RankSign
-a signature proposal for the NIST's call-

November 30, 2017

RankSign is a post-quantum signature scheme running for standardization to NIST's competition in the category "post-quantum signature scheme". Different sets of parameters are proposed for security strength categories 1, 3, and 5.

Principal Submitters, Inventors, Owners, Developers (by alphabetical order)

- Nicolas Aragon
- Philippe Gaborit
- Adrien Hauteville
- Olivier Ruatta
- Gilles Zémor

Inventors: Same as submitters

Developers: Same as submitters

Owners: Same as submitters

Main contact

Philippe Gaborit
philippe.gaborit@unilim.fr
+33-626-907-245
University of Limoges
123 avenue Albert Thomas
87 060 Limoges Cedex
France

Backup point of contact

Adrien Hauteville
adrien.hauteville@unilim.fr
+33-642-709-282
University of Limoges
123 avenue Albert Thomas
87 060 Limoges Cedex
France

Signatures

Digital copies of the signed statements are provided in Appendix A. The original paper versions will be given to Dustin Moody directly at the First PQC Standardization Conference.

Abstract

This document is the complete documentation of the proposal RankSign, a quantum resistant signature based on rank metric. It is organized as suggested in NIST's call for proposal from December 2016: Backgrounds on Coding Theory and rank metric are provided in Sec. 1 together with the description of our scheme, then a performance analysis is conducted in Sec. 2. Known Answers Tests values (*aka.* KATs) are provided Sec. 3, then Security and Known Attacks are discussed in Sec. 4 and 5 respectively. Finally, the advantages and limitations of the proposed protocol are discussed in Sec. 6.

Contents

Prologue

The RankSign cryptosystem [9] was introduced in 2014. This signature scheme is based on code in rank metric. The general idea is to use an LRPC code (which is an equivalent to the MDPC in Hamming metric or to NTRU in the euclidean metric) as a trapdoor to compute an error associated to a message. The main issue with this cryptosystem was that the probability to distinguish between a signature and a random vector was in $2/q$ (for q the cardinal of the basefield $\mathbb{F}_q$) which obliged to consider very large q.

In this proposal, we introduce a new variation on RankSign which consists in adding a small random error in the signature, so it permits to decrease the capacity for an attacker to distinguish between the distribution of the signatures and the uniform distribution, in $\frac{1}{q^2}$ or $\frac{1}{q^3}$.

Although the signature scheme may seem complex due to the inherent complexity of rank metric, the underneath ideas behind the protocol are very simple and quite similar to ideas developed in lattice based signature scheme GPV [11].

1 Specifications

In the following document, q denotes a power of a prime p. The finite field with q elements is denoted by $\mathbb{F}_q$ and more generally for any positive integer m the finite field with q^m elements is denoted by $\mathbb{F}_{q^m}$. We will frequently view $\mathbb{F}_{q^m}$ as an m-dimensional vector space over $\mathbb{F}_q$.

We use bold lowercase and capital letters to denote vectors and matrices respectively. We will view vectors here either as column or row vectors. It will be clear from the context whether it is a column or a row vector. For two matrices $\boldsymbol{A}, \boldsymbol{B}$ of compatible dimensions, we let $(\boldsymbol{A}|\boldsymbol{B})$ and $\left(\frac{\boldsymbol{A}}{\boldsymbol{B}}\right)$ respectively denote the horizontal and vertical concatenations of $\boldsymbol{A}$ and $\boldsymbol{B}$.

If S is a finite set, $x \xleftarrow{\$} S$ denotes that x is chosen uniformly at random among S.

1.1 Presentation of rank metric codes

1.1.1 General definitions

Definition 1.1 (Rank metric over $\mathbb{F}_{q^m}^n$)**.** *Let $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $(\beta_1, \ldots, \beta_m) \in \mathbb{F}_{q^m}^m$ a basis of $\mathbb{F}_{q^m}$ viewed as an m-dimensional vector space over $\mathbb{F}_q$. Each coordinate x_j is associated to a vector of $\mathbb{F}_q^m$ in this basis: $x_j = \sum_{i=1}^m m_{ij}\beta_i$. The $m \times n$ matrix associated to $\boldsymbol{x}$ is given by $\boldsymbol{M}(\boldsymbol{x}) = (m_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$.*

The rank weight $\|\boldsymbol{x}\|$ of $\boldsymbol{x}$ is defined as

$$\|\boldsymbol{x}\| \stackrel{def}{=} \operatorname{Rank} \boldsymbol{M}(\boldsymbol{x}).$$

The associated distance $d(\boldsymbol{x}, \boldsymbol{y})$ *between elements* $\boldsymbol{x}$ *and* $\boldsymbol{y}$ *in* $\mathbb{F}_{q^m}^n$ *is defined by* $d(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$.

Definition 1.2 ($\mathbb{F}_{q^m}$-linear code)**.** *An* $\mathbb{F}_{q^m}$*-linear code* $\mathcal{C}$ *of dimension* k *and length* n *is a subspace of dimension* k *of* $\mathbb{F}_{q^m}^n$ *embedded with the rank metric. It is denoted* $[n, k]_{q^m}$.

$\mathcal{C}$ *can be represented by two equivalent ways:*

- *by a generator matrix* $\boldsymbol{G} \in \mathbb{F}_{q^m}^{k \times n}$*. Each rows of* $\boldsymbol{G}$ *is an element of a basis of* $\mathcal{C}$*,*

$$\mathcal{C} = \{\boldsymbol{x}\boldsymbol{G}, \boldsymbol{x} \in \mathbb{F}_{q^m}^k\}$$

- *by a parity-check matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$*. Each rows of* $\boldsymbol{H}$ *determines a parity-check equation verified by the elements of* $\mathcal{C}$*:*

$$\mathcal{C} = \{\boldsymbol{x} \in \mathbb{F}_{q^m}^n : \boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{0}\}$$

We say that $\boldsymbol{G}$ *(respectively* $\boldsymbol{H}$*) is under systematic form iff it is of the form* $(\boldsymbol{I}_k|\boldsymbol{A})$ *(respectively* $(\boldsymbol{I}_{n-k}|\boldsymbol{B})$*).*

Definition 1.3 (Support of a word)**.** *Let* $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$*. The support* E *of* $\boldsymbol{x}$*, denoted* $\mathrm{Supp}(\boldsymbol{x})$*, is the* $\mathbb{F}_q$*-subspace of* $\mathbb{F}_{q^m}$ *generated by the coordinates of* $\boldsymbol{x}$*:*

$$E = \langle x_1, \ldots, x_n \rangle_{\mathbb{F}_q}$$

and we have $\dim E = \|\boldsymbol{x}\|$.

The number of supports of dimension w of $\mathbb{F}_{q^m}$ is denoted by the Gaussian coefficient

$$\begin{bmatrix} m \\ w \end{bmatrix}_q = \prod_{i=0}^{w-1} \frac{q^m - q^i}{q^w - q^i}$$

1.2 Difficult problems in rank metric

In this section, we introduce the difficult problems on which our cryptosystem is based. to

Problem 1.4 (Rank Syndrome Decoding)**.** *Given a full-rank matrix* $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$*, a syndrome* $\boldsymbol{\sigma}$ *and a weight* ω*, it is hard to sample a vector* $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ *of weight lower than* ω *such that* $\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{\sigma}^T$.

The RSD problem has recently been proven hard in [10] on probabilistic reduction.
The complexity of the known attacks against these problems are described in Section 5.

1.3 Bounds in rank metric

We recall here the definition of the rank Gilbert-Varshamov bound and the rank Singleton bound we need to define our algorithm.

Definition 1.5 (Rank Gilbert-Varshamov (RGV) bound)**.** *Let $\mathcal{C}$ be an $[n,k]_{q^m}$. The rank Gilbert-Varshamov bound $RGV(n,k,m,q)$ for $\mathcal{C}$ is the smallest integer r such that the volume $\mathcal{V}(n,m,q,r)$ of a ball of radius r is larger than the number $q^{(n-k)m}$ of syndromes of $\mathcal{C}$.*

By definition, $\mathcal{V}(n,m,q,r) = \sum_{i=0}^{r} S(n,m,q,i)$ where $S(n,m,q,i)$ is the cardinal of a sphere of radius i of $\mathbb{F}_{q^m}^n$, which is equal to the number of matrices $m \times n$ of rank i with coefficients in $\mathbb{F}_q$.

$$S(n,m,q,i) = \prod_{j=0}^{i-1} \frac{(q^m - q^j)(q^n - q^j)}{q^i - q^j}$$

In the case $m = n$, we have $\frac{RGV(n,k,m,q)}{n} \sim 1 - \sqrt{\frac{k}{n}}$ and in the general case, we have $RGV(n,k,m,q) \sim \frac{m+n-\sqrt{(m-n)^2+4km}}{2}$.

Definition 1.6 (Rank Singleton bound)**.** *The rank Singleton $d_{Sing}(n,k,m,q)$ bound is the smallest integer r such that the RSD problem 1.4 admits a solution for all support E of $\boldsymbol{x}$ of dimension r with strong probability.*

The parity-check equations $\boldsymbol{H}\boldsymbol{x}^T = \boldsymbol{\sigma}^T$ gives us $(n-k)m$ equations over $\mathbb{F}_q$. We can express each coordinates of $\boldsymbol{x}$ in a basis of E to obtain nr unknowns over $\mathbb{F}_q$. This system admits a solution with strong probability if $nr \geqslant (n-k)m$ so $d_{Sing}(n,k,m,q) = \left\lceil \frac{(n-k)m}{n} \right\rceil$.

In the case $m > n$, we can consider the subspace generated by the rows of the matrix associated to $\boldsymbol{x}$ (cf definition 1.1) to obtain a system of mr unknowns and $(n-k)m$ equations, hence $d_{Sing}(n,k,m,q) = n-k$

In the general case, we always have:

$$d_{Sing}(n,k,m,q) = \left\lceil \frac{(n-k)m}{\max(m,n)} \right\rceil$$

1.4 The Low Rank Parity Check codes

1.4.1 Definition

The LRPC codes have been introduced in [7]. They are good candidates for the cryptosystem of McEliece because the have a weak algebraic structure.

Definition 1.7 (LRPC codes)**.** *Let $\boldsymbol{H} = (h_{ij})_{\substack{1 \leqslant i \leqslant n-k \\ 1 \leqslant j \leqslant n}} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ a full-rank matrix such that its coefficients generate an $\mathbb{F}_q$-subspace F of small dimension d:*

$$F = \langle h_{ij} \rangle_{\mathbb{F}_q}$$

Let $\mathcal{C}$ be the code with parity-check matrix $\boldsymbol{H}$. By definition, $\mathcal{C}$ is an $[n,k]_{q^m}$ LRPC code of weight d.

Such a matrix $\boldsymbol{H}$ is called homogeneous matrix of weight d and support F.

Now, we define a larger family of code, called the augmented LRPC codes [9]. We will use these codes to hide the structure of an LRPC code in our signature scheme.

Definition 1.8 (Augmented LRPC codes)**.** *Let $\boldsymbol{H}$ be an $\mathbb{F}_{q^m}^{(n-k)\times n}$ homogeneous matrix of full-rank and of weight d and $\boldsymbol{R} \in \mathbb{F}_{q^m}^{(n-k)\times t}$ be a random matrix. Let $\boldsymbol{P} \in GL_{n-k}(\mathbb{F}_{q^m})$ and $\boldsymbol{Q} \in GL_{n+t}(\mathbb{F}_q)$ be two invertible matrices (remark that the coefficients of $\boldsymbol{Q}$ belong to the base field). Let $\boldsymbol{H}' = \boldsymbol{P}(\boldsymbol{R}|\boldsymbol{H})\boldsymbol{Q}$ be the parity-check matrix of a code $\mathcal{C}$ of type $[n+t,k+t]_{q^m}$. By definition, such a code is an augmented LRPC code. If $t=0$, $\mathcal{C}$ is an LRPC code.*

Problem 1.9 (Augmented LRPC codes indistinguishability)**.** *Given an augmented LRPC code of type $[n+t,k+t]_{q^m}$, it is hard to distinguish it from a random code with the same parameters.*

The hardness of this problem is studied in [9]. We will deal with the attacks in section 5.2.

1.4.2 Generalized Erasure Decoding algorithm

In this section, we describe the generalized erasure decoding algorithm we use in our signature scheme. This algorithm is an adaptation of the decoding algorithm for LRPC codes [7]. A more detailed desciption is given in the article [9].

Let us start with some definitions.

Definition 1.10 (Generalized erasure)**.** *Let $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ be an error of weight r and $E = \mathrm{Supp}(\boldsymbol{e})$. We call* generalized erasure *of dimension t of $\boldsymbol{e}$ a subspace $T \subset E$ of dimension t.*

Definition 1.11. *Let $\mathcal{C}$ an $[n,k]_{q^m}$ LRPC code of weight d and let $\boldsymbol{H}$ be a homogeneous parity-check matrix of $\mathcal{C}$ of support F. Let F_1 and F_2 two elements of a basis of F. We say that a syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}^{n-k}$ is T-decodable if there exists a subspace E of $\mathbb{F}_{q^m}$ of dimension r such that:*

1. $\dim\langle EF\rangle = \dim E \dim F$.
2. $\dim(F_1^{-1}\langle EF\rangle \cap F_2^{-1}\langle EF\rangle = \dim E$.
3. $\mathrm{Supp}(\boldsymbol{s}) \subset \langle EF\rangle$ *and* $\mathrm{Supp}(\boldsymbol{s}) + \langle FT\rangle = \langle EF\rangle$.

Algorithm 1: Generalized erasure decoding algorithm for LRPC codes

Input:

- a homogeneous matrix $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ of weight d and support $F = \langle F_1, \dots F_d \rangle$ which defines an $[n, k]$ LRPC code $\mathcal{C}$.
- a subspace $T = \langle T_1, \dots, T_t \rangle$ of $\mathbb{F}_{q^m}$ of dimension d.
- a T-decodable syndrome $\boldsymbol{s} \in \mathbb{F}_{q^m}$.

Output: $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ of weight r and support E such that $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}^T$ and $T \subset E$.

1 Compute a basis $B = (F_i T_j)_{\substack{1 \leqslant i \leqslant d \\ 1 \leqslant j \leqslant t}}$ of $\langle FT \rangle$.
2 Compute the subspace $S = \langle B \cup \{s_1, \dots, s_{n-k}\} \rangle$.
3 Compute the support of the error $E = F_1^{-1} S \cap F_2^{-1} S$ then a basis $(E_1, \dots E_r)$ of E.
4 Express each coordinates e_i of $\boldsymbol{e}$ in this basis : $e_i = \sum_{j=1}^{r} \lambda_{ij} E_j$
5 Express each coordinates of $\boldsymbol{s}$ in the basis $(F_i E_j)_{\substack{1 \leqslant i \leqslant d \\ 1 \leqslant j \leqslant r}}$ of $\langle EF \rangle$ and solve the system $\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s}^T$ of nr unknowns (λ_{ij}) with $(n-k)rd$ equations.

Since we assume that $\boldsymbol{s}$ is T-decodable, this algorithm is correct. If ever the syndrome were not T-decodable, one of the step fails and the algorithm would return an error value. In practice, we will choose the parameters of our scheme such that the proportion of non T-decodable syndromes is negligible. The theorem 8 of the article [9] shows that if $(r-t)(m-r) + (n-k)(rd-m) = 0$ then the proportion of T-decodable syndromes is superior to $(1 - \frac{1}{q})^2$, so it is easy to have this proportion as close to 1 as we want to.

1.5 RankSign: a signature algorithm based on rank metric

The principle of our signature scheme is to associate a syndrome to a message thank to an hash function modeled as a ROM, then to output an error of weight below the Singleton bound corresponding to this syndrome with respect to a public code $\mathcal{C}$. Only the signer knows the hidden structure of $\mathcal{C}$ which allows him to compute the error. The verifier can check the signature with the public representation of the code. We use the augmented LRPC codes to sign a message.

Formally, RankSign is composed of three algorithms:

- KeyGen: let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a random homogeneous matrix of size $(n-k) \times n$ of support F of weight d, $\boldsymbol{R} \xleftarrow{\$} \mathbb{F}_{q^m}^{(n-k)\times t}$ and $\boldsymbol{Q} \xleftarrow{\$} GL_{n+t}(\mathbb{F}_q)$. Let $\mathcal{C}$ be the augmented LRPC code of type $[n+t, k+t]_{q^m}$ of parity-check matrix $(\boldsymbol{R}|\boldsymbol{H})\boldsymbol{Q}$).

  Let $\boldsymbol{H}_{pub} = (\boldsymbol{I}_{n-k}|\boldsymbol{R}')$be the parity-check matrix under systematic form of $\mathcal{C}$[1] and $\boldsymbol{P} \in GL_{n-k}(\mathbb{F}_{q^m})$ such that $\boldsymbol{H}_{pub} = \boldsymbol{P}(\boldsymbol{R}|\boldsymbol{H})\boldsymbol{Q}$).

[1] the probability that $\mathcal{C}$ do not possess a parity-check matrix under systematic form is around $\frac{1}{q^m}$ which is completely negligible.

Let G be an hash function of range the space of the syndromes $\mathbb{F}_{q^m}^{n-k}$ of $\mathcal{C}$.

Define $\mathsf{pk} = (\boldsymbol{R}', G)$ and $\mathsf{sk} = (\boldsymbol{P}, (\boldsymbol{R}|\boldsymbol{H}), \boldsymbol{Q})$.

- Sign: the signature of a message M is described below.

Algorithm 2: Signature of a message M

Input: a message M, $\mathsf{sk} = (\boldsymbol{P}, (\boldsymbol{R}|\boldsymbol{H}), \boldsymbol{Q})$, three integers r, t' and l.
Data: an hash function G, $\boldsymbol{H}_{pub}$.
Output: a seed and a vector $\boldsymbol{e} \in \mathbb{F}_{q^m}^{n+t}$ of weight r such that $\boldsymbol{e}\boldsymbol{H}'^T = G(M, seed)$.

1 Initialize the seed: $seed \xleftarrow{\$} \{0,1\}^l$.
2 Compute $\boldsymbol{s} = G(M, seed)$.
3 Choose $\boldsymbol{e}' \in \mathbb{F}_{q^m}^{n+t}$ of weight t' uniformly at random.
4 Compute $\boldsymbol{s}' = \boldsymbol{s} - \boldsymbol{e}'\boldsymbol{H}_{pub}^T$.
5 Choose t independent elements $(e_1, \ldots, e_t) \in \mathbb{F}_{q^m}^t$ at random and define $T = \langle e_1, \ldots, e_t \rangle$.
6 Compute $\boldsymbol{s}'' = \boldsymbol{s}'(\boldsymbol{P}^T)^{-1} - (e_1, \ldots, e_t)\boldsymbol{R}^T$.
7 Compute the error $(e_{t+1}, \ldots e_{n+t})$ of weight $r' = r - t'$ with the generalized erasure decoding algorithm 1 with as inputs the matrix $\boldsymbol{H}$, the subspace T and the syndrome $\boldsymbol{s}''$. If $\boldsymbol{s}''$ is not T-decodable, go to step 1.
8 Compute $\boldsymbol{e} = \boldsymbol{e}' + (e_1, \ldots, e_{n+t})(\boldsymbol{Q}^T)^{-1}$.
9 **return** $(\boldsymbol{e}, seed)$.

- Check: the verifier checks that
  - $\boldsymbol{e}^T\boldsymbol{H}_{pub} = G(M, seed)$.
  - $\|\boldsymbol{e}\| \leqslant r$.

1.6 Parameters

In this section, we give some sets of parameters for a security parameters of 128, 192 and 256 bits. The different parameters are:

- q is the cardinal of the base field $\mathbb{F}_q$.
- n is the length the LRPC code used in the generalized erasure decoding algorithm 1.
- $n - k$ is the codimension of the LRPC. It corresponds to the number of rows of the public key $\boldsymbol{H}_{pub}$.
- m is the degree of the extension $\mathbb{F}_{2^m}$.
- d is the weight of the LRPC code.
- t is the number of random colums added to the LRPC code to obtain the public augmented LRPC.

- t' is the weight of the vector $\boldsymbol{e}'$.
- r is the weight of the signature of a message.
- Singleton is the value of the Singleton bound for the public augmented LRPC code.
- Public key is the cost in bits to represent the public augmented LRPC code.
- Signature is the size in bits of the signature $\boldsymbol{e}$. Since $\|\boldsymbol{e}\| = r$, we can represent its support by an $r \times m$ matrix with coefficients in $\mathbb{F}_q$ such that each rows is an element of a basis of $\mathrm{Supp}(\boldsymbol{e})$. Each coordinate of $\boldsymbol{e}$ is a linear combination of this basis and can be represented by a vector of $\mathbb{F}_q^m$. Thus the signature size is equal to $(rm + r(n+t))\lceil \log_2 q \rceil = r(m+n+t)\lceil \log_2 q \rceil$ bits.

The parameters of RankSign have to verify three conditions [9]:

- $m = (r - t')(d+1)$
- $n - k = d(r - t - t')$
- $n = (n-k)d$

In practice, we first choose d then a multiple $(n-k)$ of d. Finally, we fix two parameters among r, t and t'. q can be chosen independently from the other parameters. The other parameters are deduced from the three conditions.

The following table shows the parameters we propose:

Name	q	n	$n-k$	m	d	t	t'	r	Singleton	Security	Public Key size (bits)	Signature size (bits)
RankSign I	2^{32}	20	10	21	2	2	1	8	10	128	80,640	11,008
RankSign II	2^{24}	24	12	24	2	2	2	10	12	128	96,768	12,000
RankSign III	2^{32}	24	12	27	2	3	1	10	12	192	155,520	17,280
RankSign IV	2^{32}	28	14	30	2	3	2	12	14	256	228,480	23,424

Remark 1: In term of classical security hypothesis, we consider an opponent may have access up to 2^{64} signatures samples. According to theorem 4.1, we need $q^{1+t'} \geqslant 2^{64}$ for the signatures do not leak information on the key, which implies we have to choose very high q for our parameters.

Remark 2: It is possible to reduce the size of the signature by representing the matrix of its support under row echelon form: we give the index of the columns used for the pivot (which costs r bytes as long as $m \leqslant 256$) and the "free" coefficients of the echelon matrix. In practice, since we have a very high q, the probability that a square matrix is invertible is around $1 - \frac{1}{q}$ so we gain around $r^2\lceil \log_2 q \rceil - 8r$ bits in the signature size. We do not have implemented this improvement in the program we provide, but this feature will be implemented in a future version. For our parameters we obtain a signature size of:

RankSign I	9,024
RankSign II	9,680
RankSign III	14,160
RankSign IV	18,912

Remark 3: The security parameters have been chosen according to the complexity of the best attack against our scheme. These attacks are described in section 5.

Computational complexity:

- KeyGen: the most costly operation is the inversion of the matrix $\boldsymbol{P} \in GL_{n-k}(\mathbb{F}_{q^m})$ which is $\mathcal{O}\left((n-k)^3\right)$ multiplication in $\mathbb{F}_{q^m}$. Each multiplication costs $\mathcal{O}\left(m\log(m)log(log(m))\log(q)\log(\log(q))\right)$, hence a total complexity of $\mathcal{O}\left((n-k)^3 m\log(m)log(log(m))\log(q)\log(\log(q))\right)$.
- Sign and Check: the most costly operation is the product matrix vector in $\mathbb{F}_{q^m}$ which is $\mathcal{O}\left((n+t)^2\right)$. The total cost is in $\mathcal{O}\left((n+t)^2 m\log(m)log(log(m))\log(q)\log(\log(q))\right)$.

2 Performance Analysis

In this section, we provide concrete timings of our implementations. The benchmarks were performed on an Intel®Core™i7-4700HQ CPU running @ up to 3.40GHz and the software was compiled using GCC (version 6.3.0) with the following command : gcc -O3 -std=c99 -pedantic -Wall -Wextra.

Notice our implementation is not optimized. There is probably room for improvements for all operations in the field $\mathbb{F}_{q^m}$, especially since q is very large.

2.1 Reference Implementation

Tab. 1 gives timings (in ms) of the reference implementation on our benchmark platform, and Tab. 2 gives the number of CPU cycles.

Instance	Keygen	Encap	Decap
RankSign-I	79.3	7.71	3.03
RankSign-II	177	13.6	5.56
RankSign-III	228	18.2	7.40
RankSign-IV	431	28.3	11.8

Table 1: Timings (in ms) of the reference implementation for different instances of RankSign.

Instance	Keygen	Encap	Decap
RankSign-I	190	18.6	7.30
RankSign-II	432	33.1	13.6
RankSign-III	537	43.1	17.5
RankSign-IV	1030	67.8	28.2

Table 2: Millions of cycles reference implementation for different instances of RankSign.

2.2 Optimized Implementation

No optimized implementation has been realized. Therefore, the folder ../Optimized_Implementation/ is a copy of ../Reference_Implementation/.

3 Known Answer Test Values

KATs are provided in the folder ../KATS/Reference_Implementation/. As mentioned in Sec. 2.2, since the reference and optimized implementations are identical, ../KATS/Optimized_Implementation/ is just a copy of ../KATS/Reference_Implementation/.

KATs have been generated using the script provided by NIST. They are available under the folder labeled KATs. Additionally, we provide a complete example with intermediate values in the KATs folder. This complete example corresponds to a successful run of Ranksign. By successful, we mean that no decryption error occurred in the Decapsulation step.

Notice that one can also generate other such detailed instances using the verbose mode of each implementation. For instance, use make ranksignI-verbose in ../Reference_Implementation/RankSign-I/, then run ./bin/ranksignI-verbose to get a complete detailed instance with intermediate values.

4 Security

The security analysis is done in two steps. First we recall the process of the security proof in the original RankSign paper [9]. In the second subsection, we show how to extend the proof to our modified version.

4.1 Analysis of the original RankSign

We use notation from the RankSign paper [9]. Our purpose is to study the resistance to leakage of information from signatures. In the original RanSign paper, it was argued that as long as the number of signatures does not significantly exceed q, whatever can be computed with these signatures can be computed with the same complexity without them, because

one can produce q simulated signatures that with a reasonable probability (e.g. 1/2) will be indistinguishable from the genuine signatures.

Let us summarize the main points of the proof. The actual signer produces a couple $(\boldsymbol{x}, \boldsymbol{y})$ where $\boldsymbol{y}$ is the syndrome of a vector $\boldsymbol{x}$ of rank r. This means that $\boldsymbol{y}$, a random hash, is randomly chosen among the set of T-decodable vectors of the syndrome space 1.11: this is achieved by randomly choosing $\boldsymbol{y}$ and discarding it whenever it is not T-decodable. There then corresponds to $\boldsymbol{y}$ a unique vector $\boldsymbol{x}$ of $\mathbb{F}_{q^m}^n$. The couple $(\boldsymbol{x}, \boldsymbol{y})$ was called a T-decodable couple, and in the same way the vector $\boldsymbol{x}$ can by extension also be called T-decodable since it uniquely determines $(\boldsymbol{x}, \boldsymbol{y})$. Now what the simulator does is produce a couple $(\boldsymbol{x}, \boldsymbol{y})$ by uniformly choosing $\boldsymbol{x}$ among rank-r vectors, hoping he produces a T-decodable couple. For $\boldsymbol{x}$ to be T-decodable, three conditions must be satisfied. The first two conditions (i) and (ii) relate only to the support E of the vector x. The third condition requires the syndrome coordinates to be independent modulo the subspace FT. Conditional on those conditions being met, the vector x produced by the simulator is naturally uniformly distributed among the set of vectors satisfying those conditions, and so is the genuine signature x, so that as long as the simulator does not choose a non-T-decodable x, the simulated couple (x, y) is indistinguishable from a genuine couple produced by the signer.

Let $\mathcal{E}$ be the set of $\mathbb{F}_q$-subspaces or dimension r of $\mathbb{F}_{q^m}$ and let X be the set of spaces E of $\mathcal{E}$ that do not satisfy the required conditions (i) and (ii). It was shown in appendix C of the RankSign paper [9] that the proportion of spaces of $\mathcal{E}$ that belong to X is bounded from above by a quantity approximately equal to $2/q$.

4.2 Indistinguishability proof of our scheme

We now turn to the modified RankSign scheme. In this scheme the signer simply produces a vector $\boldsymbol{x}$ of rank $r+t'$ rather than of rank r, so that it will be more difficult to distinguish a genuine signature from a simulated one. In concrete terms, given the hashed value $\boldsymbol{y}$ belonging to the syndrome space of the message, the signer chooses a random vector $\boldsymbol{v} \in \mathbb{F}_{q^m}^n$ of weight t', then applies the original RankSign decoding algorithm to the vector of the syndrome space equal to $\boldsymbol{y} - \sigma(\boldsymbol{v})$ where σ denotes the syndrome function. This produces a vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$, and the signature associated to $\boldsymbol{y}$ is now declared to be

$$\boldsymbol{x}' = \boldsymbol{x} + \boldsymbol{v}$$

which clearly has syndrome $\sigma(\boldsymbol{x}') = \boldsymbol{y}$ and has rank $r + t'$ with overwhelming probability.

The simulator, as before, chooses $\boldsymbol{x}'$ uniformly at random among vectors of weight $r+t'$. Our purpose is now to evaluate how this differs from the way the genuine signer produces $\boldsymbol{x}'$.

We focus on the two ways the support E' of the vector $\boldsymbol{x}'$ is chosen. When E' is chosen by the signer, E' belongs to the set $\mathcal{E}'$ of subspaces of $\mathbb{F}_{q^m}$ of rank $r + t'$ containing T, obtained by first selecting a subspace E belonging to the space $\mathcal{E}$ of subspaces of rank r containing T, and *that does not contain the forbidden set* X. Then E' is obtained by choosing a subspace of $\mathcal{E}'$ containing E. From now on to lighten the analysis on we drop

the condition "containing T" in the definition of $\mathcal{E}$ and $\mathcal{E}'$ since this merely amounts to replacing the ambient space $\mathbb{F}_{q^m}$ by the quotient $\mathbb{F}_{q^m}/T$. It follows readily from the analysis of the original RankSign scheme that the subspace E is chosen with uniform distribution in $\mathcal{E} \setminus X$. Then E' is obtained through a uniform choice of spaces that contain E. This defines a probability distribution P over $\mathcal{E}'$. In contrast, the simulator simply chooses E' by applying the uniform probability distribution P_u on $\mathcal{E}'$. The situation is best described through a graph: define the bipartite graph $\mathcal{G}$ to have as vertex set the subspaces of $\mathcal{E}$ and $\mathcal{E}'$ and by declaring a subspace E of $\mathcal{E}$ and a subspace E' of $\mathcal{E}'$ to have their corresponding vertices in $\mathcal{G}$ joined by an edge whenever the inclusion of subspaces $E \subset E'$ holds. The graph is illustrated on Figure 1.

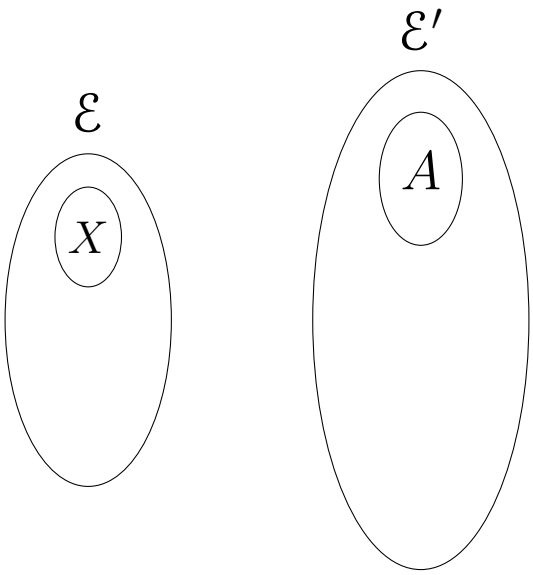


Figure 1: the inclusion incidence graph $\mathcal{G}$ between the set $\mathcal{E}$ of subspaces of rank r and the set $\mathcal{E}'$ of subspaces of rank $r+1$. It defines the probability distribution P of the support E of the signature vector $\boldsymbol{x}$ by avoiding the forbidden set X.

To recap, P is the probability measure on vertices of $\mathcal{E}'$ obtained by uniformly choosing a vertex from the complement $\overline{X}$ of X in $\mathcal{E}$ and by uniformly choosing an outgoing edge from it.

Theorem 4.1. *The number of samples necessary to significantly distinguish the distribution P from the uniform distribution P_u is at least $q^{1+t'}$.*

The demonstration of this theorem is given in section 7.

A corollary of this theorem is that an opponent cannot use the knowledge of genuine signatures to attack the cryptosystem. Indeed, any algorithm which takes as inputs the public key and N valid signatures can be simulated by an algorithm which takes as inputs the public key and N random vectors of weight r instead of the N signatures.

Corollary 4.2 (Unforgeability of signatures)**.** *As long as the number of given signatures is below* $q^{1+t'}$*, under the* Augmented LRPC indistinguishability *Problem 1.9, forging a signature is as hard as solving an instance of the RSD Problem 1.4 for a random code in the Random Oracle Model.*

The corollary implies we need to choose a large q for our parameters. In practice, we have $q = 2^{24}$ or $q = 2^{32}$. Thus, we only consider attacks on our signature scheme which only use the public key as input.

5 Known Attacks

There are two ways to attack our system, either the opponent can try to forge a signature by computing a vector of weight r of a given syndrome or he can try to recover the structure of the augmented LRPC code. To achieve this, he can search for a codeword of weight $d+t$ in the dual of the public code $\mathcal{C}$ or he can try to directly attack the masking matrix $\boldsymbol{Q}$.

There exist two types of generic attacks on these problems:

- the combinatorial attacks where the goal is to find the support of the error or of the codeword.
- the algebraic attacks where the opponent tries to solve an algebraic system by Groebner basis.

First, we deal with the combinatorial attacks, both in the forgery attacks case and structural attacks case and in a third subsection we discuss about the algebraic attacks.

5.1 Forgery attacks

The forgery attack consists to find a vector $\boldsymbol{e}$ of weight r such that $\boldsymbol{H}_{pub}\boldsymbol{e}^T = \boldsymbol{s}^T$. Under the assumption that the indistinguishability of the augmented LRPC code problem is hard, we can only use the best generic attack against the RSD problem. This attack can be found in [8].

The general idea is to found a subspace F which contains the support of $\boldsymbol{e}$ and to express each coordinates of $\boldsymbol{e}$ in a basis of F to obtained some unknowns over $\mathbb{F}_q$. Then we solve a linear system obtained from the parity-check equations and verified by these unknowns.

Let F be a subspace of $\mathbb{F}_{q^m}$ of dimension δ and $(F_1, \ldots, F_\delta)$ a basis of F. We will determine the value of δ later. Let $E = \text{Supp}(\boldsymbol{e})$. We assume that $E \subset F$.

$$\Rightarrow \forall i \in [1..n+t], e_i = \sum_{j=1}^{\delta} \lambda_{ij} F_j$$

This gives us $(n+t)\delta$ unknowns over $\mathbb{F}_q$ and we have:

$$\begin{aligned}
&\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s} && (1)\\
\Leftrightarrow &\begin{cases} H_{1,1}e_1 & +\cdots+ & H_{1,n+t}e_{n+t} & = & s_1 \\ \vdots & & \vdots & & \vdots \\ H_{n-k,1}e_1 & +\cdots+ & H_{n-k,n+t}e_{n+t} & = & s_{n-k} \end{cases} \\
\Leftrightarrow &\begin{cases} \sum_{j=1}^{\delta}(\lambda_{1j}H_{1,1}F_j & +\cdots+ & \lambda_{n+t,j}H_{1,n+t}F_j) & = & s_1 \\ \vdots & & \vdots & & \vdots \\ \sum_{j=1}^{\delta}(\lambda_{1j}H_{n-k,1}F_j & +\cdots+ & \lambda_{n+t,j}H_{n-k,n+t}F_j) & = & s_{n-k} \end{cases} && (2)
\end{aligned}$$

Let φ_i the i^{th} canonical projection from $\mathbb{F}_{q^m}$ on $\mathbb{F}_q$:

$$\begin{aligned} \varphi_i : \quad \mathbb{F}_{q^m} &\to \mathbb{F}_q \\ \sum_{i=1}^{m} x_i\beta_i &\mapsto x_i \end{aligned}$$

We apply these functions to the n equations of (2) to obtain

$$\begin{aligned}
&\boldsymbol{H}\boldsymbol{e}^T = \boldsymbol{s} \\
&\Leftrightarrow \forall i \in [1..m], \\
&\begin{cases} \sum_{j=1}^{\delta}\left(\lambda_{1j}\varphi_i(H_{11}F_j) & +\cdots+ & \lambda_{n+t,j}\varphi_i(H_{1,n+t}F_j)\right) & = & \varphi_i(c_1) \\ \vdots & & \vdots & & \vdots \\ \sum_{j=1}^{\delta}\left(\lambda_{1j}\varphi_i(H_{n-k,1}F_j) & +\cdots+ & \lambda_{n+t,j}\varphi_i(H_{n-k,n+t}F_j)\right) & = & \varphi_i(c_n) \end{cases} && (3)
\end{aligned}$$

Since we assume $E \subset F$, this system has at least one solution. We want $(n-k)m \geqslant (n+t)\delta$ to have more equations than unknowns $\implies \delta \leqslant \left\lfloor \frac{(n-k)m}{n+t} \right\rfloor = m - \left\lceil \frac{(k+t)m}{n+t} \right\rceil$. To check this assumption, we have to try and solve the system, that's why the complexity of this attack is $\mathcal{O}\left(\frac{(n-k)^3m^3}{p}\right)$ where p is the probability that $E \subset F$.
p is equal to the number of subspaces of dimension r in a subspace of dimension δ divided by the total number of subspaces of dimension r in $\mathbb{F}_{q^m}$.

$$p = \frac{\begin{bmatrix}\delta \\ r\end{bmatrix}_q}{\begin{bmatrix}m \\ r\end{bmatrix}_q} \approx q^{-w(m-\delta)}$$

By taking $delta = m - \left\lceil \frac{(k+t)m}{n+t} \right\rceil$ we obtain a complexity of $\mathcal{O}\left((n-k)^3m^3q^{r\left\lceil \frac{(k+t)m}{n+t} \right\rceil}\right)$

Since r is larger than the RGV bound for this code, there are several solutions to the RSD problem. We need to divide this complexity by the mean number of solutions,

which is equal to the number of words of weight r divided by the number of syndromes, so $\frac{S(q,m,n+t,r)}{q^{m(n-k)}} \approx q^{(m+n+t-r)r-m(n-k)}$.

Eventually the complexity of the attack is

$$\mathcal{O}\left((n-k)^3 m^3 q^{r\left\lceil \frac{(k+t)m}{n+t}\right\rceil - r(m+n+t-r)+m(n-k)}\right).$$

5.2 Structural attacks against augmented LRPC codes

Let $\mathcal{C}$ be an $[n+t, k+t]_{q^m}$ augmented LRPC code of parity-check matrix under its systematic form $\boldsymbol{H}_{pub} = \boldsymbol{P}(\boldsymbol{R}|\boldsymbol{H})\boldsymbol{Q}$, where $\boldsymbol{H}$ is an homogeneous matrix of support F of weight d.. The problem is to find the structure of $\mathcal{C}$ with only the knowledge of $\boldsymbol{H}_{pub}$. There are two way to attack this problem.

The first one is to search for a word $\boldsymbol{e}$ of weight $d+t$ in the dual code $\mathcal{C}^\perp$ of generator matrix $\boldsymbol{H}_{pub}$. This attack is very similar to the attack of the previous section, we suppose that a fixed subspace F of dimension $r = m - \left\lceil \frac{(n-k)m}{n+t} \right\rceil$ contains the support $E = \mathrm{Supp}(\boldsymbol{e})$ then we try and solve the system 3. The complexity of this attack is $\mathcal{O}\left((k+t)^3 m^3 q^{(d+t)\left\lceil \frac{(n-k)m}{n+t}\right\rceil}\right)$.

We can improve the complexity of this attack by using an amelioration found in [3]. This amelioration uses the fact that $\mathcal{C}^\perp$ is $\mathbb{F}_{q^m}$-linear, so if $\boldsymbol{e}$ is of weight $d+t$, any multiple $\alpha\boldsymbol{e}, \alpha \in \mathbb{F}_{q^m}^*$ is also of weight $d+t$. So we need to compute the probability p' such that $F \subset \alpha E$, for any $\alpha \in \mathbb{F}_{q^m}^*$. By counting the number of different subspace of the form αE, we obtain

$$p' \approx \frac{q^m - 1}{q-1} \frac{\begin{bmatrix} r \\ d+t \end{bmatrix}_q}{\begin{bmatrix} m \\ d+t \end{bmatrix}_q} \approx q^{-(d+t)(m-r)+m-1}$$

Finally the complexity of this attack is

$$\mathcal{O}\left((k+t)^3 m^3 q^{(d+t)\left\lceil \frac{(n-k)m}{n+t}\right\rceil - m}\right)$$

Another way is to try and guess the action of the matrix $\boldsymbol{Q}$ on the code generated by $(\boldsymbol{R}|\boldsymbol{H})$. This approach has been studied in the original RankSign article [9]. We do not need to guess the whole matrix $\boldsymbol{Q}$ but only $(n-k+l)$ columns nut only the action of $\boldsymbol{Q}$ on $n-k+l$ columns of $\boldsymbol{H}$ coming from the t columns of $\boldsymbol{R}$. Then we can search for a codeword of weight d in the code of type $[n-k+l, n-k]$, which will very likely reveal the support F if its RGV bound is larger than d. In practice, since we have d very small, we only need $l = d+1$. The complexity of this attack is at least $\mathcal{O}\left(q^{t(n-k+d+1)}\right)$.

All these combinatorial attack can be easily countered by increasing the size of q. Since we already need to take q of the order of 2^{24} or 2^32 to achieve the unforgeability of the signature 4.1, all these attacks are irrelevant to define the security parameter of our scheme.

5.3 Algebraic attacks

The second way to solve the equations of the system (3) is to use the Groebner basis [12]. The advantage of these attacks is that they are independent of the size of q. They mainly depend on the number of unknowns with respect to the number of equations.

Let e be a codeword of $\mathcal{C}^{\perp}$ of weight $d+t$ and of support E. Let Gv be a parity-check matrix of $\mathcal{C}^{\perp}$. Let $(E_1, \ldots, E_{d+t}$ be a basis of E. Then

$$\forall i \in 1..n+t, e_i = \sum_{j=1}^{d+t} \lambda_{ij} E_j$$

By projecting the equations of parity over $\mathbb{F}_q$ we obtain the following quadratic system

$$\begin{cases} \sum_{i=1}^{n+t} \sum_{j=1}^{d+t} \lambda_{ij} \varphi_l(G_{1i} E_j) & = & 0 \\ \vdots & & \vdots \\ \sum_{i=1}^{n+t} \sum_{j=1}^{d+t} \lambda_{ij} \varphi_l(G_{n-k,i} E_j) & = & 0 \end{cases}$$

for all $l \in \{1..m\}$. The unknowns are the λ_{ij} and the $\varphi_l(G_{1i}E_j)$, so there are $(d+t)(n+t+m)$ unknowns for $(n_k)m$ equations. It is possible to reduce the number of unknowns by $(d+t)^2$ by considering a basis of E under its systematic form. This system is also bihomogeneous, which decreases the computation cost of a Groebner basis. To estimate the complexity of this attack, we have used the results of [4] and we have chosen our parameters according to these estimations.

6 Advantages and Limitations

Our signature scheme has small parameters and is relatively fast. Since we need to take a large q, all the known combinatorial attacks are inefficient to break our cryptosystem. Thus the best attacks against it are based on the computation of a Groebner basis. In our security estimation, we do not take into account the spatial complexity of these algorithms, moreover, up to our best knowledge, there is currently no quantum speed-up for these algorithms, that is why we expect our parameters to be rather conservative.

However, our signature algorithm may seem quite complex at first sight, but the underneath ideas are simple and relatively similar to the approach in lattice-based signature, like GPV signature [11]. The parameters have to be chosen carefully in order to respect the algorithm's constraints. Furthermore, the study of the use of rank metric in cryptography are quite new [6] but the difficult problem in rank metric have been deeply studied, so we are confident that our parameters are resilient.

7 Proof of the theorem 4.1

Proof Method. We will consider every event $A \subset \mathcal{E}'$ and compare $P(A)$ with $P_u(A)$: we

use the fact that to distinguish the Bernoulli variables with parameters p and $p-\varepsilon$ one needs at least p/ε^2 samples. To evaluate $P(A)$ we will need an estimate of the number of edges that go from A to X in the graph $\mathcal{G}$. To obtain this estimate we invoke an auxiliary graph $\mathcal{G}_r$ on the vertex set $\mathcal{E}$, for which two vertices are incident if and only if they have a common neighbour in the graph $\mathcal{G}$. In other words, two subspaces of rank r are connected in $\mathcal{G}_r$ if they are included in a common subspace of rank $r+1$. The graph $\mathcal{G}_r$ is sometimes called a *Grassmann graph* and is an extensively studied distance-regular graph [5]. In particular we will call upon the following result:

Lemma 7.1. *The ratio λ/Δ, where Δ is the degree of the Grassmann graph $\mathcal{G}_r$ and λ is the second largest eigenvalue of it adjacency matrix is a quantity close to $1/q$.*

We also recall:

Lemma 7.2 (Alon-Chung [1])**.** *Let G be a graph of regular degree Δ and with n vertices. Let λ be the second largest eigenvalue of its adjacency matrix. Let S be a subset of vertices of G. Then the number of edges of the subgraph induced by S is at most*

$$\frac{1}{2}\left(\Delta\frac{|S|^2}{n}+\lambda|S|\left(1-\frac{|S|}{n}\right)\right).$$

Sketch of proof of Theorem 4.1: Let A be a subset of vertices of $\mathcal{E}'$. Disregarding small multiplicative constants we have

$$|X|=\frac{1}{q}|\mathcal{E}|$$

and let us write

$$|A|=\frac{\alpha}{q}|\mathcal{E}'|.$$

We denote by Δ_L and Δ_R the left and right degrees respectively of the $(\mathcal{E},\mathcal{E}')$ bipartite graph.

The expected average degree from A to X, which corresponds to $P(A)$ being equal to the uniform probability $P_u(A)$ of A, is:

$$\frac{|X|}{|\mathcal{E}|}\Delta_R=\frac{1}{q}\Delta_R.$$

Accordingly, the corresponding average degree from A to $\overline{X}$ is:

$$\frac{|\overline{X}|}{|\mathcal{E}|}\Delta_R=\left(1-\frac{1}{q}\right)\Delta_R.$$

Case 1. Suppose $P(A)>P_u(A)$, meaning A receives more than the expected number of edges from $\overline{X}$. Now the total number of edges incident to A is $|A|\Delta_R$, so the total number

of edges from $\overline{X}$ to A can only go from $(1-1/q)\Delta_R|A|$ to $\Delta_R|A|$, i.e. is multiplied by at most $(1-1/q)^{-1} = q/(q-1) = 1+1/(q-1)$. Therefore

$$P(A) \leq \left(1+\frac{1}{q-1}\right) P_u(A) \leq P_u(A) + \frac{1}{q-1} P_u(A).$$

Hence, to distinguish P from P_u with the event A we need

$$\frac{P_u(A)}{(\frac{1}{q-1}P_u(A))^2} = \frac{(q-1)^2}{P_u(A)} \quad \text{samples.}$$

Case 2. We now suppose $P(A) < P_u(A)$, meaning A receives fewer than the expected number of edges from $\overline{X}$, in other words more than expected from X. This case needs a more refined analysis.

In the expected case, a fraction α/q of Grassmann edges in X come from A. If the average degree from A to X is multiplied by β, then the number of Grassman edges inside A is multiplied by at least β^2. By the Alon-Chung Lemma (Lemma 7.2), since $\lambda/\Delta = 1/q$ in the Grassmann graph (Lemma 7.1), we must have

$$\beta^2 \frac{\alpha}{q} \leq 2$$

otherwise the number of edges in the Grassmann subgraph induced by X more than doubles the expected value, hence

$$\beta \leq \sqrt{\frac{2q}{\alpha}}.$$

Therefore the average degree from A to $\overline{X}$ goes from

$$\left(1-\frac{1}{q}\right)\Delta_R \quad \text{to at least} \quad \Delta_R\left(1-\frac{\beta}{q}\right) = \Delta_R\left(1-\sqrt{\frac{2}{\alpha q}}\right)$$

which implies that

$$P(A) \geq P_u(A)\left(1-\sqrt{\frac{2}{\alpha q}}\right)\left(1-\frac{1}{q}\right)^{-1}.$$

Going over all possible values of α, this is enough to ensure that for all A, at least q^2 samples are needed to distinguish P from P_u. □

We conclude the analysis with a remark concerning condition (iii). In the original RankSign scheme, the simulated signature vector $\boldsymbol{x}$ could, with probability of order $1/q$, produce a syndrome vector $\boldsymbol{y}$ whose coordinates are not necessarily linearly independent modulo FT, while this never happens with the genuine syndrome vector $\boldsymbol{y}$. This is because the simulated syndrome coordinates all fall in the prescribed space FE. In the modified RankSign variant, the simulated syndrome coordinates fall into a space FE' of larger dimension, and the probability of the appearance of an undesired linear equation is at most

$1/q^3$, which is a quantity which does not interfere when we are dealing with q^2 signature samples.

The second remark concerns what happens to the analysis when we allow the signature vector $\boldsymbol{x}$ to have rank $r+2$ rather than $r+1$. The key observation is that we will be dealing with the bipartite graph $(\mathcal{E}, \mathcal{E}'')$ where $\mathcal{E}''$ denotes the set of spaces of rank $r+2$, and the Grassmann graph $\mathcal{G}_r$ will need to be replaced by its second power $\mathcal{G}_r^2$, meaning we put an edge between two vertices of $\mathcal{G}_r^2$ when they are at distance 2 in $\mathcal{G}_r$. Since they eigenvalues of $\mathcal{G}_r^2$ are essentially the squares of those of $\mathcal{G}_r$, we get that the quantity λ/Δ crucial to the study of $P(A)$ changes from $1/q$ to $1/q^2$. When a similar analysis to that of the proof of Theorem 4.1 is carried out we obtain that the number of samples needed to distinguish P from uniform goes from q^2 to q^3. We omit the details. They will be available in [2].

References

[1] Noga Alon and Fan RK Chung. Explicit construction of linear sized tolerant networks. *Annals of Discrete Mathematics*, 38:15–19, 1988. *19*

[2] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, Oliver Ruatta, and Gilles Zémor. Improvement for the ranksign signature scheme. Available on `www.unilim.fr/pages_perso/philippe.gaborit/newRankSign.pdf`. *21*

[3] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. Improvement of Generic Attacks on the Rank Syndrome Decoding Problem. working paper or preprint, October 2017. *17*

[4] Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009. *18*

[5] AE Brouwer, AM Cohen, and A Neumaier. Distance-regular graphs. b.; heidelberg. 1989. *19*

[6] 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. *18*

[7] 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`. *6*, *7*

[8] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *CoRR*, abs/1301.1026, 2013. *15*

[9] Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor. Ranksign: An efficient signature algorithm based on the rank metric (extended version on arxiv). In *Post-Quantum Cryptography 2014*, volume 8772 of *LNCS*, pages 88–107. Springer, 2014. 4, 7, 8, 10, 12, 13, 17

[10] 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. 5

[11] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008. 4, 18

[12] Françoise Lévy-dit Vehel and Ludovic Perret. Algebraic decoding of codes in rank metric. In *proceedings of YACC06*, Porquerolles, France, June 2006. available on `http://grim.univ-tln.fr/YACC06/abstracts-yacc06.pdf`. 18

A Signed statements by the submitters

NIST requires statements about the intellectual property of the present submission. While NIST clearly mentioned they require the original paper version of these statements, the authors estimated useful to include a digital copy of these statements in this document. The paper version of these statements will be provided directly to Dustin Moody (or any other NIST member) at the first PQC Standardization Conference.

The remainder of this submission consists of statements. Below is a list of the statements included.

Statement by each submitter. Each of the authors has such a statement included.

Statement by patent owners. No patent are involved.

Statement by reference/optimized implementations' owners. Each of the authors has such a statement included.

I, Nicolas Aragon, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign;* ***OR*** *(check one or both of the following):*

☐ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, may be covered by the following U.S. and/or foreign patents: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190;*

☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

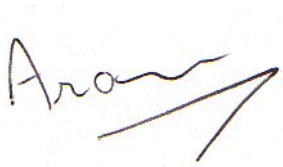
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Nicolas Aragon



Title: PhD Student
Date: November 28, 2017
Place: Limoges

I, Philippe Gaborit, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign;* ***OR*** *(check one or both of the following):*

☐ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, may be covered by the following U.S. and/or foreign patents: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190;*

☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: P. Gaborit.

Title: Professor
Date: November 28, 2017
Place: Limoges

I, Adrien Hauteville, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign;* ***OR*** *(check one or both of the following):*

☐ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, may be covered by the following U.S. and/or foreign patents: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190;*

☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

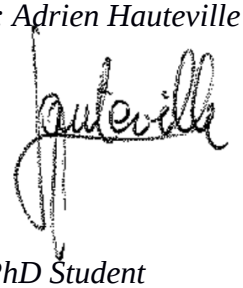
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Adrien Hauteville



Title: PhD Student
Date: November 28, 2017
Place: Limoges

I, Olivier Ruatta, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign;* ***OR*** *(check one or both of the following):*

☐ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, may be covered by the following U.S. and/or foreign patents: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190;*

☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Olivier Ruatta

Title: Associate Professor
Date: November 28, 2017
Place: Limoges

I, Gilles Zémor, of IMB, University of Bordeaux, 351 cours de la Libération, F-33405 Talence Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign; OR (check one or both of the following):

☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RankSign, may be covered by the following U.S. and/or foreign patents: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190;

☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190.*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances

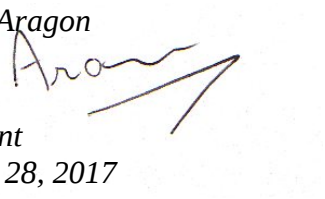
made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Gilles Zémor

Title: Professor
Date: November 28, 2017
Place: Bordeaux

I, Nicolas Aragon, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

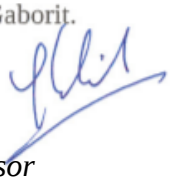
Signed: Nicolas Aragon



Title: PhD Student
Date: November 28, 2017
Place: Limoges

I, Philippe Gaborit, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: P. Gaborit.



Title: Professor
Date: November 28, 2017
Place: Limoges

I, Adrien Hauteville, University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Adrien Hauteville

Title: Ph.D. Student
Date: November 28, 2017
Place: Limoges

I, Olivier Ruatta, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Olivier Ruatta

Title: Associate Professor
Date: November 28, 2017
Place: Limoges

I, Gilles Zémor, of IMB, University of Bordeaux, 351 cours de la Libération, F-33405 Talence Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Gilles Zémor

Title: Professor
Date: November 28, 2017
Place: Bordeaux