draft-longa-cfrg-frodokem

Patrick Longa Joppe Bos Stephan Ehlen Douglas Stebila

CFRG track @ IETF 122, Bangkok

FrodoKEM: Quick recap

❑ FrodoKEM is a quantum-safe IND-CCA2 secure Key Encapsulation Mechanism (KEM) based on the hardness of the plain Learning With Errors (LWE) problem

- Uses generic, algebraically unstructured lattices
- Minimizes potential cryptanalytic attack surface: no algebraic ring structure
- Facilitates simple and compact implementations

❑ It was a **Round 3 alternate** in the NIST PQC standardization process

- Dropping FrodoKEM was primarily motivated by performance: “In terms of security, Frodo’s conservative design choices are laudable.” (NIST Round 3 Status Report)

FrodoKEM: Quick recap

❑ Ongoing standardization by ISO (started on April’23)

- Planned to be included as Amendment 2 of ISO/IEC 18033-2, together with ML-KEM and Classic McEliece
- Currently approved for Draft International Standard (DIS), Dec’24
- Ongoing DIS ballot (to be done by May’25)

➢ Effort started by German BSI, received wide support from many national bodies

FrodoKEM: Backed by European countries

❑ BSI (Germany)

“Recommendation of FrodoKEM and Classic McEliece with appropriate security parameters for PQC applications in conjunction with a previously recommended asymmetric mechanism.”

Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102-1, Version: 2024-1, 2024.

❑ ANSSI (France)

“ANSSI would encourage including FrodoKEM as a valid and conservative option in high security applications where the resulting performance penalty (in particular in terms of bandwidth) is not prohibitive.”

ANSSI views on the Post-Quantum Cryptography transition (2023 follow up), 2023.

❑ NLNCSA/AIVD (The Netherlands)

“… there may be scenarios in which a stronger level of conservatism is desired. For these scenarios, FrodoKEM and Classic McEliece provide key encapsulation functionality… However, FrodoKEM and Classic McEliece have not yet been standardised. Until this is the case, we consider these primitives merely acceptable, although we strongly support ongoing initiatives aiming to standardise them.”

The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography (second edition), 2024.

FrodoKEM: Backed by European countries

❑ SOG-IS (EU, 17 member states)

- European mutual recognition agreement for Common Criteria (CC) certifications of IT security products

SOGIS ACM v1.4 (to be released) will include FrodoKEM, alongside ML-KEM, as options for PQ KEM algorithms to be used by certified products.

First Internet-Draft ready

❑ First I-D Draft ready: TBD

- Aligned with the upcoming ISO PQC standard amendment

❑ G. Wang (FrodoKEM in IKEv2): draft-wang-hybrid-kem-ikev2-frodo-02

❑ S. Jossefson: hybrid FrodoKEM/Classical KEMs

Feedback is welcome!

➢ Draft’ source: https://github.com/dstebila/frodokem-internet-draft

Call for action

- ❑ The traditionally-labelled “conservative” algorithms are not being standardized by NIST (at the moment):
  - There is strong support for their standardization, and the IETF would be the right place to do so
- ❑ Are others interested in the CFRG working on this subject?
  - Let’s start a discussion in the mailing list

draft-longa-cfrg-frodokem

<u>Patrick Longa</u>   Joppe Bos   Stephan Ehlen   Douglas Stebila

? ? ? ? ? ? ?

https://github.com/dstebila/frodokem-internet-draft

https://frodokem.org/