2.4.1 Statement by Each Submitter

I, Alexandre Adomnicai, of Trusted Objects - Europarc de Pichaury, Bât. B8, 1330 rue Guillibert de la Lauzière, 13290 Aix-en-Provence - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LILLIPUT-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 LILLIPUT-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: PhD candidate Alexandre ADOMNICAI

Date: 14 November 2018

Place: Paris, France

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Alexandre Adomnicai, of Trusted Objects - Europarc de Pichaury, Bât. B8, 1330 rue Guillibert de la Lauzière, 13290 Aix-en-Provence - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: PhD candidate Alexandre ADOMNICAI

Date: 14 November 2018

Place: Paris, France

2.4.1 Statement by Each Submitter

I, Thierry P. Berger, of Université de 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 Lilliput-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 Lilliput-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Pr Thierry BERGER

Date: 30 octobre 2018

Place: Limoges

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Thierry P. Berger, of Université de Limoges - 123 avenue Albert Thomas, 87060 Limoges Cedex - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: Pr Thierry BERGER

Date: 30 octobre 2018

Place: Limoges

2.4.1 Statement by Each Submitter

I, Christophe Clavier, of Université de 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 Lilliput-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 Lilliput-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Professor Christophe CLAVIER

Date: November, 14th 2018

Place: PARIS, FRANCE

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Christophe Clavier, of Université de Limoges - 123 avenue Albert Thomas, 87060 Limoges Cedex - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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 Christophe CLAVIER

Date: November, 14th 2018

Place: PARIS, FRANCE

2.4.1 Statement by Each Submitter

I, Julien Francq, of Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 Elancourt Cedex - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LILLIPUT-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

- ✓ 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 LILLIPUT-AE;

- □ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Dr FRANCQ Julien

Date: 14 November 2018

Place: Paris, France

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Julien Francq, of Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 Elancourt Cedex - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:

Title: Dr FRANCQ julien

Date: 14 Novembre 2018

Place: Paris, France

2.4.1 Statement by Each Submitter

I, Paul Huynh, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Lilliput-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 Lilliput-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: PhD Student - Paul HUYNH

Date: November, 14th 2018

Place: PARIS, FRANCE

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Paul Huynh, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: PhD Student - Paul HUYNH

Date: November, 14th 2018

Place: PARIS, FRANCE

2.4.1 Statement by Each Submitter

I, Virginie Lallemand, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LILLIPUT-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 LILLIPUT-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: V.

Title: DR. Virginie LALLEMAND

Date: 19th of December 2018

Place: NANCY, FRANCE

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Virginie Lallemand, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:

Title: DR. Virginie LALLEMAND

Date: 19th of December 2018

Place: NANCY, FRANCE

2.4.1 Statement by Each Submitter

I, Kévin Le Gouguec, of Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 Elancourt Cedex - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted,known as LILLIPUT-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 LILLIPUT-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Kévin Le Gouguec

Date: 2018 / 11 / 14

Place: Paris, France

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Kévin Le Gouguec, of Airbus CyberSecurity - ZA Clef Saint-Pierre, 1 Bd Jean Moulin, CS 40001, MetaPole, 78996 Elancourt Cedex - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: Kévin Le Gouguec

Date: 2018/11/14

Place: Paris, France

2.4.1 Statement by Each Submitter

I, Marine Minier, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Lilliput-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 Lilliput-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Pr. Marine MINIER

Date: 10th of December 2018

Place: Nancy, France

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Marine Minier, of Université de Lorraine, CNRS, Inria, LORIA - Campus Scientifique, BP 239, 54506 VANDOEUVRE-LES-NANCY - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: Minier

Title: Pr. Marine MINIER

Date: 10th of December 2018

Place: Nancy, France

2.4.1 Statement by Each Submitter

I, Léo Reynaud, of Université de 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 Lilliput-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 Lilliput-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: PhD Student _ Léo REYNAUD

Date: November 14th 2018

Place: PARIS, FRANCE

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Léo Reynaud, of Université de Limoges - 123 avenue Albert Thomas, 87060 Limoges Cedex - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: PhD Student - Léo REYNAUD

Date: November, 14th 2018

Place: PARIS, FRANCE

2.4.1 Statement by Each Submitter

I, Gaël Thomas, of DGA Maîtrise de l'information - BP 7, 35998 RENNES CEDEX 9 - France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LILLIPUT-AE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

✓ 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 LILLIPUT-AE;

□ 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: DR GAËL THOMAS

Date: 2018-11-09

Place: BRUZ, FRANCE

2.4.3 Statement by Reference/Optimized/Additional Implementations' Owner(s)

I Gaël Thomas, of DGA Maîtrise de l'information - BP 7, 35998 RENNES CEDEX 9 - France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:

Title: DR GAËL THOMAS

Date: 2018-11-09

Place: BRUZ, FRANCE