

2.D.1 Statement by Each Submitter

I, Jinkyu Cho, of Seoul National University (1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, zip code: 08826), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that:

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, may be covered by the following U.S. and/or foreign patents: "Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128). IPC: H04L 9/32;

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Seoul National University

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

The following must also be included:

I, Jinkyu Cho, of Seoul National University (1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, zip code: 08826), 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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Seoul National University

2.D.1 Statement by Each Submitter

I, Zahyun Koo, of Samsung Electronics (Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, Republic of Korea, 18450), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, may be covered by the following U.S. and/or foreign patents: "Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32:

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: Zahyun Koo

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Samsung Electronics

2.D.1 Statement by Each Submitter

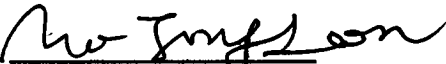
I, Jong-Seon No, of Seoul National University (1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, zip code: 08826), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that:

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, may be covered by the following U.S. and/or foreign patents: "Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32;

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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Seoul National University

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, Jong-Seon No. of Seoul National University (1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, zip code: 08826), 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): Electronic device capable of data communication through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Enhanced pqsigRM 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***
- 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: 

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

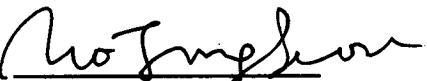
Date: 2023.3.1

Place: Seoul National University

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

The following must also be included:

I, Jong-Seon No. of Seoul National University (1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, zip code: 08826), 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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Seoul National University

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, Wijik Lee, of Samsung Electronics (Samsungjeonja-ro, Hwaseong-si, Gyeonggi-do, Republic of Korea, 18450), 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): Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Enhanced pqsigRM 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***
- 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: 이 위 적

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Samsung Electronics

2.D.1 Statement by Each Submitter

I, Yongwoo Lee, of Inha University (100, Inha-ro, Michuhol-gu, Incheon, Republic of Korea, 22212), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, may be covered by the following U.S. and/or foreign patents: “Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof.” US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32;

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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Inha University

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, Yong-Woo Lee, of Inha University (100 Inha-ro, Nam-gu, Incheon, Republic of Korea, 22212), 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): "Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Enhanced pqsigRM 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***
- 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, nontransferable, 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: Yongwoo Lee

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Inha University

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

The following must also be included:

I, Yong-Woo Lee, of Inha University (100 Inha-ro, Nam-gu, Incheon, Republic of Korea, 22212), 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: Yong-Woo Lee

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Inha University

2.D.1 Statement by Each Submitter

I, Young-Sik Kim, of Chosun University (74, Chosundae 5-gil, Dong-gu, Gwangju, Republic of Korea, zip code: 61452), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Enhanced pqsigRM, may be covered by the following U.S. and/or foreign patents: "Electronic device capable of data communication through electronic through electronic signatures based on syndrome and operating method thereof." US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32;

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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Chosun University

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, Young-Sik Kim, of Chosun University (74, Chosundae 5-gil, Dong-gu, Gwangju, Republic of Korea, zip code: 61452), 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): Electronic device capable of data communication through electronic signatures based on syndrome and operating method thereof. US patent 11128475, 20210921(application No. 16/699097, 20191128), IPC: H04L 9/32, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Enhanced pqsigRM 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):

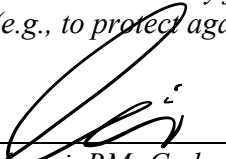
- without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, **OR***
- under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*

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: 

Title: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

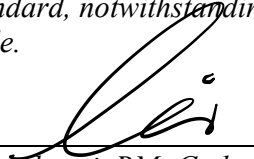
Date: 2023.3.1

Place: Chosun University

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

The following must also be included:

I, Young-Sik Kim, of Chosun University (74, Chosundae 5-gil, Dong-gu, Gwangju, Republic of Korea, zip code: 61452), 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: Enhanced pqsigRM: Code-Based Digital Signature Scheme with Short Signature for Post-Quantum Cryptography

Date: 2023.3.1

Place: Chosun University