May 31, 2023

National Institute of Standards and Technology U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Additional Digital Signature Schemes for Post-Quantum Cryptography Standardization Process Statement of Submitter (Section 2.D.1)

Dear Madam or Sir:

I, **Luk Bettale, Ph.D.**, R&D Cryptography and Security engineer, 2 Pl. Samuel de Champlain, 92400 Courbevoie, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Biscuit DSS**, is my own original work, or if submitted jointly with others**-Biscuit DSS** 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 Biscuit DSS.

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).

Biscuit-DSS Statement of Submitter Page

Luk Bettale, Ph.D.

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 by:

Name: **Luk Bettale***, Ph.D.*
Title: R&D Cryptography and Security Engineer

*Date:*5/31/2023
Place: Courbevoie, France

2 Pl. Samuel de Champlain, 92400 Courbevoie, FRANCE

May 31, 2023

National Institute of Standards and Technology U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Additional Digital Signature Schemes for Post-Quantum Cryptography Standardization Process Statement of Submitter (Section 2.D.1)

Dear Madam or Sir:

I, **Delaram Kahrobaei, Ph.D.**, Professor, Mathematics and Computer Science, Queens College, The City University of New York, of 65-30 Kissena Boulevard, Flushing, New York 11367, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Biscuit DSS,** is my own original work, or if submitted jointly with others**-Biscuit DSS** 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 ***Biscuit DSS****.*

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).

DSA Statement of Submitter Page

Delaram Kahrobaei, Ph.D.

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 by:

Name: Delaram Kahrobaei, Ph.D.
Title: Professor, Department of Mathematics and Computer Science

Date: 5/31/2023

Place: New York, NY

Departments of Mathematics and Computer Science, Queens College, The City University of New York 65-30 Kissena Boulevard, Flushing, New York, 11367

May 31, 2023

National Institute of Standards and Technology U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Additional Digital Signature Schemes for Post-Quantum Cryptography Standardization Process Statement of Submitter (Section 2.D.1)

Dear Madam or Sir:

I, **Ludovic Perret, Ph.D.**, Associate Professor, Sorbonne University, CNRS/LIP6/PolSys, Boite courier 169, 4, Place Jussieu, F-75252 Paris cedex 5, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Biscuit DSS**, is my own original work, or if submitted jointly with others**-Biscuit DSS** 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 ***Biscuit DSS****.*

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).

Biscuit-DSS Statement of Submitter Page

Ludovic Perret, Ph.D.

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 by:

Name:Ludovic Perret, Ph.D.
Title: Associate Professor, Department of Computer Science

Date: 5/31/2023
Place: Paris, France

Sorbonne University, CNRS/LIP6/PolSys, Boite courier 169, 4, Place Jussieu, F-75252 Paris cedex 5, France

May 31, 2023

National Institute of Standards and Technology U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Additional Digital Signature Schemes for Post-Quantum Cryptography Standardization Process Statement of Submitter (Section 2.D.1)

Dear Madam or Sir:

I, **Javier Verbel, Ph.D.**, Senior Cryptanalyst, Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, UAE, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Biscuit DSS**, is my own original work, or if submitted jointly with others**-Biscuit DSS** 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 ***Biscuit DSS****.*

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).

Biscuit-DSS Statement of Submitter Page

Javier Verbel, Ph.D.

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 by:

Name: **Javier Verbel***, Ph.D.*
*Title:*Senior Cryptanalyst

Date: 5/31/2023
Place: Masdar City, Abu Dhabi, UAE

Technology Innovation Institute, P.O.Box: 9639, Masdar City, Abu Dhabi, UAE

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

The following must also be included:

*I, **Luk BETTALE**, **IDEMIA - 2 Pl Samuel de Champlain 92400 Courbevoie**, 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: PhD, R&D Cryptography and Security Engineer
Date: June 1st 2023
Place: Courbevoie