

2.4.1 Statement by Each Submitter

I, Kazuo Sakiyama, of 1-5-1 Chofugaoka Chofu Tokyo 182-8585, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 SAEAES.

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and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made under Sections 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.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: 小野 山 一 男
Title: professor
Date: 25/12/2018
Place: Chofu, Tokyo

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

The following must also be included:

I, Kazuo Sakiyama, of 1-5-1 Chofugaoka Chofu Tokyo 182-8585, Japan, 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

Date: 25/18/2018

Place: Chofu, Tokyo

2.4.1 Statement by Each Submitter

I, Takeshi Sugawara, of 1-5-1 Chofugaoka Chofu Tokyo 182-8585, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 SAEAES.

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: 菅原 健

Title: Associate Professor

Date: December 25, 2018

Place: Chofu, Tokyo

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

The following must also be included:

I, Takeshi Sugawara, of 1-5-1 Chofugaoka Chofu Tokyo 182-8585, Japan, 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: 菅原 健

Title: Associate Professor

Date: December 25, 2018

Place: Chofu, Tokyo

2.4.1 Statement by Each Submitter

I, Yasuyuki Sakai, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 SAEAES.

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: 酒井康行

Title: Group Manager

Date: Dec. 21, 2018

Place: Kanagawa, Japan

2. 4. 3 Statement by Reference/Optimized/Additional Implementations' Owner (s)

The following must also be included:

I, Yasuyuki Sakai, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, 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: 酒井康行

Title: Group Manager

Date: Dec. 21, 2018

Place: Kanagawa, Japan

2.4.1 Statement by Each Submitter

I, Mitsuru Matsui, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 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: PCT Application No. : PCT/JP2017/031639.

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: 石中 亮

Title: Fellow

Date: Dec 21 2018

Place: Kanagawa, Japan

2.4.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, Mitsuru Matsui, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): PCT Application No. :PCT/JP2017/031639, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as SAEAES 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.

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 cryptosystem's specifications (e. g., to protect against a newly discovered vulnerability)

for incorporation into the standard.

Signed:

松井 亮

Title: Fellow

Date: Dec 21 2018

Place: Kanagawa, Japan

2. 4. 3 Statement by Reference/Optimized/Additional Implementations' Owner (s)

The following must also be included:

I, Mitsuru Matsui, 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, 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:

松井 亮

Title: Fellow

Date:

Dec 21 2018

Place: Kanagawa, Japan

2.4.1 Statement by Each Submitter

I, Daisuke Suzuki, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 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: PCT Application No. : PCT/JP2017/031639.

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: Daisuke Suzuki

Title: Head Researcher

Date: 12/20/2018

Place: Kanagawa, Japan

2.4.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, Daisuke Suzuki, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): PCT Application No., PCT/JP2017/031639, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as SAEAES 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.

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 cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability)

for incorporation into the standard.

Signed: *Daisuke Suzuki*

Title: *Head Researcher*

Date: *12/20/2018*

Place: *Kanagawa, Japan*

2. 4. 3 Statement by Reference/Optimized/Additional Implementations' Owner (s)

The following must also be included:

I, Daisuke Suzuki, 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, 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: Daisuke Suzuki

Title: Head Researcher

Date: 12/20/2018

Place: Kanagawa, Japan

2.4.1 Statement by Each Submitter

I, Yusuke Naito, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SAEAES, 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 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: PCT Application No. : PCT/JP2017/031639.

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: 内藤 祐介

Title: Head Researcher

Date: Dec. 21, 2018

Place: Kanagawa, Japan

2.4.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, Yusuke Naito, of 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): PCT Application No. :PCT/JP2017/031639, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as SAEAES 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.

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 cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability)

for incorporation into the standard.

Signed: 内藤 祐介

Title: Head Researcher

Date: Dec. 21, 2018

Place: Kanagawa, Japan

2. 4. 3 Statement by Reference/Optimized/Additional Implementations' Owner (s)

The following must also be included:

I, Yusuke Naito, 5-1-1 Ofuna Kamakura Kanagawa 247-8501, Japan, 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: 内藤 祐介

Title: Head Researcher

Date: Dec. 21, 2018

Place: Kanagawa, Japan