

"Cover sheet"

HILA5

Key Encapsulation Mechanism (KEM)
and Public Key Encryption Algorithm

Version 1.0

Friday 24th November, 2017

Author, Owner, and Submitter:

Markku-Juhani O. Saarinen

E-mail: mjos@iki.fi

(Independent Submission)


MARKKU - JUHANI O.
SAARINEN
24 NOVEMBER 2017
Cambridge, UK

2.D.1 Statement by Each Submitter

I, Markku-Juhani Olavi Saarinen, of 10 Regency Gate, 29 Queen Edith's Way, Cambridge CB1 7AP, United Kingdom, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as HILA5, is my own original work.

I further declare that (check one):

- I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as HILA5.*

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

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

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

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 If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3 of the Call For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

Signed:  MARKKU SAARINEN

Title: P.H.D.

Date: November 24, 2017

Place: Cambridge, UK

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

The following must also be included:

I, Markku-Juhani Olavi Saarinen, 10 Regency Gate, 29 Queen Edith's Way, Cambridge CB1 7AP, United Kingdom, 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:  MARKKU SAARINEN

Title: P.H.D.

Date: November 24, 2017

Place: Cambridge, UK