

# FrodoKEM

## Learning With Errors Key Encapsulation

### Cover Sheet for Round 3 Submission

September 30, 2020

**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 Combinatorics & Optimization MC 5132  
University of Waterloo  
200 University Ave. W.  
Waterloo, Ontario, Canada N2L 3G1  
telephone: +1 519 888 4567 ext. 37211  
email: dstebila@uwaterloo.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
- Valeria Nikolaenko
- Chris Peikert, University of Michigan
- Ananth Raghunathan
- Douglas Stebila, University of Waterloo

**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:**

