2.D.1 Statement by Each Submitter

I, ALESSANDRO BARENGHI of POLITECNICO DI MILANO,
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.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

Title: ASSOCIATE PROFESSOR

Date: 30 MARCH 2023

Place: MILAN
Since we did not identify a patent and we are not planning on filing any, we omit this statement.

2.D.3 Statement by Reference/Optimized Implementations’ Owner(s)
I, ALESSANDRO BARONGHI, of POLITÉCNICO DI MILANO, 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: Alando Bonli
Title: ASSOCIATE PROFESSOR
Date: 30th May 2023
Place: MILAN
2.D.1 Statement by Each Submitter

1. **PAVONI ALESSIO**
   of **UNIVERSITA' POLITECNICA DELLE MARCHE**

I hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: **PAVONI ALESSIO**

Title: **ING.**

Date: **30.05.23**

Place: **MONTECRAMARO, ITALY**

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

1. **QUATTRO ALESSIO**
   of **UNIVERSITÀ POLITECNICA DELLE MARCHE**

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: **Reni Alessio**

Title: **INO**

Date: **30.09.23**

Place: **MONTEGRANARDO, ITALY**
2.D.1 Statement by Each Submitter

I, Antonia Wachter-Zeh of Technical University of Munich do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: Prof. Dr.
Date: 30.5.23
Place: München
Since we did not identify a patent and we are not planning on filing any, we omit this statement.

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)
I, Antonia Wachter-Zeh
of Technical University of Munich,
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: A. Wachter-Zeh

Title: Prof. Dr.
Date: 30.5.23
Place: München
2.D.1 Statement by EachSubmitter

I, Felice Manganiello of Clemson University,
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: Dr.

Date: May 30, 2023

Place: Greenville

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, FELICIE MANGANIEU
of CLEMSON 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: [Signature]
Title: Dr.
Date: May 30, 2023
Place: Greenville
2.D.1 Statement by Each Submitter

I, Freeman Slaughter
of Clemson University, Clemson SC, USA

do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: Rev.

Date: Tues, 30th May 2023

Place: Clemson

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, Freeman Slaughter,
of Clemson University, Clemson SC, USA,
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: Rev.

Date: Tues, 30th May 2023

Place: Clemson
2.D.1 Statement by Each Submitter

I, \underline{GERARDO PELOSI},
of \underline{POLITECNICO DI MILANO, ITALY},
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that:

\(\times\) 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 CROSS;

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: \underline{GERARDO PELOSI}

Title: \underline{ASSOCIATE PROFESSOR, PH.D.}

Date: \underline{30 MAY 2023}

Place: \underline{MILAN, ITALY}

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, ____________________________,

of ____________________________,

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: ____________________________

Date: ____________________________

Place: ____________________________
2.D.1 Statement by Each Submitter

I, Jonas Schupp
of Technical University of Munich (TUM),
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: J. Schupp
Title:
Date: 30.05.2023
Place: Munich, Germany

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, [Name],
of [Institution]

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: [Signature]

Title:

Date: 30.05.2023

Place: Munich, Germany
2.D.1 Statement by Each Submitter

I, Marco Baldi
Università Politecnica delle Marche, Ancona, Italy

do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: Prof.
Date: 30 May 2023
Place: Ancona, Italy

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, Marco Baldi of Università Politecnica delle Marche, Ancona, Italy 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: [Signature]

Title: Prof.

Date: 30 May 2023

Place: Ancona, Italy
2.D.1 Statement by Each Submitter

1. Paolo Santini
   Università Politecnica delle Marche

I hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS.

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: Paolo Santini

Title: Dr

Date: May 30, 2023

Place: Ancona, Italy

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

1. Paolo Santini
   of Università Politecnica delle Marche

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: Paolo Santini

Title: Dr

Date: May 30, 2023

Place: Ancona, Italy
2.D.1 Statement by EachSubmitter

I, Patrick Karl
of Technical University of Munich, Germany

do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: Patrick Karl

Title:

Date: 30.05.2023

Place: Munich, Germany

Since we did not identify a patent and we are not planning on filing any, we omit this statement.

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

I, Patrick Kael, of Technical University of Munich, Germany, 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: Patrick Kael

Title:

Date: 30.05.2023

Place: Munich, Germany
2.D.1 Statement by EachSubmitter

I, Sebastian Bilzer

of Technical University of Munich

do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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: S. Bilzer

Title:

Date: 25.05.2023

Place: Munich, Germany
Since we did not identify a patent and we are not planning on filing any, we omit this statement.

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)
I, Sebastian Bier of Technical University of Munich, 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: [Signature]

Title:

Date: 25.05.2023

Place: Munich, Germany
2.D.1 Statement by Each Submitter

I, [Name],
of [Institution],
do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CROSS, 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 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 CROSS;

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:

Dr.

Date:

25. 05. 23

Place:

Munich, Germany
Since we did not identify a patent and we are not planning on filing any, we omit this statement.

2.D.3 Statement by Reference/Optimized Implementations’ Owner(s)
I, Violetta Wegler
of Technical University of Munich,
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: Dr.

Date: 25.05.23

Place: Munich, Germany