Name of the cryptosystem:

RYDE

Principal submitters:

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 Dyseryn, University of Limoges
Thibauld Feneuil, CryptoExperts
Philippe Gaborit, University of Limoges
Antoine Joux, CISPA
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
87060 Limoges CEDEX
France

Signed: Nicolas Aragon
Title: Dr.
Date: 31/05/2023
Place: Limoges, France

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

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

Signed : Jesús Javier Chi Domínguez
Title: Dr
Date : 31/05/2023
Place : Abu Dhabi, UAE

Signed: Victor Dyseryn
Title: Mr.
Date: 29/05/2023
Place: Limoges, France

Signed : Thibauld Feneuil
Date : May 27th, 2023
Place : Paris

For the RYDE signature scheme

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

P. Gaborit.
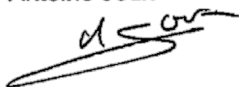
Signed : Antoine Joux
Date : May 30th, 2023
Place : Saarbrücken, Germany

Antoine Joux

Signed : Matthieu Rivain
Date : May 29, 2023
Place : Paris
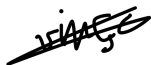
Signed :
Date : May, 29, 2023
Place : Inria de Paris, 2 rue Simone Iff, Paris 75012, France

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

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

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

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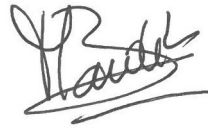
Signed: Loïc Bidoux
Title: Dr
Date: 31/05/2023
Place: Abu Dhabi, UAE

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

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

The following must also be included:

I, Thibauld 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: Thibauld Feneuil
Title: Engineer
Date: May 31, 2023
Place: Paris

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 **CISPA 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

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

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.*
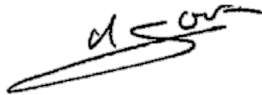
Signed:
Title: Dr.
Date: May 29, 2023
Place: Inria de Paris, 2 rue Simone Iff, Paris 75012, France

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 Emirate**, 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

I, **Jesús Javier Chi Domínguez**, **Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, United Arab Emirateprint 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**.
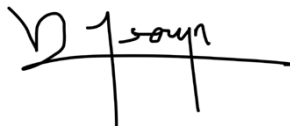
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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, Thibauld 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: Thibauld Feneuil
Title: Engineer
Date: May 27th 2023
Place: Paris

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

2.D.1 Statement by Each Submitter

I, *Antoine Joux* of *CISPA 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.
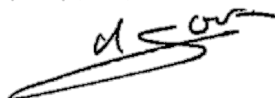
Signed: Antoine Joux
Title: Prof. Dr.
Date: May 30th, 2023
Place: Saarbrücken, Germany

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