Symbolic Path Complexity (SPC) Score for SYMCUBE

1. Introduction

This document introduces the Symbolic Path Complexity (SPC) Score, a metric designed to quantify the difficulty of predicting a SYMCUBE unlock sequence. Unlike traditional key length metrics (bits in AES, modulus size in RSA), SPC accounts for the unique properties of SYMCUBE's unlock mechanism: sequence depth, IRN topology, and timing layers. This metric is intended for cryptographers, standardization evaluators, and reviewers of post-quantum security.

2. Formal SPC Definition

The SPC Score is defined as a combination of three factors:

Sequence Depth (D): The number of symbolic transformations (rotations and SSVE applications) in the unlock sequence. A higher depth increases the number of possible paths.

IRN Topology Complexity (T): A numerical representation of the IRN's interconnectivity and the number of possible rotation states. This is calculated based on the number of units (N), the number of connections per unit (C), and the number of rotation axes (R) per unit.

Timing Layer Entropy (E): A measure of the randomness and variability introduced by the timing countermeasures (randomized delays, jitter). This quantifies the uncertainty an attacker faces when trying to reconstruct the precise timing of each step.

The SPC Score is calculated as follows:

```
SPC = D * T * E
```

Where:

D is a positive integer.

T is calculated as: $T = N * C * \log_2(R)$

E is the Shannon entropy of the timing jitter distribution, measured in bits.

3. Comparison to Traditional Key Length Metrics

Traditional key length metrics, such as the number of bits in AES or the modulus size in RSA, quantify the size of the key space. In lattice-based cryptography, security relies on the difficulty of solving problems in high-dimensional lattices. These metrics do not directly translate to SYMCUBE due to its fundamentally different unlock mechanism:

State Transition Complexity: SYMCUBE's security relies on the complexity of the state transitions within the IRN, which is a function of the sequence depth and IRN topology, not just a static key.

Temporal Uncertainty: The timing layer adds an additional dimension of complexity that is not present in traditional cryptographic systems. An attacker must not only determine the correct sequence of states but also the precise timing of those states.

Post-Quantum Relevance: SYMCUBE's design principles offer potential resistance against quantum computing attacks, a property not inherent in RSA or many elliptic curve-based systems. SPC provides a way to quantify this complexity in a post-quantum context.