RAM Usage Model (Document C3)

Version: 1.0

Date: May 11, 2025

Author: EchoPulse Initiative

1. Overview

This document provides a detailed breakdown of the estimated Random Access Memory (RAM) usage for the core components of the EchoPulse Key Encapsulation Mechanism (KEM) system during key encapsulation and decapsulation operations. The analysis focuses on typical parameter sizes and is intended to inform resource planning for embedded deployment scenarios, such as on Cortex-M0+, Cortex-M4F, and RISC-V RV64 microcontrollers. Both static (preallocated) and dynamic (operation-specific) RAM consumption are quantified.

2. Memory Breakdown Table

Component	Bytes Used	Description
Transition Table G	8192	`[[u16; 16]; 256]` = 2 × 16 × 256
Secret Key (SK)	28	`SymbolPath`, 28 symbols (1 byte each)
Public Key (PK)	28	Same as SK
Payload (r)	28	28 random symbols
SHA3 Input Buffer	64	For `v_enc || r` (30 B + internal processing)
Mutation Row Buffer	32	One row of G for overwrite / mutation
Temporary States	8	`v_priv`, `v_pub`, `v_enc`, `v_dec` (u16 each)
Result Key (K/K’)	32	SHA3-256 output
Total Estimated	**~8420**	Excludes OS/runtime buffer overhead

3. Interpretation

The estimated total RAM usage for the core EchoPulse operations, excluding operating system or runtime environment overhead, is approximately 8420 bytes (or ~8.22 KB). This falls well within the RAM capacity of even resource-constrained embedded systems with 48 KB of RAM, leaving ample space for other program code and data.

It is important to note that the graph mutation operation, which involves rewriting the transition table, can be performed on a row-by-row basis. The `Mutation Row Buffer` of 32 bytes is sufficient to hold and modify a single row of the transition table, meaning a full rewrite of $G(V,E)$ in RAM is not required during mutation cycles.

The memory allocation strategy employed by EchoPulse minimizes dynamic buffering. The major data structures, such as the transition table and key material, are expected to be preallocated, leading to predictable and manageable RAM usage during runtime.

4. Conclusion

The RAM usage profile of the EchoPulse KEM demonstrates its feasibility for execution on constrained embedded systems with as little as 64 KB of total RAM. The memory footprint is consistent across both key encapsulation and decapsulation procedures. Furthermore, the design is compatible with 32-bit microcontroller architectures where `u16` and byte-sized data types are efficiently handled. The localized nature of the graph mutation process further optimizes RAM usage during the dynamic aspects of the protocol.

Document C3 — Memory Allocation Layer — EchoPulse Initiative