Internet-Draft
Internet-Draft
Intended status: Informational
Expires: 28 November 2025

T. Wartenberg
Independent Researcher

27 May 2025

EchoPulse: Adaptive Symbolic KEM Framework for Low-Resource Cryptographic Systems
draft-wartenberg-echopulse-kem-00

Abstract

This document introduces EchoPulse, a Key Encapsulation Mechanism (KEM) designed for high efficiency and minimal resource usage, offering adaptive symbolic behavior and built-in resistance to replay and side-channel attacks. EchoPulse aims to serve as a viable lightweight PQC candidate.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 November 2025.

Table of Contents

1. Introduction

EchoPulse is a symbolic-logic-driven KEM architecture optimized for low RAM/ROM usage and real-time embedded environments. It addresses modern post-quantum challenges using mutation-dynamic graph encoding for key generation and encapsulation.

2. Key Features

- RAM usage under 9KB

- ROM footprint under 15KB

- AI-adaptive mutation paths

- Built-in session replay protection

- High resistance to side-channel analysis

3. Security Considerations

EchoPulse integrates symbolic mutation logic with post-quantum principles, complicating adversarial prediction and key recovery. It is particularly robust against pattern analysis, timing inference, and memory probing.

4. IANA Considerations

This document has no IANA actions.

5. References

None yet formalized.

Appendix A. Acknowledgements

This draft was generated with AI assistance under a multi-role verification model and symbolic simulation framework.

Author’s Address

Tom Wartenberg
Independent Researcher
Email: tom.wartenberg@web.de