2.D.1 Statement by Each Submitter

I, BASIL HESS, of HAMMERSTRASSE 28, 8008 ZURICH, SWITZERLAND, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SUPERSINGULAR ISOGENY KEY ENCAPSULATION, 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 SUPERSINGULAR ISOGENY KEY ENCAPSULATION; 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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*

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

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

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

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

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances

made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Cryptography Engineer
Date: 24 November 2017
Place: Zurich, Switzerland

2.D.1 Statement by Each Submitter

I, Craig Costello, of One Microsoft Way, Redmond, WA, 98052, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SIKE – Supersingular isogeny key encapsulation, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

> **X** *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 SIKE – Supersingular isogeny key encapsulation.*

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

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

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

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

Signed:

Title: Dr Craig Costello
Date: 04/17/18
Place: Redmond, Washington

2.D.1 Statement by Each Submitter

I, *Luca De Feo, of Université Paris Saclay, UVSQ, 45 avenue des États Unis, 78035 Versailles, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SIKE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that:

> *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SIKE.*

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

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

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

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

Signed: Luca De Feo
Title: Mr.
Date: 11/20/2017
Place: Versailles

2.D.1 Statement by Each Submitter

I, _David Jao_, of _348 Cavendish Dr Waterloo ON Canada_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SIKE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____ SIKE_____

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: _Associate Prof. Univ. of Waterloo_

Date: _4/11/18_

Place: _Ft. Lauderdale, FL_

2.D.1 Statement by Each Submitter

I, **Reza Azarderakhsh**, of *777 Glades Rd, EE 314, Boca Raton, FL 33431, Florida Atlantic University*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Supersingular Isogeny Key Encapsulation**, 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 **Supersingular Isogeny Key Encapsulation** _____; **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable) _____ ;

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

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

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

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

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived

cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Assistant Professor

Date: 09/29/2017

Place: Boca Raton, FL

2.D.1 Statement by Each Submitter

I, _MATTHEW CAMPAGNA_ _15128 Sunrise Dr, BAINBRIDGE ISLAND, WA_, do hereby declare
that the cryptosystem, reference implementation, or optimized implementations that I have
submitted, known as SIKE, is my own original work, or if submitted jointly with others, is the
original work of the joint submitters.

I further declare that:

- I do not hold and do not intend to hold any patent or patent application with a claim
  which may cover the cryptosystem, reference implementation, or optimized
  implementations that I have submitted, known as _____ SIKE_____

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: _PRINCIPLE SECURITY ENGINEER, AWS_

Date: _4/10/18_

Place: _Ft. LAUDERDALE, FL U.S._

2.D.1 Statement by Each Submitter

I, **Amir Jalali**, of **777 Glades Rd, EE 307, Boca Raton, FL 33431, Florida Atlantic University**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Supersingular Isogeny Key Encapsulation**, 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 **Supersingular Isogeny Key Encapsulation** ____; **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 ____ (print name of cryptosystem) ____, may be covered by the following U.S. and/or foreign patents: ____ (describe and enumerate or state "none" if applicable) ____ ;

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

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

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

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

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived

cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Ph.D. Candidate in Computer Science and Engineering
Date: 11/20/2017
Place: Boca Raton, FL

2.D.1 Statement by Each Submitter

I, BASIL HESS, of HAMMERSTRASSE 28, 8008 ZURICH, SWITZERLAND, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SUPERSINGULAR ISOGENY KEY ENCAPSULATION, 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 SUPERSINGULAR ISOGENY KEY ENCAPSULATION;* **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*

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

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

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

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

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

made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

Title: Cryptography Engineer
Date: 24 November 2017
Place: Zurich, Switzerland

2.D.1 Statement by Each Submitter

I, Brian Koziel of 809 Wildrye Dr, Plano, TX 75074, USA , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular Isogeny Key Encapsulation, 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 Supersingular Isogeny Key Encapsulation; **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
> *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.*

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

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

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

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

made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: *Brian Taylor*

Title: Supersingular Isogeny Key Encapsulation (SIKE)

Date: 3/19/2018

Place: Dallas, TX

2.D.1 Statement by Each Submitter

I, Brian Koziel of 809 Wildrye Dr, Plano, TX 75074, USA , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular Isogeny Key Encapsulation, 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 Supersingular Isogeny Key Encapsulation; **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
> *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.*

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

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

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

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

made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: *[signature]*
Title: Supersingular Isogeny Key Encapsulation (SIKE)
Date: 3/14/2018
Place: Dallas, TX

2.D.1 Statement by Each Submitter

I, _BRIAN A. LAMACCHIA_ , of _14150 NE 20TH S) STE F-1 #246, BELLEVUE, WA 98007_ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _SIKE_ , 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
SIKE ; **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 in the Call For Proposals for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

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

the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: [signature]

Title: DISTINGUISHED ENGINEER MICROSOFT CORPORATION

Date: 9/29/17

Place: REDMOND, WA

2.D.1 Statement by Each Submitter

I, *Patrick Longa*, of *One Microsoft Way, Redmond, WA, 98052, USA*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as *SIKE*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

> **X**   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 SIKE.

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

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

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

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

Signed:

Title: Dr.
Date: February 8, 2018
Place: Redmond, Washington

2.D.1 Statement by Each Submitter

I, Michael Naehrig, of 23426 NE 29th PL, Sammamish, WA 98074, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular Isogeny Key Encapsulation -- SIKE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

> **X** 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 SIKE.

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: *Michael Naehrig*
Title: Dr.
Date: 09/27/2017
Place: Redmond, WA

2.D.1 Statement by Each Submitter

I, Joost Renes, of Radboud University, Toernooiveld 212, 6525EC Nijmegen, The Netherlands, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular Isogeny Key Encapsulation, 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 Supersingular Isogeny Key Encapsulation; **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 Supersingular Isogeny Key Encapsulation, may be covered by the following U.S. and/or foreign patents: none;

☐ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: none.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem'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: *[signature]*
Title:
Date: 09/22/2017
Place: REDMOND

2.D.1 Statement by Each Submitter

I, Vladimir Soukharev, of 20 Frances Crescent, Toronto, ON, M1S 2E5, Canada, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular isogeny key encapsulation, 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 Supersingular isogeny key encapsulation;* **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*

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

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

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

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

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

made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: *(signature)*   (Vladimir Soukharev)

Title: Cryptographer

Date: December 1, 2017

Place: Toronto, ON, Canada

2.D.1 Statement by Each Submitter

I, _____David Urbanik_____, of __200 University Ave. W, Waterloo, ON, N2L 3G1, Canada__ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as __SIKE__, 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 __SIKE__.

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

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

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

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

Signed:

Title: Mr.
Date: Sat. Nov. 25th, 2017
Place: University of Waterloo, Waterloo ON, Canada

2.D.1 Statement by Each Submitter

I, Vladimir Soukharev, of 20 Frances Crescent, Toronto, ON, M1S 2E5, Canada, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Supersingular isogeny key encapsulation, 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 Supersingular isogeny key encapsulation; **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 _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*

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

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

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

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

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

made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: (Vladimir Soukharev)
Title: Cryptographer
Date: December 1, 2017
Place: Toronto, ON, Canada

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, _BRIAN A. LAMACCHIA_ , of _1 MICROSOFT WAY, REDMOND, WA 98052_ , 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): _US 7499544 assigned to Microsoft_, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as _SIKE_ 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):

      X   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: _[signature]_
Title: _DISTINGUISHED ENGINEER, MICROSOFT CORPORATION_
Date: _9/29/17_
Place: _REDMOND, WA_

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, Mohammed Muraj, of InfoSec Global Inc., am the authorized representative of the owner, InfoSec Global Inc., of the following patent(s) and/or patent application(s): US2018/0323973A1 and CA2984390, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as SIKE 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:
Title: General Counsel
Date: November 19, 2018
Place: Toronto, Ontario, Canada

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)
The following must also be included:

I, Brian Koziel , 809 Wildrye Dr, Plano, TX 75074, 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: *Brian Koziel*
Title: Super singular Isogeny Key Encapsulation (SIKE)
Date: 3/19/2018
Place Dallas, TX

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

The following must also be included:

I, Amir Jalali, **777 Glades Rd, EE 307, Boca Raton, FL 33431, Florida Atlantic University,** *am 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: Ph.D. Candidate in Computer Science and Engineering
Date: 11/20/2017
Place: Boca Raton, FL

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

The following must also be included:

*I, Reza Azarderakhsh, **777 Glades Rd, EE 314, Boca Raton, FL 33431, Florida Atlantic University**, 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: Assistant Professor
Date: 09/29/2017
Place: Boca Raton, FL

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

The following must also be included:

I, Patrick Longa, One Microsoft Way, Redmond, WA, 98052, USA, am the owner or authorized representative of the owner Microsoft Corporation of the submitted reference implementation and optimized implementations of SIKE 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: Dr.
Date: February 08, 2018
Place: Redmond, Washington

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

The following must also be included:

I, Vladimir Soukharev, of 20 Frances Crescent, Toronto, ON, M1S 2E5, Canada, 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: ~~[signature]~~   *(Vladimir Soukharev)*
Title: Cryptographer
Date: December 1, 2017
Place: Toronto, ON, Canada

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

The following must also be included:

I, BASIL HESS, HAMMERSTRASSE 28, 8008 ZURICH, SWITZERLAND, 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: Cryptography Engineer
Date: 24 November 2017
Place: Zurich, Swizerland

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)
The following must also be included:

I, Brian Koziel , 809 Wildrye Dr, Plano, TX 75074, 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: *Brian Koziel*
Title: Supersingular Isogeny Key Encapsulation (SIKE)
Date: 3/19/2018
Place Dallas, TX

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

The following must also be included:

I, Vladimir Soukharev, of 20 Frances Crescent, Toronto, ON, M1S 2E5, Canada, 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: *(Vladimir Soukharev)*
Title: Cryptographer
Date: December 1, 2017
Place: Toronto, ON, Canada

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

The following must also be included:

I, BASIL HESS, of HAMMERSTRASSE 28, 8008 ZURICH, SWITZERLAND, 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: Cryptography Engineer
Date: 24 November 2017
Place: Zurich, Switzerland