FrodoKEM
Learning With Errors Key Encapsulation

Cover Sheet

November 30, 2017

Name of the proposed cryptosystem: FrodoKEM – Learning With Errors Key Encapsulation.

Principal submitter:

- Michael Naehrig
  Microsoft Research
  One Microsoft Way
  Redmond, WA 98052
  telephone: +1 425 707 6035 ext. 76035
  email: mnaehrig@microsoft.com

Backup point of contact:

- Douglas Stebila
  Department of Computing and Software
  ITB-202
  McMaster University
  1280 Main St. W.
  Hamilton, Ontario, Canada L8P 4N2
  telephone: +1 905 525 9140 ext. 21186
  email: stebilad@mcmaster.ca

Auxiliary submitters:

- Erdem Alkim
- Joppe W. Bos, NXP Semiconductors
- Léo Ducas, CWI
- Karen Easterbrook, Microsoft Research
- Brian LaMacchia, Microsoft Research
- Patrick Longa, Microsoft Research
- Ilya Mironov, Google
- Valeria Nikolaenko
- Chris Peikert, University of Michigan
- Ananth Raghunathan, Google
- Douglas Stebila, McMaster University

Inventors/ developers: Erdem Alkim, Joppe W. Bos, Léo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, Douglas Stebila. Based on an extensive body of previous work as discussed in the written specification.

Owners of the cryptosystem: Same as the principal and auxiliary submitters.

Signature of the submitter: