FrodoKEM
Learning With Errors Key Encapsulation

Modifications in the Round 3 Submission

Erdem Alkim Joppe W. Bos Léo Ducas Patrick Longa Ilya Mironov
Michael Naehrig Valeria Nikolaenko Chris Peikert Ananth Raghunathan
Douglas Stebila

September 30, 2020

This document contains a list of modifications to the round-2 submission that are included in the round-3 submission.

July 2, 2019

- The March 30, 2019, revision introduced a mistranscription of the result of HHK (Reference [68] in the submission document) on the IND-CCA security of the FO transform in the classical random oracle model, incorrectly stating that it tightly relied on OW-CPA security, instead of IND-CPA security, of the underlying public-key encryption scheme. This error was pointed out by D. Bernstein on the NIST PQC mailing list. Bernstein also pointed out uncertainty in how the chain of reductions interacts with the argument involving Rényi divergence for the concrete distributions used by FrodoKEM. Section 5.1 has been revised and reorganized to address these issues. In particular, the following revisions appear in Sections 5.1.1–5.1.4:
    - A new Theorem 5.1 shows the IND-CCA security (in the classical random oracle model) of FrodoKEM, with its actual error distribution, under the assumption that FrodoPKE, with a rounded Gaussian error distribution, is IND-CPA-secure.
    - The chain of reductions (specifically, Steps 2 and 3) also yields the same conclusion as above under the assumption that the "T-transformed" FrodoPKE, with either a rounded Gaussian or the actual FrodoKEM error distribution, is OW-PCA secure.
    - Calculations for the bit security of FrodoKEM parameterizations based on Theorem 5.1 appear in a new Table 2.
    - Results of references [68] and [70] have been restated in a form closer to their original versions.
- In Section 5.2.3, the argumentation in the analysis of the dual attack was made more precise (though the ultimate conclusion remains the same).
- Ciphertext sizes were incorrectly stated in Table 1 and have been fixed (they are decreased by the size of the derived key **ss**). The March 30 version of Table 1 included estimates of OW-CPA security for FrodoPKE at different levels; since the current argument in support of IND-CCA security of FrodoKEM does not reference OW-CPA of FrodoPKE, these estimates have been removed.
- Table 2 was added to consolidate security estimates from all of the methodologies in the document.
- Tables 1–5 (and the Python scripts, under `3-media/Additional_Implementations`, generating these tables) were updated to reflect updated security estimates and ciphertext sizes.
- The text around Algorithms 7 and 8 was updated to clarify that 16-bit integers are represented in little-endian byte order.
- A typo in Table 9 that incorrectly labeled some rows was fixed.
- Typos (extra parentheses) were fixed in descriptions of Frodo, FrodoPKE, and FrodoKEM.

- An obsolete reference to hash function H was removed in Section 2.3.
- Table 10 was updated with revised estimates based on the number of samples available for each instance.

March 25, 2020

- Definition of table T_χ in Section 2.2.4 is fixed.
- The secret key matrix $\mathbf{S}$ is sampled in transposed form. This updates the specification to reflect how the C reference implementation works.
- Typos were fixed in Algorithms 10, 13, and 14.
- A Python reference implementation was made available.

September 30, 2020

- Submission to NIST Post-Quantum Cryptography standardization process round 3.
- Guo, Johansson, and Nilsson (Reference [66] in the specification document) identified a key-recovery timing attack on the reference implementation of FrodoKEM due to branching in FrodoKEM.Decaps. The pseudocode of Algorithm 14 (FrodoKEM.Decaps) was updated to make it clearer that these operations needed to be completed in constant-time, and updated our reference and optimized implementations. A brief discussion of this issue was added to Section 6.1 and performance figures were updated in Section 3.
- Parameter search scripts are now compatible with Python3.
- The parameter search procedure (Section 2.4.2) was reconciled with the scripts. Thanks to Sabrina Sewer for pointing out the discrepancy.
- A new Section 5.2.4 has been added, detailing a refinement of the security analysis with respect to concrete cryptanalytic attacks taking into account the recent state-of-the-art.
- The security estimates columns in Tables 2 and 10 were renamed and an extra column was added to use the "classical/quantum/plausible" terminology appearing elsewhere in the literature.