

Post quantum signature scheme based on modified Reed-Muller code

pqsigRM

Principal submitter This submission is from the following team.

- Wijik Lee, Seoul National University
- Young-Sik Kim, Chosen University
- Yong-Woo Lee, Seoul National University
- Jong-Seon No, Seoul National University

E-mail address: jsno@snu.ac.kr


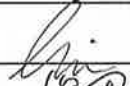
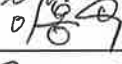
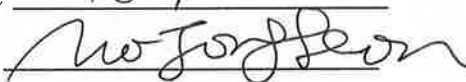
Telephone: +82-10-5241-3450 Postal address: Department of Electrical and Computer Engineering, Seoul National Univ., #011, 1, Gwanak-ro, Gwanak-gu, Seoul, 08826, Rep. of KOREA

Auxiliary submitters: There are no auxiliary submitters. The principal submitter is the team listed above.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: Same as submitter.

Signature: See also printed version of "Statement by Each Submitter".

- Wijik Lee 
- Young-Sik Kim 
- Yong-Woo Lee 
- Jong-Seon No 

B Statements

These statements “must be mailed to Dustin Moody, Information Technology Laboratory, Attention: Post-Quantum Cryptographic Algorithm Submissions, 100 Bureau Drive – Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, or can be given to NIST at the first PQC Standardization Conference (see Section 5.C).”

First blank in submitter statement: full name. Second blank: full postal address. Third, fourth, and fifth blanks: name of cryptosystem. Sixth and seventh blanks: describe and enumerate or state “none” if applicable.

First blank in patent statement: full name. Second blank: full postal address. Third blank: enumerate. Fourth blank: name of cryptosystem.

First blank in implementor statement: full name. Second blank: full postal address. Third blank: full name of the owner.

B.1 Statement by Each Submitter

I, Wijik Lee, of Dept. of ECE, Seoul National Univ., Seoul, 08826, Korea, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as pq sig RM, 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 pq sig RM 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 pq sig RM 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, 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: Ph.d. candidate
Date: Nov. 29 2017
Place: Seoul National Univ.,
Seoul, Korea

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

The following must also be included:

I, Wijik Lee, Dept. of ECE Seoul National Univ. Seoul, 08826, Korea, am the owner or authorized representative of the owner Wijik Lee 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:

phd. candidate

Date:

21. Nov. 2017

Place:

Seoul National Univ.
Seoul, Korea.

B.1 Statement by Each Submitter

I, Yang-sik Kim, of College of Electronic and Information, Chosun University, Gwangju (445), Korea, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as pq sig RM, 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 pq sig RM 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 pq sig RM 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, 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

Date:

Nov. 28, 2019


Place:

Chosun University

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

The following must also be included:

I, Young-sik Kim, College of Electronic and Information
Chosun University, Gwangju 61452, Korea, am the
owner or authorized representative of the owner Young-sik Kim of the sub-
mitted 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 corre-
sponding cryptosystem is selected for standardization and as a standard, notwithstanding that
the implementations may be copyrighted or copyrightable.

Signed: 

Title: professor

Date: Nov. 28, 2019

Place: Chosun University

B.1 Statement by Each Submitter

Seoul 00826, Korea

I, Tongwao Lee, of Dept. of ECE, Seoul Nat'l Univ., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as PSigRM, 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 PSigRM 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 PSigRM 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, 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: Yongwoo Lee

Title: Ph.D course

Date: NOV. 27. 2017

Place: Seoul National Univ. Seoul, Korea

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

Seoul, 08826, Korea

The following must also be included:

I, Yongwoo Lee, Dept. of ECE Seoul Nat'l Univ., am the owner or authorized representative of the owner Yongwoo Lee 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: Yongwoo Lee

Title: Ph.D. course

Date: Nov. 27, 2017

Place: Seoul National Univ. Seoul, Korea.

B.1 Statement by Each Submitter

Seoul, 08826, Korea.

I, Jong-Seon No, of Dept. of FCE, Seoul National Univ., do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as pgs:igRM, 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 pgs:igRM 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 pgs:igRM 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, 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

Date: NOV. 27, 2017

Place: Seoul National Univ.
Seoul, Korea

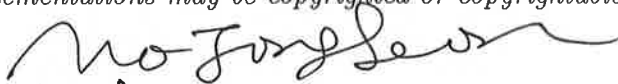
B.3 Statement by Reference/Optimized Implementations' Owner(s)

Seoul, 08826, Korea

The following must also be included:

I, Jong-Seon No, Dept. of ECE, Seoul National Univ. in the owner or authorized representative of the owner Jong-Seon No 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:

Nov. 27, 2017

Place:

Seoul National Univ.

Seoul Korea