

## 2.D.1 Statement by Each Submitter

*I, **Basil Hess**, of **IBM Research, Saeumerstrasse 4, 8803 Rueschlikon, Switzerland**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **MAYO**, 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 **MAYO**.*

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*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

Date: *28 Feb 2023*

Place: *Zurich, Switzerland*

## 2.D.1 Statement by Each Submitter

*I, **Fabio Campos**, of **Kolpingstr. 10d, 65239 Hohehim, Germany**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **MAYO**, 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 **MAYO**; **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 **MAYO**, may be covered by the following U.S. and/or foreign patents: **none**;*
- 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:*

*Title:*

*Date:*

*Place:*

*Fabio Campos*

*27/02/2023*

*Hochheim, Germany*

A handwritten signature in black ink, appearing to read 'Campos', written in a cursive style.

## 2.D.1 Statement by Each Submitter

*I, **Matthias Julius Kannwischer**, of **Institute of Information Science, Academia Sinica, No. 128, Section 2, Academia Rd, Nangang District, Taipei City, 11529, Taiwan**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **MAYO**, 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 **MAYO**; **OR** (check one or both of the following):*

*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: Matthias Julius Kannwischer

Date: 01 March 2023

Place: Taipei, Taiwan

## 2.D.1 Statement by Each Submitter

*I, **Claudia Sofia Celi Ramos**, of **Travessa das Parreiras 52, 150-252, Lisbon, Portugal**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **MAYO**, 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 **MAYO**; **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 **MAYO**, may be covered by the following U.S. and/or foreign patents: **None**;*
- *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:*

*Title: Claudia Sofia Celi Ramos*

*Date: 27/02/2023*

*Place: Lisbon, Portugal*

A handwritten signature in black ink that reads "Sofia Celi". The signature is written in a cursive style with a horizontal line underneath the name.

## 2.D.1 Statement by Each Submitter

I, Ward Beullens, of Saumerstrasse 4, 8803 Ruschlikon, Canton Zurich, Switzerland, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as MAYO, 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 MAYO; **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 MAYO, may be covered by the following U.S. and/or foreign patents: None;
  - 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:*

*Title:* Ward Beullens

*Date:* 27/02/2023

*Place:* Ruschlikon,  
Switzerland

A handwritten signature in black ink, appearing to read 'Beullens', written in a cursive style with a long horizontal stroke extending to the left.



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

The following must also be included:

*I, Basil Hess, IBM Research, Saeumerstrasse 4, 8803 Rueschlikon, Switzerland, 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: Research Engineer, IBM Research*

*Date: 28 Feb 2023*

*Place: Zurich, Switzerland*

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

The following must also be included:

*I, Fabio Campos, Kolpingstr. 10d, 65239, Hochheim, Germany, 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: Fabio Campos

Date: 27/02/2023

Place: Hochheim, Germany

A handwritten signature in black ink that reads "Campos". The signature is written in a cursive style with a large initial 'C'.

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

The following must also be included:

*I, **Matthias Julius Kannwischer** , **Institute of Information Science, Academia Sinica, No. 128, Section 2, Academia Rd, Nangang District, Taipei City, 11529, Taiwan** , 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: Matthias Julius Kannwischer

Date: 01 March 2023

Place: Taipei, Taiwan

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

The following must also be included:

*I, **Claudia Sofia Celi Ramos** , **Travessa das Parreiras 52, 150-252, Lisbon, Portugal** , 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: *Claudia Sofia Celi Ramos*

Date: *27/02/2023*

Place: *Lisbon, Portugal*

A handwritten signature in black ink that reads "Sofia Celi". The signature is written in a cursive style with a horizontal line underneath the name.

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

The following must also be included:

*I, **Ward Beullens**, Saumerstasse 4, 8803 Ruschlikon, Canton Zurich, Switzerland, 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: Ward Beullens  
Date: 27/02/2030  
Place: Ruschlikon,  
Switzerland

A handwritten signature in black ink, appearing to read 'Beullens', with a stylized flourish at the end.