

2.D.1 Statement by Each Submitter

I, Jihoon Cho, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

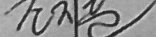
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: KR 10-2022-0155427.

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use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: Vice President

Date: 15 May 2023

Place: Seoul, South Korea

2.D.1 Statement by Each Submitter

I, MINGYU CHO, of 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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: Mingyu Cho 

Title:

Date: 05.16.2023

Place: 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

2.D.1 Statement by Each Submitter

I, JINCHEOL HA, of Daehak-ro 291, Yuseong-gu, Daejeon, 34141, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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: Jincheol Ha

Title:

Date: 12/5/2023

Place: Daehak-ro 291, Yuseong-gu, Daejeon, 34141, Korea

2.D.1 Statement by Each Submitter

I, SEONGKWANG KIM, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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.

Date: 15 May 2023

Place: Seoul, Korea

2.D.1 Statement by Each Submitter

I, Jihoon Kwon, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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: Jihoon Kwon

Title: Dr.

Date: May 12, 2023

Place: Seoul, Korea

2.D.1 Statement by Each Submitter

I, BYEONGHAK LEE, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):


- 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: KR 10-2022-0155427.*

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: Byeonghak Lee, Ph.D.

Date: 2023/05/12

Place: Seoul, KOREA

2.D.1 Statement by Each Submitter

I, Joohee Lee, of Sungshin Women's University, 2 Bomun-ro 34da-gil, Seongbuk-gu, Seoul, Republic of Korea (02844), do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMER, 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):

- 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: KR 10-2022-0155427.*

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: Joohee Lee

Title: Assistant Professor

Date: May 11th, 2023

Place: Seoul, Republic of Korea

2.D.1 Statement by Each Submitter

I, JOOYOUNG LEE, of School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMER, 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):

- 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: KR 10-2022-0155427.*

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: Prof.

Date: May 11, 2023

Place: School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, KOREA

2.D.1 Statement by Each Submitter

I, SANGYUB LEE, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AlMer, 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):

- 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: KR 10-2022-0155427.

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: *o/ Nf 078*
Title:
Date: *May 12, 2023*
Place: *Seoul, Korea*

2.D.1 Statement by Each Submitter

I, DUKJAE MOON, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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.

Date: 15 May 2023

Place: Seoul, KOREA

2.D.1 Statement by Each Submitter

I, MINCHEOL SON, of 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.*

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: *Mincheol Son*

Title: Mr.

Date: March 12th, 2023

Place: 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, KOREA

2.D.1 Statement by Each Submitter

I, HYOJIN YOON, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as AIMer, 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):

- 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: KR 10-2022-0155427.

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: *hyo jin yoon*
Title: *Dr.*
Date: *5/16/23*
Place: *Seoul, Korea*

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, JINCHEOL HA, of Daehak-ro 291, Yuseong-gu, Daejeon, 34141, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMer 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*

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: Jincchol Ha

Title:

Date: 12/5/2023

Place: Daehak-ro 291, Yuseong-gu, Daejeon, 34141, Korea.

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, SEONGKWANG KIM, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMer 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*

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: Dr.

Date: 15 May 2023

Place: Seoul, Korea

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, Jihoon Kwon, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMer 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*

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: Jihoon Kwon

Title: Dr.

Date: May 12, 2023

Place: Seoul, Korea

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, BYEONGHAK LEE, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMer 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*

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: Byeonghak Lee, Ph.D.

Date: 2023/05/12

Place: Seoul, KOREA

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, JOOYOUNG LEE, of School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMer 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*

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: Jooyoung Lee

Title: Prof.

Date: May 11, 2023

Place: School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, KOREA

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, SANGYUB LEE, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMER 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*

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: *S/ S/ Lee*
Title:
Date: *May 12, 2023*
Place: *Seoul, Korea*

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, DUKJAE MOON, of 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMER 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*

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: Dr.

Date: 15 May 2023

Place: Seoul, KOREA

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, MINCHEOL SON, of 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, KOREA, 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): KR 10-2022-0155427, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as AIMER 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*

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: *Mincheol Son*

Title: Mr.

Date: March 12th, 2023

Place: 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, KOREA

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

The following must also be included:

I, Jihoon Cho, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: Vice President

Date: 15 May 2023

Place: Seoul, South Korea

SAMSUNG SDS

14848603501684987933

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

The following must also be included:

I, MINGYU CHO, 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of 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: Mingyu Cho 

Title:

Date: 05.16.2023

Place: 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea

SAMSUNG SDS

14848603501684987901

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

The following must also be included:

I, JINCHEOL HA, of Daehak-ro 291, Yuseong-gu, Daejeon, 34141, 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: Jacheol Ha

Title:

Date: 12/5/2023

Place: Daehak-ro 291, Yuseong-gu, Daejeon, 34141, Korea.

SAMSUNG SDS

19236603501684988157

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

The following must also be included:

I, SEONGKWANG KIM, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: Dr.

Date: 15 May 2023

Place: Seoul, Korea

SAMSUNG SDS

14848603501684987790

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

The following must also be included:

I, Jihoon Kwon, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: Jihoon Kwon

Title: Dr.

Date: May 12, 2023

Place: Seoul, Korea

SAMSUNG SDS

14848603501684987778

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

The following must also be included:

I, BYEONGHAK LEE, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: 이병학

Title: Byeonghak Lee, Ph.D.

Date: 2023/05/12

Place: Seoul, KOREA

SAMSUNG SDS

14848603501684987815

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

The following must also be included:

I, Joohee Lee, of Sungshin Women's University, of 2 Bomun-ro 34da-gil, Seongbuk-gu, Seoul, Republic of Korea (02844), 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: Joohee Lee

Title: Assistant Professor

Date: May 11th, 2023

Place: Seoul, Republic of Korea

SAMSUNG SDS

14848603501684987837

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

The following must also be included:

I, JOOYOUNG LEE, School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, 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: *Joyoung Lee*

Title: Prof.

Date: May 11, 2023

Place: School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, KOREA

SAMSUNG SDS

14848603501684987855

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

The following must also be included:

I, SANGYUB LEE, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: *S/ SB OK*
Title:
Date: *May 12, 2023*
Place: *Seoul, Korea*

SAMSUNG SDS

16788873111683820432
16652603501584988087

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

The following must also be included:

I, DUKJAE MOON, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: Dr.

Date: 15 May 2023

Place: Seoul, KOREA

SAMSUNG SDS

22756603501684987737

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

The following must also be included:

I, MINCHEOL SON, of 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, 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: *Mincheol Son*

Title: Mr.

Date: March 12th, 2023

Place: 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, KOREA

SAMSUNG SDS

227586603501684987879

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

The following must also be included:

I, HYOJIN YOON, 10F, E Tower, Seongchon-gil 56, Seocho-gu, Seoul, 06765, 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: *hyojin yoon*

Title: *Dr.*

Date: *5/16/23*

Place: *Seoul, Korea.*

SAMSUNG SDS

04716603501684988016