Name of the proposed cryptosystem: NTRU-HRSS-KEM

Principal submitter:

John M. Schanck
Institute for Quantum Computing
University of Waterloo
200 University Avenue West
Waterloo, ON N2L 3G1
Canada
email: jschanck@uwaterloo.ca
phone: +1 519 888 4567 x39057

Auxiliary submitters:

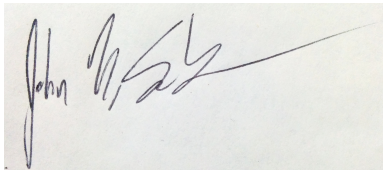
Andreas Hülsing
Joost Rijneveld
Peter Schwabe

Inventors of the cryptosystem

NTRUEncrypt was invented by Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. The transformation to an IND-CCA2-secure KEM is based largely on work of Eiichiro Fujisaki, Tatsuaki Okamoto, and Alexander Dent.

Owner of the cryptosystem

None (dedicated to the public domain)



John M. Schanck

Alternative point of contact:

Peter Schwabe
Radboud University
Toernooiveld 212
6525 EC Nijmegen
The Netherlands
email: peter@cryptojedi.org
phone: +31243653456