

Statement

I, Arnaud Sipasseuth, of KDDI Research, Inc. (Head office), Advanced Technology Laboratories, 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state "none" if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state "none" if applicable).

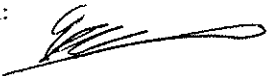
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Core Researcher at Information Security Group of KDDI Research Inc, Japan

Date: 2023-05-30

Place: KDDI Research, Inc. (Head office), Advanced Technology Laboratories,
2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan

Statement

I, Dung Hoang Duong, of University of Wollongong, Northfields Avenue, Wollongong NSW 2522, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state “none” if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state “none” if applicable).

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Senior Lecturer

Date: 30 May, 2023

Place: Wollongong, Australia

Statement

I, Gang Tang, of University of Technology Sydney, 15 Broadway, Ultimo NSW 2007, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state “none” if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state “none” if applicable).

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: PhD student
Date: 29 May 2023
Place: Sydney, Australia

Statement

I, Markus Bläser, of Saarland University, Saarland Informatics Campus E1.3, 66123 Saarbrücken, Germany, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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):

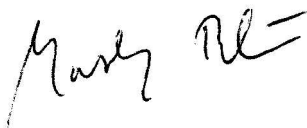
- I do not hold and do not intend to hold any patent or patent application with a claim or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state “none” if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state “none” if applicable).

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.



Signed:

Markus Bläser

Title: Prof. of Computer Science, Saarland University

Date: May 26, 2023

Place: Saarbrücken, Germany

Statement by Reference/Optimized Implementations' Owner(s)

I, Thomas Plantard, of Nokia Bell Labs, 600 Mountain Avenue - Murray Hill - NJ 07974-0636 - United States, am the owner 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: Senior Researcher

Date: May 30, 2023

Place: Murray Hill - New Jersey - United States

Statement

I, Thomas Plantard, of Nokia Bell Labs, 600 Mountain Avenue - Murray Hill - NJ 07974-0636 - United States, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state "none" if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state "none" if applicable).

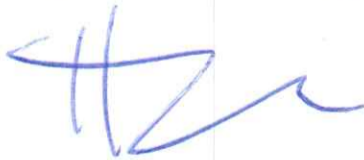
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Senior Researcher

Date: May 30, 2023

Place: Murray Hill - New Jersey - United States

Statement

I, Youming Qiao, of University of Technology Sydney, 15 Broadway, Ultimo NSW 2007, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ALTEQ; OR (check one or both of the following):
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as (print name of cryptosystem), may be covered by the following U.S. and/or foreign patents: (describe and enumerate or state “none” if applicable);
- to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: (describe and enumerate or state “none” if applicable).

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem’s specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Associate Professor

Date: 28 May 2023

Place: Sydney, Australia