2.D.1 Statement by Each Submitter

I, _____Minhye Seo_____, of _____ Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____EMBLEM and R.EMBLEM_____, 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 _____ EMBLEM and R.EMBLEM _____; **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 _____ EMBLEM and R.EMBLEM _____, 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: *Minhye*

Title: ph.d. student

Date: April 6, 2018

Place: Korea University

2.D.1 Statement by Each Submitter

I, _____Suhri Kim_____, of _____ Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____EMBLEM and R.EMBLEM_____, 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 _____ EMBLEM and R.EMBLEM _____; 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 _____ EMBLEM and R.EMBLEM _____, 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: _Sahi_

Title: Ph.d Student

Date: April 6, 2018

Place: Korea University.

2.D.1 Statement by Each Submitter

I, _____Seung-Joon Lee_____, of _____ Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____EMBLEM and R.EMBLEM_____, 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 _____ EMBLEM and R.EMBLEM _____; 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 _____ EMBLEM and R.EMBLEM _____, 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: *SJLee*

Title: *Ph.d. Student*

Date: April 6, 2018

Place: *Korea University*

2.D.1 Statement by Each Submitter

I, _____Jong Hwan Park_____, of _____ Sangmyung University, 20, Hongimun 2-Gil, Jongno-gu, Seoul, Republic of Korea (03016) _____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____EMBLEM and R.EMBLEM_____, 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 _____ EMBLEM and R.EMBLEM _____; 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 _____ EMBLEM and R.EMBLEM _____, 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: *[signature]*

Title: *Professor*

Date: *April 6, 2018*

Place: *Sangmyung Univ.*

2.D.1 Statement by Each Submitter

I, _____Dong Hoon Lee_____, of _____ Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____EMBLEM and R.EMBLEM_____, 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 _____ EMBLEM and R.EMBLEM _____; **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 _____ EMBLEM and R.EMBLEM _____, 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: *[signature]*

Title: Professor, Korea Univ.

Date: *April 6, 2018*

Place: Korea Univ.

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

The following must also be included:

I, _____ Minhye Seo _____ , Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____ , 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: Minhye

Title: Ph.d. student

Date: April 6, 2018

Place: Korea University

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

The following must also be included:

I, _____ Suhri Kim _____ , Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____ , 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: ~~Suhri~~

Title: Ph.d Student .

Date: April 6, 2018

Place: Korea University .

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

The following must also be included:

I, _____ Seung-Joon Lee _____ , Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____ , 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: SJLee

Title: Ph.d. Student

Date: April 6, 2018

Place: Korea University

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

The following must also be included:

I, _____ Jong Hwan Park _____ , Sangmyung University, 20, Hongimun 2-Gil, Jongno-gu, Seoul, Republic of Korea (03016) _____ , 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: Professor

Date: April 6, 2018

Place: Sangmyung Univ.

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

The following must also be included:

I, _____ Dong Hoon Lee _____ , Korea University, 145, Anam-ro, Seongbuk-gu, Seoul, Republic of Korea (02841) _____ , 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: Professor

Date: April 6, 2018

Place: Korea Univ.