EchoPulse: A Post-Quantum Symbolic KEM Framework for Embedded Systems and Secure Protocols

1. Executive Summary

The escalating threat of quantum computing necessitates an urgent transition to post-quantum cryptography (PQC). Existing PQC candidates, however, often impose significant computational and memory demands, rendering them impractical for resource-constrained environments like embedded systems, IoT devices, and smartcards. This presents a critical gap in securing the vast ecosystem of edge devices against future quantum attacks.

EchoPulse emerges as a groundbreaking solution: a novel Post-Quantum Key Encapsulation Mechanism (KEM) framework designed specifically for these constrained environments. By leveraging deterministic symbolic graph transitions and a unique per-session mutation mechanism, EchoPulse offers a compact, efficient, and robust approach to post-quantum key establishment. It delivers built-in resistance to replay attacks and sophisticated AI-based decryption modeling, ensuring forward secrecy and quantum resilience where traditional PQC falls short. EchoPulse provides a viable path to secure next-generation embedded applications and protocols.

2. Technical Overview

EchoPulse is a symbolic KEM protocol that fundamentally rethinks cryptographic primitives for the post-quantum era, emphasizing resource efficiency and inherent security properties.

- **Symbolic KEM with Deterministic Graph Transitions:** At its core, EchoPulse operates on a dynamically evolving symbolic graph $G(V,E)$. Key encapsulation involves traversing this graph using a secret symbol path (r) to derive a unique shared secret. The graph's state transitions, $\delta(v,s) \rightarrow v'$, are entirely deterministic, ensuring consistent key derivation between legitimate parties. This graph-based approach offers a flexible framework for constructing KEMs with tunable security and performance.
- **Per-Session Mutation for Enhanced Security:** A distinguishing feature of EchoPulse is its deterministic graph mutation function, $\mu(G,t)$. For each new key establishment session, the underlying symbolic graph G evolves to G_t based on a public, session-specific index t. This mutation significantly alters the graph's structure, making past ciphertexts non-reusable and preventing replay attacks. This dynamic nature inherently resists static analysis and AI-based decryption

modeling by introducing a time-varying attack surface.

- **Symbol-Path Security and Efficiency:** The security of EchoPulse relies on the computational difficulty of reconstructing the secret symbol path (r) from the publicly exchanged ciphertext components and the mutated graph Gt. The symbolic nature allows for highly compact representations of the keying material and efficient operations, crucial for performance on low-power processors. The symbol_path_length and alphabet size are configurable parameters that directly influence the security strength and computational overhead.
- **Optimized for Constrained Devices:** EchoPulse's design prioritizes minimal resource consumption. Its core operations are typically iterative and stateless, allowing for very low RAM usage (demonstrated to be under 9 KB for practical security levels). This makes it exceptionally well-suited for deployment on constrained microcontrollers (e.g., ARM Cortex-M0+, RISC-V), FPGAs, and other embedded platforms where traditional PQC algorithms exceed memory or computational budgets.

3. Competitive Differentiators

EchoPulse offers compelling advantages over leading PQC candidates, particularly for embedded and real-time applications.

Feature / Metric	EchoPulse (Symbolic KEM)	Kyber (Lattice)	FrodoKEM (Lattice)	NTRU (Lattice)
RAM Footprint	**< 9 KB (Critical Advantage)**	~20-50 KB (depending on security)	~35-70 KB (depending on security)	~20-60 KB (depending on security)
ROM Footprint	**Highly Compact (Target < 15 KB)**	~30-100 KB	~50-150 KB	~30-100 KB
Encapsulation Speed	**Fast (Optimized for iteration)**	Moderate-Fast	Moderate-Slow	Moderate-Fast

Payload Size (CT)	**Very Small (e.g., ~34-66 bytes)**	~768-1568 bytes	~600-1100 bytes	~600-1000 bytes
Side-Channel Behav.	**Designed for Constant-Time Operations**	Requires careful constant-time impl.	Requires careful constant-time impl.	Requires careful constant-time impl.
Replay Mitigation	**Built-in per-session mutation**	Relies on higher-layer protocols (TLS)	Relies on higher-layer protocols (TLS)	Relies on higher-layer protocols (TLS)
Attack Model Focus	Symbolic graph & path reconstruction	Lattice problems (LWE, Module-LWE)	Learning with Errors (LWE)	Shortest Vector Problem (SVP)

- **Resource Efficiency:** EchoPulse's dramatically lower RAM/ROM footprint and compact ciphertext size make it the only practical PQC KEM for many constrained embedded systems that cannot accommodate the memory demands of lattice-based schemes.
- **Inherent Replay Resistance:** Unlike other KEMs that rely on external protocol mechanisms (like TLS 1.3's handshake transcript) for replay protection, EchoPulse's per-session graph mutation inherently prevents replay attacks at the KEM layer. This simplifies protocol design and adds a layer of security.
- **Side-Channel Considerations:** The design promotes constant-time operations through deterministic graph traversal, making it highly amenable to side-channel resistance without complex countermeasures often needed for arithmetic-heavy lattice operations.
- **AI-Resilience:** The dynamic nature of the underlying graph frustrates AI/ML-based cryptanalysis efforts that depend on observing patterns over static cryptographic artifacts.

4. Applications and Collaboration Call

EchoPulse is poised to secure a wide array of critical applications in the post-quantum era, particularly where resource constraints are paramount.

- **Post-Quantum TLS 1.3 Integration:** EchoPulse is a natural fit for TLS 1.3's key exchange, providing quantum-safe key establishment for secure communication

channels, even for low-power IoT devices that currently cannot support other PQC KEMs. Its small ciphertext size is ideal for minimizing bandwidth overhead.
- **Smartcard-Based Key Exchange:** EchoPulse can enable quantum-safe key exchange on smartcards and secure elements, protecting sensitive operations like digital signatures, authentication, and secure element provisioning against future quantum attacks, extending the lifespan of existing infrastructure.
- **Secure Messaging under Low-Power Constraints:** For battery-powered sensors, industrial control systems, and other remote devices, EchoPulse provides a lightweight solution for establishing secure communication channels, ensuring data confidentiality and integrity with minimal energy consumption.
- **Post-Quantum Token Authentication and Identity Protocols:** Enabling secure token issuance, validation, and identity verification in environments with limited computational capabilities, such as connected vehicles, medical devices, and industrial IoT.

We invite collaboration with industry partners, standardization bodies, and research institutions to further refine, evaluate, and integrate the EchoPulse framework. Our goal is to provide a robust, efficient, and standardized post-quantum KEM solution that meets the unique demands of embedded systems and secures the next generation of connected devices against the quantum threat.