

# Cover Sheet

**Name of the submitted cryptosystem**

FALCON

**Principal submitter**

Thomas Prest  
Thales Communications & Security  
4, Avenue des Louvresses, 92 622 Gennevilliers, France  
thomas.prest@thalesgroup.com  
Tel: +33 (0)1 41 30 30 00 and ask for Thomas Prest

**Auxiliary submitters**

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang.

**Owner of the cryptosystem**

Thomas Prest.

**Inventor(s)/developer(s) of the cryptosystem**

Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang.

**Backup point of contact**

Thomas Pornin  
2977 rue de Deschambault, Québec, QC, G1W 1B4, Canada  
thomas.pornin@nccgroup.trust  
Tel: +1 418 558-0148

**Signature of the submitter**

## 2.D.1 Statement by Each Submitter

*I, Vadim Lyubashevsky, of Saeumerstrasse 4, 8803 Rueschlikon, Switzerland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON; OR (check one or both of the following):*
- X to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: US7308097B2;*
- 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.D.2 and 2.D.3 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.*

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For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

*owner(s), as appropriate.*

Signed: 

Title:

Date: 3.4.2018

Place: Ruschlikon.

## 2.D.1 Statement by Each Submitter

*I, Gregor Seiler, of Saeumerstrasse 4, 8803 Rueschlikon, Switzerland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON; OR (check one or both of the following):*

*to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: US7308097B2;*

- 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.D.2 and 2.D.3 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.*

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

*owner(s), as appropriate.*

*Signed:* G. Seeler

*Title:*

*Date:* 4/2/2018

*Place:* Rueschlikon

**From:**

Thomas Pornin  
2977 rue de Deschambault  
Quebec, QC  
G1W 1B4  
Canada

**To:**

Dustin Moody  
Information Technology Laboratory  
Attention: Post-Quantum Cryptographic Algorithm Submissions  
100 Bureau Drive – Stop 8930  
National Institute of Standards and Technology  
Gaithersburg, MD  
20899-8930  
USA

**Object:** intellectual property statement 2.D.1 and 2.D.3 for FALCON

Dear Sir,

Please find enclosed my signed intellectual property statements (sections 2.D.1 and 2.D.3) for the FALCON submission to the Post-Quantum Cryptography Standardization Process.

Sincerely,

Thomas Pornin

## **Statement by Each Submitter**

I, Thomas Pornin, of NCC Group, 720 3rd Avenue, Suite 2101, Seattle, WA 98104, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, 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 FALCON; **OR** (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_ ;
- I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_ .

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and

2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title:

Date: 2017/11/29

Place: Québec City

## **Statement by Each Submitter**

I, Pierre-Alain FOUQUE, of IRISA, 263 avenue du Général Leclerc, 35042 Rennes Cedex, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one manually or with ):

- 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 FALCON; **OR** (check one or both of the following):
  - to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: none ;
  - 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 specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

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

Signed:

 Fouque

Title: Professor Pierre-Alain FOUQUE

Date: 13/3/2018

Place: Rennes (France)

## **Statement by Each Submitter**

I, Paul KIRCHNER, of IRISA, 263 avenue du Général Leclerc, 35042 Rennes Cedex, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one manually or with ):

- 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 FALCON; **OR** (check one or both of the following):
  - to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: none ;
  - 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 specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

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

Signed: *Kirchner*

Title: Paul KIRCHNER

Date: 13/3/2018

Place: Rennes (France)

## **Statement by Each Submitter**

I, Thomas Ricosset, of Thales Communications & Security, 4 Avenue des Louvresses, 92622 Gennevilliers, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, 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 FALCON; **OR** (check one or both of the following):
  - to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: \_\_\_\_\_ (describe and enumerate or state “none” if applicable)\_\_\_\_\_ ;
  - I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate or state “none” if applicable)\_\_\_\_\_ .

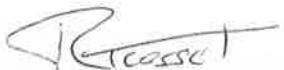
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and

2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: Mister

Date: March 8th 2018

Place: Gennevilliers, France

## **Statement by Each Submitter**

I, Thomas Prest, of Thales Communications & Security, 4 Avenue des Louvresses, 92622 Gennevilliers, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (answer marked with ):

- 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 FALCON; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: \_\_\_\_\_ (describe and enumerate or state "none" if applicable)\_\_\_\_\_ ;
- I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate or state "none" if applicable)\_\_\_\_\_ .

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and

2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Dr

Date: March 30th 2018

Place: Gennevilliers, France



### **Statement by Each Submitter**

*William Uyek, of 235 Clifton St, Belmont, MA 02478*

I, William Uyek, of 235 Clifton St, Belmont, MA 02478, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one manually or with ):

- 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 FALCON; OR (check one or both of the following):

To the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_ ; US 7308097 B2

- I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and

**Statement by Each Submitter**

I, Jeffrey Holtzen, of 353 Shaffer Ave., Providence, RI 02106,

do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one manually or with ):

- 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 FALCON; OR (check one or both of the following):
  - to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FALCON, may be covered by the following U.S. and/or foreign patents: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_;
  - I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate or state "none" if applicable) \_\_\_\_\_.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and

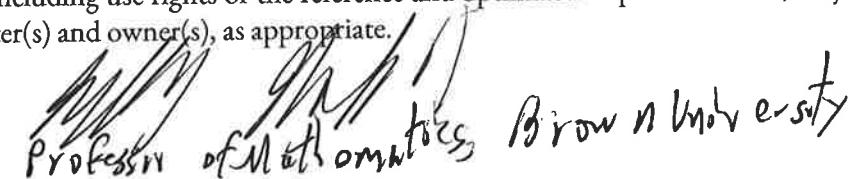
2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title:

Date:

Place:

  
Professor of Mathematics, Brown University

11/6/17  
Providence, RI 02906

## **Statement by Patent (and Patent Application) Owner(s)**

I, William Whyte, of 187 Ballardvale St. Suite A202, Wilmington MA 01803, U.S., am the owner or authorized representative of the owner, OnBoard Security, of the following patent(s) and/or patent application(s): US 7308097 B2 ("Digital signature and authentication method and apparatus"), and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as FALCON is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard:

- without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, OR
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:



Title: CTO

Date: 2018-04-05

Place: Wilmington, MA

2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: CTO, OnBoard Security Inc.

Date: 2018-04-05

Place: Wilmington, MA

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

I, Thomas Pornin, of NCC Group, 720 3rd Avenue, Suite 2101, Seattle, WA 98104, USA, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 

Title:

Date: 2017/11/29

Place: Québec City

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

The following must also be included:

*I, Alessandro Curioni , Saeumerstrasse 4, 8803 Rueschlikon, Switzerland , am the owner or authorized representative of the owner IBM Research – Zurich of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.*

Signed:   
Title: Lab Director IBM Research - Zurich  
Date: 2018, 4.9  
Place: Rueschlikon

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

I Zhenfei Zhang, of 7 Williams rd. Lynnfield MA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Falcon signature, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- \* I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Falcon signature scheme;

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

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

Signed: 

Title:

Date: 03/30/2022

Place: 7 Williams Rd. Lynnfield