Statement by Reference/Optimized Implementations' Owner

I, Markku-Juhani Saarinen, Oxford, UK, 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: Markku-Juhani Saarinen

Title: Staff Cryptography Architect

Date: 31 May 2023

Place: Oxford, UK

Statement by Each Submitter

I, Rafaël del Pino, of PQShield SAS, 259 rue Saint Honoré, 75001 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☑ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.
  - **Title:** Lattice-based cryptographic digital signature scheme utilising masking
    Abstract: The present invention relates to a cryptographic digital signature scheme to verify the integrity and origin of an electronic message. The invention has relevance to a post-quantum lattice-based cryptographic digital signature scheme utilising masking as a countermeasure to side channel attacks.
    Application number: PCT/EP2023/052730

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: Rafaël del Pino

Title: Senior cryptography researcher

Date: 31 May 2023

Place: Paris, France

Statement by Each Submitter

I, Thomas Espitau, of PQShield SAS, 259 rue Saint Honoré, 75001 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, 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.

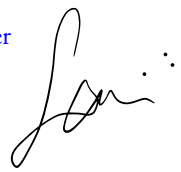
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and 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: Thomas Espitau

Title: Senior cryptography researcher

Date: 31 May 2023

Place: Paris, France



Statement by Each Submitter

I, Shuichi Katsumata, of PQShield Ltd, 267 Banbury Road, Oxford, OX2 7HT, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, 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: 勝又秀一

Title: Lead cryptography researcher

Date: 31 May 2023

Place: Oxford, U.K.

Statement by Each Submitter

I, Mary Maller , of PQShield, UK, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, 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: Mary Maller 

Title: Cryptography researcher

Date: 31 May 2023

Place: London, UK

Statement by Each Submitter

I, Fabrice Mouhartem, of PQShield SAS, 259 rue Saint Honoré, 75001 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, 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: Fabrice Mouhartem

Title: Cryptography researcher

Date: 31 May 2023

Place: Paris, France

Statement by Each Submitter

I, Thomas Prest, of PQShield SAS, 259 rue Saint Honoré, 75001 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;

☑ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.

- **Title:** Lattice-based cryptographic digital signature scheme utilising masking

  Abstract: The present invention relates to a cryptographic digital signature scheme to verify the integrity and origin of an electronic message. The invention has relevance to a post-quantum lattice-based cryptographic digital signature scheme utilising masking as a countermeasure to side channel attacks.

  Application number: PCT/EP2023/052730

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: Thomas Prest

Title: Lead cryptography researcher

Date: 31 May 2023

Place: Paris, France

Statement by Each Submitter

I, Mélissa Rossi, of ANSSI, 51 Bd de la Tour-Maubourg, 75007 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, 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.

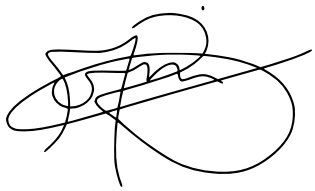
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and 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: Mélissa Rossi

Title: Cryptography researcher

Date: 31 May 2023

Place: Paris, France



Statement by Each Submitter

I, Markku-Juhani O. Saarinen, of PQShield LTD, Prama House, 267 Banbury Rd, Summertown, Oxford OX2 7HT, UK, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;
- ☑ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, may be covered by the following U.S. and/or foreign patents:
  - **UK Patent Application no. 2207808.3:** "Secure processing system and method"
  - **UK Patent Application no. 2211124.9:** "Method and Apparatus for Storing/Recovering a Plurality of Secret Shares"

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: Markku-Juhani O. Saarinen

Title: Staff Cryptography Architect

Date: 31 May 2023

Place: Oxford, UK

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

I, Ali El Kaafarani, of PQShield Ltd, Prama House, 267 Banbury Rd, Summertown, Oxford OX2 7HT, UK, am the owner or authorized representative of the owner (PQShield Ltd, Prama House, 267 Banbury Rd, Summertown, Oxford OX2 7HT, UK) of the following patent(s) and/or patent application(s):

1. **PCT/EP2023/052730:** "Lattice-based cryptographic digital signature scheme utilising masking"
2. **UK Patent Application no. 2207808.3:** "Secure processing system and method"
3. **UK Patent Application no. 2211124.9:** "Method and Apparatus for Storing/Recovering a Plurality of Secret Shares"

and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Raccoon 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, **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: Ali El Kaafarani

Title: Founder & CEO

Date: 31 May 2023

Place: Oxford, UK

DocuSigned by:

837A80E6CE01437...