2.D.1 Statement by Each Submitter

I, Gustavo Banegas of Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB EINDHOVEN, The Netherlands, *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

✓ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***OR*** *(check one or both of the following):*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*

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

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

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

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

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

Signed:
Title: PhD Student
Date: 11/25/2017
Place: Eindhoven

2.D.1 Statement by Each Submitter

I, Edoardo Persichetti, of Florida Atlantic University, Department of Mathematical Sciences, 777 Glades Rd, Boca Raton 33431 FL, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as DAGS, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- ☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as DAGS;* ***OR*** *(check one or both of the following):*

  - □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
  - □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:

Title: Assistant Professor
Date: 4/16/18
Place: Boca Raton, FL

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

The following must also be included:

I, Edoardo Persichetti, of Florida Atlantic University, Department of Mathematical Sciences, 777 Glades Rd, Boca Raton 33431 FL, am the owner or authorized representative of the submitted reference implementation and optimized implementations of DAGS and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title: Assistant Professor
Date: 4/16/18
Place: Boca Raton, FL

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

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

I, Gustavo Banegas of Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB EINDHOVEN, The Netherlands, *am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as* ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

[✓ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**]

- *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:
Title: PhD Student
Date: 11/25/2017
Place: Eindhoven

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

The following must also be included:

I, Gustavo Banegas of Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB EINDHOVEN, The Netherlands, *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 of* ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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 Student
Date: 11/25/2017
Place: Eindhoven

2.D.1 Statement by Each Submitter

I, PAULO SERGIO LICCIARDI MESSEDER BARRETO, of the Institute of Technology - University of Washington Tacoma - Campus Box 358426 - 1900 Commerce Street - Tacoma WA 98402-3100, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**; **OR** (check one or both of the following):

□ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;

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

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

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

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

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

Signed:

Title: Prof. Dr., PhD

Date: 11/19/2017

Place: Tacoma, WA, USA

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

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

*I, PAULO SERGIO LICCIARDI MESSEDER BARRETO, of the Institute of Technology - University of Washington Tacoma - Campus Box 358426 - 1900 Commerce Street - Tacoma WA 98402-3100, am the owner of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as **DAGS: Key Encapsulation from Dyadic GS Codes** is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:
Title: Prof. Dr., PhD
Date: 11/19/2017
Place: Tacoma, WA, USA

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

The following must also be included:

I, PAULO SERGIO LICCIARDI MESSEDER BARRETO, of the Institute of Technology - University of Washington Tacoma - Campus Box 358426 - 1900 Commerce Street - Tacoma WA 98402-3100, am the owner of the submitted reference implementation and optimized implementations of ***DAGS: Key Encapsulation from Dyadic GS Codes****, 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: Prof. Dr., PhD

Date: 11/19/2017

Place: Tacoma, WA, USA

2.D.1 Statement by Each Submitter

I, Brice Odilon BOIDJE , of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

✓ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes; OR*** *(check one or both of the following):*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
  I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.
- *I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).*

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

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

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

Signed:

Title: Phd Student
Date: 11/24/17
Place: Dakar-Senegal

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

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

I, Brice Odilon BOIDJE , of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE , and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

- [✓ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**]

- *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: PHD Student
Date: 11/25/17
Place:Dakar-Fann

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

The following must also be included:

I, Brice Odilon BOIDJE , of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, 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 of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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 Student
Date: 11/25/17
Place:Dakar-Fann

2.D.1 Statement by Each Submitter

I, Pierre-Louis Cayrel , of Laboratoire Hubert Curien, 42000 Saint-Etienne, France , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes,** is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☒ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes; OR** (check one or both of the following):

- □ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;
- □ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.

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

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

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

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

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

Signed:

CAYREL

Title: Assistant Professor
Date: 11/27/17
Place: Saint-Etienne

LABORATOIRE HUBERT CURIEN
UMR CNRS 5516 Université Jean Monnet
18 rue Pr. Benoît Lauras - Bât. F
F-42000 SAINT-ETIENNE
(33) 04 77 91 57 80 / Fax (33) 04 77 91 57 81

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

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

I, Pierre-Louis Cayrel , of Laboratoire Hubert Curien, 42000 Saint-Etienne, France , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE , and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

X without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed: CAYREL

Title: Assistant Professor
Date: 11/27/17
Place: Saint-Etienne

LABORATOIRE HUBERT CURIEN
UMR CNRS 5516 Université Jean Monnet
18 rue Pr. Benoît Lauras - Bât. F
F-42000 SAINT-ETIENNE
(33) 04 77 91 57 80 / Fax (33) 04 77 91 57 81

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

The following must also be included:

I, Pierre-Louis Cayrel , of Laboratoire Hubert Curien, 42000 Saint-Etienne, France, 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 of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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: Cayrel

Title: Assistant Professor
Date: 11/27/17
Place: Saint-Etienne

LABORATOIRE HUBERT CURIEN
UMR CNRS 5516 Université Jean Monnet
18 rue Pr. Benoît Lauras - Bât. F
F-42000 SAINT-ETIENNE
(33) 04 77 91 57 80 / Fax (33) 04 77 91 57 81

2.D.1 Statement by Each Submitter

I, Gilbert Ndollane DIONE, of Department of Mathmaticals and Informatics, University Cheikh Anta DIOP of Dakar (UCAD), BP-5005 Dakar-Fann,Dakar,Sénégal, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**; **OR** (check one or both of the following):

□ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;

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

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

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

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

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

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

Signed:

Title: PhD Student
Date: 11/25/17
Place: Dakar-Sénégal

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

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

I, Gilbert Ndollane DIONE, of Departement of Mathmaticals and Informatics, University Cheikh Anta DIOP of Dakar(UCAD), BP-5005 Dakar-Fann,Dakar,Sénégal, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: PhD Student
Date: 11/24/17
Place: Dakar-Sénégal

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

The following must also be included:

I, Gilbert Ndollane DIONE, of Faculté des Sciences et Techniques, Université Cheikh Anta DIOP de Dakar(UCAD), BP-5005 Dakar-Fann,Dakar,Sénégal, 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 ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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 Student
Date: 11/24/17
Place: Dakar-Fann

2.D.1 Statement by Each Submitter

I, Kris Gaj, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030, U.S.A., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

- ✓ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***OR*** *(check one or both of the following):*

  - □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
  - □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:

KGaj

Title: Associate Professor
Date: 11/30/17
Place: Fairfax, VA

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

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

*I, Kris Gaj, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030, U.S.A., am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): **NONE**, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as **DAGS: Key Encapsulation from Dyadic GS Codes** is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

✓ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

KGaj

Title: Associate Professor
Date: 11/30/17
Place: Fairfax, VA

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

The following must also be included:

I, Kris Gaj, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030,U.S.A., am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementation of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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:

KGaj

Title: Associate Professor
Date: 11/30/17
Place: Fairfax, VA

2.D.1 Statement by Each Submitter

I, Cheikh Thiecoumba Gueye, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***OR*** *(check one or both of the following):*

- □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
- □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:

Title: Professor
Date: 11/24/17
Place: Dakar-Senegal

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

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

I, Cheikh Thiecoumba Gueye, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: Professor
Date: 11/24/17
Place:Dakar-Senegal

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

The following must also be included:

I, Cheikh Thiecoumba Gueye, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP:5005 Dakar-Fann, 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 of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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: Professor
Date: 11/24/17
Place: Dakar-Senegal

2.D.1 Statement by Each Submitter

I, Richard Haeussler, graduate student in the Electrical & Computer Engineering Department of George Mason University, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

☒ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***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* ***DAGS: Key Encapsulation from Dyadic GS Codes****, may be covered by the following U.S. and/or foreign patents: NONE ;*
- □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: ____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:
Title: Graduate student GMU
Date: 11/24/2017
Place: ~~Home~~ Alexandria VA

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

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

I, Richard Haeussler, graduate student in the Electrical & Computer Engineering Department of George Mason University, 4400 University Dr, Fairfax VA 22030 am the owner or authorized representative of the owner of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard:*

☒ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:
Title: Graduate Student GMU
Date: 11/29/2017
Place: Alexandria VA

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

The following must also be included:

I, Richard Haeussler, graduate student in the Electrical & Computer Engineering Department of George Mason University, 4400 University Dr. Fairfax VA 22030, 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: Graduate Student- GMU
Date: 11/24/2017
Place: Alexandria, VA

2.D.1 Statement by Each Submitter

I, Jean Belo KLAMTI, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as DAGS: Key Encapsulation from Dyadic GS Codes, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as DAGS: Key Encapsulation from Dyadic GS Codes; OR (check one or both of the following):

- □ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ *(describe and enumerate or state "none" if* applicable)_____ ;
- □ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ *(describe and enumerate or state "none" if applicable)* ______.

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

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

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

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

Signed:

Title: Phd Student
Date: 11/24/17
Place: Dakar-Senegal

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

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

I, Jean Belo KLAMTI, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP: 5005 Dakar-Fann, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as DAGS: Key Encapsulation from Dyadic GS Codes is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

☑ without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, OR

□ under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: Phd student
Date: 11/24/17
Place: Dakar-Senegal

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

The following must also be included:

I, Jean Belo KLAMTI, of Department of Mathematical and Informatics, University Cheikh Anta Diop of Dakar, BP:5005 Dakar-Fann, 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 of DAGS: Key Encapsulation from Dyadic GS Codes 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 Student
Date: 11/24/17
Place: Dakar-Senegal

2.D.1 Statement by Each Submitter

*I, **Ousmane NDIAYE** , of the Department of Math & Info, Cheikh Anta Diop University, Dakar, Senegal, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

☒ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes** **OR** (check one or both of the following):*

- □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
- □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:

Title: PhD, Researcher
Date: 2017/11/24
Place: Dakar, Senegal

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

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

*I, **Ousmane NDIAYE** , of the Department of Math & Info, Cheikh Anta Diop University, Dakar, Senegal , am the owner or authorized representative of the owner of the following patent(s) and/or patent application(s):NONE, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as **DAGS: Key Encapsulation from Dyadic GS Codes** is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☒ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.
I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: PhD, Researcher
Date: 2017/11/24
Place: Dakar, Senegal

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

The following must also be included:

*I, **Ousmane NDIAYE** , of the Department of Math & Info, Cheikh Anta Diop University, Dakar, Senegal, am the owner or authorized representative of the owner of the submitted reference implementation and optimized implementations of **DAGS: Key Encapsulation from Dyadic GS Codes** 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, Researcher
Date: 2017/11/24
Place: Dakar, Senegal

2.D.1 Statement by Each Submitter

I, Duc Tri Nguyen, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030, U.S.A., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

✓ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***OR*** *(check one or both of the following):*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____ (print name of cryptosystem)_____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
- *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.*

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

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

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

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove

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

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

I, Duc Tri Nguyen, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030,U.S.A., am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): **NONE**, *and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as* **DAGS: Key Encapsulation from Dyadic GS Codes** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

✓ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

- *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

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

The following must also be included:

I, Duc Tri Nguyen, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030,U.S.A., am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementation of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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:

Tri

Title: Graduate Research Assistant
Date: 11/30/17
Place: Fairfax, VA

2.D.1 Statement by Each Submitter

I, Edoardo Persichetti, of Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Rd, Boca Raton 33431 FL, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***OR*** *(check one or both of the following):*

- □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____;*
- □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.*

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

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

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

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

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

Signed:

Title: Assistant Professor
Date: 11/23/17
Place: Boca Raton

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

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

I, Edoardo Persichetti, of Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Rd, Boca Raton 33431 FL, USA, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): NONE , and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:

Title: Assistant Professor
Date: 11/23/17
Place: Boca Raton

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

The following must also be included:

I, Edoardo Persichetti, of Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Rd, Boca Raton 33431 FL, USA , am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementation of **DAGS: Key Encapsulation from Dyadic GS Codes** *and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.*

Signed:

Title: Assistant Professor
Date: 11/23/17
Place: Boca Raton

2.D.1 Statement by Each Submitter

I, JEFFERSON EVANDI RICARDINI FERNANDES DE OLIVEIRA, of University of Sao Paulo - Av. Professor Luciano Gualberto, travessa 3, 158 Prédio da Engenharia Elétrica (Bloco C, sala CM-43) 05508-010 – Cidade Universitária – São Paulo- SP – Brazil, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **DAGS: Key Encapsulation from Dyadic GS Codes; OR** (check one or both of the following):

- □ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;
- □ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) ______.

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

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

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

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

Signed: Jefferson E. Ricardini F. de Oliveira
Title: M. Sc.
Date: NOVEMBER, 24, 2017
Place: São Paulo, SP, Brazil

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

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

I, JEFFERSON EVANDI RICARDINI FERNANDES DE OLIVEIRA, of University of Sao Paulo - Av. Professor Luciano Gualberto, travessa 3, 158 Prédio da Engenharia Elétrica (Bloco C, sala CM-43) 05508-010 – Cidade Universitária – São Paulo-SP – Brazil, am the owner of the following patent(s) and/or patent application(s): NONE, *and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as* ***DAGS: Key Encapsulation from Dyadic GS Codes*** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):*

☑ *without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,* **OR**

□ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed: Jefferson E. Ricardini F. de Oliveira

Title: M. Sc.

Date: NOVEMBER, 24, 2017

Place: São Paulo, SP, Brazil

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

The following must also be included:

I, JEFFERSON EVANDI RICARDINI FERNANDES DE OLIVEIRA, of University of Sao Paulo - Av. Professor Luciano Gualberto, travessa 3, 158 Prédio da Engenharia Elétrica (Bloco C, sala CM-43) 05508-010 – Cidade Universitária – São Paulo-SP – Brazil, am the owner of the submitted reference implementation and optimized implementations of ***DAGS: Key Encapsulation from Dyadic GS Codes****, 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: Jefferson E. Ricardini F. de Olíveira
Title: M. Sc.
Date: NOVEMBER, 24, 2014
Place: São Paulo, SP, Brazil

2.D.1 Statement by Each Submitter

I, _____ Richard Haeussler _____, of _____5314 Ridley Court Alexandria VA 22315______, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ DAGS___, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

☑ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____DAGS___* ***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 ____ DAGS____, may be covered by the following U.S. and/or foreign patents: _____ none_____ ;*
- ☐ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ none ______.*

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

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

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

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

Signed:
Title: Student GMU
Date: 4/22/18
Place: Home

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

The following must also be included:

I, Richard Haeussler of 5314 Ridley Court Alexandria VA 22315, *am the owner or authorized representative of the submitted reference implementation and optimized implementations of DAGS 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: Student GMU
Date: 4/22/18
Place: Home

2.D.1 Statement by Each Submitter

I, _____Duc Tri Nguyen_____, of _____10570 Main Street VA 22030______ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ DAGS____, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- ✓ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____ DAGS____; **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 ____ DAGS____, may be covered by the following U.S. and/or foreign patents: _____ None_____ ;
  - I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: _____ None______.

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

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

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

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

Signed:
Title: Student GMU
Date: 4/23/18
Place: Home

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

The following must also be included:

I, Duc Tri Nguyen of 10570 Main Street VA 22030, am the owner or authorized representative of the submitted reference implementation and optimized implementations of DAGS 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: Tri

Title: Student GMU
Date: 4/23/18
Place: Home

2.D.1 Statement by Each Submitter

I, Kris Gaj, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030, U.S.A., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***DAGS: Key Encapsulation from Dyadic GS Codes****, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.*

I further declare that (check one):

- ✓ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***DAGS: Key Encapsulation from Dyadic GS Codes****;* ***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 DAGS may be covered by the following U.S. and/or foreign patents: none;*
  - □ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: none.*

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

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

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

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

Signed:

KGaj

Title: Associate Professor
Date: 11/30/17
Place: Fairfax, VA

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

The following must also be included:

I, Kris Gaj, of Department of Electrical and Computer Engineering, George Mason University, MS 1G5, 4400 University Drive, Fairfax, VA, 22030,U.S.A., am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementation of ***DAGS: Key Encapsulation from Dyadic GS Codes*** *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:

KGaj

Title: Associate Professor
Date: 11/30/17
Place: Fairfax, VA