Statement by Each Submitter

I, _Ludovic PERRET_, _of Sorbonne Université – 4 place Jussieu 75252 Paris Cedex 05, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as_ GeMSS _, 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_ GeMSS _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 _____ may be covered by the following U.S. and/or foreign patents: _____

☐ _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:_ _____

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: Dr (Doctor)
Date: 04/26/2018
Place: Paris

2

Statement by Each Submitter

I, _Jean-Charles FAUGÈRE_, of _Sorbonne Université – 4 place Jussieu 75252 Paris Cedex 05_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _GeMSS_____, 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 _GeMSS_____ 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 _____ may be covered by the following U.S. and/or foreign patents: _____

    ☐ 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: _____

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: SENIOR RESEARCHER
Date: 04/26/2018
Place: Paris

2

Statement by Each Submitter

I, *Jocelyn RYCKEGHEM*, of *Sorbonne Université – 4 place Jussieu 75252 Paris Cedex 05*, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as GeMSS_____, 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 GeMSS_____ 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 _____ may be covered by the following U.S. and/or foreign patents: _____

    ☐ 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: _____

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: PHD STUDENT
Date: 04/26/2018
Place: Paris

2

Statement by Each Submitter

I, _CASANOVA_ , of _CS - Communication Systemes_,
do hereby declare that the cryptosystem, reference implementation, or optimized implementations
that I have submitted, known as _GEMSS_, 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):

[X] 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 _GEMSS_ 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 _____ may
be covered by the following U.S. and/or foreign patents: _____

    [ ] 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, refer-
ence implementation or optimized implementations: _____

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 stan-
dardization, 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 imple-
mentation 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 cryptosys-
tem) 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: Strategy and development Manager
Date: 02 May 18
Place: 22, avenue Galilée, 92350 Le Plessis Robinson
FRANCE

Statement by Each Submitter

I, _Jacques PATARIN_, of _University of Versailles (UVSQ)_,
do hereby declare that the cryptosystem, reference implementation, or optimized implementations
that I have submitted, known as _GeMSS_, is my own original work, or if submitted
jointly with others, is the original work of the joint submitters.
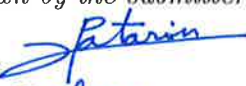
I further declare that (check one):

[X] 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 (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 _____ may
   be covered by the following U.S. and/or foreign patents: _____

   [ ] 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, refer-
   ence implementation or optimized implementations: _____

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 stan-
dardization, 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 imple-
mentation 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 cryptosys-
tem) 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: _Patarin_
Title: _Professor_
Date: _2 may 2018_
Place: _Versailles, France_

Statement by Each Submitter

I, _Gilles MACARIO-RAT_, of _Orange_ ,
do hereby declare that the cryptosystem, reference implementation, or optimized implementations
that I have submitted, known as _GEMSS_ , 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 _GEMSS_ 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 _____ may
be covered by the following U.S. and/or foreign patents: _____

    ☐ 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, refer-
ence implementation or optimized implementations: _____

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 stan-
dardization, 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 imple-
mentation 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 cryptosys-
tem) 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: _Macarit_
Title: _Ingineer_
Date: _May the 3rd 2018_
Place: _Chatillon France_

1.2 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, _Jacques Patarin_, _____, am the owner or authorized representative of the owner _GeMSS / DUALMODEMS_ 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: _Patarin_

Title: _Professor_

Date: _2 may 2018_

Place: _Versailles, France_