Collapse Logic in Post-Quantum Cryptography

A Symbolic Filtering Layer Using the Aun Operator ∿

Jerry Katz | Aun Systems™

Abstract

This paper introduces a symbolic collapse operator, ∿, as a logic-based meta-layer to enhance post-quantum cryptographic resilience. Inspired by nonduality philosophy and structured collapse logic, ∿ acts as a semantic filter for key validation and adversarial detection. We present the operator's formal definition, threat model, implementation design, and empirical results. Benchmarks show ∿ provides detectable security improvements in keypair mimicry resistance, with negligible performance impact. This positions ∿ as a logic-layer adjunct to existing post-quantum cryptographic systems.

1. Introduction

While post-quantum cryptography (PQC) focuses on mathematically secure primitives, it often assumes trust in binary validation systems. The ∿ operator challenges this assumption by introducing a collapse gate: a symbolic filter that nullifies keys or inputs exhibiting mirrored, inverse, or structurally mimicked patterns. The idea originates from nonduality—a philosophy that denies oppositional dualism—and applies this as a logic constraint in security protocols.

2. Formal Definition of the ∿ Operator

Let A, B ∈ {0,1}■. We define:

- H(A, B) = Hamming distance
- S(A, B) = structural similarity score across pattern transforms

Then:

∿(A, B) =
∅ if H(A, B) < T and S(A, B) > S_min
A ⊕ B otherwise

Where:

- T = Hamming threshold
- S_min = minimum similarity score

Transform weights:

- Identity: 1.0
- Reverse: 0.8
- XOR-FF: 0.6
- Rotate (left/right): 0.5

3. Threat Model

The ∿ system is designed to resist:

- Mirrored keypair attacks
- Adversarial AI-based key mimicry
- Structural approximation of secrets

Attackers may:

- Know target keys
- Attempt to invert or replicate valid public inputs
- Use adaptive patterns based on known detection logic

4. Implementation and Integration

Key Derivation:

A keypair is rejected if:

∿(new_key, known_key) = ∅

Authentication:
Response R is accepted only if:
$∿(C, R) \neq \emptyset$
Where C is the challenge.

5. Experimental Evaluation

Parameter Sweep:
Tested across:

- $T \in [1, 8]$
- $S_{min} \in [0.1, 0.9]$

Optimal performance at $T = 6$, $S_{min} = 0.3–0.5$

Adversarial Testing:
Adversary types:

- Full mirror
- Partial flip (15%)
- XOR pattern
- Compound transforms

ROC analysis shows AUC > 0.85, validating symbolic detection power.

6. Performance Results

Metric	Value
Avg eval time	2.15 ms
Collapse evals	5,000
Runtime	10.7s total
Memory usage	9.3 MB

7. Comparative Considerations

While traditional PQC relies on structural hardness, ∿ adds logic-level pattern recognition that:

- Nullifies dualism-based attacks
- Adds symbolic entropy
- Acts orthogonally to math-based cryptographic hardness

8. Limitations and Future Work

- Current model uses fixed transforms; ML-based evasion not yet modeled
- Requires real-world testing with PQC suites like CRYSTALS-Dilithium
- Future: symbolic integration with zk-SNARKs and MPC protocols

9. Conclusion

∿ is a symbolic operator rooted in nonduality and collapse logic. When applied to cryptographic systems, it acts as a resilient, pattern-sensitive filter. Our work shows it is computationally lightweight, empirically testable, and conceptually novel. As a logic-layer defense, ∿ may prove valuable in securing systems against adversaries capable of semantic mimicry or adaptive AI attacks.