

**Name of the proposed cryptosystem:**

RYDE

**Principal submitter:**

Nicolas Aragon, Naquidis Center, Talence

Magali Bardet, University of Rouen and INRIA

Loïc Bidoux, Technology Innovation Institute, UAE

Jesús-Javier Chi-Domínguez, Technology Innovation Institute, UAE

Victor Dyesryn, University of Limoges

Thibault Feneuil, CryptoExperts

Philippe Gaborit, University of Limoges

Antoine Joux, CISPÀ

Romàric Neveu, University of Limoges

Matthieu Rivain, CryptoExperts

Jean-Pierre Tillich, INRIA

Adrien Vinçotte, University of Limoges

**Inventors:**

Same as submitters

**Owners:**

Same as submitters

**E-mail address:**

team@pqc-ryde.org

**Postal address:**

RYDE Consortium

XLIM - DMI

Université de Limoges

123 Avenue Albert Thomas

87 060 Limoges CEDEX

FRANCE

Signed: Nicolas Aragon

Title: Dr.

Date: 31/05/2023

Place: Limoges, France

A handwritten signature in blue ink, appearing to read 'Aragon', with a stylized flourish extending from the end.

*Signed: Magali Bardet*  
*Date: May 28, 2023*  
*Place: Rouen*

A handwritten signature in black ink, appearing to read 'Magali Bardet', with a horizontal line underneath.

Signed: Loïc Bidoux  
Title: Dr  
Date: 31/05/2023  
Place: Abu Dhabi, UAE

A handwritten signature in black ink, consisting of a stylized 'B' with a vertical line through it, followed by a horizontal line.

Signed : Jesús Javier Chi Domínguez

Title: Dr

Date : 31/05/2023

Place : Abu Dhabi, UAE

A handwritten signature in blue ink, appearing to read 'Jesús Javier Chi Domínguez', written in a cursive style.

Signed: Victor Dyseryn

Title: Mr.

Date: 29/05/2023

Place: Limoges, France

A handwritten signature in black ink, appearing to read 'V. Dyseryn', written over a horizontal line.

Signed : Thibault Feneuil

Date : May 27<sup>th</sup>, 2023

Place : Paris

A handwritten signature in black ink. The first part, 'Thibault', is written in a cursive style with a large, stylized 'T' that loops back. The second part, 'FENEUIL', is written in a more formal, uppercase, sans-serif style. A long horizontal line underlines the entire signature.

For the RYDE signature scheme

Signed : Philippe Gaborit  
Date : May 29 2023  
Place : Limoges

P. Gaborit.

A handwritten signature in blue ink, appearing to be 'Philippe Gaborit', with a long, sweeping underline.

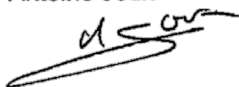


Signed : Antoine Joux

Date : May 30th, 2023

Place : Saarbrücken, Germany

Antoine Joux

A handwritten signature in black ink, appearing to be 'AJ' followed by a stylized flourish.

Signed: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges

A handwritten signature in black ink, appearing to read 'R Neveu'. The signature is stylized, with a large, bold 'R' and the name 'Neveu' written in a cursive script.

Signed : Matthieu Rivain

Date : May 29, 2023

Place : Paris

A handwritten signature in black ink, consisting of a stylized 'M' and 'R' intertwined, with a large loop at the bottom.

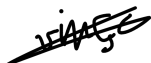
Signed :

Date : May, 29, 2023

Place : Inria de Paris, 2 rue Simone Iff, Paris 75012, France

A handwritten signature in blue ink, appearing to be 'filla' with a stylized flourish at the end.

Signed: Adrien Vinçotte  
Date: May 28, 2023  
Place: Limoges

A handwritten signature in black ink, appearing to read 'Adrien Vinçotte', with a long horizontal stroke extending to the left.

I, **Nicolas Aragon**, from **Naquidis Center, 1, avenue François Mitterand, 33400 Talence, 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: Dr.

Date: 31/05/2023

Place: Limoges, France

A handwritten signature in blue ink, appearing to read 'Aragon', with a stylized flourish extending from the end.

### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

*I, **Magali BARDET**, of **LITIS, Université de Rouen Normandie, avenue de l'Université, 76800 Saint-Étienne-du-Rouvray**, am the owner of the RYDE 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: Magali Bardet  
Title: Maître de conférences  
Date: May 28, 2023  
Place: Rouen*

A handwritten signature in black ink, appearing to read 'Magali Bardet', with a horizontal line underneath.

I, **Loïc Bidoux, Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, United Arab Emirate**, 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: Dr

Date: 31/05/2023

Place: Abu Dhabi, UAE

A handwritten signature in black ink, consisting of a stylized 'B' with a horizontal line through it, followed by a long horizontal stroke.



I, **Jesús Javier Chi Domínguez**, **Technology Innovation Institute, P.O.Box 9639, Masdar City, Abu Dhabi, United Arab Emirates**, am the owner or authorized representative of 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: Jesús Javier Chi Domínguez

Title: Dr

Date: 31/05/2023

Place: Abu Dhabi, UAE



I, **Victor Dyseryn**, from **XLIM, University of Limoges, 123, avenue Albert Thomas, 87000 Limoges, 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: Victor Dyseryn

Title: Mr.

Date: 29/05/2023

Place: Limoges, France

A handwritten signature in black ink, appearing to read 'V. Dyseryn', written over a horizontal line.

### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

*I, Thibault Feneuil, of CryptoExperts, 41 Boulevard des Capucines, 75002 Paris, France, am the owner of the RYDE 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: Thibault Feneuil*

*Title: Engineer*

*Date: May 31, 2023*

*Place: Paris*

A handwritten signature in black ink. The first part of the signature is 'Thibault' written in a cursive style. Below it, the name 'FENEUIL' is written in a straight, blocky, uppercase font.

### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

*I, Philippe Gaborit, **XLIM University of Limoges, 123 av. A. Thomas, 87000 Limoges, FRANCE**, am the owner or authorized representative of the owner (**print full name, if different than the signer**) of the RYDE 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:Philippe Gaborit

Title: Professor

Date: May 29 2023

Place:Limoges

P. Gaborit.



### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

*I, Antoine Joux of CISP Helmholtz Center for Information Security, Stuhlsatzenhaus 5, 66123 Saarbrücken, am the owner of the RYDE 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.*

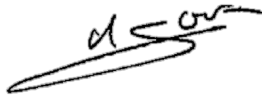
*Signed: Antoine Joux*

*Title: Prof. Dr.*

*Date: May 30th, 2023*

*Place: Saarbrücken, Germany*

Antoine Joux

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

I, **Romaric NEVEU, XLIM, 123 Avenue Albert Thomas, 87000 Limoges, France** , am the owner of the **RYDE** 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: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges

A handwritten signature in black ink, appearing to read 'R Neveu', is positioned to the right of the typed signature information.

### **2.D.3 Statement by Reference/Optimized Implementations' Owner(s)**

The following must also be included:

*I, **Matthieu Rivain**, of **CryptoExperts**, 41 boulevard des Capucines, 75002 Paris, France, am the owner of the RYDE 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: **Matthieu Rivain***

*Title: **CEO and Senior Cryptography Expert***

*Date: **May 31, 2023***

*Place: **Paris***

A handwritten signature in black ink, consisting of a stylized 'M' and 'R' followed by a large, sweeping loop.

### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

*I, Jean-Pierre Tillich, at **Inria de Paris, 2 rue Simone Iff, Paris 75012**, am the owner or authorized representative of the owner (**print full name, if different than the signer**) of the RYDE 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:

Title: Dr.

Date: May 29, 2023

Place: Inria de Paris, 2 rue Simone Iff, Paris 75012, France





### 2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

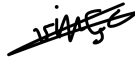
*I, **Adrien Vinçotte** , of **University of Limoges**, 123 Avenue Albert Thomas, 87000 Limoges, **France**, am the owner of the RYDE submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative 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 Vinçotte*

*Title: Mr*

*Date: May 28, 2023*

*Place: Limoges*



I, **Nicolas Aragon, from Naquidis Center, 1, avenue François Mitterand, 33400 Talence, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, may be covered by the following U.S. and/or foreign patents: **NONE**;
- ☐ 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: **NONE**.

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: Dr.  
Date: 31/05/2023  
Place: Limoges, France



## 2.D.1 Statement by Each Submitter

**I, Magali BARDET, of LITIS, Université de Rouen Normandie, avenue de l'Université, 76800 Saint-Étienne-du-Rouvray,** do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE;

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: Magali Bardet  
Title: Maître de conférences  
Date: May 28, 2023  
Place: Rouen



I, **Loïc Bidoux**, of the **Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, may be covered by the following U.S. and/or foreign patents: **NONE**;
- ☐ 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: **NONE**.

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: Dr  
Date: 31/05/2023  
Place: Abu Dhabi, UAE

A handwritten signature in black ink, appearing to be 'LB' or a stylized 'B', with horizontal lines drawn through it.

I, **Jesús Javier Chi Domínguez, Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, United Arab Emirates** print full postal address, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, may be covered by the following U.S. and/or foreign patents: **NONE**;
- ☐ 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: **NONE**.

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: Jesús Javier Chi Domínguez

Title: Dr

Date: 31/05/2023

Place: Abu Dhabi, UAE



I, **Victor Dyseryn, from XLIM, University of Limoges, 123, avenue Albert Thomas, 87000 Limoges, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, may be covered by the following U.S. and/or foreign patents: **NONE**;
- ☐ 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: **NONE**.

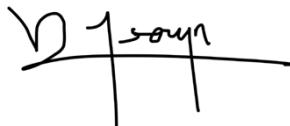
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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: Victor Dyseryn  
Title: Mr.  
Date: 29/05/2023  
Place: Limoges, France



I, Thibault Feneuil, of CryptoExperts, Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **the RYDE signature scheme**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE.

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: Thibault Feneuil

Title: Engineer

Date: May 27<sup>th</sup> 2023

Place: Paris

A handwritten signature in black ink. The first name 'Thibault' is written in a cursive script. The last name 'FENEUIL' is written in all capital letters, with a horizontal line underneath it.

## 2.D.1 Statement by Each Submitter

*I, Philippe Gaborit, of XLIM, University of Limoges 123 av A. Thomas, 87000 Limoges, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE;*

*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: Philippe Gaborit  
Title: Professor  
Date: May 29 2023  
Place: Limoges*

P. Gaborit.  




## 2.D.1 Statement by Each Submitter

*I, Antoine Joux of CISA Helmholtz Center for Information Security, Stuhlsatzenhaus 5, 66123 Saarbrücken, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE;*

*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.*

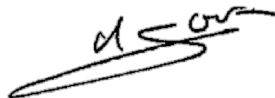
*Signed: Antoine Joux*

*Title: Prof. Dr.*

*Date: May 30th, 2023*

*Place: Saarbrücken, Germany*

Antoine Joux



I, **Romaric NEVEU**, of **XLIM, 123 Avenue Albert Thomas, 87000 Limoges, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 **RYDE**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, may be covered by the following U.S. and/or foreign patents: **NONE** ;
- ☐ 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: **NONE**.

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: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges



## 2.D.1 Statement by Each Submitter

*I, **Matthieu Rivain**, of **CryptoExperts**, 41 boulevard des Capucines, 75002 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that:*

- ☐ *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 **RYDE**;*

*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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

*Signed: Matthieu Rivain*

*Title: CEO, Senior Cryptography Expert*

*Date: May 29, 2023*

*Place: Paris*



## 2.D.1 Statement by Each Submitter

I, Jean-Pierre TILLICH, of Inria de Paris, 2 rue Simone Iff, Paris 75012, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RYDE;

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:

Title: Dr

Date: May, 29, 2023

Place: 2 rue Simone Iff Paris



## 2.D.1 Statement by Each Submitter

*I, **Adrien Vinçotte** , of **University of Limoges, 123 Avenue Albert Thomas, 87000 Limoges, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **RYDE**;*

*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 Vinçotte**

Title: **Mr**

Date: **May 28, 2023**

Place: **Limoges**

