Statement by Each Submitter

I, Daniel J. Bernstein*, of* CS, 851 S. Morgan (M/C 152), Chicago, IL 60607-7053*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* NTRU Prime*, 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* NTRU Prime *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* _____ *may be covered by the following U.S. and/or foreign patents:* _____
  - ☐ *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:* _____

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: D. J. Bernstein

Title: Research Professor

Date: 14 March 2018

Place: Eindhoven

Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Daniel J. Bernstein, (CS, 851 S. Morgan (M/C 152), Chicago, IL 60607-7053), *am the owner or authorized representative of the owner* Daniel J. Bernstein *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: D. J. Bernstein

Title: Research Professor

Date: 14 March 2018

Place: Eindhoven

Statement by Each Submitter

I, Chitchanok Chuengsatiansup, *of* INRIA and ENS de Lyon, 46 allée d'Italie, 69364 Lyon, FR, *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTRU Prime**, *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* **NTRU Prime** *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* _____ *may be covered by the following U.S. and/or foreign patents:* _____
- ☐ *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:* _____

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: Chitchanok Chuengsatiansup

Title: Dr.

Date: 16 March 2018

Place: Lyon, France

Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Chitchanok Chuengsatiansup, INRIA and ENS de Lyon, 46 allée d'Italie, 69364 Lyon, FR, *am the owner or authorized representative of the owner* Chitchanok Chuengsatiansup *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: Chitchanok Chuengsatiansup

Title: Dr.

Date: 16 March 2018

Place: Lyon, France

Statement by Each Submitter

I, TANJA LANGE *, of* TU/e, POSTBUS 513, 5600MB EINDHOVEN, NL *, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTRU Prime** *, 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* **NTRU Prime** *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* _____ *may be covered by the following U.S. and/or foreign patents:* _____
- ☐ *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:* _____

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: T. Lange

Title: PROFESSOR

Date: 14 MAR 2018

Place: EINDHOVEN

Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, TANJA LANGE, TU/e, POSTBUS 513, EINDHOVEN NL, *am the owner or authorized representative of the owner* TANJA LANGE *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: Tanja Lange

Title: PROFESSOR

Date: 14 MAR 2018

Place: EINDHOVEN

Statement by Each Submitter

I, Christine van Vredendaal *, of* TUE, Den Dolech 2, 5612 AZ Eindhoven, NL *, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* NTRU Prime *, 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* NTRU Prime *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* _____ *may be covered by the following U.S. and/or foreign patents:* _____
  - ☐ *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:* _____

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: C. van Vredendaal

Title: ~~PhD Student~~ Ir.

Date: 14-03-2018

Place: Eindhoven, NL

Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Christine van Vredendaal. TUE, Den Dolech 2, 5612 AZ Eindhoven, NL. *am the owner or authorized representative of the owner* Christine van Vredendaal *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: C. van Vredendaal

Title: Ir.

Date: 14-03-2018

Place: Eindhoven, NL