SYMCUBE Dossier Addendum: IRN-SQX Topology & Symbol Chain Logic

Date: May 5, 2025

Subject: Detailed Exposition of the Iterative Rotational Network - Sequential Key eXchange (IRN-SQX) Topology and Symbolic Chain Logic

This document provides a detailed explanation of the internal topology and operational logic of the IRN-SQX symbolic unlocking system within the SYMCUBE defense core. It elaborates on how individual symbols interact, how unlock sequences propagate through the network, and how valid unlock attempts are differentiated from invalid ones.

1. Symbol Interaction Model:

The Iterative Rotational Network (IRN) within SYMCUBE defines the relationships and dependencies between the 100 symbolic units. This topology can be implemented using various models, offering different levels of complexity and security. Two potential models are:

 * Neighborhood Logic (2D Toroidal Matrix): The 100 symbols are conceptually arranged in a 10x10 toroidal grid. Each symbol has immediate neighbors (up, down, left, right), with the edges wrapping around. A rotation applied to one symbol can, based on the IRN configuration, trigger or enable subsequent rotations of its neighbors after a defined temporal delay or upon a specific condition being met (e.g., reaching a particular rotational state). The IRN configuration, defining these neighbor dependencies and triggering conditions, can be fixed or dynamically influenced by the unlock sequence itself.

 * Recursive Dependency Chains: Symbols are linked in directed acyclic graphs (DAGs) or more complex cyclic graphs, forming dependency chains. A rotation of a "parent" symbol in the chain might be a prerequisite for enabling the rotation of its "child" symbols. The unlock sequence would then need to apply rotations in a specific order that respects these dependencies. The depth and branching factor of these chains contribute to the complexity of the unlock process. The IRN configuration dictates the structure and rules of these dependency chains.

In both models, the IRN introduces a layer of complexity beyond simple independent symbol rotations. The correct unlock sequence must not only specify the right symbols and rotation directions but also adhere to the topological constraints and temporal dependencies defined by the IRN.

2. Chain Propagation Logic:

A valid unlock sequence unfolds over time, propagating through the symbolic network according to the IRN topology and defined constraints:

- Temporal Delay: Rotations applied to one symbol might not instantaneously enable subsequent rotations. A defined temporal delay (e.g., a fixed number of clock cycles or a state-dependent duration) can be introduced before the effect propagates to dependent symbols. This temporal element is crucial for resisting automated brute-force attempts.

- Directional Dependencies: The direction of rotation of a symbol can influence which of its neighbors or dependent symbols become eligible for rotation next, or the required direction of their subsequent rotation. For example, a clockwise rotation might enable a counter-clockwise rotation of a specific neighbor.

- Mutation Resistance: The IRN topology and the associated propagation rules can be designed to be resistant to minor deviations or mutations in the unlock sequence. Incorrect rotations or rotations applied out of sequence will disrupt the intended propagation flow, leading to a failure to reach the target unlocked state. The interconnectedness of the symbols means that a single incorrect step can have cascading negative effects.

- State-Dependent Propagation: The propagation of rotational effects can also be dependent on the current rotational state of the triggering symbol or its neighbors. For instance, a rotation might only propagate if the triggering symbol is in a specific one of its four states. This adds another layer of complexity to the unlock process.

3. Sequence Evaluation (Valid/Invalid Case Study):

Consider a simplified SYMCUBE with a 2x2 toroidal grid (4 symbols: S1, S2, S3, S4). Assume a basic IRN where a clockwise rotation of a symbol enables a counter-clockwise rotation of its right neighbor after one time unit. The target unlocked state is a specific configuration of the four symbols.

- Valid Unlock Attempt:
  - Time T=0: Apply clockwise rotation to S1.
  - Time T=1: (IRN triggers) Apply counter-clockwise rotation to S2 (right neighbor of S1).
  - Time T=2: Apply clockwise rotation to S3 (independent action in the valid sequence).

  * Time T=3: (IRN triggers) Apply counter-clockwise rotation to S4 (right neighbor of S3).

If the final states of S1, S2, S3, and S4 at T=3 match the predefined target state, the unlock is successful. The sequence adhered to both the explicit rotation instructions and the implicit IRN propagation rules within the allowed temporal window.

* Invalid Unlock Attempt (Incorrect Sequence):

  * Time T=0: Apply counter-clockwise rotation to S1 (incorrect initial direction).

  * Time T=1: (IRN does not trigger as the initial rotation was wrong) Attempt to rotate S2 clockwise (incorrect action).

  * Time T=2: Apply clockwise rotation to S3.

  * Time T=3: Attempt to rotate S4 counter-clockwise.

In this case, the initial incorrect rotation of S1 prevents the subsequent IRN-triggered rotation of S2 from occurring correctly. Even if later steps are partially correct, the disrupted flow prevents the system from reaching the target unlocked state. The system differentiates this invalid attempt by the final symbolic configuration not matching the expected unlocked state after the attempted sequence within the defined time constraints.

* Invalid Unlock Attempt (Temporal Violation):

  * Time T=0: Apply clockwise rotation to S1.

  * Time T=3: (Temporal delay exceeded) Apply counter-clockwise rotation to S2.

  * Time T=4: Apply clockwise rotation to S3.

  * Time T=5: Apply counter-clockwise rotation to S4.

Even if the sequence of rotations is correct, the delay in applying the second rotation beyond the allowed temporal window for IRN propagation will result in a failed unlock. The system monitors the timing of each step and rejects sequences that do not adhere to the defined temporal constraints.

4. Integration into Boot Validation Path:

The IRN-SQX unlock validation is a critical gatekeeper in the secure boot process:

 * During the early boot stages, the SYMCUBE core is initialized in a locked state with a predefined initial symbolic configuration.

 * The secure bootloader initiates the IRN-SQX unlock process, awaiting the input of the valid rotation sequence.

 * The Symbol Sequence Validation Engine (SSVE) processes each input rotation instruction, applying it to a shadow representation of the SYMCUBE state and tracking the temporal progression and IRN-based propagation.

 * The SSVE verifies that each step in the sequence adheres to the defined temporal constraints and the rules of the IRN topology.

 * Only upon successful completion of the entire valid sequence, resulting in the shadow SYMCUBE reaching the predefined target unlocked state within the allowed time, will the bootloader proceed to load and execute the next stage of the system.

 * Any deviation from the correct sequence, timing, or IRN propagation will result in a validation failure, halting the boot process and preventing unauthorized access.

5. Summary of Operational Flow and Risk Mitigation:

The IRN-SQX system provides a robust and multi-layered security mechanism based on:

 * Topological Complexity: The interconnectedness of symbols through the IRN creates complex dependencies that are difficult to reverse-engineer or predict.

 * Sequential Dependency: The correct unlock requires a specific sequence of rotations, where each step can be contingent on the preceding ones and the IRN state.

 * Temporal Constraints: The timing of the unlock sequence is critical, preventing rapid automated attempts and adding another dimension to the security.

 * Mutation Resistance: Minor errors in the sequence or timing will disrupt the intended flow and prevent successful unlocking.

By integrating this intricate topological and sequential logic into the SYMCUBE defense core, a highly resilient security barrier is established, effectively mitigating risks associated with brute-force attacks, replay attacks, and inference-based cryptanalysis. The next stage of the SYMCUBE dossier will explore potential applications and integration strategies across various defense and critical infrastructure domains.