

2.D.1 Statement by Each Submitter

I, [Maria Corte-Real Santos](#), of [University College London](#), Gower St, London WC1E 6BT, [United Kingdom](#), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known [SQIsign](#), 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 [SQIsign](#); **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 _____ (**print name of cryptosystem**) _____, may be covered by the following U.S. and/or foreign patents: _____ (**describe and enumerate or state “none” if applicable**) _____ ;
- ☐ 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: _____ (**describe and enumerate or state “none” if applicable**) _____.

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: Maria Corte-Real Santos

Title: Ms

Date: 1st June 2023

Place: London

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

2.D.1 Statement by Each Submitter

I, Luca De Feo, of IBM Research Europe, Säumerstrasse 4, 8803 Rüschlikon, Switzerland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQISign, 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 SQISign.*

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: Research Staff Member, IBM Research

Date: May 31, 2023

Place: Rüschlikon, Switzerland

2.D.1 Statement by Each Submitter

*I, **Basil Hess**, of **IBM Research**, **Saeumerstrasse 4**, **8803 Rueschlikon**, **Switzerland** , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SQIsign**, 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 **SQIsign**.*

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: Senior Engineer, IBM Research

Date: 28 May 2023

Place: Zurich, Switzerland

2.D.1 Statement by Each Submitter

I, David Kohel, of 150 Boulevard de la Libération, 13004 Marseille, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQISign, 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 SQISign.*

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: David Kohel

Title: M

Date: 31 May 2023

Place: Marseille, France



2.D.1 Statement by Each Submitter

I, Antonin Leroux, of DGA-MI, Bruz, France , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQIsign 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 SQIsign.

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: Antonin Leroux



Title: Dr

Date: 1. June 2023

Place: Cesson-Sévigné, France

2.D.1 Statement by Each Submitter

I, Patrick Longa Pierola, of 8659 233rd PI NE, Redmond, Washington, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQIsign 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 SQIsign.*

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: Patrick Longa Pierola
Title: Principal Researcher, Microsoft Research
Date: 1. June 2023
Place: Redmond, USA

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: Michael Meyer

Title: Dr

Date: 2023-05-31

Place: Regensburg

A handwritten signature in black ink, consisting of a stylized 'M' followed by a cursive 'Y' and a long horizontal stroke.

2.D.1 Statement by Each Submitter

I, [Lorenz Panny](#), of [Academia Sinica](#), No. 128 Academia Rd. Sect. 2, 115 Nangang Dist., Taipei City, Taiwan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as [SQIsign](#), 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 [SQIsign](#); **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 _____ **(print name of cryptosystem)**_____, may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state “none” if applicable)**_____ ;
- ☐ 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: _____ **(describe and enumerate or state “none” if applicable)**_____.

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: Lorenz Panny

Title: Dr

Date: 2023-05-31

Place: Taipei, Taiwan

LP

2.D.1 Statement by Each Submitter

I, Sikhar Patranabis, of IBM Research India, Manyata Embassy Business Park, 8th Floor, G2, Outer Ring Road, Rachenahalli, Bangalore, Karnataka-560045, India, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQISign 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 SQISign.*

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: Sikhar Patranabis

Title: Staff Research Scientist, IBM Research India

Date: June 01, 2023

Place: Bangalore, India

2.D.1 Statement by Each Submitter

I, Christophe Petit, of Université libre de Bruxelles, Avenue Franklin Roosevelt 50 - 1050 Bruxelles, Belgium and University of Birmingham, Edgbaston, Birmingham, B15 2TT, UK , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQIsign, 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):

X 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 SQIsign_;
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 _____ (**print name of cryptosystem**)_____, may be covered by the following U.S. and/or foreign patents: _____ (**describe and enumerate or state “none” if applicable**)_____ ;*
- ☐ *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: _____ (**describe and enumerate or state “none” if applicable**) _____.*

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

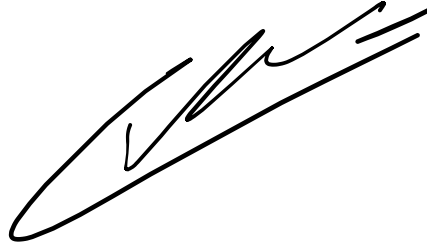
cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Christophe Petit

Title: Professor

Date: 15/09/2023

Place: Rixensart, Belgium

A handwritten signature in black ink, consisting of a large, sweeping loop on the left and several sharp, angular strokes on the right, forming a stylized representation of the name 'Christophe Petit'.

2.D.1 Statement by Each Submitter

I, Sina Schaeffler, of IBM Research Europe, Säumerstrasse 4, 8803 Rüschlikon, Switzerland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SQIsign, 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 SQIsign;

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: *Sina Schaeffler*

Title:

Date: 31 May 2023

Place: Zürich, Switzerland

2.D.1 Statement by Each Submitter

I, Benjamin Wesolowski, of ENS de Lyon site Monod, UMPA UMR 5669 CNRS, 46 allée d'Italie, 69007 Lyon, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known SQIsign, 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 SQIsign; **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 _____ (**print name of cryptosystem**) _____, may be covered by the following U.S. and/or foreign patents: _____ (**describe and enumerate or state "none" if applicable**) _____ ;
- ☐ 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: _____ (**describe and enumerate or state "none" if applicable**) _____.

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: Benjamin Wesolowski

Title: Dr

Date: May 26, 2023

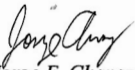
Place: Lyon, France



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

The following must also be included:

I, Jorge Emmanuel Chavez-Saab , of 389 Yacatas, Mexico City 03020, Mexico, 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: Jorge E. Chavez-Saab

Title: Senior Cryptographer, Technology Innovation Institute

Date: June 1, 2023

Place: Mexico City

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

The following must also be included:

I, Maria Corte-Real Santos, University College London, Gower St, London WC1E 6BT, United Kingdom, 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: Maria Corte-Real Santos

Title: Ms

Date: 1st June 2023

Place: London

A handwritten signature in black ink, appearing to read 'Maria Santos', 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, Luca De Feo, Säumerstrasse 4, 8803, Rüschlikon, Switzerland, 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: 

Title: Research Staff Member, IBM Research

Date: May 31, 2023

Place: Rüschlikon, Switzerland

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

The following must also be included:

I, Francisco Rodríguez-Henríquez, of CRC-TII, Accelerator 2 Building, on Plot M12, 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: 

Title: Technical Director of the Cryptographic Research Center at the Technology Innovation Institute

Date: June First 2023

Place: Abu Dhabi, United Arab Emirates

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

The following must also be included:

I, Antonin Leroux, of DGA-MI, Bruz, France, 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: Antonin Leroux



Title: Dr

Date: 1. June 2023

Place: Cesson-Sévigné France

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

The following must also be included:

I, Patrick Longa Pierola, of 8659 233rd PI NE, Redmond, Washington, USA, 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: Patrick Longa Pierola

Title: Principal Researcher, Microsoft Research

Date: 1. June 2023

Place: Redmond, USA

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

The following must also be included:

I, Lorenz Panny, Academia Sinica, No. 128 Academia Rd. Sect. 2, 115 Nangang Dist., Taipei City, Taiwan, 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: Lorenz Panny

Title: Dr

Date: 2023-05-31

Place: Taipei, Taiwan

LP

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

The following must also be included:

I, Sina Schaeffler, IBM Research, Säumerstrasse 4, 8803 Rüschlikon, Switzerland, 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: *Sina Schaeffler*

Title:

Date: 31 May 2023

Place: Zürich, Switzerland

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

The following must also be included:

I, Benjamin Wesolowski, ENS de Lyon site Monod, UMPA UMR 5669 CNRS, 46 allée d'Italie, 69007 Lyon, 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: Benjamin Wesolowski

Title: Dr

Date: May 26, 2023

Place: Lyon, France

