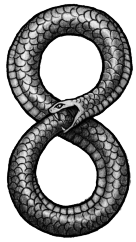
Ouroboros-R

November 30, 2017



Ouroboros-R 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):

- Carlos Aguilar Melchor
- Nicolas Aragon
- Slim Bettaieb
- Loïc Bidoux
- Olivier Blazy
- Jean-Christophe Deneuville
- Philippe Gaborit
- Adrien Hauteville
- 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

Jean-Christophe Deneuville
jch.deneuville@gmail.com
+33-631-142-705
INSA-CVL Bourges &
University of Limoges
4 rue Jean le Bail
87 000 Limoges
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

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 for decryption.

This idea of having as a trapdoor 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 [5]. 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.

The previous schemes have many nice features in terms of size of keys, size of exchanged data and efficiency but suffer from the same weakness: their security do not reduce to a well known problem but rather to a specific problem where a special structure is hidden in the public matrix. Indeed the public matrix is generated by small weight vectors. Although this problem is less specific that hidden structure in the McEliece setting, it remains a potential weakness for these schemes (even if practically, one does not really know how to use this type of structure for strongly more efficient attacks in the more general cases).

Recently a new approach called Ouroboros was presented in [1], this approach permits to benefit from the nice features of the previous schemes, but at the same time has a reduction to decoding random quasi-cyclic codes, rather than a more specific code. Of course this comes at a cost: doubling the size of the ciphertext. This proposal follows the idea of [1] for rank metric. The resulting scheme benefits from the nice features of NTRU-like schemes but has also a reduction to a generic problem, at the cost of doubling the size of the ciphertext, also as all associated decoding algorithm for the NTRU-like family of schemes, there is a decryption failure, but in the case of rank metric this decryption failure is low and perfectly estimated.

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 (resp. uppercase) letters to denote vectors (resp. matrices). As it will be clear from the context, no distinction will be made between column and row vectors. For two matrices $\mathbf{A}, \mathbf{B}$ of compatible dimensions, we let $(\mathbf{A}|\mathbf{B})$ and $\left(\frac{\mathbf{A}}{\mathbf{B}}\right)$ 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 1.1.1 (Rank metric over $\mathbb{F}_{q^m}^n$)**.** *Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ 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 $\mathbf{x}$ is given by $\mathbf{M}(\mathbf{x}) = (m_{ij})_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$.*

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

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

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 1.1.2 ($\mathbb{F}_{q^m}$-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 row 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 row 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 1.1.3 (Support of a word)**.** *Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$. The support E of $\mathbf{x}$, denoted $\operatorname{Supp}(\mathbf{x})$, is the $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}$ generated by the coordinates of $\mathbf{x}$:*

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

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

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

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 1.1.1. $\mathcal{M}_n(\mathbb{F}_{q^m})$ *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*

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

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

Definition 1.1.5 (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 $\mathcal{C}=\{(\mathbf{xa},\mathbf{xb}),\mathbf{x}\in\mathbb{F}_{q^m}^n\}$. If $\mathbf{a}$ is invertible in $\mathbb{F}_{q^m}[X]/(X^n-1)$, then $\mathcal{C}=\{(\mathbf{x},\mathbf{xg}),\mathbf{x}\in\mathbb{F}_{q^m}^n\}$ 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.

1.2 Difficult problems in rank metric

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

Problem 1.1 (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* ω*, it is hard to sample a vector* $\mathbf{x} \in \mathbb{F}_{q^m}^n$ *of weight lower than* ω *such that* $\mathbf{H}\mathbf{x}^T = \boldsymbol{\sigma}^T$*.*

The RSD problem has recently been proven hard in [7] on probabilistic reduction.

Problem 1.2 (Quasi-Cyclic Rank Syndrome Decoding)**.** *Given a vector* $\mathbf{h} \in \mathbb{F}_{q^m}^n$*, a syndrome* $\boldsymbol{\sigma}$ *and a weight* ω*, 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* ω *such that* $\mathbf{x}_1 + \mathbf{x}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{X^n - 1}$*.*

Since $\mathbf{h}$ and $P = X^n - 1$ define a systematic parity-check matrix of an $[2n, n]_{q^m}$ double circulant (quasi-cyclic) code, the QCRSD problem is a particular case of the RSD problem.

Problem 1.3 (Quasi-Cyclic Rank Support Recovery)**.** *Given a vector* $\mathbf{h} \in \mathbb{F}_{q^m}^n$*, a syndrome* $\boldsymbol{\sigma}$ *and a weight* ω*, it is hard to recover the support* E *of dimension lower than* ω *such that* $\mathbf{e}_1 + \mathbf{e}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{X^n - 1}$ *where the vectors* $\mathbf{e}_1$ *and* $\mathbf{e}_2$ *were sampled from* E*.*

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

Reciprocally, the QCRSD problem can also be reduced to the QCRSR problem. Let us suppose we know the support E of a solution of the QCRSR problem for a weight ω. We want to find $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2)$ of weight lower than ω such that $\mathbf{x}_1 + \mathbf{x}_2\mathbf{h} = \boldsymbol{\sigma} \pmod{X^n - 1}$.

This equation is equivalent to

$$\left(\begin{array}{c|c} \mathbf{I}_n & \mathbf{H} \end{array}\right) (x_{1,0} \dots x_{1,n-1}, x_{2,0} \dots x_{2,n-1})^T = \boldsymbol{\sigma}^T \tag{2}$$

where $\mathbf{H} = \begin{pmatrix} \mathbf{h} \\ X\mathbf{h} \pmod{X^n - 1} \\ \vdots \\ X^{n-1}\mathbf{h} \pmod{X^n - 1} \end{pmatrix}^T$ and $\mathbf{x}_1 = (x_{1,0} \dots x_{1,n-1}), \mathbf{x}_2 = (x_{2,0} \dots x_{2,n-1})$.

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:

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

Then we rewrite the equations of (2) in the new unknowns λ_{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 $\mathbf{e}_1 + \mathbf{e}_2\mathbf{h} = \boldsymbol{\sigma} \mod P$, the system has at least one solution and by construction all the solutions have their support included in E of dimension ω, so we can find a solution

to the QCRSD problem by solving this system.

The complexity of known attacks against these problems are described in Section 5.

1.3 A support recovery algorithm

Notation 1.4. *In the following, S is the vector space generated by the coordinates of the syndrome $\langle s_1, ..., s_n \rangle$. Its dimension is at most rd, and it is a subspace of the product vector space $E.F = \langle E_1.F_1, E_2.F_1, ..., E_r.F_d \rangle$. S_i is defined by $S_i = F_i^{-1}.S$ with F_i an element of a basis of F, and $S_{ij} = S_i \cap S_j$.*

1.3.1 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 Ouroboros-R we only need to recover the support of the error. The probabilistic support recovery algorithm was recently improved in [3]. The algorithm we present here, uses both the general decoding algorithm of the LRPC codes described in [5] and a tweak of the improved algorithm described in [3] designed to run in constant time. This algorithm is an improved version of the the general decoding algorithm of the LRPC codes described in [5].

Algorithm 1: QCRS-Recover algorithm

Data: $F = \langle F_1, ..., F_d \rangle$, $\mathbf{s} = (s_1, \cdots, s_n)$ (a vector), r (the dimension of E)
Result: A candidate for the vector space E
`//Part 1 :  Compute the vector space` $E.F$
Compute $S = \langle s_1, \cdots, s_n \rangle$
Precompute every S_i for $i = 1$ to d
Precompute every $S_{i,i+1}$ for $i = 1$ to $d - 1$
for i *from* 1 *to* $d - 2$ **do**
    $tmp \leftarrow S + F.(S_{i,i+1} \oplus S_{i+1,i+2} \oplus S_{i,i+2})$
    if $dim(tmp) \leqslant rd$ **then**
        $S \leftarrow tmp$
    end
end
`//Part 2 :  Recover the vector space` E
$E \leftarrow F_1^{-1}.S \cap ... \cap F_d^{-1}.S$
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.

1.3.2 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 1.5. *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 $P_{c=i}(failure)$ if the probability of not recovering $E.F$ when $c = i$.*

Proposition 1.6. *The probability of failure of the new algorithm is* $\sum_{i=1}^{rd-1} P(c = i) \times P_{c=i}(failure)$

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

This algorithm uses the fact that $\dim(S_i \cap E) >= r - c$ ($r - 1$ 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 $\mathbf{x}$) is not in S, then $S + \mathbf{x} = E.F$: 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 1.7. *From [5] 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 $P_{c=2}(failure)$ is harder to study. Notice that the algorithm supposes that m is sufficiently higher than $2rd - r$ to work, which will be the case for all parameters considered.

1.4 Presentation of Ouroboros-R as a KEM

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

Ouroboros-R is depicted in fig. 1, then formally described in fig. 2. The algorithm QCRS-recover was presented in previous section. In the description, $\mathcal{S}_w^n(\mathbb{F}_{q^m})$ stands for a random vector of length n and rank weight w over $\mathbb{F}_{q^m}$ and $\mathcal{S}_{1,w}^n(\mathbb{F}_{q^m})$ stands for a random vector of length n of rank weight w, *such that its support contains* 1 (choose a random subspace of dimension w of $\mathbb{F}_{q^m}$ containing 1, then consider random coordinates in this support).

We now present Ouroboros-R, the IND-CPA KEM we propose, both informally in Fig. 1 and formally in Fig. 2 (recall that Supp is the support of a vector, see Def. 1.1.3).

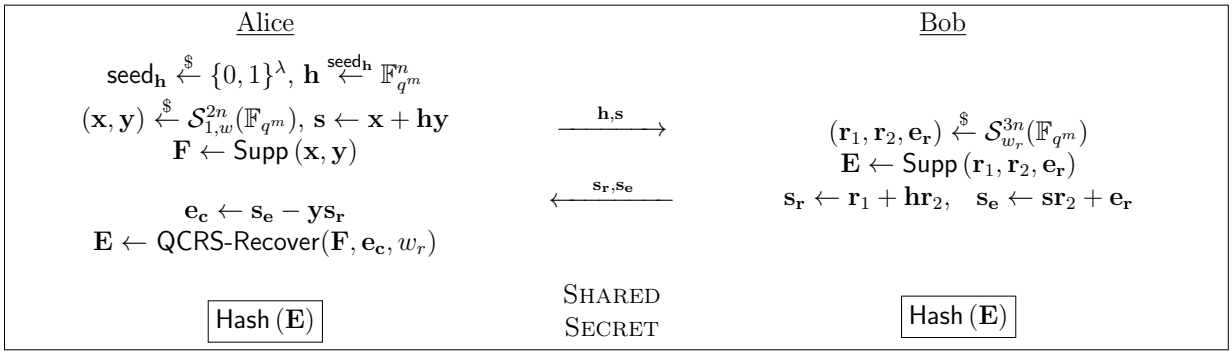


Figure 1: Informal description of our new Key Exchange protocol. $\mathbf{h}$ and $\mathbf{s}$ constitute the public key. $\mathbf{h}$ can be recovered by publishing only the λ bits of the seed (instead of the n coordinates of $\mathbf{h}$).

Correctness: Alice recovers $\mathbf{e_c} = \mathbf{s_e} - \mathbf{ys_r} = \mathbf{sr}_2 + \mathbf{e_r} - \mathbf{y}(\mathbf{r}_1 + \mathbf{hr}_2) = (\mathbf{x} + \mathbf{hy})\mathbf{r}_2 + \mathbf{e_r} - \mathbf{y}(\mathbf{r}_1 + \mathbf{hr}_2) = \mathbf{xr}_2 - \mathbf{yr}_1 + \mathbf{e_r}$, since $\mathbf{E} = \mathsf{Supp}(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e_r})$ and $\mathbf{F} = \mathsf{Supp}(\mathbf{x}, \mathbf{y})$, and since $1 \in \mathbf{F}$, the coordinates of $\mathbf{e_c}$ generate a subspace of $E.F$ on which one can apply the QCRS-Recover algorithm to recover E.

□

- KeyGen(1^λ): Picks $\mathsf{seed}_\mathbf{h} \xleftarrow{\$} \{0,1\}^\lambda$, $\mathbf{h} \xleftarrow{\mathsf{seed}_\mathbf{h}} \mathbb{F}_{q^m}^n$, $(\mathbf{x},\mathbf{y}) \xleftarrow{\$} \mathcal{S}_{1,w}^{2n}(\mathbb{F}_{q^m})$.
  Sets $\mathbf{s} \leftarrow \mathbf{x} + \mathbf{hy}$ and returns $\mathsf{pk} = (\mathbf{h}, \mathbf{s})$, $\mathsf{sk} = (\mathbf{x}, \mathbf{y})$.
- Encap(pk): Picks $(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e_r}) \xleftarrow{\$} \mathcal{S}_{w_r}^{3n}(\mathbb{F}_{q^m})$, sets $\mathbf{E} = \mathsf{Supp}(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e_r}), \mathbf{s_r} = \mathbf{r}_1 + \mathbf{hr}_2, \mathbf{s_e} = \mathbf{sr}_2 + \mathbf{e_r}$
  Computes $K = \mathsf{Hash}(\mathbf{E})$, and returns $\mathbf{c} = (\mathbf{s_r}, \mathbf{s_e})$
- Decap(sk): Sets $\mathbf{e_c} = \mathbf{s_e} - \mathbf{ys_r}$, $\mathbf{F} = \mathsf{Supp}(x, y)$and $E \leftarrow \mathsf{QCRS\text{-}Recover}(F, \mathbf{e_c}, w_r)$
  Recovers $K = \mathsf{Hash}(\mathbf{E})$

Figure 2: Formal description of our key exchange protocol.

1.5 Parameters for Ouroboros-R

In this Section, we propose several sets of parameters for Ouroboros-R, achieving 128, 192, or 256 bits of security and corresponding therefore to NIST's security strength categories 1, 3, and 5 respectively.

Choice of parameters. In section 4, the security of the protocol is reduced to the 2-QCRSD problem for weight w for the secret key, and the 3-QCRSD problem for weight w_r and a $[3n, n]$ code. Since 1 is contained in the support of $(\mathbf{x}, \mathbf{y})$, the security is straightforwardly reduced to attacking a $[2n, n]$ 2-QCRSD instance for weight $w - 1$ rather than w. The probability of decryption failure (DFR) comes from the probability that the QCRS-recover algorithm fails. The best attacks for these cases are combinatorial attacks described in the next section. These parameters have been chosen so that the best known attack requires at least 2^λ elementary operations for λ bits of security. We refer the reader to Sec. 4 for more details on best known attacks.

Size of parameters and computational costs. The public key has size nm, the ciphertext has size $2nm$. The Encap cost corresponds to a matrix-vector product over $\mathbb{F}_{q^m}$, for a multiplication cost of elements of $\mathbb{F}_{q^m}$ in $m \log(m) \log(\log(m))$, we obtain an encryption complexity in $\mathcal{O}\left(n^2 m \log\left(m\right) \log\left(\log\left(m\right)\right)\right)$. The Decap cost is also a matrix-vector multiplication plus the decoding cost of the QCRS-recover algorithm (intersections of subspaces of dimension ww_r in F_{q^m}) in $\mathcal{O}((ww_r)^2 m)$.

The resulting public key, secret key, ciphertext and shared secret sizes are given in Tab. 2. One may use seeds to shorten keys thus obtaining sizes presented in Tab. 3. The aforementioned sizes are the ones used in our reference implementation.

Instance	q	n	m	w	$w_{\mathbf{r}}$	security	DFR
Ouroboros-R-I	2	53	89	5	6	128	2^{-36}
Ouroboros-R-II	2	59	101	6	8	192	2^{-36}
Ouroboros-R-III	2	67	127	7	8	256	2^{-42}

Table 1: Parameters for Ouroboros-R.

Instance	pk size	sk size	ct size	ss size	Security
Ouroboros-R-I	1180	1180	1180	64	128
Ouroboros-R-II	1490	1490	1490	64	192
Ouroboros-R-III	2128	2128	2128	64	256

Table 2: Resulting theoretical sizes in bytes for Ouroboros-R. The public key pk is composed of ($\mathbf{h}$, $\mathbf{s}$) and has size $2nm$. The secret key sk is composed of ($\mathbf{x}$, $\mathbf{y}$) and has size $2nm$. The ciphertext ct is composed of ($\mathbf{sr}$, $\mathbf{se}$) and has size $2nm$. The shared secret ss is composed of K and has size 64 (SHA512 output size). The security is expressed in bits.

Instance	pk size	sk size	ct size	ss size	Security
Ouroboros-R-I	676	40	1272	64	128
Ouroboros-R-II	807	40	1534	64	192
Ouroboros-R-III	1112	40	2144	64	256

Table 3: Resulting sizes in bytes for Ouroboros-R using NIST seed expander initialized with 40 bytes long seeds. The public key pk is composed of (**seed1**, **s**) and has size $40 + n(\lfloor m/8 \rfloor + 1)$. The secret key sk is composed of (**seed2**) and has size 40. The ciphertext ct is composed of (**sr**, **se**) and has size $2n(\lfloor m/8 \rfloor + 1)$. The shared secret ss is composed of K and has size 64 (SHA512 output size). The security is expressed in bits. Vectors may be shortened to fit into their theoretical size of $2(\lfloor nm/8 \rfloor + 1)$ bytes rather than $2n(\lfloor m/8 \rfloor + 1)$ bytes if necessary.

2 Performances

In this section, we provide concrete performance measures of our implementation. For each parameter set, results have been obtained by running 100,000 random instances and computing their average execution time. The benchmarks have been performed on a machine running Ubuntu 16.04 LTS. The latter has 32GB of memory and an Intel® Core™ i7-4770 CPU @ 3.4GHz for which the Hyper-Threading, Turbo Boost and SpeedStep features were disabled. The scheme have been compiled with `gcc` (version 7.2.0) using the compilation flags `-O2 -pedantic`. The following third party libraries have been used: `openssl` (version 1.1.0f), `gmp` (version 6.1.2) and `ntl` (version 10.5.0) [12].

2.1 Reference Implementation

The performances of our reference implementation on the aforementioned benchmark platform are described in Tab. 4 (timings in ms) and Tab. 5 (millions of CPU cycles required).

Instance	KeyGen	Encrypt	Decrypt
Ouroboros-R-I	0.18	0.29	0.53
Ouroboros-R-II	0.19	0.33	0.97
Ouroboros-R-III	0.24	0.40	1.38

Table 4: Timings (in ms) of the reference implementation for different instances of Ouroboros-R.

2.2 Optimized Implementation

No optimized implementation has been provided. As a consequence, the folders `Optimized_Implementation/` and `Reference_Implementation/` are identical. Additional

Instance	KeyGen	Encrypt	Decrypt
Ouroboros-R-I	0.60	0.98	1.78
Ouroboros-R-II	0.65	1.12	3.26
Ouroboros-R-III	0.82	1.39	4.73

Table 5: Millions of cycles of the reference implementation for different instances of Ouroboros-R.

implementation (optimized variant using vectorization, constant-time implementation...) might be provided later.

3 Known Answer Test Values

Known Answer Test (KAT) values have been generated using the script provided by the NIST. They are available in the folder `KAT/Reference_Implementation/`. As mentioned in Sec. 2.2, since the reference and optimized implementations are identical, `KAT/Optimized_Implementation/` is just a copy of `KAT/Reference_Implementation/`.

In addition, we provide, for each parameter set, an example with *intermediate values* in the folder `KAT/Reference_Implementation/`.

Notice that one can generate the aforementioned test files using respectively the `kat` and `verbose` modes of our implementation. The procedure to follow in order to do so is detailed in the technical documentation.

4 Security

4.1 Security Models and Hybrid Argument

IND-CPA. IND-CPA is generally proved through the following game: the adversary $\mathcal{A}$ chooses two plaintexts μ_0 and μ_1 and sends them to the challenger who flips a coin $b \in \{0,1\}$, encrypts μ_b into ciphertext c and returns c to $\mathcal{A}$. The encryption scheme is said to be IND-CPA secure if $\mathcal{A}$ has a negligible advantage in deciding which plaintext c encrypts. This game is formally described hereunder on Fig. 3.

The global advantage for polynomial time adversaries (running in time less than t) is:

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{E}}(\lambda, t) = \max_{\mathcal{A} \leq t} \mathsf{Adv}^{\mathsf{ind}}_{\mathcal{E},\mathcal{A}}(\lambda), \tag{3}$$

where $\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{E},\mathcal{A}}(\lambda)$ is the advantage the adversary $\mathcal{A}$ has in winning game $\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$:

$$\mathsf{Adv}^{\mathsf{ind}}_{\mathcal{E},\mathcal{A}}(\lambda) = \left|\Pr[\mathbf{Exp}^{\mathsf{ind}-1}_{\mathcal{E},\mathcal{A}}(\lambda) = 1] - \Pr[\mathbf{Exp}^{\mathsf{ind}-0}_{\mathcal{E},\mathcal{A}}(\lambda) = 1]\right|. \tag{4}$$

$\mathbf{Exp}^{\mathsf{ind}-b}_{\mathcal{E},\mathcal{A}}(\lambda)$
1. $\mathsf{param} \leftarrow \mathsf{Setup}(1^\lambda)$
2. $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\texttt{FIND} : \mathsf{pk})$
4. $\mathbf{c}^* \leftarrow \mathsf{Encrypt}(\mathsf{pk}, \mu_\mathbf{b}, \theta)$
5. $b' \leftarrow \mathcal{A}(\texttt{GUESS} : \mathbf{c}^*)$
6. `RETURN` b'

Figure 3: Experiment against the indistinguishability under chosen plaintext attacks

Hybrid argument. Alternatively (and equivalently by the hybrid argument), it is possible to construct a sequence of games from a valid encryption of a first message μ_0 to a valid encryption of another message μ_1 and show that these games are two-by-two indistinguishable. We follow this latter approach and prove the security of our KEM similarly to [1].

4.2 Security Reduction

We now turn to our main theorem, namely the security of the proposed key exchanged protocol.

Theorem 4.1. *Ouroboros-R is* IND-CPA *secure under the 2-*QCRSD *and 3-*QCRSD *assumptions.*

The proof follows the same ideas as the one from [1, Proof of Theorem 1].

Proof. It is worth noticing first that an adversary $\mathcal{A}$ succeeds in breaking the scheme if he manages to recover the support $\mathbf{E} = \mathrm{Supp}\,(\mathbf{r}_1, \mathbf{r}_2, \mathbf{e}_\mathbf{r})$ given only the public key $\mathsf{pk} = (\mathbf{h}, \mathbf{s})$ and the transcripts $(\mathbf{s}_\mathbf{r} = \mathbf{r}_1 + \mathbf{h}\mathbf{r}_2, \mathbf{s}_\mathbf{e} = \mathbf{s}\mathbf{r}_2 + \mathbf{e}_\mathbf{r})$. This is exactly an instance of the QCRSR problem defined in Sec. 1.2 (see Pb. 1.3). It has also been shown in that section that the QCRSR problem is equivalent to the QCRSD problem, and the security reduction exploits the equivalence between these problems.

The aim is to prove that an adversary distinguishing one game from another can be exploited to break either the 2-QCRSD or the 3-QCRSD assumption (respectively on $[2n, n]$ or $[3n, n]$ codes) in polynomial time. We are going to proceed in a sequence of games moving from the real world with a valid encryption, to an idealistic version where both the ciphertext and the key are random. Let $\mathcal{A}$ be a probabilistic polynomial time adversary against the IND-CPA of our scheme and consider the following games where we consider that $\mathcal{A}$ receives the encapsulation at the end of each game.

Game $\mathbf{G}_1$: This game corresponds to an honest run of the protocol. In particular, the simulator has access to all keys / randomness.

Game $\mathbf{G}_2$: Now the simulator picks uniformly at random $\mathbf{x}, \mathbf{y}$ (resulting in a random $\mathbf{s}$). He then proceeds honestly.

An adversary distinguishing between those two games, can distinguish between a well-formed pk and a random one. The public key in the first game correspond to a valid 2-QCRSD instance, while it is a random one in the second.

Hence $\mathsf{Adv}^{G_1-G_2}_{\mathcal{A}_{1,2}} \leq \mathsf{Adv}(\text{2-QCRSD})(\lambda)$

Game $\mathbf{G}_3$: Now the simulator also picks uniformly at random $\mathbf{e}_\mathbf{r}$, $\mathbf{r}_1$ and $\mathbf{r}_2$ and uses them to generate $\mathbf{s}_\mathbf{r}, \mathbf{s}_\mathbf{e}$. We denote φ the operator that on input a vector returns the corresponding double circulant matrix (see Eq. (1) of Def. 1.1.4).

An adversary has access to:

$$\begin{pmatrix} \mathbf{s}_\mathbf{r} \\ \mathbf{s}_\mathbf{e} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \varphi(\mathbf{h}) \\ \mathbf{0} & \mathbf{I}_n & \varphi(\mathbf{s}) \end{pmatrix} (\mathbf{r}_1, \mathbf{e}_\mathbf{r}, \mathbf{r}_2)^\top$$

The syndrome $(\mathbf{s}_\mathbf{r}, \mathbf{s}_\mathbf{e})$ follows the QCRSD distribution in game $\mathbf{G}_2$ and the uniform distribution over $(\mathbb{F}_2^n)^2$ in $\mathbf{G}_3$. If an adversary is able to distinguish games $\mathbf{G}_2$ from $\mathbf{G}_3$, then a simulator can break the underlying problem.

Hence $\mathsf{Adv}^{G_2-G_3}_{\mathcal{A}_{2,3}} \leq \mathsf{Adv}(\text{3-QCRSD})(\lambda)$.

$$\mathsf{Adv}^{indcpa}_{\mathsf{KEM}}(\mathcal{A}) \leq \mathsf{Adv}^{\text{2-QCRSD}}(\lambda) + \mathsf{Adv}^{\text{3-QCRSD}}(\lambda).$$

Therefore, a PPT adversary $\mathcal{A}$ breaking the protocol with non negligible advantage can be used to solve the QCRSD problem. □

5 Known Attacks

There are two ways to attack our system: either the opponent can try to recover the structure of the QC 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 QCRSR 1.3 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 QC LRPC case and in a third subsection we discuss about the algebraic attacks.

5.1 Generic attacks

For C a $[n, k]$ rank codes over $\mathbb{F}_{q^m}$ the best combinatorial attacks to decode a word with an error of weight r is:

$$\mathcal{O}\big((nm)^3 q^{r\left\lceil \frac{m(k+1)}{n} \right\rceil - m}\big)$$

This attack is an improvement of a previous attack described in [6], a detailed description of the attack can be found in [2]. The general idea of the attack is to adapt the Information Set Decoding attack for Hamming distance to rank metric. For rank metric the attacker tries to guess a subspace which contains the support of the error and test whether the choice of the subspace contains the support of the error or not, by solving a system of syndrome equations. There is no known attack which uses the quasi-cyclicity of a code to improve this attack.

5.2 Structural attack from LRPC

There exists a specific attack on the QC 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 QC codes, since the generator matrix of the code is not generated by a small weight vector.

5.3 Algebraic attacks

The second way to solve the equations of the system $\mathbf{He} = \mathbf{c}$ 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 [4].

6 Advantages and Limitations

6.1 Ouroboros' Strengths

The Ouroboros protocol benefits from the nice features of the LRPC protocol but with a tight reduction to the generic s-QCRSD problems. The Ouroboros has also a probability of failure (like other NTRU-like protocols) related to the way the decoding algorithms works. In the case of Ouroboros this probability can be well studied and estimated. It comes at price, since the ciphertext size is doubled, but due to the inherent difficulty of decoding codes in rank metric, parameters are rather low, and compare very well to other type of protocols.

References

[1] Carlos Aguilar Melchor, Olivier Blazy, Jean Christophe Deneuville, Philippe Gaborit, and Gilles Zémor. Efficient encryption from random quasi-cyclic codes. *CoRR*, abs/1612.05572, 2016. http://arxiv.org/abs/1612.05572.

[2] Nicolas Aragon, Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. Improvement of generic attacks on the rank syndrome decoding problem., 2017. Pre-print, available at https://www.unilim.fr/pages_perso/philippe.gaborit/newGRS.pdf.

[3] 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.

[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.

[5] 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] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2016. https://arxiv.org/pdf/1301.1026.pdf.

[7] 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. https://arxiv.org/pdf/1404.3482.pdf.

[8] Adrien Hauteville and Jean-Pierre Tillich. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem. In *2015*, pages 2747–2751, Hong Kong, China, June 2015.

[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, pages 267–288. Springer, 1998.

[10] Françoise Levy-dit Vehel and L Perret. Algebraic decoding of rank metric codes. *Proceedings of YACC*, 2006.

[11] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE, 2013. https://eprint.iacr.org/2012/409.pdf.

[12] Victor Shoup. Ntl: A library for doing number theory. *www. shoup. net/ntl/*, 2001.

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. Carlos Aguilar Melchor and Philippe Gaborit have a patent owner statement. This patent also involves the CNRS (french national center for scientific research), represented by Éric Buffenoir. Therefore a patent statement for the CNRS is also included.

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

I, Carlos Aguilar Melchor, of University of Toulouse, 2 rue Charles Camichel, 31000 Toulouse, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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: Carlos AGUILAR MELCHOR

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

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 Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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).

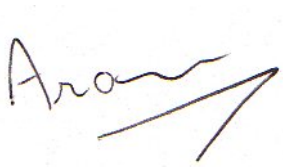
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

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, Slim Bettaieb, of Worldline, Zone Industrielle A, rue de la Pointe, 59113 Seclin, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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: Slim Bettaieb

Title: Research Engineer, Ph.D.
Date: November 28, 2017
Place: Seclin

I, Loïc Thierry Bidoux, of Worldline, Zone Industrielle A, rue de la Pointe, 59113 Seclin, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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: Loïc Bidoux

Title: Research Engineer, Ph.D.
Date: November 28, 2017
Place: Seclin

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 Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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).

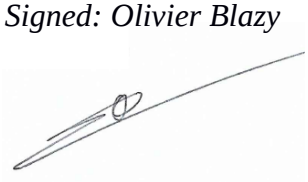
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

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



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 Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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).

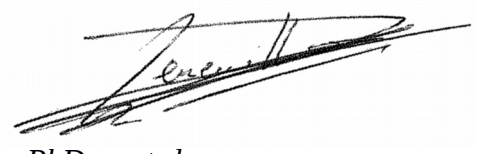
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

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-ChristopheDeneuville



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 Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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 Ouroboros-R, 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 Ouroboros-R;* ***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 Ouroboros-R, 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, 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 Ouroboros-R, 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 Ouroboros-R; 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 Ouroboros-R, 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, Carlos Aguilar Melchor, of University of Toulouse, 2 rue Charles Camichel, 31000 Toulouse, FRANCE, am the owner of the following patents and/or patent applications: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Ouroboros-R is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

☐ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed: Carlos AGUILAR MELCHOR

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

I, Philippe Gaborit, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the following patents and/or patent applications: "Cryptographic method for communicating confidential information" US9094189 B2, and "Procédé cryptographique de communication d'une information confidentielle" FR 10/51190, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Ouroboros-R is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

☐ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed: P. Gaborit.

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

Délégation Centre Limousin
Poitou-Charentes

www.cnrs.fr

3E avenue de la Recherche Scientifique
CS 10065
45071 Orléans Cedex 2

T. 02 38 25 52 00
F. 02 38 69 70 31

Statement by Patent Owner

I, Marion BLIN, interim Regional Delegate of CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE, 3 rue Michel Ange, 75794 PARIS cedex 16 FRANCE, am the authorized representative of the owner of the following patent(s) and/or patent application(s):

- French Priority Patent: Procédé cryptographique de communication d'une information confidentielle, FR 10/51190, February 18th, 2010, and its validated extensions in France, in Germany, in Swiss, in United Kingdom, United States, and in Japan,

and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as OUROBOROS R is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

√ without compensation and under reasonable terms and conditions that are demon- strably free of any unfair discrimination, OR

☐ under reasonable terms and conditions that are demonstrably free of any unfair dis- crimination.

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are in- tended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted

cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Pour le (la) Président(e) du CNRS
et par délégation,
La Déléguée Régionale par intérim
Marion BLIN

Title: Regional Delegate

Date: 20.11.2017

Place: Orléans, France

I, Carlos Aguilar Melchor, of University of Toulouse, 2 rue Charles Camichel, 31000 Toulouse, 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: Carlos AGUILAR MELCHOR

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

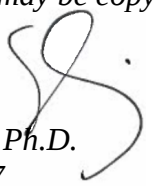
I, Nicolas Aragon, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based 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, Slim Bettaieb, of Worldline, Zone Industrielle A, rue de la Pointe, 59113 Seclin, 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: Slim Bettaieb



Title: Research Engineer, Ph.D.
Date: November 28, 2017
Place: Seclin

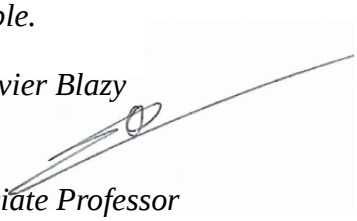
I, Loïc Thierry Bidoux, of Worldline, Zone Industrielle A, rue de la Pointe, 59113 Seclin, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based 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: Loïc Bidoux

Title: Research Engineer, Ph.D.
Date: November 28, 2017
Place: Seclin

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



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

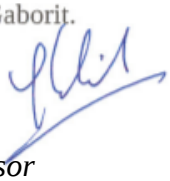
I, Jean-Christophe Deneuville, of INSA-CVL Bourges, 88 boulevard Lahitolle, 18000 Bourges, FRANCE, and University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government 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

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

Title: Ph.D. Student
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