

## 2.D.1 Statement by Each Submitter

*I, **Carsten Baum**, of Anker Englands Vej 101, 2800 Kongens Lyngby, Denmark , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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**)\_\_\_\_\_ ;*

*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: Associate Professor*

*Date: 2023/24/05*

*Place: Copenhagen, Denmark*

## 2.D.1 Statement by Each Submitter

I, **Christian Majenz**, of Anker Englands Vej 101, 2800 Kongens Lyngby, Denmark , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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**) \_\_\_\_\_ ;

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: Associate Professor*

*Date: 2023/25/05*

*Place: Copenhagen, Denmark*

## 2.D.1 Statement by Each Submitter

*I, Christian Rechberger, of Institute of Applied Information Processing and Communications, Technical University of Graz, Inffeldgasse 16a, Graz, Austria, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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**)\_\_\_\_\_ ;*

*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: Professor*

*Date: 24 May, 2023*

*Place: Graz, Austria*

A handwritten signature in blue ink, consisting of two distinct parts. The first part is a cursive 'A' followed by a horizontal line. The second part is a larger, more complex cursive signature that appears to be 'R' followed by several loops and a horizontal line.

## 2.D.1 Statement by Each Submitter

*I, Cyprien Delpuch de Saint Guilhem, of Kasteelpark Arenberg 10 bus 2452, Leuven, Belgium, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST; 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) \_\_\_\_;*
- 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:

A handwritten signature in blue ink, appearing to read "Gertjan de Jongh", with a horizontal line drawn through it.

Title: FWO Postdoctoral Fellow

Date: 25 May, 2023

Place: Leuven, Belgium



## 2.D.1 Statement by Each Submitter

*I, Emanuela Orsini, of Department of Computing Sciences, Bocconi University, Via Sarfatti 25, 20100 Milano, Italy, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

- I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST; **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**)\_\_\_\_\_ ;*
- 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: 27/05/2023*

*Place: Milano, Italy*

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

The following must also be included:

*I, Lawrence Roy, of Department of Computer Science, Aarhus University, Åbogade 34, 8200 Aarhus N, Denmark, 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: *Lawrence Roy*

Title: Postdoc Researcher

Date: 2023-05-31

Place: Aarhus, Denmark

## 2.D.1 Statement by Each Submitter

*I, Lawrence Roy, of Department of Computer Science, Aarhus University, Åbogade 34, 8200 Aarhus N, Denmark, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST; 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)\_\_\_\_ ;*

*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: *Laurance Roy*

Title: Postdoc Researcher

Date: 2023-05-31

Place: Aarhus, Denmark

## 2.D.1 Statement by Each Submitter

I, **Lennart Braun**, of Aarhus University, Åbogade 34, 8200 Aarhus N, DENMARK, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**;  
**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**) \_\_\_\_\_ ;
- 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: Lennart Braun  
Title: PhD Student  
Date: 2023-05-24  
Place: Aarhus, Denmark



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

The following must also be included:

*I, Lennart Braun , Aarhus University, Abogade 34, 8200 Aarhus N, DENMARK , 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: Lennart Braun  
Title: PhD Student  
Date: 2023-05-24  
Place: Aarhus, Denmark





### 2.D.1 Statement by Each Submitter

**I, Michael Klooss, of Department of Computer Science, Aalto University, Konemiehentie 2, 02150, Espoo, Finland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.**

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as FAEST; 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) \_\_\_\_\_ ;*

*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: Postdoctoral Researcher*

*Date: 2023-05-24*

*Place: Espoo, Finland*

## 2.D.1 Statement by Each Submitter

*I, Peter Scholl, of Department of Computer Science, Aarhus University, Åbogade 34, Aarhus, Denmark, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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**) \_\_\_\_\_ ;*
- 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: Associate Professor  
Date: 24 May, 2023  
Place: Aarhus, Denmark

## 2.D.1 Statement by Each Submitter

*I, Sebastian Ramacher, of AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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**) \_\_\_\_\_ ;*

*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:* Dr. Sebastian Ramacher, i.A.

*Title:* Scientist

*Date:* 24/5/2023

*Place:* Vienna, Austria

*Signed:* Dr. Martin Stierle, i.V.

*Title:* Head of Competence Unit Security & Communications Technologies

*Date:* 24/5/2023

*Place:* Vienna, Austria



**AIT Austrian Institute of Technology GmbH**  
Giefinggasse 4 | 1210 Wien, Austria  
T +43 (0) 50550-0 | F +43 (0) 50550-2201  
office@ait.ac.at | www.ait.ac.at

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

The following must also be included:

*I, Sebastian Ramacher, AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria, am the owner or authorized representative of the owner AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210, Vienna, Austria 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:* Dr. Sebastian Ramacher , i.A.

*Title:* Scientist

*Date:* 24/5/2023

*Place:* Vienna, Austria

*Signed:* Dr. Martin Stierle , i.V.

*Title:* Head of Competence Unit Security & Communications Technologies

*Date:* 24/5/2023

*Place:* Vienna, Austria



**AIT Austrian Institute of Technology GmbH**  
Giefinggasse 4 | 1210 Wien, Austria  
T +43 (0) 50550-0 | F +43 (0) 50550-2201  
office@ait.ac.at | www.ait.ac.at

## 2.D.1 Statement by Each Submitter

*I, Shibam Mukherjee, of Institute of Applied Information Processing and Communications, Technical University of Graz, Inffeldgasse 16a, Graz, Austria, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

*I further declare that (check one):*

*I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **FAEST**; **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) \_\_\_\_\_ ;*

*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:

Date: 24 May, 2023

Place: Graz, Austria



sign. Head of Institute, Stefan MANGARD

Institut f. Angewandte Informations-  
verarbeitung u. Kommunikations-  
technologie  
Technische Universität Graz  
Inffeldgasse 16a  
A-8010 Graz / Austria

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

The following must also be included:

*I, Shibam Mukherjee, Institute of Applied Information Processing and Communications, Technical University of Graz, Inffeldgasse 16a, Graz, Austria, 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:

Date: 24 May, 2023

Place: Graz, Austria



sign. Head of Institute, Stefan MANGARD

Institut f. Angewandte Informations-  
verarbeitung u. Kommunikations-  
technologie  
Technische Universität Graz  
Inffeldgasse 16a  
A-8010 Graz / Austria