

2.4.1 Statement by Each Submitter

I, *André Schrottenloher of Inria Paris, 2 Rue Simone IFF, 75012 Paris, France*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *Saturnin*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *Saturnin*;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *Saturnin*, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;
- 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: *André Schrottenloher*

Title: *Mr.*

Date: *12/02/2019.*

Place: *Paris, France*

Signature :



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

The following must also be included:

I, André Schrottenloher of Inria Paris, 2 Rue Simone IFF, 75012 Paris, 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.

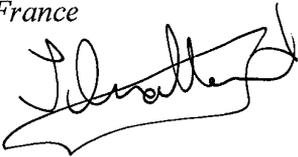
Signed: André Schrottenloher

Title: Mr.

Date: 12/02/2019.

Place: Paris, France

Signature :

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

2.4.1 Statement by Each Submitter

I, Anne Canteaut of Inria Paris, 2 Rue Simone Iff, 75012 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;
- 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: Anne Canteaut

Title: Pr.

Date:12/02/2019.

Place: Paris, France

Signature :

A handwritten signature in black ink, consisting of a stylized 'A' followed by 'LLT' and a horizontal line extending to the right.

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

The following must also be included:

I, Anne Canteaut, 2 Rue Simone Iff, 75012 Paris, 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.

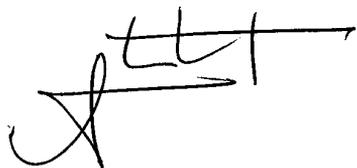
Signed: Anne Canteaut

Title: Pr.

Date: 12/02/2019.

Place: Paris, France

Signature :

A handwritten signature in black ink, appearing to be 'AC', with a long horizontal line extending to the right from the top of the second letter.

2.4.1 Statement by Each Submitter

I, Gaëtan Leurent of Inria Paris, 2 Rue Simone IFF, 75012 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;*
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;*
- 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: Gaëtan Leurent,

Title: Dr.

Date: 22/02/2019.

Place: Paris, France

Signature :



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

The following must also be included:

I, Gaëtan Leurent of Inria Paris, 2 Rue Simone IFF, 75012 Paris, 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: Gaëtan Leurent

Title: Dr.

Date: 25/02/2019.

Place: Paris, France

Signature :

A handwritten signature in black ink, appearing to read 'Leurent', with a large, sweeping flourish above the name.

2.4.1 Statement by Each Submitter

I, Léo Perrin of Inria Paris, 2 Rue Simone Iff, 75012 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;*
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;*
- 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: Léo Perrin

Title: Dr.

Date: 21/02/2019

Place: Paris, France

Signature :



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

The following must also be included:

I, Léo Perrin of Inria Paris, 2 Rue Simone Iff, 75012 Paris, 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: Léo Perrin

Title: Dr.

Date: 21/02/2019

Place: Paris, France

Signature :

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

2.4.1 Statement by Each Submitter

I, María Naya-Plasencia of Inria Paris, 2 Rue Simone IFF, 75012 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;*
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;*
- 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.

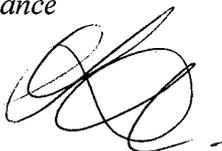
Signed: Maria Naya-Plasencia.

Title: Pr.

Date: 12/02/2019.

Place: Paris, France

Signature :



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

The following must also be included:

I, María Naya-Plasencia of Inria Paris, 2 Rue Simone IFF, 75012 Paris, 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: Maria Naya-Plasencia.

Title: Pr.

Date: 12/02/2019.

Place: Paris, France

Signature :

A handwritten signature in black ink, appearing to be 'M. Naya-Plasencia', written over a horizontal line.

2.4.1 Statement by Each Submitter

I, Sébastien Duval of Université catholique de Louvain, place du Levant 3, B1348 Louvain-la-Neuve, Belgium, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;*
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;*
- 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.

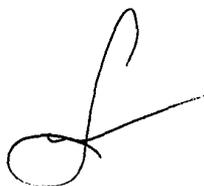
Signed: Sébastien Duval.

Title: Dr.

Date:12/02/2019.

Place: Louvain-la-Neuve, Belgium

Signature :



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

The following must also be included:

I, Sébastien Duval of Université catholique de Louvain, place du Levant 3, B1348 Louvain-la-Neuve, Belgium, 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.

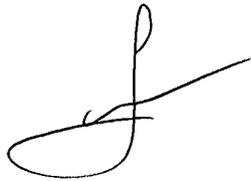
Signed: Sébastien Duval.

Title: Dr.

Date:12/02/2019.

Place: Louvain-la-Neuve, Belgium

Signature :

A handwritten signature in black ink, appearing to be 'S. Duval', written in a cursive style.

2.4.1 Statement by Each Submitter

I, Thomas Pornin of NCC Group, 2977 rue de Deschambault, Quebec, QC, G1W 1B4, Canada, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Saturnin, may be covered by the following U.S. and/or foreign patents: US patents 7,949,129 and 8,321,675 on OCB;
- 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: Thomas Pornin

Title: Dr.

Date: 2019/02/12

Place: Quebec, Canada

Signature :



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

The following must also be included:

I, Thomas Pornin of NCC Group, 2977 rue de Deschambault, Quebec, QC, G1W 1B4, Canada 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.

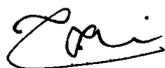
Signed: Thomas Pornin

Title: Dr.

Date: 2019/02/12

Place: Quebec, Canada

Signature :

A handwritten signature in black ink, appearing to read 'T. Pornin', written in a cursive style.