Statement by Reference/Optimized Implementations’ Owner

I, Alessandro Barenghi, Milano, Italy, 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: Alessandro Barenghi
Title: Professor
Date: 31 May 2023
Place: Milano, Italy
Statement by Reference/Optimized Implementations’ Owner

I, Luke Beckwith, Fairfax, VA, 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: Luke Beckwith

Title: Mr.

Date: 31 May 2023

Place: Fairfax, VA, USA
Statement by Reference/Optimized Implementations’ Owner

I, Kris Gaj, Fairfax, VA, 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: Kris Gaj
Title: Professor
Date: 31 May 2023
Place: Fairfax, VA, USA
Statement by Reference/Optimized Implementations’ Owner

I, Kamyar Mohajerani, Fairfax, VA, USA, am the owner or authorized representative of the owner 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: Kamyar Mohajerani

Title: Graduate Research Assistant

Date: 31 May 2023

Place: Fairfax, VA, USA
Statement by Reference/Optimized Implementations’ Owner

I, Gerardo Pelosi, Milano, Italy, 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: Gerardo Pelosi
Title: Professor
Date: 31 May 2023
Place: Milano, Italy
Statement by Reference/Optimized Implementations’ Owner

I, Robert Wallace, Fairfax, VA, 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: Robert Wallace
Title: Student
Date: 31 May 2023
Place: Fairfax, VA, USA
Statement by EachSubmitter

I, Marco Baldi, of Università Politecnica delle Marche, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Marco Baldi
Title: Professor
Date: 31 May 2023
Place: Ancona, Italy
Statement by Each Submitter

I, Alessandro Barenghi, of Politecnico di Milano, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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 cryptosystems specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.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: Alessandro Barenghi
Title: Professor
Date: 31 May 2023
Place: Milano, Italy
Statement by Each Submitter

I, Luke Beckwith, of George Mason University, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Luke Beckwith
Title: Mr.
Date: 31 May 2023
Place: Fairfax, VA, USA
Statement by Each Submitter

I, Jean-François Biasse, of University of South Florida, do hereby declare that
the cryptosystem, reference implementation, or optimized implementations that
I have submitted, known as LESS, 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 implementa-
   tions that I have submitted, known as LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign
   patent applications may cover the practice of LESS, reference implementa-
   tion 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 dis-
closed 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 evalua-
tion process, and, if my submitted cryptosystem is selected for standardization,
during the lifetime of the standard, modify my submitted cryptosystem’s speci-
fications (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 Sec-
tions 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 ap-
propriate.

Signed: Jean-François Biasse
Title: Associate Professor
Date: 31 May 2023
Place: Tampa, FL, USA
Statement by EachSubmitter

I, Andre Esser, of Technology Innovation Institute, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Andre Esser
Title: Dr.
Date: 31 May 2023
Place: Abu Dhabi, UAE
Statement by EachSubmitter

I, Kris Gaj, of George Mason University, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Kris Gaj
Title: Professor
Date: 31 May 2023
Place: Fairfax, VA, USA
Statement by EachSubmitter

I, Kamyar Mohajerani, of George Mason University, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Kamyar Mohajerani
Title: Graduate Research Assistant
Date: 31 May 2023
Place: Fairfax, VA, USA
Statement by EachSubmitter

I, Gerardo Pelosi, of Politecnico di Milano, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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 cryptosystems specifications (e.g., to protect against a newly discovered vulnerability).

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

I do hereby agree to provide the statements required by Sections 2.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: Gerardo Pelosi
Title: Professor
Date: 31 May 2023
Place: Milano, Italy
Statement by EachSubmitter

I, Edoardo Persichetti, of Università “Sapienza”, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Edoardo Persichetti
Title: Assistant Professor
Date: 31 May 2023
Place: Rome, Italy
Statement by Each Submitter

I, Markku-Juhani 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 LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Markku-Juhani Saarinen  
Title: Staff Cryptography Architect  
Date: 31 May 2023  
Place: Oxford, UK
Statement by EachSubmitter

I, Paolo Santini, of Università Politecnica delle Marche, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, is my 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Paolo Santini
Title: Dr.
Date: 31 May 2023
Place: Ancona, Italy
Statement by Each Submitter

I, Robert Wallace, of George Mason University, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as LESS, 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 LESS;

☐ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of LESS, 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: Robert Wallace
Title: Student
Date: 31 May 2023
Place: Fairfax, VA, USA