$ by expressing each coordinate c_i of a codeword $\mathbf{c} = (c_i)_{1 \leq i \leq n}$ in a fixed $\mathbb{F}_q$ basis of $\mathbb{F}_{q^m}$. When the $\mathbb{F}_{q^m}$-linear code is of dimension k the dimension of the matrix code viewed as an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{m \times n}$ is $K = k.m$.

More precisely we bring in the following definition.

Definition 1 (Matrix code associated to an $\mathbb{F}_{q^m}$ linear code)**.** Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}_{q^m}$, that is a subspace of $\mathbb{F}_{q^m}^n$ of dimension k over $\mathbb{F}_{q^m}$, and let $(\beta_1 \dots \beta_m)$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Each word $\mathbf{c} \in \mathscr{C}$ can be represented by an $m \times n$ matrix $\mathbf{Mat}(\mathbf{c}) = (M_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ over $\mathbb{F}_q$, with $c_j = \sum_{i=1}^m M_{ij}\beta_i$. The set $\{\mathbf{Mat}(\mathbf{c}), \mathbf{c} \in \mathscr{C}\}$ is the $[m \times n, k.m]$ matrix code over $\mathbb{F}_q$ associated to the $\mathbb{F}_{q^m}$ linear code $\mathscr{C}$. The (rank) weight of $\mathbf{c}$ is defined as the rank of the associated matrix, that is $|\mathbf{c}| \overset{\triangle}{=} |\mathbf{Mat}(\mathbf{c})|$.

This definition depends of course of the basis chosen for $\mathbb{F}_{q^m}$. However changing the basis does not change the distance between codewords. The point of defining matrix codes in this way is that they have a more compact description. It is readily seen that an $[m \times n, k.m]$ matrix code over $\mathbb{F}_q$ can be specified from a systematic generator matrix (i.e. a matrix of the form $\left(\mathbf{1}_{k.m}\mathbf{P}\right)$ with $\mathbf{1}_{k.m}$ being the identity matrix of size $k.m$) by $k(n-k)m^2 \log_2 q$ bits whereas an $\mathbb{F}_{q^m}$-linear code uses only $k(n-k)\log_2 q^m = k(n-k)m \log_2 q$ bits. This is particularly interesting for cryptographic applications where this notion is directly related to the public key size. This is basically what explains why in general McEliece cryptosystems based on rank metric matrix codes have a smaller keysize than McEliece cryptosystems based on the Hamming metric. All of these proposals (see for instance [GPT91, GO01, Gab08, GMRZ13, GRSZ14, ABD$^+$17b, AMAB$^+$17]) are actually built from matrix codes over $\mathbb{F}_q$ obtained from $\mathbb{F}_{q^m}$-linear codes. In a sense, they can be viewed as structured matrix codes, much in the same way as quasi-cyclic linear codes can be viewed as structured versions of linear codes. In the latter case, the code is globally invariant by a linear isometric transform on the codewords corresponding to shifts of a certain length. In the $\mathbb{F}_{q^m}$ linear case the code is globally invariant by an isometric linear transformation that corresponds to multiplication in $\mathbb{F}_{q^m}$.

2.2 Rank code-based cryptography

Rank-based cryptography relies on the hardness of decoding for the rank metric. This problem is the rank metric analogue of the well known decoding problem in the Hamming metric [BMvT78]. We give it here its syndrome formulation:

Definition 2 (Rank (Metric) Syndrome Decoding Problem)**.** Let $\mathbf{H}$ be a full-rank $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $k \leq n$, $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$ and w an integer. The problem is to find $\mathbf{e} \in \mathbb{F}_{q^m}^{n}$ such that $|\mathbf{e}| = w$ and $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$.

This problem has recently been proven hard in [GZ16] by a probabilistic reduction to the decoding problem in the Hamming metric which is known to be NP-complete [BMvT78]. This problem has typically a unique solution when w is below the Varshamov Gilbert distance $w_{\text{rVG}}(q, m, n, k)$ for the rank metric which is defined as

Definition 3 (Varshamov Gilbert distance for the rank metric)**.** The Varshamov Gilbert distance $w_{\text{rVG}}(q, m, n, k)$ for $\mathbb{F}_{q^m}$ linear codes of dimension k in the rank metric is defined as the smallest t for which

$$q^{m(n-k)} \geq B_t$$

where B_t is the size of the ball of radius t in the rank metric.

Remark 1.

1. $q^{m(n-k)}$ can be viewed as the number of different syndromes $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$.
2. $B_t = \sum_{i=0}^{t} S_i$ where S_i is the size of a sphere of radius i in the rank metric over $\mathbb{F}_q^{m \times n}$. This latter quantity is equal to
$$S_i = \prod_{j=0}^{i-1} \frac{(q^n - q^j)(q^m - q^j)}{(q^i - q^j)} = \Theta\left(q^{i(m+n-i)}\right).$$
3. From this last asymptotic expression it is straightforward to check that (for more details see [Loi14])
$$w_{\text{rVG}} = \frac{m + n - \sqrt{(m-n)^2 + 4km}}{2}(1 + o(1)),$$
when either m or n tend to infinity.

The best algorithms for solving the decoding problem in the rank metric are exponential in n^2 as long as $m = \Theta(n)$, $w = \Theta(n)$ but stays below the Singleton bound which is defined by

Definition 4 (Singleton distance in the rank metric)**.** The Singleton distance $w_{\text{rS}}(q, m, n, k)$ for $\mathbb{F}_{q^m}$ linear codes of dimension k in the rank metric is defined as

$$w_{\text{rS}}(q, m, n, k) \stackrel{\triangle}{=} \left\lfloor \frac{(n-k)m}{\max(m, n)} \right\rfloor + 1$$

The usual notion of the support of a vector is generally relevant to decoding in the Hamming metric and corresponds for a vector $\mathbf{x} = (x_i)_{1 \leq i \leq n}$ to the set of positions i in $\{1, \ldots, n\}$ such that $x_i \neq 0$. Various decoding algorithms for the Hamming metric [Pra62, LB88, Ste88, Dum91, FS09, BLP11, MMT11, BJMM12, MO15, DT17, BM17] use this notion in a rather fundamental way. The definition of the support of a vector has to be changed a little bit to be relevant to the rank metric. This notion was first put forward in [GRS13, GRS16] to obtain an analogue of the Prange decoder [Pra62] for the rank metric.

Definition 5 (Support)**.** Let $\mathbf{x} = (x_i)_{1 \leq i \leq n}$ be a vector of $\mathbb{F}_{q^m}^n$, its support is defined as:

$$\mathrm{Supp}(\mathbf{x}) \overset{\triangle}{=} \langle x_1, \cdots, x_n \rangle_{\mathbb{F}_q}.$$

This notion of support is relied to the rank metric as it is easily verified that for any $\mathbf{x}$ vector of $\mathbb{F}_{q^m}^n$ we have:

$$|\mathbf{x}| = \dim(\mathrm{Supp}(\mathbf{x}))$$

3 The RankSign scheme

We recall in this section basic facts about RankSign. It is based on augmented LRPC codes. Roughly speaking it is a hash and sign signature scheme: the message $\mathbf{m}$ that has to be signed is hashed by a hash function $\mathscr{H}$ and the signature is equal to $f^{-1}(\mathscr{H}(\mathbf{m}))$ where f is a trapdoor one-way function. Here the input to f is the set of vectors of $\mathbb{F}_{q^m}^n$ of some (rank) weight w and f is given by $f(\mathbf{e}) \overset{\triangle}{=} \mathbf{H}\mathbf{e}^\intercal$ where $\mathbf{H}$ is a fixed $r \times n$ parity-check matrix of the augmented LRPC code used for the scheme. When the underlying LRPC structure is known (roughly speaking, this is the trapdoor), there is a decoding algorithm based on the LRPC structure that computes for any (or for a good fraction) $\mathbf{s} \in \mathbb{F}_q^r$ an $\mathbf{e} \in \mathbb{F}_q^n$ of weight w such that $\mathbf{H}\mathbf{e}^\intercal = \mathbf{s}^\intercal$. This decoding algorithm is probabilistic and the parameters of the code have to be chosen in a very specific fashion in order to have a probability of success very close to 1 (see Fact 1 at the end of this section).
An LRPC code is a code that admits a parity-check check matrix that is homogeneous and of small weight. A homogeneous matrix is defined as

Definition 6 (Homogeneous Matrix)**.** A matrix $\mathbf{H} = (H_{ij})_{\substack{1 \leq i \leq n-k \\ 1 \leq j \leq n}}$ over $\mathbb{F}_{q^m}$ is homogeneous of weight d if all its coefficients generate an $\mathbb{F}_q$-vector space of dimension d:

$$\dim\left(\langle H_{ij} : 1 \leq i \leq n-k,\ 1 \leq j \leq n \rangle_{\mathbb{F}_q}\right) = d$$

LRPC (Low Rank Parity Check) codes of weight d and augmented LRPC codes of type (d, t) are defined from such matrices as

Definition 7 (LRPC and augmented LRPC code)**.** An LRPC code over $\mathbb{F}_{q^m}$ of weight d is a code that admits a parity-check matrix $\mathbf{H}$ with entries in $\mathbb{F}_{q^m}$ that is homogeneous of weight d whereas an augmented LRPC code of type (d, t) over $\mathbb{F}_{q^m}$ is a code that admits a parity-check matrix $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right] \mathbf{P}$ where $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$.

Remark 2. Note that $\mathbf{P} \in \mathbb{F}_q^{n \times n}$ is an isometry for the rank metric, since for any $\mathbf{x} \in \mathbb{F}_{q^m}^n$ we have $\mathrm{Supp}(\mathbf{x}) = \mathrm{Supp}(\mathbf{x}\mathbf{P})$ and therefore

$$|\mathbf{x}| = |\mathbf{x}\mathbf{P}|.$$

The public key and the secret key for RankSign are given by:

public key: $\mathbf{H}_{\text{pub}}$ which is a random $(n-k) \times n$ parity-check matrix of an augmented LRPC code of type (d,t). It is of the form

$$\mathbf{H}_{\text{pub}} = \mathbf{Q}\mathbf{H}'$$

with $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right] \mathbf{P}$ where $\mathbf{Q}$ is an invertible $(n-k) \times (n-k)$ matrix over $\mathbb{F}_{q^m}$, $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$.

secret key: The matrix $\mathbf{H}_{\text{sec}} \overset{\triangle}{=} \left[\mathbf{H}|\mathbf{R}\right]$.

From the knowledge of this last matrix a signature is computed by using a decoding algorithm devised for LRPC codes. Recall that LRPC codes can be viewed as analogues of LDPC codes for the rank metric. In particular, they enjoy an efficient decoding algorithm based on their low rank parity-check matrix. Roughly speaking, Algorithm 1 of [GMRZ13] decodes up to w errors when $dw \leq n-k$ in polynomial time (see [GMRZ13, Theorem 1]). It uses in a crucial way the notion of the linear span of a product of subspaces of $\mathbb{F}_{q^m}$:

Definition 8. Let U and V be two subspaces of $\mathbb{F}_{q^m}$, then

$$U \cdot V \overset{\triangle}{=} \langle uv : u \in U,\ v \in V \rangle_{\mathbb{F}_q}.$$

Roughly speaking, Algorithm 1 of [GMRZ13] works as follows when we have to recover an error $\mathbf{e}$ of weight w from the knowledge of its syndrome $\mathbf{s}$ with respect to a parity-check matrix $\mathbf{H} = (H_{ij})_{\substack{1 \leq i \leq n-k \\ 1 \leq j \leq n}}$ over $\mathbb{F}_{q^m}$ that is homogeneous of weight d, that is

$$\mathbf{s}^{\intercal} = \mathbf{H}\mathbf{e}^{\intercal}. \tag{1}$$

1. Let $U \overset{\triangle}{=} \langle H_{ij} : 1 \leq i \leq n-k,\ 1 \leq j \leq n \rangle_{\mathbb{F}_q}$, $V \overset{\triangle}{=} \text{Supp}(\mathbf{e})$ and $W \overset{\triangle}{=} \text{Supp}(\mathbf{s})$. U and W are known, whereas V is unknown to the decoder. By definition U is of dimension d and it is convenient to bring in a basis $\{f_1, \dots, f_d\}$ for it.

2. It turns out that we typically have $W = U \cdot V$. Moreover it is clear that in such a case $V \subset f_1^{-1}W \cap f_2^{-1}W \cdots f_d^{-1}W$. It also turns out that we typically have

   $$V = f_1^{-1}W \cap f_2^{-1}W \cdots f_d^{-1}W.$$

   V is therefore computed by taking the intersection of all the $f_i^{-1}W$'s.

3. Once we have the support of $\mathbf{e}$ ($V = \text{Supp}(\mathbf{e})$), the error $\mathbf{e} = (e_1, \dots, e_n)$ can be recovered by solving the linear equation $\mathbf{H}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$ with the additional constraints $e_i \in \text{Supp}(\mathbf{e})$ for $i \in \{1, \dots, n\}$. There are in this case enough linear constraints to recover a unique $\mathbf{e}$.

The last algorithm seems to apply when there is a unique solution to (1). It can also be used with a slight modification (by adding "erasures" [GRSZ14]) for weights for which there are many solutions to it (this is typically the regime which is used for the RankSign scheme). It namely turns out, see [GRSZ14], that this decoder can for a certain range of parameters be used for a large fraction of possible syndromes $\mathbf{s} \in \mathbb{F}_{q^m}^r$ to produce an error $\mathbf{e}$ of weight

w that satisfies (1). It can even be required that $\text{Supp}(\mathbf{e})$ contains a subspace T of some dimension t. Furthermore this procedure can also be generalized to a parity-check matrix of an augmented LRPC code. More precisely to summarize the discussion that can be found in [GRSZ14, AGH$^+$17]

Fact 1. Let $\mathbf{H}$ be a random homogeneous matrix of weight d in $\mathbb{F}_{q^m}^{(n-k)\times n}$, $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$ and $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$. There is a probabilistic polynomial time algorithm that outputs for a large fraction of syndromes $\mathbf{s} \in \mathbb{F}_{q^m}^{n-k}$, subspaces T of $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$–dimension t', an error $\mathbf{e}$ of weight w whose support contains the subspace T that satisfies

$$\mathbf{H}'\mathbf{e}^\intercal = \mathbf{s}^\intercal$$

as soon as the parameters n, k, t, t', d, w satisfy

$$\begin{aligned} m &= (w-t')(d+1) && (2)\\ n-k &= d(w-t-t') && (3)\\ n &= (n-k)d. && (4) \end{aligned}$$

4 Attack on RankSign

4.1 The problem with RankSign : low rank codewords in the augmented LRPC code

A natural way to attack RankSign is to find low weight codewords in the dual of the augmented LRPC code. Recall that the public parity-check matrix used in the scheme is a matrix $\mathbf{H}_{\text{pub}}$ where

$$\mathbf{H}_{\text{pub}} = \mathbf{Q}\mathbf{H}'$$

with $\mathbf{H}' = \left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where $\mathbf{H}$ is a homogeneous matrix of rank d over $\mathbb{F}_{q^m}$, $\mathbf{R}$ is a matrix with t columns that has its entries in $\mathbb{F}_{q^m}$, $\mathbf{P}$ is a square and invertible matrix with entries in $\mathbb{F}_q$ that has the same number of columns as $\mathbf{H}'$ and $\mathbf{Q}$ is a square and invertible matrix over $\mathbb{F}_{q^m}$ which has the same number of rows as $\mathbf{H}'$. If we call $\mathscr{C}_{\text{pub}}$ the "public code" with parity-chek matrix $\mathbf{H}_{\text{pub}}$, then the dual code $\mathscr{C}_{\text{pub}}^\perp$ that has for generator matrix $\mathbf{H}_{\text{pub}}$ has codewords of weight $\leq d+t$ since rows of $\mathbf{H}'\mathbf{P}$ belong to this code, and all of its rows have rank weight $\leq d+t$ since the rows of $\mathbf{H}'$ have weight at most $d+t$ and $\mathbf{P}$ is an isometry for the rank metric. The authors have chosen the parameters of the RankSign scheme so that finding codewords of weight $t+d$ in $\mathscr{C}_{\text{pub}}^\perp$ is above the security level of the scheme. However, it turns out that due to the peculiar parameters chosen in the RankSign scheme (see Fact 1), $\mathscr{C}_{\text{pub}}$ has many very low weight codewords. This is the main problem in RankSign. Before we give a precise statement together with its proof, we will give a general result showing that LRPC codes may have under certain circumstances low weight codewords.

Lemma 1. *Let $\mathscr{C}$ be an LRPC code of length n and dimension k over $\mathbb{F}_{q^m}$ that is associated to a homogeneous matrix $\mathbf{H}$ that has all its entries in a subspace F of $\mathbb{F}_{q^m}$. Furthermore we suppose there exists a subspace F' of $\mathbb{F}_{q^m}$ such that*

$$(n-k)\dim(F \cdot F') < n \cdot \dim F'.$$

Then there exist nonzero codewords in the LRPC code whose support is included in F'. They are therefore of rank weight at most $\dim F'$. Furthermore this set of codewords, that is $\mathscr{C}' \stackrel{\triangle}{=} \{\mathbf{c} \in \mathscr{C} : c_i \in F',\ \forall i \in [\![1, n]\!]\}$, forms an $\mathbb{F}_q$ subspace of $\mathbb{F}_{q^m}^n$ that is of dimension $\geq n \dim F' - (n-k)\dim(F \cdot F')$.

Proof. Denote the entry in row i and column j of $\mathbf{H}$ by $H_{i,j}$. A codeword $\mathbf{c}$ of the LRPC code satisfies

$$\forall i \in [\![1, n-k]\!] \quad \sum_{j=1}^{n} H_{i,j} c_j = 0. \tag{5}$$

Looking in addition for a codeword $\mathbf{c}$ that has all its entries in F' and expressing these $n-k$ linear equations over $\mathbb{F}_{q^m}$ in a basis of $F \cdot F'$ (since $\sum_{j=1}^{n} H_{i,j} c_j$ belongs by definition to $F \cdot F'$) and expressing each c_j in a $\mathbb{F}_q$ basis $\{f'_1, \dots, f'_{d'}\}$ of F' as $c_j = \sum_{\ell=1}^{d'} c_{j,\ell} f'_\ell$ we obtain $(n-k)\dim(F \cdot F')$ linear equations over $\mathbb{F}_q$ involving $n \cdot \dim F'$ unknowns (the c_j's) in $\mathbb{F}_q$. The solution space is therefore of dimension greater $\geq n \cdot \dim F' - (n-k)\dim(F \cdot F')$. □

Remark 3. This theorem proves the existence of low rank codewords in an LRPC-code under some conditions but it does not give any efficient way to find them.

By using this lemma, we will prove the following corollary that explains that the augmented LRPC codes that are used in the RankSign signature necessarily contain many rank weight 2 codewords. This is in a sense a consequence of Equation (4) on the parameters of RankSign.

Corollary 2. *Let $\mathscr{C}_{\text{pub}}$ be an $[n+t, k+t]$ public code of* RankSign *over $\mathbb{F}_{q^m}$ which has been obtained from an $[n, k]$* LRPC*-code that is associated to a homogeneous matrix $\mathbf{H}$ that has all its entries in an $\mathbb{F}_q$ subspace F of $\mathbb{F}_{q^m}$. Consider a subspace F' of F of dimension 2 and let*

$$\mathscr{C}'_{\text{pub}} \stackrel{\triangle}{=} \left\{\mathbf{c} \in \mathscr{C}_{\text{pub}} : c_i \in F',\ \forall i \in [\![1, n]\!]\right\}.$$

$\mathscr{C}'_{\text{pub}}$ is an $\mathbb{F}_q$ subspace of $\mathbb{F}_{q^m}^n$. If (4) holds, that is $n = (n-k)d$, then

$$\dim_{\mathbb{F}_q} \mathscr{C}'_{\text{pub}} \geq n/d.$$

Proof. Let $\mathbf{H}_{\text{pub}} \in \mathbb{F}_{q^m}^{(n-k)\times(n+t)}$ be the public parity-check matrix for the RankSign public code $\mathscr{C}_{\text{pub}}$. Recall that $\mathbf{H}_{\text{pub}}$ has been obtained as $\mathbf{H}_{\text{pub}} = \mathbf{Q}\left[\mathbf{H}|\mathbf{R}\right]\mathbf{P}$ where:

- $\mathbf{P}$ is a non-singular matrix with entries in $\mathbb{F}_q$ of size $(n+t) \times (n+t)$,
- $\mathbf{Q}$ is an invertible matrix of $\mathbb{F}_{q^m}$ of size $(n-k) \times (n-k)$,
- $\mathbf{R}$ is a random matrix of $\mathbb{F}_{q^m}$ of size $(n-k) \times t$,
- $\mathbf{H}$ is a homogeneous $(n-k) \times n$ matrix of weight d with all its entries in F.

Choose a basis $\{x_1, x_2, \dots, x_d\}$ of F such that $\{x_1, x_2\}$ is a basis of F'. We observe now that

$$F \cdot F' = \langle x_i x_j : i \in [\![1, d]\!],\ j \in [\![1, 2]\!]\rangle_{\mathbb{F}_q}.$$

The cardinality of the set $\{x_i x_j : i \in [\![1, d]\!],\ j \in [\![1, 2]\!]\}$ is actually $2d-1$ because $x_1 x_2 = x_2 x_1$. This implies that

$$\dim(F \cdot F') \leq 2d - 1.$$

It leads to the following inequalities,

$$\begin{aligned} n \cdot \dim(F') - (n-k)\dim(F \cdot F') &\geq 2n - (n-k)(2d-1) \\ &= 2d(n-k) - (n-k)(2d-1) \quad \text{(since } n = (n-k)d) \\ &= n-k \\ &= \frac{n}{d} \quad \text{(since } n = (n-k)d). \end{aligned}$$

Let $\mathscr{C}_{\text{LRPC}}$ be the LRPC code of weight d associated to the parity-check matrix $\mathbf{H}$ and let $\mathscr{C}'_{\text{LRPC}}$ be an $\mathbb{F}_q$ subspace of it that is defined by

$$\mathscr{C}'_{\text{LRPC}} \overset{\triangle}{=} \left\{ \mathbf{c} \in \mathscr{C}_{\text{LRPC}} : c_i \in F', \ \forall i \in [\![1, n]\!] \right\}.$$

By applying Lemma 1 we know that

$$\dim_{\mathbb{F}_q} \mathscr{C}'_{\text{LRPC}} \geq \frac{n}{d}. \tag{6}$$

Consider now

$$\mathscr{C}'_{\text{pub}} \overset{\triangle}{=} \{(\mathbf{c}_{\text{LRPC}}, \mathbf{0}_t)(\mathbf{P}^{-1})^\intercal : \mathbf{c}_{\text{LRPC}} \in \mathscr{C}'_{\text{LRPC}}\},$$

where $\mathbf{0}_t$ denotes the vector with t zeros. From (6) we deduce that

$$\dim_{\mathbb{F}_q} \mathscr{C}'_{\text{pub}} \geq \frac{n}{d}.$$

Moreover the entries of any element $\mathbf{c}'$ in $\mathscr{C}_{\text{pub}}$ belong to F' because the entries of $\mathbf{P}$ are in $\mathbb{F}_q$. Let us now prove that $\mathscr{C}'_{\text{pub}}$ is contained in $\mathscr{C}_{\text{pub}}$. To verify this, consider an element $\mathbf{c}'$ in $\mathscr{C}'_{\text{pub}}$. It can be written as

$$\mathbf{c}' = (\mathbf{c}_{\text{LRPC}}, \mathbf{0}_t)(\mathbf{P}^{-1})^\intercal.$$

We observe now that

$$\begin{aligned} \mathbf{H}_{\text{pub}} \mathbf{c}'^\intercal &= \mathbf{H}_{\text{pub}} \mathbf{P}^{-1} (\mathbf{c}_{\text{LRPC}}, \mathbf{0}_t)^\intercal \\ &= \mathbf{Q} \left[\mathbf{H} | \mathbf{R} \right] \mathbf{P} \mathbf{P}^{-1} (\mathbf{c}_{\text{LRPC}}, \mathbf{0}_t)^\intercal \\ &= \mathbf{Q} \left[\mathbf{H} | \mathbf{R} \right] (\mathbf{c}_{\text{LRPC}}, \mathbf{0}_t)^\intercal \\ &= \mathbf{Q} \mathbf{H} \mathbf{c}_{\text{LRPC}}{}^\intercal \quad (\ \mathbf{R} \in \mathbb{F}_{q^m}^{(n-k) \times t}\ ) \\ &= \mathbf{0} \quad (\mathbf{c}_{\text{LRPC}} \text{ belongs to the code of parity-check matrix } \mathbf{H}) \end{aligned}$$

This proves that $\mathscr{C}'_{\text{pub}} \subset \mathscr{C}_{\text{pub}}$ which concludes the proof. □

4.2 Weight 1 codewords in a projected code

Corollary 2 shows that there are many weight 2 codewords in $\mathscr{C}_{\text{pub}}$. We can even restrict our search further by noticing that without loss of generality we may assume that the space F in which the entries of the secret parity-check matrix $\mathbf{H}$ of the LRPC code are taken contains 1. Indeed, for any α in $\mathbb{F}_{q^m}^\times$, $\alpha\mathbf{H}$ is also a parity-check matrix of the LRPC code and has its entries in αF. By choosing α such that αF contains 1 we get our claim.

Consider now a supplementary space V of $\langle 1 \rangle_{\mathbb{F}_q} = \mathbb{F}_q$ with respect to $\mathbb{F}_{q^m}$, that is an $\mathbb{F}_q$-space of dimension $m-1$ such that

$$\mathbb{F}_{q^m} = V \oplus \mathbb{F}_q.$$

The previous discussion implies that there is a matrix-code in $\mathbb{F}_q^{(m-1)\times(n+t)}$ which can be deduced from $\mathscr{C}_{\text{pub}}$ by projecting the entries onto V that contains codewords of weight 1. More specifically, consider an $\mathbb{F}_q$ basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ of $\mathbb{F}_{q^m}$ such that $\beta_m = 1$ and for $\mathbf{c} = (c_i)_{1\leq i\leq n+t} \in \mathbb{F}_{q^m}^{n+t}$ consider

$$\mathbf{Mat}^{\text{proj}}(\mathbf{c}) = (M_{ij})_{\substack{1\leq i\leq m-1\\ 1\leq j\leq n+t}} \in \mathbb{F}_q^{(m-1)\times n}$$

where $c_j = \sum_{i=1}^{m} M_{ij}\beta_i$. Now let $\mathscr{C}_{\text{pub}}^{\text{proj}}$ be the matrix-code in $\mathbb{F}_q^{(m-1)\times(n+t)}$ defined by

$$\mathscr{C}_{\text{pub}}^{\text{proj}} \stackrel{\triangle}{=} \left\{\mathbf{Mat}^{\text{proj}}(\mathbf{c})\right\}.$$

It is clear that

Fact 2. $\mathscr{C}_{\text{pub}}^{\text{proj}}$ contains codewords of rank weight 1.

These are just the codewords $\mathbf{c}'$ which are of the form $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ where $\mathbf{c} \in \mathscr{C}'_{\text{pub}}$ with $\mathscr{C}'_{\text{pub}}$ being defined from a subspace F' of F that contains 1 (we can make this assumption since we can assume that F contains 1).

$\mathscr{C}_{\text{pub}}^{\text{proj}}$ has the structure of an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{(m-1)\times(n+t)}$. It is typically of dimension $(k+t)m$ (i.e. the same as the $\mathbb{F}_q$ dimension of $\mathscr{C}_{\text{pub}}$). Moreover once we have these rank weight 1 codewords in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ we can lift them to obtain rank weight ≤ 2 codewords in $\mathscr{C}_{\text{pub}}$ because for any $\mathbf{c} \in \mathscr{C}_{\text{pub}}$ the first row of $\mathbf{Mat}(\mathbf{c})$ can be uniquely recovered from $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ by performing linear combinations of the entries of $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$. We call this operation deducing $\mathbf{c}$ from $\mathbf{Mat}^{\text{proj}}(\mathbf{c})$ *lifting* from $\mathscr{C}_{\text{pub}}^{\text{proj}}$ to $\mathscr{C}_{\text{pub}}$.

4.3 Outline of the attack

Finding codewords of rank 1 in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ obviously reveals much of the secret LRPC structure. Lifting elements in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ that are of rank 1 to $\mathscr{C}_{\text{pub}}$ as explained at the end of Subsection 4.2 yields codewords of $\mathscr{C}_{\text{pub}}$ that have typically rank weight 2. This can be used to reveal F' and actually the whole subspace F by finding enough rank 1 codewords in $\mathscr{C}_{\text{pub}}^{\text{proj}}$. Once F is recovered a suitable form for a parity-check matrix of $\mathscr{C}_{\text{pub}}$ can be found that allows signing like a legitimate user. For the case of the parameters of RankSign proposed in [GRSZ14, AGH$^+$17] for which we always have $d = 2$ we will proceed slightly differently here. Roughly speaking, our attack can be decomposed as follows

1. We find a particular element $\mathbf{M}$ in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ of rank weight 1 by solving a certain bilinear system with Gröbner bases techniques.

2. We lift $\mathbf{M} \in \mathscr{C}_{\text{pub}}^{\text{proj}}$ to $\mathbf{c} \in \mathscr{C}_{\text{pub}}$ and compute $F' \stackrel{\triangle}{=} \text{Supp}(\mathbf{c})$.

3. We compute from F' the $\mathbb{F}_q$-subspace $\mathscr{C}'_{\text{pub}} \stackrel{\triangle}{=} \{\mathbf{c} = (c_i)_{1\leq i\leq n+t} \in \mathscr{C}_{\text{pub}} : c_i \in F' \ \forall i \in [\![1, n+t]\!]\}$. When $d = 2$ this set has typically dimension k.

4. We use this subspace of $\mathscr{C}_{\text{pub}}$ to find a suitable parity-check matrix for $\mathscr{C}_{\text{pub}}$ which allows us to sign like a legitimate user.

Steps 2. and 3. are straightforward. We just give details for Steps 1. and 4. in what follows.

4.4 Finding rank 1 matrices in $\mathscr{C}_{\mathbf{pub}}^{\mathbf{proj}}$ by solving a bilinear system

The basic bilinear system. Finding rank 1 matrices in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ can be formulated as an instance of the MinRank problem [BFS99, Cou01]. We could use standard techniques for solving this problem [KS99, FLdVP08, FDS10, Spa12] but we found that it is better here to use the algebraic modeling suggested in [AGH+17]. It basically consists in setting up an algebraic system with unknowns $\mathbf{x} = (x_1, \ldots, x_{m-1}) \in \mathbb{F}_q^{m-1}$ and $\mathbf{y} \in \mathbb{F}_q^{n+t}$ where the unknown matrix $\mathbf{M}$ in $\mathscr{C}_{\text{pub}}^{\text{proj}}$ that should be of rank 1 has the form

$$\mathbf{M} = \begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_{n+t} \\ x_2y_1 & x_2y_2 & \cdots & x_2y_{n+t} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m-1}y_1 & x_{m-1}y_2 & \cdots & x_{m-1}y_{n+t} \end{pmatrix}.$$

Recall that $\mathscr{C}_{\text{pub}}^{\text{proj}}$ has the structure of an $\mathbb{F}_q$ subspace of $\mathbb{F}_q^{(m-1)\times(n+t)}$ of dimension $(k+t)m$. By viewing the elements of $\mathscr{C}_{\text{pub}}^{\text{proj}}$ as vectors of $\mathbb{F}_q^{(m-1)(n+t)}$, i.e. the matrix $\mathbf{M} = (M_{ij})_{\substack{1\leq i\leq m-1\\1\leq j\leq n+t}}$ is viewed as the vector $\mathbf{m} = (m_\ell)_{1\leq \ell\leq (m-1)(n+t)}$ where $m_{(i-1)(n+t)+j} = M_{i,j}$, we can compute a parity-check matrix $\mathbf{H}_{\text{pub}}^{\text{proj}}$ for it. It is an $((m-1)(n+t)-(k+t)m)\times(m-1)(n+t)$ matrix that we denote by $\mathbf{H}_{\text{pub}}^{\text{proj}} = (H_{ij}^{\text{proj}})_{\substack{1\leq i\leq (m-1)(n+t)-(k+t)m\\1\leq j\leq (m-1)(n+t)}}$. This matrix gives $(m-1)(n+t)-(k+t)m$ bilinear equations that have to be satisfied by the x_i's and the y_j's:

$$\begin{cases} \sum_{j=1}^{n+t}\sum_{i=1}^{m-1} H_{1,(i-1)(n+t)+j}^{\text{proj}} x_i y_j = 0 \\ \vdots \\ \sum_{j=1}^{n+t}\sum_{i=1}^{m-1} H_{(n+t)(m-1)-(k+t)m,(i-1)(n+t)+j}^{\text{proj}} y_j x_l = 0 \end{cases} \tag{7}$$

Restricting the number of solutions. We have solved the bilinear system (7) with standard Gröbner bases techniques that are implemented in Magma. To speed-up the resolution of the bilinear system with Gröbner bases techniques (especially the change of order that is performed after a first computation of a Gröbner basis for a suitable order to deduce a basis for the lexicographic order which is more suited for outputting a solution) it is helpful to use additional equations that restrict the solution space which is otherwise really huge in this case. The purpose of the following discussion is to show where these solutions come from and how to restrict them.

By bilinearity of System (7) we may fix $x_1 = 1$ (when there is a solution $\mathbf{x}$ such that $x_1 \neq 0$). Furthermore, the fact that $\mathscr{C}'_{\text{pub}}$ is an $\mathbb{F}_q$ vector space of dimension n/d induces that for a given $\mathbf{x}$ solution to (7) the set of corresponding $\mathbf{y}$'s also forms a vector space of dimension n/d. We may therefore rather safely assume that we can choose

$$\forall i \in [\![1, \frac{n}{d}-1]\!],\ y_i = 0 \quad \text{and} \quad y_{n/d} = 1.$$

There is an additional degree of freedom on $\mathbf{x}$ coming from the fact that even if $d = 2$ there are several spaces αF for which $1 \in \alpha F$. To verify this, let us study in more detail the case when F is of dimension 2, say

$$F = \langle a, b\rangle_{\mathbb{F}_q}.$$

Intended Security [AGH+17]	(n,k,m,d,t,q)	Time	Maximum Memory Usage
128 bits	$(20,10,21,2,2,2^{32})$	20.12 s	49 MB
128 bits	$(24,12,24,2,2,2^{24})$	31.75 s	65 MB
192 bits	$(24,12,27,2,3,2^{32})$	125.64 s	97 MB
256 bits	$(28,14,30,2,3,2^{32})$	256.90 s	137 MB

Table 1: Attack on NIST's parameters of RankSign

We wish to understand what are the possible values for $z \in \mathbb{F}_{q^m}$ such that there exists $c \neq 0$ for which

$$\langle a, b\rangle_{\mathbb{F}_q} = c\langle 1, z\rangle_{\mathbb{F}_q}. \tag{8}$$

The possible values for $\mathbf{x}$ will then be the projection of those z to the $\mathbb{F}_q$ space $\langle \beta_1, \dots, \beta_{m-1}\rangle_{\mathbb{F}_q}$. The possible values for z are then obtained from studying the possible values for c. There are two cases to consider:

- **Case 1:** $c = \frac{\mu}{a+b\nu}$ for $\mu \in \mathbb{F}_q^\times$ and $\nu \in \mathbb{F}_q$. In such a case
$$z = \frac{\beta b}{a+b\nu} + \delta$$
for $\beta \in \mathbb{F}_q^\times$, $\delta \in \mathbb{F}_q$.
- **Case 2:** $c = \frac{\mu}{b}$ for $\mu \in \mathbb{F}_q^\times$. Here
$$z = \alpha\frac{a}{b} + \delta$$
for $\alpha \in \mathbb{F}_q^\times$, $\delta \in \mathbb{F}_q$.

Since the δ term vanishes after projecting x onto $\langle \beta_1, \dots, \beta_{m-1}\rangle_{\mathbb{F}_q}$ we have essentially two degrees of freedom over $\mathbb{F}_q$ for x. One has already been taken into account when setting $x_1 = 1$. We can add a second one $x_2 = \alpha$ where α is arbitrary in $\mathbb{F}_q$. We have actually chosen in our experiments that $(x_2 - \alpha)(x_2 - \beta) = 0$ for some random α and β in $\mathbb{F}_q$. This has resulted in some gain in the computation of the solution space.

4.5 Numerical results

We give in Table 1 our numerical results to find a codeword of rank 2 in any public code of the RankSign scheme for parameters chosen according to [AGH+17].

4.6 Finishing the attack

We present in this subsection the end of our attack which consists in being able to sign with only the knowledge of the public key. It holds for the parameters chosen for the NIST competition [AGH+17] for which $d = 2$. Observe that (4) implies that we have $k = n-k = n/2$.

We have at that point obtained the code $\mathscr{C}'_{\text{pub}}$ that is dimension (over $\mathbb{F}_q$) $\geq n/d = n/2 = k$. This code is just $\mathbb{F}_q$-linear, but it will be convenient to extend this code by considering its $\mathbb{F}_{q^m}$-linear extension, that we denote $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$ that is defined by the $\mathbb{F}_{q^m}$-linear subspace of

$\mathbb{F}_{q^m}^{n+t}$ obtained from linear combinations over $\mathbb{F}_{q^m}$ of codewords in $\mathscr{C}'_{\text{pub}}$. In other words if we denote by $\{\mathbf{c}'_1, \dots, \mathbf{c}'_{k'}\}$ an $\mathbb{F}_q$-basis of $\mathscr{C}'_{\text{pub}}$, then

$$\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}} = \langle \mathbf{c}'_1, \dots, \mathbf{c}'_{k'} \rangle_{\mathbb{F}_{q^m}}.$$

To simplify the discussion we make now the following assumption (which was corroborated by our experiments)

Assumption 1.

$$\dim \mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}} = k.$$

The rationale behind this assumption is that (i) the dimension of $\mathscr{C}'_{\text{pub}}$ is very likely to be n/d which is equal to k and (ii) an $\mathbb{F}_q$ basis of $\mathscr{C}'_{\text{pub}}$ is very likely to be an $\mathbb{F}_{q^m}$ basis too.

Lemma 3. *Under Assumption 1 the code* $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ *has length* $n+t$*, dimension* $n+t-k$ *and is an* LRPC*-code that is associated to a homogeneous matrix that has all its entries in an* $\mathbb{F}_q$ *subspace* F *of* $\mathbb{F}_{q^m}$ *of dimension* 2 *which contains* 1*. Furthermore, the sets*

$$\mathscr{D} \stackrel{\triangle}{=} \{\mathbf{c} \in \left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp} : \text{Supp}(\mathbf{c}) \subseteq \mathbb{F}_q\} \quad \text{and} \quad \mathscr{D}' \stackrel{\triangle}{=} \{\mathbf{c} \in \left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp} : \text{Supp}(\mathbf{c}) \subseteq F\}$$

are $\mathbb{F}_q$*-subspaces of dimension* $\geq t$*. and* $\geq n-k+2t$ *respectively.*

Proof. By Assumption 1, $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$ is of dimension k and its dual $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ has therefore dimension $n+t-k$. There is a generator matrix for $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$ that is formed by rows taken from $\mathscr{C}'_{\text{pub}}$. It is homogeneous of weight 2. Say that its entries generate a space F. This is also a parity-check matrix of the dual code. $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ is therefore an LRPC code of weight 2.

By applying now Lemma 1 to it with $F' = \mathbb{F}_q$, we have

$$\begin{aligned}(n+t) \cdot \dim_{\mathbb{F}_q}(\mathbb{F}_q) - (n+t-(n+t-k)) \dim(F \cdot \mathbb{F}_q) &= n+t-2k \\ &= t \text{ (because } 2k = n)\end{aligned}$$

which gives the result for the set $\mathscr{D}$. We apply once again Lemma 1 but this time with $F' = F$. Say $F = \langle 1, x_1 \rangle_{\mathbb{F}_q}$. This gives a lower bound on the dimension of $\mathscr{D}'$ which is

$$\begin{aligned}(n+t)\dim(F) - (n+t-(n+t-k))\dim(F \cdot F) &\geq 2(n+t) - 3k \text{ (because } F \cdot F = \langle 1, x_1, x_1^2 \rangle_{\mathbb{F}_q}) \\ &= n-k+2t \text{ (because } 2k = n).\end{aligned}$$

□

To end our attack we make now the following assumption that was again corroborated in our experiments.

Assumption 2. We can extract from sets $\mathscr{D}$ and $\mathscr{D}'$ a basis of $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ with

1. t codewords of support $\mathbb{F}_q$,

2. $n-k$ codewords of a same support of rank 2 which contains 1.

Lemma 4. *Under Assumptions 1 and 2 there exists a parity-check matrix* $\mathbf{H}' \in \mathbb{F}_{q^m}^{(n+t-k)\times(n+t-k)}$ *of* $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$*, an invertible matrix* $\mathbf{P}$ *of size* $n+t$ *with entries in the small field* $\mathbb{F}_q$ *and an invertible matrix* $\mathbf{S}$ *of size* $n+t-k$ *with entries in* $\mathbb{F}_{q^m}$ *such that*

$$\mathbf{S}\mathbf{H}'\mathbf{P} = \begin{pmatrix} I_t & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

where $\mathbf{R}$ *is homogeneous of degree* 2 *and of size* $(n-k) \times n$*.*

Proof. Under Assumptions 1 and 2 there is a generator matrix of $\left(\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}\right)^{\perp}$ and thus a parity-check matrix of $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$ which is homogeneous of degree 2 with the particularity that t rows of it are of rank 1. Let $\mathbf{H}'$ be such a matrix, thus by making a Gaussian elimination on its rows we have an invertible matrix $\mathbf{S} \in \mathbb{F}_{q^m}^{(n+t-k)\times(n+t-k)}$ such that:

$$\mathbf{S}\mathbf{H}' = \begin{pmatrix} I_t & \mathbf{Q} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

where $\mathbf{Q}$ is a matrix of size $t \times (n+t)$ whose entries lie in the small field $\mathbb{F}_q$ and $\mathbf{R}$ is a homogeneous matrix of weight 2 and of size $(n-k) \times n$. In this way there exists an invertible matrix $\mathbf{P}$ of size $(n+t) \times (n+t)$ with coefficients in the field $\mathbb{F}_q$ such that

$$\mathbf{S}\mathbf{H}'\mathbf{P} = \begin{pmatrix} I_t & \mathbf{0} \\ \mathbf{0} & \mathbf{R} \end{pmatrix}$$

which concludes the proof. □

The idea now to sign as a legitimate user will be to use the matrix $\mathbf{R}$ and the decoder of Fact 1 (see Section §3). Recall that to make a signature for the matrix $\mathbf{H}_{\text{pub}}$ (which defines the public code $\mathscr{C}_{\text{pub}}$) and a message $\mathbf{m}$, we look for an error $\mathbf{e}$ of rank w satisfying $n-k = d(w-t-t')$ (see Equation (3) of Fact 1), such that $\mathbf{H}_{\text{pub}}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$ with $\mathbf{s} = \mathscr{H}(\mathbf{m})$ (the hash of the message). The algorithm that follows performs this task:

1. We compute $\mathbf{y} \in \mathbb{F}_{q^m}^{n+t}$ such that $\mathbf{H}_{\text{pub}}\mathbf{y}^{\intercal} = \mathbf{s}^{\intercal}$.
2. Let $\mathbf{y}' = \mathbf{y}(\mathbf{P}^{-1})^{\intercal}$ and we compute $\mathbf{s}' = (\mathbf{S}\mathbf{H}'\mathbf{P})\mathbf{y}'^{\intercal}$.
3. Let $\mathbf{s}'_1$ be the first t coordinates of $\mathbf{s}'$, $\mathbf{s}'_2$ its last $n-k$ ones. We apply the decoder of §3 with:

   - The subspace $T \triangleq \text{Supp}(\mathbf{s}'_1) + T'$ where T' is a random subspace of $\mathbb{F}_{q^m}$ of dimension t'.

   - The parity-check matrix $\mathbf{R}$ and the syndrome $\mathbf{s}'_2$.

   Then we get a vector $\mathbf{e}'$ such that $T \subseteq \text{Supp}(\mathbf{e}')$ and $\mathbf{R}\mathbf{e}'^{\intercal} = \mathbf{s}'^{\intercal}_2$.
4. We compute $\mathbf{e} = (\mathbf{s}'_1, \mathbf{e}')\mathbf{P}^{\intercal}$.

Let us now show the correctness of this algorithm, in other words we show that $\mathbf{H}_{\text{pub}}\mathbf{e}^{\intercal} = \mathbf{s}^{\intercal}$ with $|\mathbf{e}| = w$ satisfying $n-k = 2(w-t-t')$.

Proof of Correctness. First we have:

$$\begin{aligned}
\mathbf{H}'\mathbf{e}^{\intercal} &= \mathbf{H}'\mathbf{P}(\mathbf{s}'_1, \mathbf{e}')^{\intercal}\\
&= \mathbf{S}^{-1}(\mathbf{S}\mathbf{H}'\mathbf{P})(\mathbf{s}'_1, \mathbf{e}')^{\intercal}\\
&= \mathbf{S}^{-1}\begin{pmatrix} I_t & \mathbf{0}\\ \mathbf{0} & \mathbf{R}\end{pmatrix}(\mathbf{s}'_1, \mathbf{e}')^{\intercal}\\
&= \mathbf{S}^{-1}\begin{pmatrix} \mathbf{s}'^{\intercal}_1\\ \mathbf{R}\mathbf{e}'^{\intercal}\end{pmatrix} \text{ (because } \mathbf{s}'_1 \text{ of size } t)\\
&= \mathbf{S}^{-1}\mathbf{s}'^{\intercal} \text{ (because } \mathbf{R}\mathbf{e}'^{\intercal} = \mathbf{s}'^{\intercal}_2)\\
&= \mathbf{S}^{-1}(\mathbf{S}\mathbf{H}'\mathbf{P})\mathbf{y}'^{\intercal}\\
&= \mathbf{H}'\mathbf{P}(\mathbf{P}^{-1}\mathbf{y}^{\intercal})\\
&= \mathbf{H}'\mathbf{y}^{\intercal}
\end{aligned}$$

which implies that $\mathbf{H}'(\mathbf{e}-\mathbf{y})^{\intercal} = \mathbf{0}$ and $\mathbf{y}-\mathbf{e} \in \mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}}$. Recall now that $\mathbb{F}_{q^m} \otimes \mathscr{C}'_{\text{pub}} \subseteq \mathscr{C}_{\text{pub}}$ and therefore $\mathbf{H}_{\text{pub}}(\mathbf{e}-\mathbf{y})^{\intercal} = \mathbf{0}$. By linearity we get $\mathbf{H}_{\text{pub}}\mathbf{e}^{\intercal} = \mathbf{H}_{\text{pub}}\mathbf{y}^{\intercal} = \mathbf{s}^{\intercal}$.
Thus under the condition that the decoder in Point 3 works for the matrix $\mathbf{H}'$, the syndrome $\mathbf{s}$ and the subspace T our algorithm decodes the syndrome $\mathbf{s}$ relatively to $\mathbf{H}_{\text{pub}}$.
The parity-check matrix $\mathbf{R}$ is homogeneous of degree 2, has $n-k$ rows and n columns. We can therefore apply to it the decoder of §3. It will output (we use here Fact 1) an error $\mathbf{e}'$ of weight w' that satisfies $n-k = 2(w'-t-t')$. Note that this implies that $w' = w$ which is the error weight we want to achieve. Then the error $\mathbf{e} = (\mathbf{s}'_1, \mathbf{e}')\mathbf{P}^{\intercal}$ has the same rank as $\text{Supp}(\mathbf{s}'_1) \subseteq T \subseteq \text{Supp}(\mathbf{e}')$ and $\mathbf{P}$ is an invertible matrix in the small field which concludes the proof.

□

To summarize, in essence with codewords of rank 2 in the public code of RankSign and under Assumptions 1 and 2 we find the decoder that was used to sign with the secret key.

5 Concluding remarks

This paper is only a preliminary version of our work which gives a quick report on our attack on RankSign. It will be followed by a more elaborated version which will analyze more precisely the complexity of this attack and which will show that it is actually polynomial for all possible strategies for choosing the parameters of RankSign. Repairing the RankSign seems to require to modify the scheme itself and not just adjust the parameters.

It might be tempting to conjecture that this approach could also be used to mount an attack on the NIST submissions based on LRPC codes such as [ABD+17a, ABD+17b]. Roughly speaking our approach consists in looking for low weight codewords in the LRPC code instead of looking for low weight codewords in the usual suspect, that is the dual of the LRPC code, that has in this case low weight codewords by definition of the LRPC code. This approach does not seem to carry over to the LRPC codes considered in these submissions. The point is that our approach was successful for RankSign because of the way the parameters of the LRPC code had to be chosen. In particular the length n, the dimension k and the weight of the LRPC code have to satisfy

$$n = (n-k)d.$$

It is precisely this equality that is responsible for the weight 2 codewords in the LRPC code. If d is not too small (say > 3) and $(n-k)d$ is not too close to n then all the approach considered here fails at the very beginning.

References

[ABD⁺17a] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LAKE–Low rAnk parity check codes Key Exchange —-. first round submission to the NIST post-quantum cryptography call, November 2017.

[ABD⁺17b] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, and Gilles Zémor. LOCKER–LOw rank parity ChecK codes EncRyption –. first round submission to the NIST post-quantum cryptography call, November 2017.

[AGH⁺17] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Oliver Ruatta, and Gilles Zémor. Ranksign -a signature proposal for the NIST's call-. first round submission to the NIST post-quantum cryptography call, November 2017. NIST Round 1 submission for Post-Quantum Cryptography.

[AMAB⁺17] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Rank quasi cyclic (RQC). first round submission to the NIST post-quantum cryptography call, November 2017.

[BFS99] Jonathan F. Buss, Gudmund S. Frandsen, and Jeffrey O. Shallit. The computational complexity of some problems of linear algebra. *J. Comput. System Sci.*, 58(3):572–596, June 1999.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1+1=0$ improves information set decoding. In *Advances in Cryptology - EUROCRYPT 2012*, LNCS. Springer, 2012.

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Smaller decoding exponents: ball-collision decoding. In *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *LNCS*, pages 743–760, 2011.

[BM17] Leif Both and Alexander May. Optimizing BJMM with Nearest Neighbors: Full Decoding in $2^{2/21n}$ and McEliece Security. In *WCC Workshop on Coding and Cryptography*, September 2017. To appear, see `https://www.google.fr/?gfe_rd=cr&ei=lEyVWcPPBuXU8gfAj5ygBg`.

[BMvT78] Elwyn Berlekamp, Robert McEliece, and Henk van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, 24(3):384–386, May 1978.

[CFS01] Nicolas Courtois, Matthieu Finiasz, and Nicolas Sendrier. How to achieve a McEliece-based digital signature scheme. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 157–174, Gold Coast, Australia, 2001. Springer.

[Cou01] Nicolas Courtois. Efficient zero-knowledge authentication based on a linear algebra problem MinRank. In *Advances in Cryptology - ASIACRYPT 2001*, volume 2248 of *LNCS*, pages 402–421, Gold Coast, Australia, 2001. Springer.

[DT17] Thomas Debris-Alazard and Jean-Pierre Tillich. Statistical decoding. preprint, January 2017. arXiv:1701.07416.

[Dum91] Ilya Dumer. On minimum distance decoding of linear codes. In *Proc. 5th Joint Soviet-Swedish Int. Workshop Inform. Theory*, pages 50–52, Moscow, 1991.

[FDS10] Jean-Charles Faugère, Mohab Safey El Din, and Pierre-Jean Spaenlehauer. Computing loci of rank defects of linear matrices using gröbner bases and applications to cryptology. In *Symbolic and Algebraic Computation, International Symposium, ISSAC 2010, Munich, Germany, July 25-28, 2010, Proceedings*, pages 257–264, 2010.

[FLdVP08] Jean-Charles Faugère, Françoise Levy-dit Vehel, , and Ludovic Perret. Cryptanalysis of Minrank. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *LNCS*, pages 280–296, 2008.

[FS09] Matthieu Finiasz and Nicolas Sendrier. Security bounds for the design of code-based cryptosystems. In M. Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 88–105. Springer, 2009.

[Gab08] Ernst. M. Gabidulin. Attacks and counter-attacks on the GPT public key cryptosystem. *Des. Codes Cryptogr.*, 48(2):171–177, 2008.

[GHPT17] Philippe Gaborit, Adrien Hauteville, Duong Hieu Phan, and Jean-Pierre Tillich. Identity-based encryption from rank metric. In *Advances in Cryptology - CRYPTO2017*, volume 10403 of *LNCS*, pages 194–226. Springer, August 2017.

[GMRZ13] Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. Available on `www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf`.

[GO01] Ernst M. Gabidulin and Alexei V. Ourivski. Modified GPT PKC with right scrambler. *Electron. Notes Discrete Math.*, 6:168–177, 2001.

[GPT91] Ernst M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their applications to cryptography. In *Advances in Cryptology - EUROCRYPT'91*, number 547 in LNCS, pages 482–489, Brighton, April 1991.

[GRS13] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *CoRR*, abs/1301.1026, 2013.

[GRS16] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Trans. Information Theory*, 62(2):1006–1019, 2016.

[GRSZ14] Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor. New results for rank-based cryptography. In *Progress in Cryptology - AFRICACRYPT 2014*, volume 8469 of *LNCS*, pages 1–12, 2014.

[GZ16] Philippe Gaborit and Gilles Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Information Theory*, 62(12):7245–7252, 2016.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology - CRYPTO'99*, volume 1666 of *LNCS*, pages 19–30, Santa Barbara, California, USA, August 1999. Springer.

[LB88] Pil J. Lee and Ernest F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In *Advances in Cryptology - EUROCRYPT'88*, volume 330 of *LNCS*, pages 275–280. Springer, 1988.

[Loi14] Pierre Loidreau. Asymptotic behaviour of codes in rank metric over finite fields. *Des. Codes Cryptogr.*, 71(1):105–118, 2014.

[MMT11] Alexander May, Alexander Meurer, and Enrico Thomae. Decoding random linear codes in $O(2^{0.054n})$. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 107–124. Springer, 2011.

[MO15] Alexander May and Ilya Ozerov. On computing nearest neighbors with applications to decoding of binary linear codes. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 203–228. Springer, 2015.

[Nie86] Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[Pra62] Eugene Prange. The use of information sets in decoding cyclic codes. *IRE Transactions on Information Theory*, 8(5):5–9, 1962.

[Spa12] Pierre-Jean Spaenlenhauer. *Résolution de systèmes multi-homogènes et determinantiels.* PhD thesis, Univ. Pierre et Marie Curie- Paris 6, October 2012.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In G. D. Cohen and J. Wolfmann, editors, *Coding Theory and Applications*, volume 388 of *LNCS*, pages 106–113. Springer, 1988.