

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 BIKE, 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 BIKE; **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 3<sup>rd</sup>, 2018*

*Place: Limoges*

## 2.D.1 Statement by Each Submitter

*I, Edoardo Persichetti, of Florida Atlantic University, Department of Mathematical Sciences, 777 Glades Rd, Boca Raton 33431 FL, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as BIKE, 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 BIKE; **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 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.*

*I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances*

*made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

*Signed:*

A handwritten signature in black ink, appearing to be 'F. J. ...', written over a horizontal line.

*Title: Assistant Professor*

*Date: 11/27/17*

*Place: Boca Raton*

## 2.D.1 Statement by Each Submitter

I, *Edoardo Persichetti, of Florida Atlantic University, Department of Mathematical Sciences, 777 Glades Rd, Boca Raton 33431, FL*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *BIKE*, 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 \_\_\_\_\_ (print name of cryptosystem) \_\_\_\_\_; **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:

A handwritten signature in black ink, appearing to be 'L. Lee' or similar, written in a cursive style.

*Title: Assistant Professor*

*Date: 11/23/17*

*Place: Boca Raton, FL*

## 2.D.1 Statement by Each Submitter

I, **PAULO SERGIO LICCIARDI MESSER BARRETO**, of the Institute of Technology - University of Washington Tacoma - Campus Box 358426 - 1900 Commerce Street - Tacoma WA 98402-3100, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE – Bit-flipping Key Encapsulation**, 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 **BIKE – Bit-flipping Key Encapsulation**; **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 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

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

Signed:



Title: Prof. Dr., PhD

Date: 11/19/2017

Place: Tacoma, WA, USA

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 BIKE, 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 BIKE; **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 BIKE, 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: Slim Bettaieb*

A handwritten signature in black ink, consisting of stylized cursive letters that appear to be 'S.B.' with a period at the end.

*Title: Research Engineer, Ph.D.*

*Date: April the 3<sup>rd</sup>, 2018*

*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 *BIKE*, 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 *BIKE*; **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, 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 BIKE, 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 BIKE; **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 BIKE, 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: Loïc Bidoux*

A handwritten signature in black ink, consisting of a stylized capital letter 'B' with a horizontal line through it, followed by a long horizontal stroke extending to the left.

*Title: Research Engineer, Ph.D.*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Seclin, 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 BIKE, 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 BIKE; **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 read 'Jean-Christophe Deneuille', with a long horizontal flourish extending to the right.

*Title: Ph.D. post-doc*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Bourges*

I, Philippe CADET 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 \_\_\_\_\_, 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 \_\_\_\_\_ (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 4054189 B2 and FR 10151190

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:  
Date:  
Place:

I, Carlos AGUILAR MELCHOR of ENSEEIH 2 rue Charles Comichel 31000 Toulouse FRANCE  
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I  
have submitted, known as BIKE, 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 BIKE (~~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 9094189 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: \_\_\_\_\_ (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: Associated Professor  
Date: Nov, 2, 2017  
Place: Toulouse FRANCE



## 2.D.1 Statement by Each Submitter

I, **RAFAEL MISOCZKI**, of **Intel Corporation**, 2111 NE 25<sup>th</sup> Avenue, Hillsboro, Oregon, 97124, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE – Bit Flipping Key Encapsulation**, 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 **BIKE – Bit Flipping Key Encapsulation**; 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: Rafael Misoczki*

*Title: Dr.*

*Date: Nov. 28, 2017*

*Place: Hillsboro, Oregon, USA*

A handwritten signature in blue ink that reads "Rafael Misoczki". The signature is written in a cursive style with a distinct loop at the end.

## 2.D.1 Statement by Each Submitter

I, SHAY GURRON, of UNIVERSITY OF HAIFA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as BIKE, 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 BIKE of cryptosystem; **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 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: APRIL 12, 2018

Place: FORT LAUDERDALE

## 2.D.1 Statement by Each Submitter

I, *Tim Güneysu, of Ruhr-Universität Bochum, Universitätsstr. 150, 44780 Bochum, GERMANY*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE – Bit Flipping Key Encapsulation**, 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 **BIKE – Bit Flipping Key Encapsulation**; **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 **BIKE**, 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: Tim Güneysu*

*Title: Prof. Dr.-Ing.*

*Date: Nov 23, 2017*

*Place: Bochum, Germany*

A handwritten signature in blue ink, consisting of a large, sweeping initial 'T' followed by the name 'Güneysu' in a cursive script.

## 2.D.1 Statement by Each Submitter

*I, Nicolas Sendrier, of Inria de Paris, 2 rue Simone Iff, CS 42112, 75589 Paris Cedex 12, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE**, 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 **BIKE**;*

*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:

Date: November 28, 2017

Place: Paris, France



**2.D.1 Statement by Each Submitter**

FRANCE

I, Jean-Pierre TILLICH (full name) \_\_\_\_\_, of India, 2 rue Simone Iff, Paris 75012, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as BIKE-Bitflipping Key Encapsulation, 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 \_\_\_\_\_ (print name of cryptosystem) \_\_\_\_\_; **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-Pierre TILLICH

Title: Dr

Date: 28 November 2017

Place: Paris



## 2.D.1 Statement by Each Submitter

I, Gilles ZEMOR, of Institut de Mathématiques, université de Bordeaux, UMR 5251, 351 cours de la Libération, 33400 Talence, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE – Bit Flipping Key Encapsulation**, 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 **BIKE – Bit Flipping Key Encapsulation**; **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 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.



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

Signed:

Title: Professor

Date: November 24, 2017

Place: Talence, France

A handwritten signature in black ink, appearing to be 'G. Chou' or similar, written over the 'Signed:' label.

## Statement by Patent Owner

I, Marion Blin, 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 BIKE 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, nontransferable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted



Délégation Centre Limousin  
Poitou-Charentes

[www.cnrs.fr](http://www.cnrs.fr)

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

T. 02 38 25 52 00  
F. 02 38 89 70 31

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

Signed: 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, Philippe GABORIS, 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, **BIKE**, 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:

Date:

Place:

I, *Carlos* AGUILAR MELCHOR of ENSEE IHT 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, *Bike*, 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, 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 'Nicolas Aragon', with a stylized flourish at the end.

*Title: Ph. D. Student*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Limoges*

*I, Slim Bettaieb, 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: Slim BETTAIEB

A handwritten signature in black ink, appearing to be 'SB', written over the printed name 'Slim BETTAIEB'.

*Title: Research Engineer, Ph.D.*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Seclin*

*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: Loïc BIDOUX*

A handwritten signature in black ink, appearing to be 'Loïc Bidoux', written over a horizontal line.

*Title: Research Engineer, Ph.D.*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Seclin*



I, Olivier Blazy, University of Limoges, 123 Av. Albert Thomas,  
87000 Limoges, France, am the owner of the submitted reference implementation  $\text{BEKE}$  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 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', with a large, sweeping flourish underneath.

*Title: Ph. D. post-doc*

*Date: April the 3<sup>rd</sup>, 2018*

*Place: Bourges*

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

The following must also be included:

I, Nir Ducker (name), UNIVERSITY OF HAIFA, am the owner or authorized representative of the owner (print full name, if different than the signer) 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: MA

Date: APRIL

Place: PORT LAUDERDALE

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

, am the owner of the submitted reference implementation **BiKE** 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. Aubert  
Title: Prof.  
Date: 28 Nov. 2017  
Place: Limoges



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

The following must also be included:

I, SHAY GUERON, UNIVERSITY OF HAIFA am the owner or authorized representative of the owner *(print full name, if different than the signature)* 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: APRIL

Place: FORT LAUDERDALE



I, Carlos AGUILAR MELCHOR of ENSEEIHT, 2 rue Charles Camichel, 31000  
Toulouse, FRANCE

, am the owner of the submitted reference implementation **BIKE** 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

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

The following must also be included:

*I, Rafael Misoczki, 260 NE 66<sup>th</sup> Avenue, Hillsboro, OR, 97124, USA, am the owner or authorized representative of the owner (print full name, if different than the signer) 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: *Rafael Misoczki*  
Title: *Doctor, Research Scientist*  
Date: *08/22/2017*  
Place: *HILLSBORO, OR, USA.*

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

The following must also be included:

*I, Sridhar Iyengar, of Intel Corporation, 2111 NE 25<sup>th</sup> Avenue, Hillsboro, Oregon, 97124, am an authorized representative of Intel Corporation, the owner of the submitted reference implementation and optimized implementations, which hereby grants 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.*

*Intel Corporation*

By: *Sridhar Iyengar*

*Name: Sridhar Iyengar*

*Title: Vice President, Intel Labs; Director, Security and Privacy Research*

*Date: September 29, 2017*

*Place: Hillsboro, Oregon*





## 2.D.1 Statement by Each Submitter

*I, Valentin Vasseur, of Inria de Paris, 2 rue Simone Iff, CS 42112, 75589 Paris Cedex 12, France and Université Paris Descartes, Sorbonne Paris Cité, 12 rue de l'École de Médecine, 75270 Paris Cedex 06, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **BIKE**, 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 **BIKE**.*

*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 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.*

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

Signed:



Title:

Date: March 28, 2019

Place: Paris, France