FrodoKEM

A simple and conservative KEM from generic lattices

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

FrodoKEM: Introduction

- FrodoKEM is a quantum-safe IND-CCA2 secure Key Encapsulation Mechanism (KEM) based on the hardness of the plain Learning With Errors (LWE) problem
  - It uses generic, algebraically unstructured lattices
- 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 has been recommended for use by several European countries (Germany [BSI24], France, Sweden)
- Ongoing standardization by ISO (started on April’23)
  - To be included as Amendment 2 of ISO/IEC 18033-2 (together with ML-KEM and Classic McEliece)
  - Currently approved for Draft Amendment (DAM), Sept/Oct’24

[BSI24] “BSI – Technical Guideline (Cryptographic Mechanisms: Recommendations and Key Lengths)”, BSI TR-02102-1, version February 2024.

Design principles

A simple, conservative yet practical design

- ❑ Plain LWE: generic, algebraically unstructured lattices
  - Minimizes potential attack surface: no algebraic ring structure
- ❑ Cautious parameterization: ‘medium-sized’ errors conforming to a worst-case/average-case reduction
  - (Non-tight) reduction from worst-case bounded distance decoding with discrete Gaussian samples (BDDwDGS) problem to decision LWE
  - Narrower errors ⇒ smaller parameters, better efficiency
- ❑ Concrete parameters chosen according to ‘core-SVP’ methodology
  - Lower-bound the first-order exponential time and space of SVP

IND-CCA KEM transformation

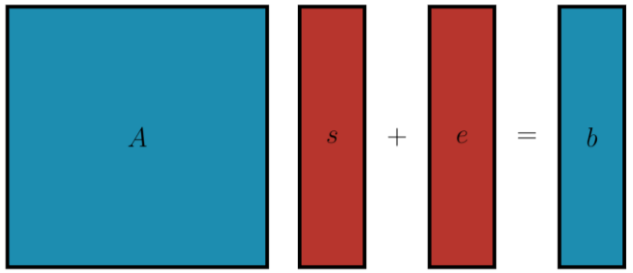
- Begin with an **IND-CPA PKE** scheme called FrodoPKE
- Transform it to IND-CCA KEM using a variant of Fujisaki-Okamoto (FO) transform
  - Hofheinz–Hovelmanns–Kiltz (HHK) give explicit variant **IND-CPA PKE → IND-CCA KEM**
  - HHK transform is secure in **both the classical and quantum ROM models**
  - Jiang et al. [JZC+18] eliminates need of some extra hashing
- Similar to ML-KEM, FrodoKEM uses a slight variant based on Jiang et al. (some additional values in hash computations to reduce risk of multi-target attacks)

[JZC+18] H. Jiang, Z. Zhang, L. Chen, H. Wang, and Z. Ma. “IND-CCA-secure key encapsulation mechanism in the quantum random oracle model, revisited.” CRYPTO 2018.

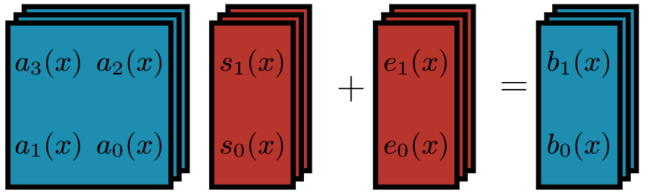
Implementation aspects (part I)

FrodoKEM has a simple design and implementation

- Matrix-vector products over $\mathbb{Z}_q^n$ with a power-of-2 modulus q
  - Not use of NTT, no prime modulus



Matrix multiplication based (FrodoKEM)



Polynomial multiplication based (ML-KEM)

Implementation aspects (part I)

FrodoKEM has a simple design and implementation

- ❑ Matrix-vector products over $\mathbb{Z}_q^n$ with a power-of-2 modulus q
  - Not use of NTT
- ❑ Straightforward error sampling: approximation to rounded Gaussian

  E.g., using inversion sampling:
  - Table T_χ stores $(s+1)$ integers related to discrete cumulative distribution function
  - Given a random value r, determine smallest index i such that $r \leq T_\chi[i]$
  - Output $(-1)^b i$ for a random bit b

Implementation aspects (part II)

FrodoKEM has a simple design and implementation

- ❑ x64 implementation consists of ~350 lines of C code
  (+ existing symmetric primitives)
- ❑ Facilitates compiler's work to produce optimized code
  - E.g., x64 implementation does not require hand-assembly code
- ❑ Easier to secure against side-channel attacks
  - E.g., negligible overhead of first-order masking for arithmetic operations

FrodoKEM: Variants and parameters

- Two (2) options for generating the public matrix A
  - Uses either AES128 or SHAKE128
- Two variants depending on the reuse of public keys
  - Standard and ephemeral FrodoKEM
- Twelve (12) parameter sets in total:

- (e)FrodoKEM-640-XXX: targets security level 1 (≥ AES-128)
- (e)FrodoKEM-976-XXX: targets security level 3 (≥ AES-192)
- (e)FrodoKEM-1344-XXX: targets security level 5 (≥ AES-256)

Dimension $n \in \{640, 976, 1344\}$, XXX $\in \{\text{AES}, \text{SHAKE}\}$

Performance profile

- On an x64 AMD Ryzen 9 3900XT @3.8GHz:
  - One full FrodoKEM execution (at level 1) is completed in **0.79 msec.**
  - Encaps + Decaps runs in **0.55 msec.**
- Public keys and ciphertexts are roughly 9KB, 15KB and 21KB for levels 1, 3 and 5 (resp.)

- Speed and bandwidth comparison with ML-KEM: FrodoKEM roughly **one order of magnitude slower and larger**
- In comparison with Classic McEliece: FrodoKEM public keys are **more than an order of magnitude smaller**, Encaps + Decaps is **an order of magnitude slower**, full FrodoKEM run is **more than an order of magnitude faster**

LWE security profile

- Quantum security estimates based on core-SVP hardness (in log2)

Level	ML-KEM	FrodoKEM
1	107	**137**
3	165	**195**
5	232	**255**

- Classical security estimates in terms of gates (in log2) and memory (bits in log2)

Level	ML-KEM		FrodoKEM	
	gates	mem	gates	mem
1	152	94	**175**	**110**
3	215	139	**240**	**156**
5	287	190	**305**	**202**

Summary

- FrodoKEM is practical for many applications
  - Takes more running time and bandwidth than ML-KEM
  - Brings attractive trade-offs in comparison with Classic McEliece
- It offers several attractive features:
  - Conservative LWE security, and parameters with larger (classical and quantum) security margins against known attacks
  - Enables simple, compact and easier-to-protect implementations

➢ **FrodoKEM** is a great alternative for security-sensitive applications

Proposal for Internet-Draft

- We have a draft ready that is in good shape and is aligned with the upcoming ISO standard amendment
  - It can be improved further with the help of the CFRG community
- Editors:
  - Joppe Bos (NXP)
  - Stephan Ehlen (BSI)
  - Patrick Longa (Microsoft)
  - Douglas Stebila (University of Waterloo)

Links

- Website (specification and updates):

  https://frodokem.org/

- Official implementation:

  https://github.com/microsoft/PQCrypto-LWEKE

FrodoKEM

A simple and conservative KEM from generic lattices

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

https://frodokem.org/