2.D.1 Statement by Each Submitter

I, <u>Lucky Galvez</u>, of <u>Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea</u>, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as <u>McNie</u>, 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 <u>McNie</u>; **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, 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

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

The following must also be included:

I, _Lucky Galvez_ , _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

2.D.1 Statement by Each Submitter

I, _Jon-Lark Kim_, of _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _McNie_, 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 _McNie_; **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, 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

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

The following must also be included:

I, _Jon-Lark Kim_ , _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

2.D.1 Statement by Each Submitter

I, _Myeong Jae Kim_, of _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _McNie_, 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 _McNie_; **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, 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

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

The following must also be included:

I, _Myeong Jae Kim_ , _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea,_ 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

2.D.1 Statement by Each Submitter

I, _Young-Sik Kim_, of _College of Electronic and Information 7111, Chosun University, Gwangju, 61452, South Korea,_ do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _McNie_, 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 McNie;_ **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).
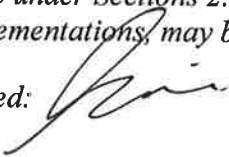
I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, 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:

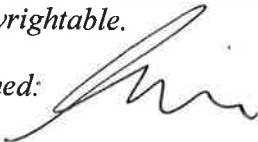Title: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: College of Electronic and Information 7111, Chosun University, Gwangju, 61452, South Korea

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

The following must also be included:

I, _Young-Sik Kim_, of _College of Electronic and Information 7111, Chosun University, Gwangju, 61452, South Korea,_ 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: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: College of Electronic and Information 7111, Chosun University, Gwangju, 61452, South Korea

2.D.1 Statement by Each Submitter

I, _Nari Lee_, of _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _McNie_, 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_ McNie; **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, 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: *M*

Title: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea

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

The following must also be included:

I, _Nari Lee_ , _Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea_, 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: _ℳ_ .

Title: McNie: Compact McEliece-Niederreiter Cryptosystem

Date: Nov.28, 2017

Place: Ricci 1401, Sogang University, 35 Baekbeom-ro, Mapo-gu, Seoul 04107, South Korea