1. Suggested Reduction Target/Assumption

Target: Indistinguishability under Chosen Ciphertext Attack (IND-CCA2) in the Random Oracle Model (ROM).

Assumption: Symbolic Graph Path Unpredictability (SGPU)

Informally: Given a public graph G, a starting state, and a sequence of transition mutations, it's computationally hard to predict the exact path (sequence of states) taken through the graph, even when observing the public symbols emitted at each transition.

2. Model Sketch (Game-Based)

Let's define a game between a Challenger (C) and an Adversary (A):

Setup:
C generates a random graph G(V, E), a starting state v&lt;sub>0&lt;/sub>, and a mutation schedule μ. C also samples a random key K from the key space and stores it. C sends (G, v&lt;sub>0&lt;/sub>, μ) to A.
C initializes a random oracle H (SHA3-256).
Phase 1 (Queries):
A can make various queries:
H(x): Queries to the random oracle H. C responds with H(x).
Encapsulate(): C runs the encapsulation algorithm to generate (ct, K), where ct is the ciphertext. C returns (ct, K).
Decapsulate(ct', K'): C runs the decapsulation algorithm on (ct', K'). If K' is correct, C returns the encapsulated key. Otherwise, it returns an error symbol.
Challenge:
A chooses two equal-length messages m&lt;sub>0&lt;/sub>, m&lt;sub>1&lt;/sub> and sends them to C.
C chooses a random bit b ∈ {0, 1}.
C calculates (ct*, K&lt;sub>b&lt;/sub>) = Encapsulate(m&lt;sub>b&lt;/sub>).
C sends ct* to A.
Phase 2 (More Queries):
A continues to make H(), Encapsulate(), and Decapsulate() queries, with the restriction that Decapsulate() cannot be queried on ct*.
Guess:
A outputs a guess b' for b.
Adversary's Advantage:
The adversary's advantage is defined as |Pr[b' = b] - 1/2|.

3. Proof Outline (Stepwise)

The IND-CCA2 security proof sketch relies on the SGPU assumption and the ROM:

IND-CCA1 Security:
First, we show that EchoPulse is IND-CCA1 secure. In this case, the adversary has no access to decapsulation oracle. The security relies on the hardness of predicting the key from the ciphertext.
SGPU Reduction:
We reduce the SGPU assumption to the adversary's inability to distinguish between ciphertexts.
If A can distinguish ciphertexts, then A can predict the internal state transitions of the graph, which contradicts the SGPU assumption.
The random oracle H hides the relationship between the final state and the key, making it hard to recover the key even if the state is known.
IND-CCA2 Security: