Name of the proposed cryptosystem:
DME a public key, signature and KEM system based on double exponentiation.

Principal submitter;
Ignacio Luengo
iluengo@ucm.es
+34 913944573, +34 649921423 (mv.)
Universidad Complutense de Madrid, Madrid, Spain
Facultad de Matemáticas, Plaza de Ciencias 3, Madrid 28040 Spain

Names of auxiliary submitters:
Martin Avendaño and Michel Marco.

Name of the inventor
Ignacio Luengo

Name of the owner of the cryptosystem<<.
Universidad Complutense de Madrid

Signature:

2.D.1 Statement by Each Submitter

I, Ignacio Luengo Velasco of Facultad de Matemáticas, Universidad Complutense de Madrid, Plaza de Ciencias 3, Madrid 28040 SPAIN, do hereby declare that the cryptosystem known as DME, is my own original work. 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 ___; **OR***
  - *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as DME, may be covered by the following U.S. and/or foreign patents: none ;*

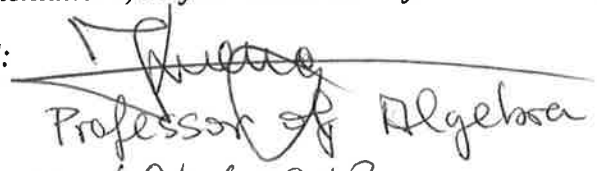
X I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem : P201700779 (Spain)

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

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

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

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

Signed: 

Title: Professor of Algebra

Date: 23/04/2018

Place:- Madrid.

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, José Manuel Pingarrón-Carrazón , of UNIVERSIDAD COMPLUTENSE DE MADRID, located at Avda. Seneca 2, 28040 Madrid (Spain), 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): P201700779 (Spain), and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as DME 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**

X 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: José Manuel Pingarrón Carrazón
Title: Vicechancellor for Knowledge Transfer and Entrepreneurship
Date: Madrid, 26th April, 2018
Place: Madrid (Spain)

SECCIÓN CONTRATOS
Y PATENTES

OTRI - UCM

2.D.1 Statement by Each Submitter

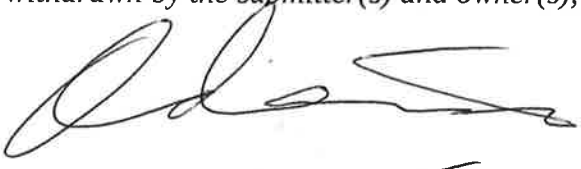
I, Martin Avendaño, of Av. Compromiso de caspe 26 , 1º Drcha. 50002 Zaragoza (Spain), do hereby declare that the reference implementation and optimized implementations that I have submitted, known as DME, is my own original work, is the original work of the joint with Miguel Angel Marco Buzunariz

I further declare that (check one):

X I do not hold and do not intend to hold any patent or patent application with a claim which may cover the reference implementation and optimized implementations that I have submitted, known as DME

- *to the best of my knowledge, the practice of the reference implementation and optimized implementations that I have submitted, known as DME, 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 he reference implementation and optimized implementations that I have submitted, known as DME, may be covered by the following U.S. and/or foreign patents: none*

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment
I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.
Signed:
Title:
Date:
Place:



MARTIN AVENDAÑO
24 / April / 2018

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

The following must also be included:

I, Martin Avendaño, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: 
Title: MARTIN AVENDAÑO
Date: 24 / April / 2018
Place:

2.D.1 Statement by Each Submitter

I, Miguel Angel Marco Buzunariz, of Calle Predicadores 67 1º D, 50003 Zaragoza (Spain), do hereby declare that the reference implementation and optimized implementations that I have submitted, known as DME, is the original work of the joint with Martín Avendaño

I further declare that (check one):

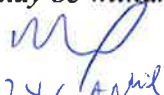
> *X I do not hold and do not intend to hold any patent or patent application with a claim which may cover the reference implementation and optimized implementations that I have submitted, known as DME*
>
> *to the best of my knowledge, the practice of the reference implementation and optimized implementations that I have submitted, known as DME, 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 he reference implementation and optimized implementations that I have submitted, known as DME, may be covered by the following U.S. and/or foreign patents: none*

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

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

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

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

Signed: 
Title:
Date: 24/April/2018
Place: Zaragoza

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

The following must also be included:

I, Miguel Angel Marco Buzunariz , Calle Predicadores 67 1º D, 50003 Zaragoza (Spain) , am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title:
Date: Zaragoza, 24 april 2018
Place: