Optimizing ML-KEM for IoT Devices: ASCON Integration Study

Research Overview

Exploring memory optimization of ML-KEM for resource-constrained devices by replacing Keccak with the lightweight ASCON hash function.

Current Achievements

Memory Improvements

- Flash usage: Reduced by 36% (43,389B → 31,911B)
- RAM usage: Reduced by 12% (1,232B → 1,096B)

Function Mapping Strategy

ML-KEM Function	Keccak Original	ASCON Replacement
Key Derivation	SHA3-512	ASCON-Hash256 (2x)
Public Key Hash	SHA3-256	ASCON-Hash256
Matrix Gen	SHAKE128	ASCON-XOF128
Noise Sampling	SHAKE256	ASCON-CXOF128

Trade-offs

- State size reduction: 1600-bit → 320-bit
- Throughput adjustments needed for security maintenance
- Memory efficiency vs. processing time balance

Ongoing Work

- Security parameter verification
- Implementation optimization
- Performance analysis on IoT devices

Current Status

Work in Progress - Research implementation phase

Note: This research focuses on memory optimization through ASCON integration. All implementations are experimental and for research purposes only.