

## Statement by Submitter

I, Jérémy Jean, of 51, boulevard de la Tour-Maubourg, 75700 Paris 07 SP, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, 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 SKINNY-AEAD and SKINNY-Hash;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: none.

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 cryptosystems 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:

Jérémy JEAN




Title: Dr.

Date: 13 March 2019

Place: Paris, France.

## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, Jérémy Jean, of 51, boulevard de la Tour-Maubourg, 75700 Paris 07 SP, France, am the owner or authorized representative of the owner Jérémy Jean 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: Jérémy JEAN   
Title: Dr.  
Date: 13 March 2019  
Place: Paris, France

## Statement by Submitter

I, Siang Meng Sim, of 21 Nanyang Link, Singapore 637371, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, 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 SKINNY-AEAD and SKINNY-Hash;

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, may be covered by the following U.S. and/or foreign patents: U.S. patent 7,949,129, \_\_\_\_\_;  
U.S. patent 8,321,675.

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: none.

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 cryptosystems 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.

Date: 25 Feb 2019

Place: Singapore, Singapore

## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, Siang Meng Sim, of 21 Nanyang Link, Singapore 637371, am the owner ~~or authorized representative of the owner~~ 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.*

Date: *25 Feb 2019*

Place: *Singapore, Singapore.*

## Statement by Submitter


I, <sup>Kölbl</sup> Stefan Kölbl, of Strandvejen 141a, 2900 Hellerup, Denmark, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash v.1.0, 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 SKINNY-AEAD and SKINNY-Hash v.1.0;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash v.1.0, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: "none".

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 cryptosystems 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:

Date: 11.03.2019

Place: Hellerup, Denmark

# Statement by Reference/Optimized/Additional Implementations Owner(s)

I, Stefan <sup>Kolk</sup>~~Kibi~~, of Strandvejen 141a, 2900 Hellerup, Denmark, am the owner or authorized representative of the owner Stefan <sup>Kolk</sup>~~Kibi~~ 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:

Date: 11.03.2019

Place: Hellerup, Denmark

## Statement by Submitter

I, Gregor Leander, of Ruhr-University Bochum, Universitaetsstr. 150, D-44801 Bochum, Germany, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, 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 **SKINNY-AEAD and SKINNY-Hash v.1.0**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: **"none"**.

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 cryptosystems 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: Gregor Leander

Title: Prof

Date: 5.3.2019

Place: Bochum



## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, Gregor Leander, of Ruhr-University Bochum, Universitaetsstr. 150, D-44801 Bochum, Germany, am the owner or authorized representative of the owner Gregor Leander 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: Gregor Leander

Title: Prof.

Date: 5.3.19

Place: Bochum





## Statement by Submitter

I, Amir Moradi, of Ruhr-University Bochum, Universitätsstr. 150, D-44801 Bochum, Germany, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, 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 **SKINNY-AEAD and SKINNY-Hash v.1.0**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: **"none"**.

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 cryptosystems 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:

*Amir Moradi*

Title:

*Dr.*

Date:

*05.03.2019*

Place:

*Bochum, Germany*

*Amir Moradi*

## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, Amir Moradi, of Ruhr-University Bochum, Universitaetsstr. 150, D-44801 Bochum, Germany, am the owner or authorized representative of the owner Amir Moradi 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: *Amir Moradi*  
Title: *Dr.*  
Date: *05.03.2019*  
Place: *Bochum, Germany*

A handwritten signature in blue ink, appearing to read "Amir Moradi", with a long horizontal flourish underneath.

## Statement by Submitter

I, **Christof Beierle**, of **6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, 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 **SKINNY-AEAD and SKINNY-Hash v.1.0**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;<sup>1</sup>
- 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: **"none"**.

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 cryptosystems 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.

Date:

1st March 2019

Place:


Esch-sur-Alzette, Luxembourg

---

<sup>1</sup>We note that since SKINNY-AEAD uses a mode that presents similarities with the generic  $\Theta$ CB3 framework, it is unclear if patents relative to OCB (such as United States Patent No. 7,949,129; United States Patent No.8,321,675) apply to our proposal.

## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, **Christof Beierle**, of **6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg**, am the owner or authorized representative of the owner **Christof Beierle** 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.  
Date: 1st March 2019  
Place: Esch-sur-Alzette, Luxembourg

## Statement by Submitter

I, **Pascal Sasdrich**, of **Rambus Cryptography, Stationsplein 45, A6.016, 3013 AK Rotterdam, The Netherlands**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, 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):

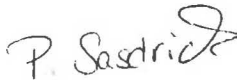
- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **SKINNY-AEAD and SKINNY-Hash v.1.0**, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: **"none"**.

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 cryptosystems 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: Pascal Sasdrich



Title: Dr.-Ing.

Date: March 13, 2019

Place: Rotterdam

## Statement by Reference/Optimized/Additional Implementations Owner(s)

I, **Pascal Sasdrich**, of **Rambus Cryptography, Stationsplein 45, A6.016, 3013 AK Rotterdam, The Netherlands**, am the owner or authorized representative of the owner **Pascal Sasdrich** 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: Pascal Sasdrich

A handwritten signature in black ink that reads "P. Sasdrich" with a stylized flourish at the end.

Title: Dr.-Ing.

Date: March 13, 2019

Place: Rotterdam

## Statement by Submitter

I, Yu Sasaki, of 3-9-11 Midori-cho Musashino-shi Tokyo 180-8585 Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, 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 SKINNY-AEAD and SKINNY-Hash;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, may be covered by the following U.S. and/or foreign patents: US7949129, US8321675;
- 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: none.

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 cryptosystems 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:

*yu Sasaki*

Title:

*Dr.*

Date:

*28 Feb 2019*

Place:

*Tokyo Japan*

## Statement by Submitter

I, Thomas Peyrin, of SPMS, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, 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 SKINNY-AEAD and SKINNY-Hash;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SKINNY-AEAD and SKINNY-Hash, may be covered by the following U.S. and/or foreign patents: US Patent 7,949,129 - US Patent 8,321,675;
- 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: none.

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: PEYRIN THOMAS 

Title: DR.

Date: 06/04/2019

Place: LYON, FRANCE



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

I, Thomas Peyrin, of SPMS, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, am the owner or authorized representative of the owner 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: PEYRIN THOMAS



Title: DR.

Date: 06/04/2019

Place: LYON, FRANCE