I, Jeffrey Hoffstein, of 353 Slater Avenue, Providence, RI 02906 , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, may be covered by the following U.S. and/or foreign patents:
    - Ring-based digital signature and authentication method and apparatus, U.S. Patent publication No.: WO2002009348 A3
    - Digital signature and authentication method and apparatus, U.S. Patent publication number: US7913088 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:
    - Digital signature method, U.S. Patent Application No. 20150229478

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: Professor of Mathematics, Brown University
Date: 11/4/15
Place: Providence, RI

I, _____ William Whyte____, of _____235 Claflin St, Belmont, MA 02478, USA_____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, may be covered by the following U.S. and/or foreign patents:
    - Ring-based digital signature and authentication method and apparatus, U.S. Patent publication No.: WO2002009348 A3
    - Digital signature and authentication method and apparatus, U.S. Patent publication number: US7913088 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:
    - Digital signature method, U.S. Patent Application No. 20150229478

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: William Whyte
Title: CTO, Onboard Security
Date: 2017-11-22
Place: Wilmington, MA

I, *William Whyte*, of *187 Ballardvale st. suite A202, Wilmington MA 01887, U.S.,* am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s):

- Ring-based digital signature and authentication method and apparatus, U.S. Patent publication No.: WO2002009348 A3
- Digital signature and authentication method and apparatus, U.S. Patent publication number: US7913088 B2
- Digital signature method, U.S. Patent Application No. 20150229478

and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as *pqNTRUSign* 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 11 discovered vulnerability) for incorporation into the standard.

Signed: William Whyte
Title: CTO, Onboard Security
Date: 2017-11-22
Place: Wilmington, MA

I, Zhenfei Zhang, 187 Ballardvale st. Suite A202, Wilmington MA 01887, U.S., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, may be covered by the following U.S. and/or foreign patents:
    - Ring-based digital signature and authentication method and apparatus, U.S. Patent publication No.: WO2002009348 A3
    - Digital signature and authentication method and apparatus, U.S. Patent publication number: US7913088 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:
    - Digital signature method, U.S. Patent Application No. 20150229478

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.

I, *Zhenfei Zhang, 187 Ballardvale st. suite A202, Wilmington MA 01887, U.S.*, 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:

Title: Senior Research Scientist, Onboard Security

Date: Nov 30, 2017

Place: 187 Ballardvale st. Suite 202A, Wilmington MA 01887, U.S.

Cong Chen

187 Ballardvale Street, Suite A202
Wilmington, MA 01887

I, _____ (print submitter's full name) _____, of _____(print full postal address)_____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *pqNTRUSign*, may be covered by the following U.S. and/or foreign patents:
    - Ring-based digital signature and authentication method and apparatus, U.S. Patent publication No.: WO2002009348 A3
    - Digital signature and authentication method and apparatus, U.S. Patent publication number: US7913088 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:
    - Digital signature method, U.S. Patent Application No. 20150229478

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).

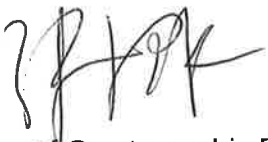
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, 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: Cong Chen
Title: Research Engineer
Date: 11/08/2017
Place: Onboard Security, Wilmington, MA

pqNTRUSign

I, *Zhenfei Zhang, 187 Ballardvale st. suite A202, Wilmington MA 01887, U.S.*, 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: Director of Cryptographic Research, Onboard Security

Date: May 1, 2018

Place: 187 Ballardvale st. Wilmington MA 01887, U.S.