Délégation Centre Limousin
Poitou-Charentes

www.cnrs.fr

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

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

Statement by Patent Owner

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

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

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

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

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

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

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

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

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

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

Signed:

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

Title: Regional Delegate

Date: 20.11.2017

Place: Orléans, France

I, Carlos AGUILAR MELCHOR, of ENSEEIHT, 2 rue Charles Camichel, 31000 Toulouse, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC; **OR**:
  - ☒ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Associate Professor
Date: November 6, 2017
Place: Toulouse, France

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

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

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

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

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

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

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

Signed: 

Title: Associated Professor
Date: Nov 2, 2017
Place: Toulouse FRANCE

I, Carlos AGUILAR MELCHOR, of ENSEEIHT, 2 rue Charles Camichel, 31000 Toulouse, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 

Title: Associate Professor
Date: November 2, 2017
Place: Toulouse, France

I, Nicolas Aragon, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC;* ***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)_____ ;*

☐ *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: _____ (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: Nicolas Aragon

Title: Ph. D. Student
Date: April the 3rd, 2018
Place: Limoges

I, Nicolas Aragon, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Nicolas ARAGON

Title: Ph. D. Student
Date: April the 3rd, 2018
Place: Limoges

I, Slim BETTAIEB, of Worldline, Zone Industrielle A, Rue de la Pointe, 59113 Seclin, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC; **OR**:

  - ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: Research Engineer, PhD
Date: November 9, 2017
Place: Seclin, France

I, Loïc (Thierry) BIDOUX, of Worldline, Zone Industrielle A, Rue de la Pointe, 59113 Seclin, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC; **OR**:
  - ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

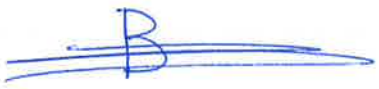
I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: Research Engineer, PhD
Date: November 9, 2017
Place: Seclin, France

I, Loïc (Thierry) BIDOUX, of Worldline, Zone Industrielle A, Rue de la Pointe, 59113 Seclin, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 

Title: Research Engineer, PhD
Date: November 9, 2017
Place: Seclin, France

I, Olivier Blazy of University of Limoges, 123 Av. Albert Thomas, 87000 Limoges, France do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC ,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* RQC *; **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)_____ ;*

☐ *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: _____ (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

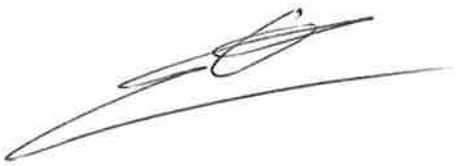
I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public 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: Olivier Blazy
Title: Assistant Prof
Date: November 28 2017
Place: Limoges, France

I, Olivier Blazy, University of Limoges, 123 Av. Albert Thomas, 87 000 Limoges, France, *am the owner of the submitted reference implementation* RQC *and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.*

Signed: Olivier Blazy
Title: Assistant Prof
Date: November 28, 2017
Place: Limoges, France



I, Jean-Christophe Deneuville, of INSA-CVL, 88 boulevard Lahitolle, 18000 Bourges, FRANCE, and University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC;* ***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)_____ ;*

☐ *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: _____ (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.

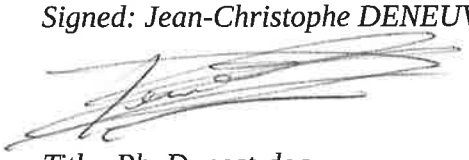
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and 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: Jean-Christophe Deneuville

Title: Ph.D. post-doc
Date: April the 3rd, 2018
Place: Bourges

I, Jean-Christophe Deneuville, of INSA-CVL Bourges, 88 boulevard Lahitolle, 18000 Bourges, FRANCE, and University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Jean-Christophe DENEUVILLE



Title: Ph. D. post-doc
Date: April the 3rd, 2018
Place: Bourges

I, Philippe GABORIT of 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 RQC *,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 ; **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* RQC *(print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: ____ (describe and enumerate or state "none" if applicable)_____;* US 9054189 B2 / FR 10/51150

☐ *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: _____ (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: P. GABORIT
Title: Prof.
Date: 28 NOV. 2017
Place: Limoges.

I, Philippe GABORIT, University of Limoges, 123 av. A. Thomas 87000 Limoges France

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

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

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

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

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

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

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

Signed: P. GABORIT

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

I, Philippe GABORIT, University of Limoges, 123 av A. Thomas 87000 Limoges France

, am the owner of the submitted reference implementation RQC *and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.*

Signed: P. GABORIT
Title: Professor
Date: NOV. 28. 2017
Place: Limoges

I, Gilles ZÉMOR, of Institut de Mathématiques de Bordeaux, 351 cours de la Libération, 33405 Talence Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC; **OR**:
  - ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

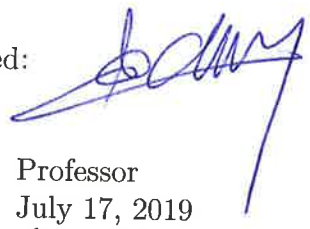
Signed: Gilles Zémor

Title: Professor
Date: November 6, 2017
Place: Bordeaux, France

I, Gilles Zémor , IMB, University of Bordeaux, 351 Cours de la libération 33400 Talence, France , *am the owner of the submitted reference implementation* RQC *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: Gemz
Title: Professor
Date: November 2, 2017
Place: Bordeaux France

I, Alain COUVREUR, of INRIA Saclay, École Polytechnique, 91128 Palaiseau Cedex, France, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 

Title: Professor
Date: July 17, 2019
Place: École Polytechnique, 91128 Palaiseau Cedex, France

I, Alain COUVREUR, of INRIA Saclay, École Polytechnique, 91128 Palaiseau Cedex, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

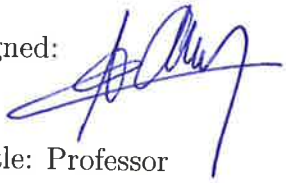
- ☒ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC; **OR**:
  - ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: Professor
Date: July 17, 2019
Place: École Polytechnique, 91128 Palaiseau Cedex, France

I, Adrien HAUTEVILLE, of INRIA Saclay, École Polytechnique, 91128 Palaiseau Cedex, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, 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 RQC; **OR**:
  - ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RQC, may be covered by the following U.S. and/or foreign patents: US9094189 B2 and FR 10/51190;
  - ☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: US9094189 B2 and FR 10/51190.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: Post-doc researcher
Date: July 17, 2019
Place: École Polytechnique, 91128 Palaiseau Cedex, France

I, Adrien HAUTEVILLE, of INRIA Saclay, École Polytechnique, 91128 Palaiseau Cedex, France, am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 

Title: Post-doc researcher
Date: July 16, 2019
Place: École Polytechnique, 91128 Palaiseau Cedex, France