

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 LAKE, 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 LAKE; **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

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

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

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

Title: Ph. D. Student

Date: April the 3rd, 2018

Place: Limoges

I, Olivier Blazy of University of Limoges, 120 av. A. Thomas 87000 Limoges France
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I
have submitted, known as LAKE, 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 LAKE; **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.

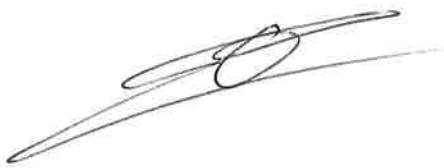
Signed: Olivier Blazy
Title: Assistant Prof.
Date: November 28 2017
Place: Limoges



I, Olivier Blazy, University of Limoges, 123 Av. Albert Thomas
87000 Limoges

, am the owner of the submitted reference implementation LAKE 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



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 LAKE, 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 LAKE; **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) ____.

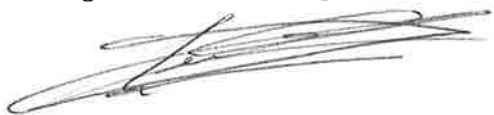
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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 Deneuille

A handwritten signature in black ink, appearing to be 'Jean-Christophe Deneuille', written over a horizontal line.

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

A handwritten signature in black ink, appearing to read 'Jean-Christophe Deneuville', written over a horizontal line.

Title: Ph. D. post-doc

Date: April the 3rd, 2018

Place: Bourges

I, Philip 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 LARKÉ, 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 LARKÉ; **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)_____;

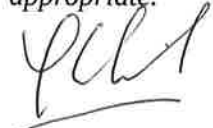
I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.

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: P. Gaborit 
Title: Professeur
Date: 28 nov. 2017
Place: Limoges

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

, am the owner of the submitted reference implementation CAKE 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: 26 nov. 2017
Place: ~~Paris~~ Limoges

I, Adrien Hauteville, of University of Limoges, 123 avenue Albert Thomas, 87060 Limoges Cedex, FRANCE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LAKE, 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 LAKE; **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: Adrien Hauteville

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

Title: Ph.D. post-doc

Date: April the 3rd, 2018

Place: Limoges

I, Adrien HAUTEVILLE, 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: Adrien HAUTEVILLE

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

Title: Ph. D. post-doc

Date: April the 3rd, 2018

Place: Limoges

I, Olivier Ruatta of University of Limoges, 123, av. A. Thomas 87000
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I
have submitted, known as LAKE, is my own original work, or if submitted jointly with
others, is the original work of the joint submitters. Limoges
France

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 LAKE; **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) _____.

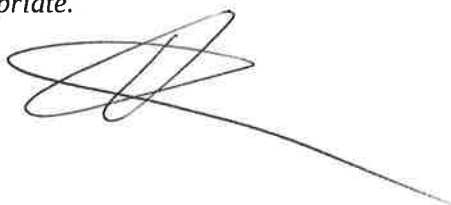
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for
review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I
further acknowledge that I will not receive financial or other compensation from the U.S. Government 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

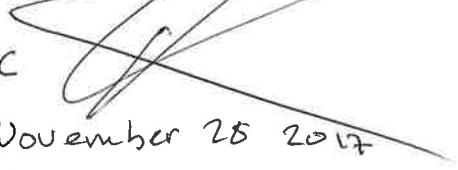
I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or
patent application identified to cover the practice of my cryptosystem, reference implementation or
optimized implementations and the right to use such implementations for the purposes of the public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



I, Olivier Ruatta of university of Limoges, 123 avenue A. Thomas 87000 Limoges France, am the owner of the submitted reference implementation LAKE 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: NAC
Date:
Place: November 28 2017
Limoges.

I, *Jean Pierre Tillich* of *INRIA-Paris, Zene Simone Iff. HOV3 Paris* ^{France}
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I
have submitted, known as *LAKE*, 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 *LAKE*; **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: *J.P. Tillich*
Title: *Director of Research*
Date: *28 Nov 2017*
Place: *Paris*



I, Jean-Pierre Tillich, INRIA - Paris, Zone Simone ~~IA~~, 75013 Paris, France

, am the owner of the submitted reference implementation ^{LAKE} 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-Pierre Tillich
Title: Director of Research
Date: 28 Nov. 2017
Place: Paris



I, Gilles Zemor of IMB, University of Bordeaux, 351 Cours de la Libération, Talence, FRANCE
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LAKE, 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 LAKE; **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: 
Title: Professor
Date: Nov 2, 2017
Place: Bordeaux, FRANCE

I, Gilles Zémor, of IMB, University of Bordeaux 351 Cours de la Libération
33400 Talence FRANCE

, am the owner of the submitted reference implementation LAKE 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: Nov, 2, 2017

Place:

Bordeaux, FRANCE

