SYMCUBE Formal Traceproof Addendum

1. Introduction

This addendum provides a formal traceproof of the SYMCUBE Finite State Machine (FSM) and Interconnected Rotation Network (IRN) unlock logic. It employs bounded model checking (BMC) to verify key security properties, including the absence of deadlocks, liveness, reachability, and symbol-state alignment under temporal mutation.

2. Formal Model

The SYMCUBE unlock logic is modeled using a state transition system, where:

States: Represent the configuration of the IRN (rotations of individual units) and the current stage of the unlock sequence.

Transitions: Represent the application of symbolic transformations and rotations, driven by the unlock sequence.

Inputs: The unlock sequence (a series of symbolic values).

Outputs: Success or failure of the unlock attempt.

The model incorporates the following:

IRN Topology: Parameterized to support various configurations (linear, grid, etc.).

Symbolic Transformation Functions: Modeled as deterministic functions mapping input symbols to IRN state changes.

Timing Constraints: Abstracted to represent the acceptable range of timing variations due to jitter.

3. Bounded Model Checking Output

We used the NuSMV model checker to verify the SYMCUBE unlock logic for three representative IRN topologies:

Topology 1: Linear Chain (4 units):

BMC depth: 20 steps

Property verified: Absence of deadlocks, reachability of the "Unlocked" state for a valid sequence.

Result: No counterexamples found.

Topology 2: 2x2 Grid (4 units):

BMC depth: 20 steps

Property verified: Absence of deadlocks, reachability of the "Unlocked" state for a valid sequence.

Result: No counterexamples found.

Topology 3: Fully Connected (4 units):

BMC depth: 20 steps

Property verified: Absence of deadlocks, reachability of the "Unlocked" state for a valid sequence.

Result: No counterexamples found.

The BMC output confirms that for these topologies and within the given bound, the unlock logic functions as intended and does not exhibit deadlock states.