EchoPulse – Security Considerations & Open Verification

This document outlines potential security considerations, assumptions, and recommended paths for community-driven open verification of the EchoPulse symbolic KEM system.

1. Assumptions

- Adversaries do not know the internal δ-transition structure
- Replay resistance is based on public path entropy and mutation timing
- Mutation is non-deterministic but synchronized via shared schedule

2. Attack Vectors (Hypothetical)

- Symbol replay attacks (entropy prediction)
- Graph inversion via transition inference
- Structural weakness in δ-cycle collisions
- Side-channel timing in embedded transitions

3. Verification Needs

- Formal proof of mutation unpredictability
- Symbol-path coverage testing
- Statistical analysis of symbol reuse
- Code-level open-source audit suggestions

4. Recommendations

- Public test suite with randomized δ-generation
- Symbolic mutation trace visualizer
- Invite open contributions for state transition stress testing

Document 18 – EchoPulse Security Considerations & Open Verification