



**HAL**  
open science

## LAKE

Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit,  
Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor

► **To cite this version:**

Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, et al.. LAKE: Low rAnk parity check codes Key Exchange. 2017. hal-04317561

**HAL Id: hal-04317561**

**<https://inria.hal.science/hal-04317561>**

Submitted on 1 Dec 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# LAKE

– Low rAnk parity check codes Key Exchange –

November 30, 2017

*LAKE is an IND-CPA KEM running for standardization to NIST's competition in the category "post-quantum key exchange". Different sets of parameters are proposed for security strength categories 1, 3, and 5.*

## Principal Submitters (by alphabetical order):

- Nicolas ARAGON
- Olivier BLAZY
- Jean-Christophe DENEUVILLE
- Philippe GABORIT
- Adrien HAUTEVILLE
- Olivier RUATTA
- Jean-Pierre TILlich
- Gilles ZÉMOR

**Inventors:** Same as submitters

**Developers:** Same as submitters

**Owners:** Same as submitters

## Main contact

✉ Philippe GABORIT  
@ [philippe.gaborit@unilim.fr](mailto: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](mailto: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.

# Contents

<b>1</b>	<b>Specifications</b>	<b>3</b>
1.1	Presentation of rank metric codes . . . . .	3
1.1.1	General definitions . . . . .	3
1.1.2	Double circulant and ideal codes . . . . .	4
1.2	Difficult problems in rank metric . . . . .	6
1.3	The Low Rank Parity Check codes . . . . .	7
1.3.1	Definition . . . . .	7
1.4	A support recovery algorithm . . . . .	8
1.4.1	Algorithm . . . . .	9
1.4.2	Probability of failure . . . . .	9
1.5	LAKE an IND-CPA KEM based on rank metric . . . . .	10
1.5.1	KEM: definition and security model . . . . .	10
1.5.2	Description of the scheme . . . . .	11
1.6	Parameters . . . . .	12
<b>2</b>	<b>Performance Analysis</b>	<b>13</b>
2.1	Reference Implementation . . . . .	14
2.2	Optimized Implementation . . . . .	14
<b>3</b>	<b>Known Answer Test Values</b>	<b>14</b>
<b>4</b>	<b>Security</b>	<b>15</b>
<b>5</b>	<b>Known Attacks</b>	<b>15</b>
5.1	Generic attacks . . . . .	16
5.2	Structural attack against ideal LRPC codes . . . . .	18
5.3	Algebraic attacks . . . . .	18
<b>6</b>	<b>Advantages and Limitations</b>	<b>19</b>
6.1	Advantages . . . . .	19
6.2	Limitations . . . . .	19
<b>A</b>	<b>Signed statements by the submitters</b>	<b>20</b>

## Prologue

The public key encryption protocol NTRU [9] was introduced in 1998, the main idea behind the protocol is that the secret key consists in the knowledge of a small Euclidean weight vector, which is used to derive a double circulant matrix. This matrix is then seen as a dual matrix of an associated lattice and a specific decoding algorithm based on the knowledge of this small weight dual matrix is used as decryption.

This idea of having as a trapdoor, the knowledge of a small weight dual matrix (with a specific associated decoding algorithm) can naturally be generalized to other metrics. It was done in 2013 with MDPC [11] for Hamming metric and also in 2013 for Rank metric with LRPC codes [4]. These three protocols derive from the same basic main idea, adapted for different metrics, which have different properties in terms of efficiency, size of parameters and security reduction.

In this proposal we build on a small variation of the LRPC rank metric approach, by introducing Ideal-LRPC codes, and propose an IND-CPA Key Encapsulation Mechanism (KEM) for Key Exchange, efficient in terms of size of parameters and computational complexity which benefits from the nice properties of rank metric. The scheme has a failure probability but this probability is well understood and can be made very low.

# 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  $\mathbf{A}, \mathbf{B}$  of compatible dimensions, we let  $(\mathbf{A}|\mathbf{B})$  and  $\begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix}$  respectively denote the horizontal and vertical concatenations of  $\mathbf{A}$  and  $\mathbf{B}$ .

## 1.1 Presentation of rank metric codes

### 1.1.1 General definitions

**Definition 1.1** (Rank metric over  $\mathbb{F}_{q^m}^n$ ). *Let  $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$  and  $(\beta_1, \dots, \beta_m) \in \mathbb{F}_{q^m}^m$  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  $\mathbf{x}$  is given by  $\mathbf{M}(\mathbf{x}) = (m_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ .*

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

$$\|\mathbf{x}\| \stackrel{\text{def}}{=} \text{Rank } \mathbf{M}(\mathbf{x}).$$

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

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

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

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

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

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

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

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

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

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

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

### 1.1.2 Double circulant and ideal codes

To describe an  $[n, k]_{q^m}$  linear code, we can give its systematic generator matrix or its systematic parity-check matrix. In both case, the number of bits needed to represent such a matrix is  $k(n-k)m \lceil \log_2 q \rceil$ . To reduce the size of a representation of a code, we introduce the double circulant codes.

First we need to define the circulant matrices.

**Definition 1.4** (Circulant matrix). *A square matrix  $\mathbf{M}$  of size  $n \times n$  is said circulant if it is of the form*

$$\mathbf{M} = \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ m_{n-1} & m_0 & \ddots & m_{n-2} \\ \vdots & \ddots & \ddots & \vdots \\ m_1 & m_2 & \dots & m_0 \end{pmatrix}$$

We denote  $\mathcal{M}_n(\mathbb{F}_{q^m})$  the set of circulant matrices of size  $n \times n$  over  $\mathbb{F}_{q^m}$ .

The following proposition states an important property of circulant matrices.

**Proposition 1.5.**  *$\mathcal{M}_n(\mathbb{F}_{q^m})$  is an  $\mathbb{F}_{q^m}$ -algebra isomorphic to  $\mathbb{F}_{q^m}[X]/(X^n - 1)$ , that-is-to-say the set of polynomials with coefficients in  $\mathbb{F}_{q^m}$  modulo  $X^n - 1$ . The canonical isomorphism is given by*

$$\begin{aligned} \varphi : \mathbb{F}_{q^m}[X]/(X^n - 1) &\longrightarrow \mathcal{M}_n(\mathbb{F}_{q^m}) \\ \sum_{i=0}^{n-1} m_i X^i &\longmapsto \begin{pmatrix} m_0 & m_1 & \dots & m_{n-1} \\ m_{n-1} & m_0 & \ddots & m_{n-2} \\ \vdots & \ddots & \ddots & \vdots \\ m_1 & m_2 & \dots & m_0 \end{pmatrix} \end{aligned}$$

In the following, in order to simplify the notation, we will identify the polynomial  $G(X) = \sum_{i=0}^{n-1} g_i X^i \in \mathbb{F}_{q^m}[X]$  with the vector  $\mathbf{g} = (g_0, \dots, g_{n-1}) \in \mathbb{F}_{q^m}^n$ . We will denote  $\mathbf{u}\mathbf{g} \pmod P$  the vector of the coefficients of the polynomial  $\left(\sum_{j=0}^{n-1} u_j X^j\right) \left(\sum_{i=0}^{n-1} g_i X^i\right) \pmod P$  or simply  $\mathbf{u}\mathbf{g}$  if there is no ambiguity in the choice of the polynomial  $P$ .

**Definition 1.6** (Double circulant codes). *An  $[2n, n]_{q^m}$  linear code  $\mathcal{C}$  is said double circulant if it has a generator matrix  $\mathbf{G}$  of the form  $\mathbf{G} = (\mathbf{A}|\mathbf{B})$  where  $\mathbf{A}$  and  $\mathbf{B}$  are two circulant matrices of size  $n$ .*

With the previous notations, we have  $\mathcal{C} = \{(\mathbf{x}\mathbf{a}, \mathbf{x}\mathbf{b}), \mathbf{x} \in \mathbb{F}_{q^m}^n\}$ . If  $\mathbf{a}$  is invertible in  $\mathbb{F}_{q^m}[X]/(X^n - 1)$ , then  $\mathcal{C} = \{(\mathbf{x}, \mathbf{x}\mathbf{g}), \mathbf{x} \in \mathbb{F}_{q^m}^n\}$  where  $\mathbf{g} = \mathbf{a}^{-1}\mathbf{b}$ . In this case we say that  $\mathcal{C}$  is generated by  $\mathbf{g} \pmod{X^n - 1}$ . Thus we only need  $nm \lceil \log_2 q \rceil$  bits to describe an  $[2n, n]_{q^m}$  double circulant code.

We can generalize the double circulant codes by choosing another polynomial  $P$  to define the quotient-ring  $\mathbb{F}_{q^m}[X]/(P)$ .

**Definition 1.7** (Ideal codes). *Let  $P(X) \in \mathbb{F}_q[X]$  be a polynomial of degree  $n$  and  $\mathbf{g}_1, \mathbf{g}_2 \in \mathbb{F}_{q^m}^n$ . Let  $G_1(X) = \sum_{i=0}^{n-1} g_{1i} X^i$  and  $G_2(X) = \sum_{j=0}^{n-1} g_{2j} X^j$  the polynomials associated respectively to  $\mathbf{g}_1$  and  $\mathbf{g}_2$ .*

By definition, the  $[2n, n]_{q^m}$  ideal code  $\mathcal{C}$  of generator  $(\mathbf{g}_1, \mathbf{g}_2)$  is the code with generator matrix

$$\mathbf{G} = \left( \begin{array}{c|c} G_1(X) \bmod P & G_2(X) \bmod P \\ XG_1(X) \bmod P & XG_2(X) \bmod P \\ \vdots & \vdots \\ X^{n-1}G_1(X) \bmod P & X^{n-1}G_2(X) \bmod P \end{array} \right)$$

More concisely, we have  $\mathcal{C} = \{(\mathbf{x}\mathbf{g}_1 \bmod P, \mathbf{x}\mathbf{g}_2 \bmod P), \mathbf{x} \in \mathbb{F}_{q^m}^n\}$ . We will often omit to precise the polynomial  $P$  if there is no ambiguity.

If  $\mathbf{g}_1$  is invertible, under systematic form,  $\mathcal{C} = \{(\mathbf{x}, \mathbf{x}\mathbf{g}), \mathbf{x} \in \mathbb{F}_{q^m}^n\}$  with  $\mathbf{g} = \mathbf{g}_1^{-1}\mathbf{g}_2 \bmod P$ .

## Relation between polynomial and matrix forms for the syndrome computation

We need to be careful when we use these notations in the case of parity-check matrix. Indeed, if we have a syndrome  $\boldsymbol{\sigma} = \mathbf{e}_1\mathbf{h}_1 + \mathbf{e}_2\mathbf{h}_2 \bmod P$ , this equality is equivalent in term of product matrix-vector to  $(\mathbf{H}_1|\mathbf{H}_2)(\mathbf{e}_1|\mathbf{e}_2)^T = \boldsymbol{\sigma}^T$  where

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{h}_1 \bmod P \\ X\mathbf{h}_1 \bmod P \\ \vdots \\ X^{n-1}\mathbf{h}_1 \bmod P \end{pmatrix}^T \quad \text{and} \quad \mathbf{H}_2 = \begin{pmatrix} \mathbf{h}_2 \bmod P \\ X\mathbf{h}_2 \bmod P \\ \vdots \\ X^{n-1}\mathbf{h}_2 \bmod P \end{pmatrix}^T$$

Thus, we said that  $(\mathbf{h}_1, \mathbf{h}_2)$  and  $P$  generate a parity-check matrix of a code  $\mathcal{C}$  if  $(\mathbf{H}_1^T|\mathbf{H}_2^T)$  is a parity-check matrix of  $\mathcal{C}$ .

## 1.2 Difficult problems in rank metric

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

**Problem 1.8** (Rank Syndrome Decoding). *Given a full-rank matrix  $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$ , a syndrome  $\boldsymbol{\sigma}$  and a weight  $\omega$ , it is hard to sample a vector  $\mathbf{x} \in \mathbb{F}_{q^m}^n$  of weight lower than  $\omega$  such that  $\mathbf{H}\mathbf{x}^T = \boldsymbol{\sigma}^T$ .*

The RSD problem has recently been proven hard in [6] on probabilistic reduction.

**Problem 1.9** (Ideal-Rank Syndrome Decoding). *Given a vector  $\mathbf{h} \in \mathbb{F}_{q^m}^n$ , a polynomial  $P \in \mathbb{F}_q[X]$  of degree  $n$ , a syndrome  $\boldsymbol{\sigma}$  and a weight  $\omega$ , it is hard to sample a vector  $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2) \in \mathbb{F}_{q^m}^{2n}$  of weight lower than  $\omega$  such that  $\mathbf{x}_1 + \mathbf{x}_2\mathbf{h} = \boldsymbol{\sigma} \bmod P$ .*

Since  $\mathbf{h}$  and  $P$  define a systematic parity-check matrix of an  $[2n, n]_{q^m}$  ideal code, the I – RSD problem is a particular case of the RSD problem.

**Problem 1.10** (Ideal-Rank Support Recovery). *Given a vector  $\mathbf{h} \in \mathbb{F}_{q^m}^n$ , a polynomial  $P \in \mathbb{F}_q[X]$  of degree  $n$ , a syndrome  $\boldsymbol{\sigma}$  and a weight  $\omega$ , it is hard to recover the support  $E$  of dimension lower than  $\omega$  such that  $\mathbf{e}_1 + \mathbf{e}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{P}$  where the vectors  $\mathbf{e}_1$  and  $\mathbf{e}_2$  were sampled from  $E$ .*

The I – RSR problem is trivially reduced to the I – RSD problem. Indeed to recover the support  $E$  of an instance of the I – RSD problem from a solution  $\mathbf{x}$  of the I – RSD problem, we just have to compute the support of  $\mathbf{x}$ .

Reciprocally, the I – RSD problem can also be reduced to the I – RSR problem. Let us suppose we know the support  $E$  of a solution of the I – RSR problem for a weight  $\omega$ . We want to find  $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2)$  of weight lower than  $\omega$  such that  $\mathbf{x}_1 + \mathbf{x}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{P}$ .

This equation is equivalent to

$$\left( \begin{array}{c|c} \mathbf{I}_n & \mathbf{H} \end{array} \right) (x_{10} \dots x_{1,n-1}, x_{20} \dots x_{2,n-1})^T = \boldsymbol{\sigma}^T \quad (1)$$

where  $\mathbf{H} = \begin{pmatrix} \mathbf{h} \\ X\mathbf{h} \pmod{P} \\ \vdots \\ X^{n-1}\mathbf{h} \pmod{P} \end{pmatrix}^T$  and  $\mathbf{x}_1 = (x_{10} \dots x_{1,n-1})$ ,  $\mathbf{x}_2 = (x_{20} \dots x_{2,n-1})$ .

Let  $(E_1, \dots, E_\omega)$  be a basis of  $E$ . We can express the coordinates of  $\mathbf{x}_1$  and  $\mathbf{x}_2$  in this basis:

$$\forall i \in \{1, 2\}, 0 \leq j \leq n-1, x_{ij} = \sum_{k=1}^{\omega} \lambda_{ijk} E_k, \text{ with } \lambda_{ijk} \in \mathbb{F}_q$$

Then we rewrite the equations [1](#) in the new unknowns  $\lambda_{ijk}$ . We obtain a system of  $2n\omega$  unknowns over  $\mathbb{F}_q$  and  $n$  equations over  $\mathbb{F}_{q^m}$ , so  $nm$  equations over  $\mathbb{F}_q$ .

Since  $\mathbf{e}_1 + \mathbf{e}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{P}$ , the system has at least one solution and by construction all the solutions have their support included in  $E$  of dimension  $\omega$ , so we can find a solution the I – RSD problem by solving this system.

Even if there is no reduction proof as for the generic RSD problem, the ideal (and quasi-cyclic double circulant) versions of the RSD problem are considered hard. The situation is similar to Hamming and Euclidean metrics for double circulant codes, for which there is known strong improvement on the attack complexity whenever one avoids weak keys, typically choosing a polynomial  $P$  with many small factors: in our case  $P$  is chosen irreducible. The complexity of known attacks against these problems are described in [Section 5](#).

## 1.3 The Low Rank Parity Check codes

### 1.3.1 Definition

The LRPC codes have been introduced in [\[4\]](#). They are good candidates for the cryptosystem of McEliece because they have a weak algebraic structure.



**Definition 1.11** (LRPC codes). Let  $\mathbf{H} = (h_{ij})_{\substack{1 \leq i \leq n-k \\ 1 \leq j \leq n}} \in \mathbb{F}_{q^m}^{(n-k) \times n}$  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  $\mathbf{H}$ . By definition,  $\mathcal{C}$  is an  $[n, k]_{q^m}$  LRPC code of weight  $d$ .

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

We can now define the ideal LRPC codes as we have defined the ideal codes.

**Definition 1.12** (Ideal LRPC codes). Let  $F$  be a  $\mathbb{F}_q$ -subspace of dimension  $d$  of  $\mathbb{F}_{q^m}$ ,  $(\mathbf{h}_1, \mathbf{h}_2)$  two vectors of  $\mathbb{F}_{q^m}^n$  of support  $F$  and  $P \in \mathbb{F}_q[X]$  a polynomial of degree  $n$ . Let

$$\mathbf{H}_1 = \begin{pmatrix} \mathbf{h}_1 \\ X\mathbf{h}_1 \bmod P \\ \vdots \\ X^{n-1}\mathbf{h}_1 \bmod P \end{pmatrix}^T \quad \text{and} \quad \mathbf{H}_2 = \begin{pmatrix} \mathbf{y} \\ X\mathbf{h}_2 \bmod P \\ \vdots \\ X^{n-1}\mathbf{h}_2 \bmod P \end{pmatrix}^T$$

By definition, the code  $\mathcal{C}$  with parity check matrix  $\mathbf{H} = (\mathbf{H}_1 | \mathbf{H}_2)$  is an ideal LRPC code of type  $[2n, n]_{q^m}$ .

As we can see, since  $P \in \mathbb{F}_q[X]$ , the support of  $X^i \mathbf{h}_1$  is still  $F$  for all  $1 \leq i \leq n-1$  hence the necessity to choose  $P$  with coefficients in the base field  $\mathbb{F}_q$  to keep the LRPC structure of the ideal code.

To hide the structure of an ideal LRPC, we only reveal its systematic parity-check matrix.

**Definition 1.13** (Ideal LRPC codes indistinguishability). Given a polynomial  $P \in \mathbb{F}_q[X]$  of degree  $n$  and a vector  $\mathbf{h} \in \mathbb{F}_{q^m}^n$ , it is hard to distinguish whether the ideal code  $\mathcal{C}$  with the parity-check matrix generated by  $\mathbf{h}$  and  $P$  is a random ideal code or if it is an ideal LRPC code of weight  $d$ .

In other words, it is hard to distinguish if  $\mathbf{h}$  was sampled uniformly at random or as  $\mathbf{x}^{-1} \mathbf{y} \bmod P$  where the vectors  $\mathbf{x}$  and  $\mathbf{y}$  have the same support of small dimension  $d$ .

The ideal LRPC codes are particularly interesting if we choose an irreducible polynomial for  $P$ . In this case we counter a structural attack against double circulant LRPC which can be found in [7].

## 1.4 A support recovery algorithm

The decoding algorithm of LRPC codes first recover the support of the error vector then solve a linear system in order to recover the error coordinates. For our protocol LAKE we only need to recover the support of the error. The probabilistic support recovery algorithm was recently improved in [2]. The algorithm we present here, uses both the general decoding algorithm of the LRPC codes described in [4] and a tweak of the improved algorithm described in [2] designed to run in constant time.

**Notation 1.14.** In the following,  $S$  is the vector space generated by the coordinates of the syndrome  $\langle s_1, \dots, s_n \rangle$ . Its dimension is at most  $rd$ , and it is a subspace of the product vector space  $E.F = \langle E_1.F_1, E_2.F_1, \dots, E_r.F_d \rangle$ .  $S_i$  is defined by  $S_i = F_i^{-1}.S$  with  $F_i$  an element of a basis of  $F$ , and  $S_{ij} = S_i \cap S_j$ .

### 1.4.1 Algorithm

---

**Algorithm 1:** Rank Support Recover algorithm (RS-Recover)

---

**Data:**  $F = \langle F_1, \dots, F_d \rangle$ ,  $s = (s_1, \dots, s_n)$  (a vector),  $r$  (the dimension of  $E$ )  
**Result:** A candidate for the vector space  $E$   
//Part 1 :     Compute the vector space  $E.F$   
1 Compute  $S = \langle s_1, \dots, s_n \rangle$   
2 Precompute every  $S_i$  for  $i = 1$  to  $d$   
3 Precompute every  $S_{i,i+1}$  for  $i = 1$  to  $d - 1$   
4 **for**  $i$  from 1 to  $d - 2$  **do**  
5      $tmp \leftarrow S + F.(S_{i,i+1} \oplus S_{i+1,i+2} \oplus S_{i,i+2})$   
6     **if**  $\dim(tmp) \leq rd$  **then**  
7          $S \leftarrow S \cup tmp$   
8     **end**  
9 **end**  
//Part 2 :     Recover the vector space  $E$   
10  $E \leftarrow F_1^{-1}.S \cap \dots \cap F_d^{-1}.S$   
11 **return**  $E$

---

The algorithm is designed in two parts : the first one is used to recover the whole vector space  $E.F$  in case  $S$  is of dimension  $< rd$ . This ensures that the second part, which is the general decoding of the LRPC codes, outputs the right  $E$ . Note that we don't need to recover the coordinates of the error vector  $e$  since we only use the support  $E$  in the protocol.

### 1.4.2 Probability of failure

The second part of the algorithm will fail if and only if  $S \neq E.F$ , thus the global probability of failure depends both from the probability of  $\dim(S)$  being smaller than  $rd$  and the probability of not recovering  $E.F$  using the first part of the algorithm.

**Notation 1.15.** In the following,  $c$  is the codimension of  $S$  inside  $E.F$  :  $\dim(S) = rd - c$ .  $P(c = i)$  is the probability of  $S$  being of codimension  $i$  inside  $E.F$  and  $P_{c=i}(\text{failure})$  if the probability of not recovering  $E.F$  when  $c = i$ .

**Proposition 1.16.** The probability of failure of the new algorithm is  $\sum_{i=1}^{rd-1} P(c = i) \times P_{c=i}(\text{failure})$

**Analysis of  $P_{c=1}(\text{failure})$**

This algorithm uses the fact that  $\dim(S_i \cap E) \geq r - c$  ( $r - 1$  in this case), which means each  $S_i$  contains at least  $r - 1$  vectors of  $E$ . Since all other vectors in  $S_i$  are random, we need to intersect two different  $S_i$  in order to recover  $r - 2$  vectors of  $E$ : those are the  $S_{ij}$ .

At each iteration, we compute  $S_{i,i+1} \oplus S_{i+1,i+2} \oplus S_{i,i+2}$  to find vectors of  $E$ . Once we have those, we multiply them by the vector space  $F$  to find vectors of  $S$ . If one of these vectors (we note it  $x$ ) is not in  $S$ , then  $S + x = E.F$ : we can decode successfully.

We know that every  $S_{ij}$  contains at least  $r - 2$  vectors of  $E$ . To study what happens during each iteration of the algorithm, we suppose that  $S_{ij}$  contains exactly  $r - 2$  vectors of  $E$ . Two cases may occur during each of the  $d - 2$  iterations:

- If  $S_{i,i+1} = S_{i+1,i+2}$ , then  $\dim(S_{i,i+1} \oplus S_{i+1,i+2} \oplus S_{i,i+2}) = r - 2$ , since the equality implies that each vector that we find is in  $S_i$ ,  $S_{i+1}$  and  $S_{i+2}$  at the same time. In that case the algorithm might not find new vectors of  $E.F$ . This equality happens with probability  $q^{2-r}$ .
- $S_{i,i+1} \neq S_{i+1,i+2}$ , then  $\dim(S_{i,i+1} \oplus S_{i+1,i+2} \oplus S_{i,i+2}) = r$ : the inequality implies that  $\dim(S_{i,i+1} \oplus S_{i+1,i+2}) = r - 1$  and, since  $S_{i,i+2}$  is different from both of the other  $S_{ij}$  (otherwise we would be in the first case), the union of the three  $S_{ij}$  is exactly  $E$ . In that case the algorithm always finds  $E.F$ .

Since each iteration can fail to recover  $E.F$  with probability  $q^{2-r}$ , the probability of not finding  $E.F$  when  $\dim(S) = rd - 1$  is  $q^{(2-r)(d-2)}$ .

**Proposition 1.17.** *From [4] we know that  $P(c = i) = q^{-i(n-rd+i)}$  thus the probability of failure of this algorithm is  $\max(q^{(2-r)(d-2)} \times q^{-(n-rd+1)}, q^{-2(n-rd+2)})$ .*

In practice, this algorithm can decode event when  $c > 1$ , but  $P_{c=2}(\text{failure})$  is harder to study. Notice that the algorithm supposes that  $m$  is sufficiently higher than  $2rd - r$  to work, which is the case for all parameters considered.

## 1.5 LAKE an IND-CPA KEM based on rank metric

### 1.5.1 KEM: definition and security model

A Key-Encapsulation scheme  $\text{KEM} = (\text{KeyGen}, \text{Encap}, \text{Decap})$  is a triple of probabilistic algorithms together with a key space  $\mathcal{K}$ . The key generation algorithm  $\text{KeyGen}$  generates a pair of public and secret key  $(\text{pk}, \text{sk})$ . The encapsulation algorithm  $\text{Encap}$  uses the public key  $\text{pk}$  to produce an encapsulation  $c$ , and a key  $K \in \mathcal{K}$ . Finally  $\text{Decap}$  using the secret key  $\text{sk}$  and an encapsulation  $c$ , recovers the key  $K \in \mathcal{K}$  or fails and return  $\perp$ .

We define IND-CPA-security of KEM formally via the following experiment, where  $\text{Encap}_0$  returns a valid key pair  $c^*, K^*$ , while  $\text{Encap}_1$  return a valid  $c^*$  and a random  $K^*$ .

*Indistinguishability under Chosen Plaintext Attack:* This notion states that an adversary should not be able to efficiently guess which key is encapsulated.

**Exp** $_{\mathcal{E},\mathcal{A}}^{\text{ind-}b}(\lambda)$

1. param  $\leftarrow$  Setup( $1^\lambda$ )
2. (pk, sk)  $\leftarrow$  KeyGen(param)
3. ( $c^*$ ,  $K^*$ )  $\leftarrow$  Encap $_b$ (pk)
4.  $b' \leftarrow \mathcal{A}(\text{GUESS} : c^*, K^*)$
5. RETURN  $b'$

**Definition 1.18** (IND-CPA Security). *A key encapsulation scheme KEM is IND-CPA-secure if for all PPT adversary  $\mathcal{A}$ ,  $\text{Adv}_{\text{KEM}}^{\text{indcpa}}(\mathcal{A}) := |\Pr[\text{IND-CPA}_{\text{real}}^{\mathcal{A}} \Rightarrow 1] - \Pr[\text{IND-CPA}_{\text{rand}}^{\mathcal{A}} \Rightarrow 1]|$  is negligible.*

### 1.5.2 Description of the scheme

Our scheme contains a hash function  $G$  modeled as a ROM.

- KeyGen( $1^\lambda$ ):
  - choose an irreducible polynomial  $P \in \mathbb{F}_q[X]$  of degree  $n$ .
  - choose uniformly at random a subspace  $F$  of  $\mathbb{F}_{q^m}$  of dimension  $d$  and sample a couple of vectors  $(\mathbf{x}, \mathbf{y}) \xleftarrow{\$} F^n \times F^n$  such that  $\mathbf{x}$  is invertible mod  $P$ ,  $\text{Supp}(\mathbf{x}, \mathbf{y}) = F$ .
  - compute  $\mathbf{h} = \mathbf{x}^{-1}\mathbf{y} \pmod P$ .
  - define pk =  $(\mathbf{h}, P)$  and sk =  $(\mathbf{x}, \mathbf{y})$ .
- Encap(pk):
  - choose uniformly at random a subspace  $E$  of  $\mathbb{F}_{q^m}$  of dimension  $r$  and sample a couple of vectors  $(\mathbf{e}_1, \mathbf{e}_2) \xleftarrow{\$} E^n \times E^n$  with  $\text{Supp}(\mathbf{e}_1, \mathbf{e}_2) = E$ .
  - compute  $\mathbf{c} = \mathbf{e}_1 + \mathbf{e}_2\mathbf{h} \pmod P$ .
  - define  $K = G(E)$  and return  $\mathbf{c}$ .
- Decap(sk):
  - compute  $\mathbf{x}\mathbf{c} = \mathbf{x}\mathbf{e}_1 + \mathbf{y}\mathbf{e}_2 \pmod P$  and recover  $E$  with the support recovery algorithm of previous section.
  - recover  $K = G(E)$ .

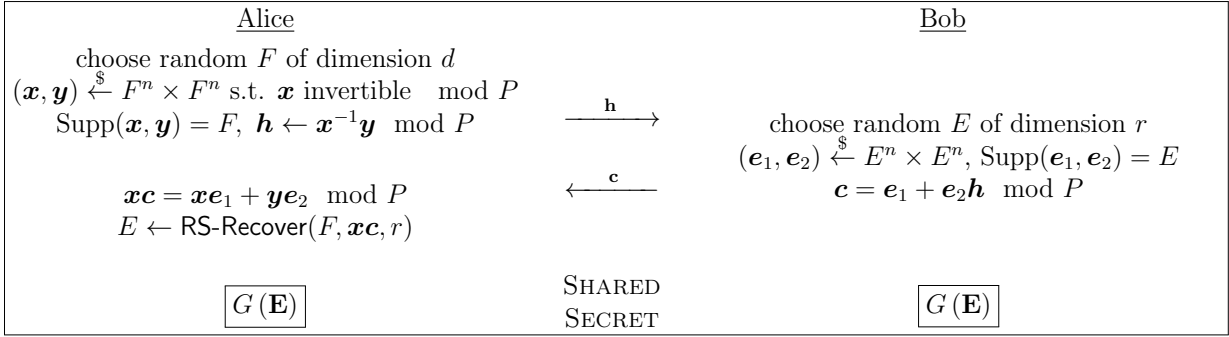


Figure 1: Description of LAKE key exchange protocol.

We need to have a common representation of a subspace of dimension  $r$  of  $\mathbb{F}_{q^m}$ . The natural way is to choose the unique matrix  $\mathbf{M} \in \mathbb{F}_q^{r \times m}$  of size  $r \times m$  in its rows echelon form such that the rows of  $\mathbf{M}$  are a basis of  $E$ .

We deal with the semantic security of the KEM in Section 4.

**Correctness:** since  $P$  is in  $\mathbb{F}_q[X]$ ,  $\mathbf{xc}$  has a support in the product space  $\langle E, F \rangle$ . Hence knowing  $F$ , one can apply the RS-Recover algorithm of the previous section which recovers  $E$ . □

**Computational costs.** The Encapcost corresponds to a polynomial inversion mod  $P$  in  $\mathbb{F}_{q^m}$ , for a multiplication cost of elements of  $\mathbb{F}_{q^m}$  in  $m \log(m) \log(\log(m))$ , we obtain an encryption complexity in  $\mathcal{O}(n^2 \log(n) m \log(m) \log(\log(m)))$ . The Decapcost is a matrix-vector multiplication of cost  $\mathcal{O}(n^2 m \log(m) \log(\log(m)))$  plus the decoding cost of the RS-Recover algorithm (intersections of subspaces of dimension  $rd$  in  $\mathbb{F}_{q^m}$ ) in  $\mathcal{O}((rd)^2 m)$ .

## 1.6 Parameters

In this section, we give some sets of parameters for a security parameters of 128, 192 and 256 corresponding to NIST security levels 1, 3 and 5 respectively. In all cases, we have chosen  $q = 2$ . The parameters are :

- $n$  is the length the vectors  $\mathbf{h}$  and  $\mathbf{c}$  sent on the public channel.
- $m$  is the degree of the extension  $\mathbb{F}_{2^m}$ .
- $d$  is the weight of the ideal LRPC code used in the protocol.
- $r$  is the weight of the error.
- $P$  is the irreducible polynomial of degree  $n$  of  $\mathbb{F}_2[X]$  which defines the ideal LRPC code. We have chosen sparse polynomials in order to diminish the computation costs.
- the structural attack parameter is the logarithm in basis 2 of the complexity of the best attack to recover the structure of the ideal LRPC code. It consists in looking for

a codeword of weight  $d$  in an ideal LRPC of type  $[2n, n]_{2^m}$  defined by the parity-check matrix  $(\mathbf{I}_n | \mathbf{H})$  where

$$\mathbf{H} = \begin{pmatrix} \mathbf{h}(X) \bmod P & \\ X\mathbf{h}(X) \bmod P & \\ \vdots & \\ X^{n-1}\mathbf{h}(X) \bmod P & \end{pmatrix}$$

- the generic attack parameter is the logarithm in basis 2 of the complexity of the best attack to recover the support  $E$ . It consists in solving the I – RSD problem for a random ideal code of type  $[2n, n]_{2^m}$  and an error of weight  $r$ .
- $p_f$  is the probability of failure of the decoding algorithm. We have chosen the parameters such that the theoretic upper bound is below  $2^{-30}$ .
- the entropy parameter is the entropy of the subspace  $E$ . It is equal to  $\log_2 \left( \begin{bmatrix} m \\ w \end{bmatrix}_q \right)$  and have to be greater than the security parameter. We represent  $E$  by a matrix of size  $w \times m$  in its row echelon form.
- the public key size is the number of bits needed to represent the public key  $\mathbf{h} \in \mathbb{F}_{q^m}^n$ . It is equal to  $mn$ .

Name	LAKE I	LAKE II	LAKE III
Security	128	192	256
$n$	47	53	59
$m$	67	89	107
$d$	6	7	8
$r$	5	6	6
$P$	$X^{47} + X^5 + 1$	$X^{53} + X^6 + X^2 + X + 1$	$X^{59} + X^7 + X^4 + X^2 + 1$
Structural Attack	130	207	301
Generic Attack	146	221	258
$p_f$	$2^{-30}$	$2^{-32}$	$2^{-36}$
Entropy	311	499	607
Public key (bits)	3149	4717	6313

## 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 : `g++ -O2 -pedantic -Wall -Wextra -Wno-vla`.

## 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
LAKE-I	0.65	0.13	0.53
LAKE-II	0.73	0.13	0.88
LAKE-III	0.77	0.15	1.24

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

Instance	KeyGen	Encap	Decap
LAKE-I	1.58	0.30	1.27
LAKE-II	1.74	0.31	2.09
LAKE-III	1.79	0.35	2.89

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

## 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 LAKE. 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 lakeI-verbose` in `../Reference_Implementation/LAKE-I/`, then run `./bin/lakeI-verbose` to get a complete detailed instance with intermediate values.

## 4 Security

**Theorem 4.1.** *Under the Ideal LRPC indistinguishability 1.13 and the Ideal-Rank Syndrome Decoding 1.9 Problems, the KEM presented earlier in section 1.5.2 is indistinguishable against Chosen Plaintext Attack in the Random Oracle Model.*

*Proof.* We are going to proceed in a sequence of games. The simulator first starts from the real scheme. First we replace the public key matrix by a random element, and then we use the ROM to solve the Ideal-Rank Support Recovery.

- Game  $G_0$  is the regular scenario: We generate the public key  $\mathbf{h}$  honestly, and  $E, \mathbf{c}$  also.
- In game  $G_1$ , we now replace  $\mathbf{h}$  by a random vector, the rest is identical to the previous game. From an adversary point of view, the only difference is the distribution on  $\mathbf{h}$ , which is either generated at random, or as a product of low weight vectors. This is exactly the *Ideal LRPC indistinguishability* problem, hence

$$\text{Adv}_{\mathcal{A}}^{G_0} \leq \text{Adv}_{\mathcal{A}}^{G_1} + \text{Adv}_{\mathcal{A}}^{\text{I-LRPC}}$$

- In game  $G_2$ , we now proceed as earlier except we receive  $\mathbf{h}, \mathbf{c}$  from a Support Recovery challenger. After sending  $\mathbf{c}$  to the adversary, we monitor the adversary queries to the Random Oracle, and pick a random one that we forward as our simulator answer to the Ideal-Rank Support Recovery problem. Either the adversary was able to predict the random oracle output, or with probably  $1/q_G$ , we picked the query associated with the support  $E$  (by  $q_G$  we denote the number of queries to the random oracle  $G$ ), hence

$$\text{Adv}_{\mathcal{A}}^{G_1} \leq 2^{-\lambda} + 1/q_G \cdot \text{Adv}_{\mathcal{A}}^{\text{I-RSR}}.$$

Since we saw in Sec. 1.2 that the problems I – RSR and I – RSD were equivalent it leads to the conclusion.

□

## 5 Known Attacks

There are two ways to attack our system: either the opponent can try to recover the structure of the ideal LRPC code by searching a codeword of weight  $d$  in the ideal code generated by  $\mathbf{h}$ , or he can try to solve an instance of the I – RSR 1.10 problem of weight  $r$  for a random ideal code.

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 generic case and in the ideal LRPC case and in a third subsection we discuss about the algebraic attacks.

## 5.1 Generic attacks

In this section, we give the complexity of the best attack on the I – RSR 1.10 problem: the inputs are a vector  $\mathbf{h} \in \mathbb{F}_{q^m}^n$  which defines the systematic parity-check matrix of an  $[2n, n]_{q^m}$  ideal code  $\mathcal{C}$ , a syndrome  $\mathbf{c} = \mathbf{e}_1 + \mathbf{e}_2\mathbf{h} \pmod{P}$  and an integer  $r$  which is the dimension of the support  $E$  of  $\mathbf{e} = (\mathbf{e}_1, \mathbf{e}_2)$ . The goal is to find  $E$ .

This attack is an improvement of a previous attack described in [5], a detailed description of the attack can be found in [1]. For a better understanding, we first describe the first attack, then the new attack can easily be deduced from it. These attacks do not take account on the ideal structure of the code but in the current state-of-the-art, we do not know any generic combinatorial attack which uses this structure.

The first step is to compute a parity check matrix  $\mathbf{H}$  of size  $n \times 2n$  of  $\mathcal{C}$  from  $\mathbf{h}$  such that we have the system  $\mathbf{H}\mathbf{e}^T = \mathbf{c}^T$  of  $n$  equations over  $\mathbb{F}_{q^m}$ . This step is polynomial so its cost is negligible.

Let  $F$  be a subspace of  $\mathbb{F}_{q^m}$  of dimension  $t$  and  $(F_1, \dots, F_t)$  a basis of  $F$ . We will determine the value of  $t$  later. Let us assume that  $E \subset F$ .

$$\Rightarrow \forall i \in [1..2n], e_i = \sum_{j=1}^t \lambda_{ij} F_j$$

This gives us  $2nt$  unknowns over  $\mathbb{F}_q$  and we have:

$$\begin{aligned} \mathbf{H}\mathbf{e}^T &= \mathbf{c}^T & (2) \\ \Leftrightarrow \begin{cases} H_{1,1}e_1 + \dots + H_{1,2n}e_{2n} &= c_1 \\ \vdots & \vdots \\ H_{n,1}e_1 + \dots + H_{n,2n}e_{2n} &= c_n \end{cases} \\ \Leftrightarrow \begin{cases} \sum_{j=1}^t (\lambda_{1j}H_{1,1}F_j + \dots + \lambda_{2n,j}H_{1,2n}F_j) &= c_1 \\ \vdots & \vdots \\ \sum_{j=1}^t (\lambda_{1j}H_{n,1}F_j + \dots + \lambda_{2n,j}H_{n,2n}F_j) &= c_n \end{cases} & (3) \end{aligned}$$

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

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

We apply these functions to the  $n$  equations of (3) to obtain

$$\begin{aligned}
\mathbf{H}\mathbf{e}^T &= \mathbf{c}^T \\
\Leftrightarrow \forall i \in [1..m], \\
\left\{ \begin{array}{l} \sum_{j=1}^t (\lambda_{1j}\varphi_i(H_{1,1}F_j) + \dots + \lambda_{2n,j}\varphi_i(H_{1,2n}F_j)) = \varphi_i(c_1) \\ \vdots \\ \sum_{j=1}^t (\lambda_{1j}\varphi_i(H_{n,1}F_j) + \dots + \lambda_{2n,j}\varphi_i(H_{n,2n}F_j)) = \varphi_i(c_n) \end{array} \right. & \quad (4)
\end{aligned}$$

Since we assume  $E \subset F$ , this system has at least one solution. We want  $nm \geq 2nt$  to have more equations than unknowns  $\implies t \leq \lfloor \frac{m}{2} \rfloor$ . To check this assumption, we have to try and solve the system, that's why the complexity of this attack is  $\mathcal{O}\left(\frac{n^3 m^3}{p}\right)$  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  $t$  divided by the total number of subspaces of dimension  $r$  in  $\mathbb{F}_{q^m}$ .

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

By taking  $t = \lfloor \frac{m}{2} \rfloor$  we obtain a complexity of

$$\mathcal{O}\left(n^3 m^3 q^{r \lceil \frac{m}{2} \rceil}\right)$$

The new attack take account on the  $\mathbb{F}_{q^m}$ -linearity of the code  $\mathcal{C}$ . Let  $\mathbf{x}$  be any solution of the system  $\mathbf{H}\mathbf{e}^T = \mathbf{c}$  without consider its weight. Let  $\mathcal{C}' = \mathcal{C} + \mathbb{F}_{q^m}\mathbf{x}$  be the  $[2n, n+1]_{q^m}$  code generated by  $\mathcal{C}$  and  $\mathbf{x}$ . By construction,  $\mathbf{e} \in \mathcal{C}'$  and by  $\mathbb{F}_{q^m}$ -linearity any multiples  $\alpha\mathbf{e} \in \mathcal{C}'$ ,  $\alpha \in \mathbb{F}_{q^m}$ . If  $r$  is small, then with overwhelming probability, all the codewords of  $\mathcal{C}'$  of weight  $r$  are multiple of  $\mathbf{e}$ . If we know a codeword  $\mathbf{e}' = \alpha\mathbf{e}$  of weight  $r$  of  $\mathcal{C}'$ , we can recover  $\mathbf{e}$  then  $E$  by solving the equation  $\mathbf{H}\mathbf{e}' = \alpha\mathbf{c}$  of unknown  $\alpha \in \mathbb{F}_{q^m}$ .

The rest of the algorithm is the same as previously. We choose a subspace  $F'$  of dimension  $t'$  and assume that  $F'$  contains the support  $\alpha E$  of a codeword  $\alpha\mathbf{e}$ . There are at most  $\frac{q^m-1}{q-1}$  subspaces of this form, because  $\alpha E = \beta E$  if  $\alpha/\beta \in \mathbb{F}_q^*$  and this bound is reached if  $m$  is prime, which is always the case in the parameters we have proposed. Since we have  $\frac{q^m-1}{q-1} \begin{bmatrix} t' \\ r \end{bmatrix}_q \ll \begin{bmatrix} m \\ r \end{bmatrix}_q$ , we can approximate the probability  $p'$  that  $F' \supset \alpha E$  by the product of the probability that  $F' \supset E$  by the number of subspaces of the form  $\alpha E$

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

Then we express the coordinates of  $\alpha e$  in a basis of  $F'$ , which gives us  $2nt'$  unknowns over  $\mathbb{F}_q$ . Since  $\mathcal{C}'$  is an  $[2n, n+1]_{q^m}$  code, the parity-check equations give us  $m(n-1)$  equations over  $\mathbb{F}_q$ , so we need  $t' \leq \left\lfloor \frac{m(n-1)}{2n} \right\rfloor = m - \left\lceil \frac{m(n+1)}{2n} \right\rceil$  to solve the system. The complexity of the attack is

$$\mathcal{O}\left(\frac{(nm)^3}{p'}\right) = \mathcal{O}\left((nm)^3 q^{r \lceil \frac{m(n+1)}{2n} \rceil - m}\right)$$

and the gain is almost  $q^m$  with respect to the previous attack.

## 5.2 Structural attack against ideal LRPC codes

Let  $\mathcal{C}$  be an  $[2n, n]_{q^m}$  ideal LRPC code generated by the two polynomials  $(\mathbf{x}, \mathbf{y})$  of support  $F$  of dimension  $d$ . Let  $\mathbf{h} = \mathbf{x}^{-1}\mathbf{y}$  which generates the systematic parity-check matrix of  $\mathcal{C}$ . The problem is to recover the structure of  $\mathcal{C}$ , given only access to  $\mathbf{h}$ .

The most efficient known attack is to find a codeword of weight  $d$  in the dual code  $\mathcal{C}^\perp$  generated by  $\mathbf{h}$ . The algorithm described in the previous section is the best known algorithm to solve this problem. However its complexity is better in the case of the dual of an ideal LRPC code than in a random code with the same parameters.

Indeed, let  $\mathbf{H}$  be the matrix of size  $nn$  generated by  $(\mathbf{x}, \mathbf{y})$ . By definition,  $\mathbf{H}$  is a generator matrix of  $\mathcal{C}^\perp$ . Let  $(\mathbf{h}_i)_{1 \leq i \leq n}$  be the rows of  $\mathbf{H}$ . For all  $1 \leq i \leq n$ ,  $\text{Supp}(\mathbf{h}_i) = F \implies \mathcal{C}^\perp$  contains  $q^n$  codewords of the same support, so the complexity of the algorithm is divided by  $q^n$ . Thus, the complexity of the attack is

$$\mathcal{O}\left(n^3 m^3 q^{d \lceil \frac{m}{2} \rceil - m - n}\right)$$

There exists a specific attack on the ideal LRPC codes which can be found in [8]. In this article, the authors present an attack against double circulant LRPC codes but it can be adapted straightforwardly in the case of ideal LRPC codes. However, the crucial point of this attack is that the polynomial  $X^n - 1$  has always  $X - 1$  as divisor and may have many more factors depending on  $n$  and  $q$ . In the case of ideal LRPC codes, we can choose an irreducible polynomial  $P$  of degree  $n$  of  $\mathbb{F}_q[X]$  to generate the quotient-ring  $\mathbb{F}_q[X]/(P)$ , which completely negates this specific attack.

## 5.3 Algebraic attacks

The second way to solve the equations of the system (4) is to use the Groebner basis [10]. 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. However, in the case  $q = 2$  the number of unknowns is generally too high for that the algorithms by Groebner basis are more efficient than the combinatorial attacks. We have chosen our parameters such that the best attacks are combinatorial, the expected complexity of the algorithms by Groebner basis is based on the article [3].

## 6 Advantages and Limitations

### 6.1 Advantages

The proposed scheme is very efficient, both in terms of size of keys and computational complexity. The scheme also benefits from a constant time decoding algorithm. The choice of parameters is very versatile. There is a reduction to a well understood generic problem I – RSD, which is a natural generalization of Quasi-Cyclic RSD. This type of problem is the same type of problem which has been used for many years for Hamming and Euclidean distances.

### 6.2 Limitations

Rank metric has very nice features, the use of rank metric for cryptographic purposes is not very old (1991), it may be seen as a limitation, but still in recent years there has been a lot activities on understanding the inherent computational difficulty of the problem and it seems very hard to improve on the general complexity of the problem.

#### ACKNOWLEDGEMENT

Philippe Gaborit and Jean-Pierre Tillich thank the RISQ project for its support.

## References

- [1] 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. [16](#)
- [2] Nicolas Aragon, Philippe Gaborit, Olivier Ruatta, and Gilles Zémor. More on lrpc codes and their cryptographic applications, 2017. Pre-print, available at [https://www.unilim.fr/pages\\_perso/philippe.gaborit/newLRPC.pdf](https://www.unilim.fr/pages_perso/philippe.gaborit/newLRPC.pdf). [8](#)
- [3] 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](#)
- [4] 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](http://www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf). [3](#), [7](#), [8](#), [10](#)

- [5] 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. [16](#)
- [6] 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. [6](#)
- [7] Adrien Hauteville and Jean-Pierre Tillich. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem, 2015. [abs/1504.05431](#). [8](#)
- [8] Adrien Hauteville and Jean-Pierre Tillich. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT 2015*, pages 2747–2751, Hong Kong, China, June 2015. [18](#)
- [9] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *LNCS*, pages 267–288. Springer, 1998. [3](#)
- [10] 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](#)
- [11] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In *Proc. IEEE Int. Symposium Inf. Theory - ISIT*, pages 2069–2073, 2013. [3](#)

## 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 LOCKER, 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 LOCKER; **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 LOCKER, 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).*

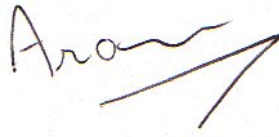
*I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment*

*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*

A handwritten signature in black ink, appearing to read 'Aragon', with a long, sweeping horizontal stroke underneath.

*Title: PhD Student*

*Date: November 28, 2017*

*Place: Limoges*

*I, Olivier Blazy, 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 LOCKER, 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 LOCKER; **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 LOCKER, 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 Blazy*

A handwritten signature in black ink, appearing to read 'Olivier Blazy', written over a light gray rectangular background.

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

*I, Jean-Christophe Deneuville, of INSA-CVL, 88 boulevard Lahitolle, 18000 Bourges, FRANCE, and 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 LOCKER, 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 LOCKER; **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 LOCKER, 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).*

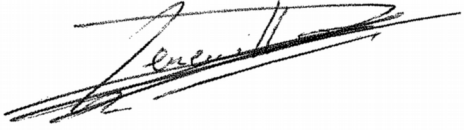
*I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment*

*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: Jean-ChristopheDeneuille*

A handwritten signature in black ink, appearing to read 'Deneuille', is written over a light gray rectangular background. The signature is stylized and somewhat obscured by several horizontal lines drawn across it.

*Title: PhD, post-doc*

*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 LOCKER, 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 LOCKER; **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 LOCKER, 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.*

A handwritten signature in blue ink, appearing to read 'P. Gaborit', with a long horizontal flourish extending to the right.

*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 LOCKER, 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 LOCKER; **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 LOCKER, 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*

A handwritten signature in black ink, appearing to read 'Hauteville', written in a cursive style.

*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 LOCKER, 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 LOCKER; **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 LOCKER, 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*

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

*Title: Associate Professor*

*Date: November 28, 2017*

*Place: Limoges*

I, Jean-Pierre Tillich, of INRIA Rocquencourt, B.P. 105 78153 Le Chesnay Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LOCKER, 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 LOCKER; **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 LOCKER, 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: Jean-Pierre Tillich*

A handwritten signature in black ink, appearing to read 'J. Tillich', with a stylized flourish extending from the bottom left.

*Title: Research Director, Professor*

*Date: November 28, 2017*

*Place: Paris*

*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 LAKE, 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 LAKE; 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 LAKE, 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*

A handwritten signature in black ink, consisting of a large, stylized 'G' followed by 'Zémor' in a cursive script.

*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*

A handwritten signature in black ink, appearing to read 'Aragon', with a long, sweeping horizontal stroke extending to the right.

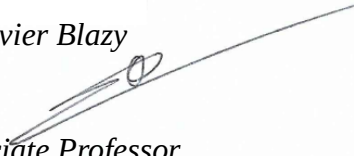
*Title: PhD Student*

*Date: November 28, 2017*

*Place: Limoges*

*I, Olivier Blazy, 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 Blazy*

A handwritten signature in black ink, appearing to read 'Olivier Blazy', is written over a light gray rectangular background.

*Title: Associate Professor*

*Date: November 28, 2017*

*Place: Limoges*

*I, Jean-Christophe Deneuville, of INSA-CVL Bourges, 88 boulevard Lahitolle, 18000 Bourges, FRANCE, and 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: Jean-Christophe Deneuville*

A handwritten signature in black ink, appearing to read 'Deneuville', written over a light blue horizontal line.

*Title: Ph.D. post-doc*

*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*

A handwritten signature in black ink, appearing to read 'Hauteville', with a stylized flourish at the end.

*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.*

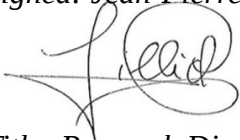
*Signed: Olivier Ruatta*

A handwritten signature in black ink, appearing to be 'Olivier Ruatta', with a long horizontal line extending to the right.

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

*I, Jean-Pierre Tillich, of INRIA Rocquencourt, B.P. 105 78153 Le Chesnay 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: Jean-Pierre Tillich*

A handwritten signature in black ink, appearing to read 'J. Tillich', with a stylized flourish extending from the bottom left.

*Title: Research Director, Professor*

*Date: November 28, 2017*

*Place: Paris*

*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*

A handwritten signature in black ink, consisting of a large, stylized 'G' followed by 'Zémor' in a cursive script.

*Title: Professor*

*Date: November 28, 2017*

*Place: Bordeaux*