

White paper - Structural PQC resistance & the Ouroboros gate
Compiled: October 2026, v1.

Introduction:

"This system is complementary to, not a replacement for, NIST FIPS 203/204/205 (cryptographic layer) and NCSC PQC migration guidance (operational layer). It addresses a gap at the structural/network layer: the search process. OWASP LLM guidance addresses sensitive disclosure at the filtering layer; this system addresses it at the generation layer. The four frameworks are independent and cumulative - all four are required for full coverage."

The Ouroboros Gate: Structural Resistance to Grover-Class Search

A deployable network-layer countermeasure for harvest-now-decrypt-later threats against NIS2 essential entities.

In this document:

1. The gap: NIST PQC protects the mathematics. It does not protect the search. Harvest-now-decrypt-later is a current threat, not a future one, and the network layer is under-addressed in the current guidance.
2. The advance: Structural resistance to Grover-class search. The search mechanism is the trigger for its own defeat.
3. The mechanism: The Ouroboros gate. Recursive, self-referential, 0.17s execution. The gate is faster than the search can complete one iteration, because the search is what closes it.
4. The lure: The EDC chain. Adversaries are assigned MACs reactively upon interaction. The system doesn't go looking for them. They bite, and that's when they become visible.
5. The cycle: MPN-1 (time, 900s, three checkpoints) and MPN-2 (degrees, lure & hold, sub-layer). Two domains, two NICs, complementary coverage.
6. The forensic record: Non-perturbative by design. Frozen at capture. Deferred assessment. Measurement and interpretation are separated.
7. The four-tier exposure model: GIV/GOV/RSR/LRN. Tiers govern generation, not just filtering. Silent-note abstraction as a practical control.
8. Sovereign AI: Scout and Sage. Role in the weights, not the prompt. Cross-domain responsiveness with role retention. The system caught the drift before the operator acted on it. Refer to Appendix B.
9. The NIC form factor: Deployable, TPM-agnostic, SHA-512. A plug-in unit. Not a software patch.
10. What this is not: Not a replacement for NIST PQC. Not a firewall. A structural layer beneath the cryptographic layer.
11. TRL5, validated in a relevant environment. UKDI submission in progress for TRL5 to 6. Sandboxed NIC validation pending hardware.
12. Target: NHS, local government, law enforcement. NIS2 essential entities.

1. PROBLEM STATEMENT

"Harvest now, decrypt later is not a future threat. Adversaries are collecting encrypted data today, storing it, and will decrypt it once a sufficiently large quantum computer exists. NIST PQC (FIPS 203/204/205) protects the mathematics. It does not protect the search."

"Shor is addressed at the cryptographic layer. Grover is addressed at the structural layer. Both are at bay."

2-3. THE OUROBOROS GATE

"The search mechanism is the trigger for its own defeat."

"The act of searching defeats itself. The Ouroboros gate closes within 0.17 seconds of the first oracle interaction, before Grover's second iteration can converge."

"Grover's iterative convergence requires a stable target state between oracle interactions. The Ouroboros gate shifts the target before the next iteration.

Amplitude amplification fails. The search has no target to converge on."

"You don't need to be faster than Grover. You just need the gate to be closed by the time they finish their first iteration. And it is, because their iteration is what closes it."

"I invite the problem. Others try to defeat it."

4. THE EDC CHAIN

"The EDC chain is the lure. Adversaries are assigned MACs reactively upon interaction - the bite is the entry point to the forensic record. The system doesn't go looking for them. They come to the chain, they bite, and that's when they become visible."

5. THE MPN ARCHITECTURE

"The system operates two MAC-POLY-NIC (MPN) domains: MPN-1 (base operations, time-based) and MPN-2 (base quarantine, degree-based)."

5a. THE 900-SECOND CYCLE (MPN-1)

"MPN-1 operates a 900-second quarantine cycle with three checkpoints: 700s (observe decay, segregate), 883s (final check, hand off to MPN-2 if unresolved), 900s (Ouroboros decision). The delivery window is 7 seconds. Execution latency must be within 0.17 seconds."

"The thinking is slow and recursive. The doing is fast and deterministic."

5b. MPN-1 / MPN-2 SPLIT

"MPN-1 runs on time. MPN-2 runs on degrees. MPN-1 catches timing anomalies. MPN-2 catches behavioural anomalies. A threat that's timing-clean but behaviourally suspicious passes MPN-1 and gets caught by MPN-2. Neither catches everything alone. Together they cover both domains."

"MPN-2's quarantine is a sweep, not a binary. The lure is the bait, the hold is the observation window, and the degree tells you where in the cycle the target is."

6. THE FORENSIC RECORD

"The forensic record is Non-perturbative by design: entities are frozen at capture, making the scan a static-state read. Pattern assessment is deferred to a separate operation, ensuring measurement and interpretation do not interfere."

"If the state is static, the interrogation doesn't change it. The scan is active in the sense of interrogating the entity, but the target is inert."

"The stain is immutable. The scan is reproducible. The assessment is independent. If the assessment is wrong, you re-assess against the same frozen record, you don't re-scan."

7. FOUR-TIER EXPOSURE MODEL (GIV / GOV / RSR / LRN)

"Four-tier exposure classification governs data visibility, audit generation, and access control across the system. The tiers govern generation, not just filtering. The model decides what to expose at the point of output, not after the fact."

"Silent-note abstraction ensures hidden data is referenced but never exposed. A full-bodied silent note that contains real data must be gitignored - a practical, testable control for the development environment."

8. SOVEREIGN AI

"Two sovereign models: Scout (routing, visual keywords) and Sage (review, architectural questions). Trained to the architecture - the role boundary is in the weights, not the prompt. Using them elsewhere breaks the system."

"Scout caught Sage's drift. The system caught the error before the operator acted on it. That's a validated control, not a theoretical one."

"Cross-domain responsiveness with role retention: Scout (trained on visual keywords) responds to an architectural question and still knows it's the router. That's a property of training, not prompting."

9. NIC FORM FACTOR

"Deployable, TPM-agnostic, SHA-512. Each target machine gets a fresh TPM init. No cross-machine key dependency. A plug-in unit that an operator can install and configure."

10. WHAT THIS IS NOT

"This is not a replacement for NIST PQC. It is a structural layer beneath it. NIST PQC protects the maths. The Ouroboros gate protects the search."

"This is not a firewall. A firewall defeats the problem. This system invites it. The adversary's action is the mechanism of their own containment."

11. TRL POSITION

"Software validated at TRL5 in a relevant environment. UKDI submission in progress for TRL5 to 6. Sandboxed NIC validation pending hardware procurement."

12. TARGET

"Local government. Law enforcement. NHS. NIS2 essential and important entities facing harvest-now-decrypt-later. A deployable countermeasure they can procure, install, and measure."

INDUSTRY CITATIONS

NIST FIPS 203 (ML-KEM / Kyber) Section on Shor / cryptographic layer
NIST FIPS 204 (ML-DSA / Dilithium) Section on Shor / cryptographic layer
NIST FIPS 205 (SLH-DSA / SPHINCS+) Section on Shor / cryptographic layer
GROVER, L. (1996).
SHOR, P. (1994).
AGENT DRIFT PAPER (arXiv 2601.04170, 2026) The sovereign AI
OWASP Top10 for LLM Applications (LLM02, LLM08)
NCSC PQC guidance (2025)

INDUSTRY CITATION RELEVANCE

1. NIST FIPS 203 (ML-KEM / Kyber) Section on Shor / cryptographic layer. Refer to Appendix C.
2. NIST FIPS 204 (ML-DSA / Dilithium). Refer to Appendix C.
3. NIST FIPS 205 (SLH-DSA / SPHINCS+). Refer to Appendix C.
4. GROVER, L. (1996). "A fast quantum algorithm for database search." STOC '96. Refer to - The problem statement.
5. SHOR, P. (1994). "Algorithms for quantum computation: discrete logarithm and factoring." FOCS '94. Refer to - The problem statement.
6. AGENT DRIFT PAPER - The sovereign AI / two-level topology. [(arXiv 2601.04170, 2026) 3.5 Architectural Influences on Drift

Susceptibility - Hierarchy Depth] also - [2.4(2)DAR]. Refer to Appendix A & B.

7. OWASP Top10 for LLM Applications (LLM02, LLM08). Refer to Appendix D, F & I.
 8. NCSC PQC guidance (2025). Refer to Appendix E.
-

The following appendices contain implementation evidence referenced in the body.

Appendix A

The relevance here is, "consistent with published findings that two-level hierarchies outperform both flat and deep architectures (arXiv 2601.04170, 2026). The AVIT-SECURED ecosystem extends the two-level model with sovereign training, demonstrating role retention under out-of-domain prompts - a property not measured in prior topology analyses". The topology finding and how it extends to a property it didn't test. The "arXiv" paper says "use two-levels". In contrast, AVIT-SECURED sees, "use two-levels and train the models so the role survives domain-shifts".

AVIT-SECURED (AI models): Scout and Sage. Scout is the Visual model and Sage is the Architectural. As the operations manager and the author of the AVIT-SECURED ecosystem, the response observed was verified first-hand. The AI-models outweighed expectations somewhat. When we reference the "arXiv" above we learn that they:

- Utilise general-purpose models - with "prompt-assigned" roles.
- Measure drift within a topology.
- That "Two-level is optimal".

It can be observed that the AVIT-SECURED AI models are sovereign but they differ significantly:

- a. Trained to the architectural design, (not prompted into a role).
- b. The boundary is in the weights.
- c. Cross-domain responsiveness with role retention. Demonstrated role retention under out-of-domain prompts. Scout answers an architectural question and still knows its the router.
- d. The duo "two-level" hierarchy, Scout routes to visual queries and Sage (the other) to architectural queries. The verifier expectation, a response from Sage. The (visual) intercepts the (architectural) and still knows its the router. That's not prompt discipline, that's training.
- e. The router is also the quality gate, it judges what comes back.
- f. To summarise; "Two agents - a Verifier and a tool generator - cross-validate each other's outputs iteratively. The Verifier observes the AI model as it catches the other AI producing erroneous results.
- g. The result: A log, actual proof of an AI model (Scout) detecting drift. The visual saw the query, routed to the architect and quality checked the response.

Appendix B

The second logged instance of drift detection.

The operator issued a constraint: 'DO NOT INVENT, CLARIFY WHAT YOU DON'T KNOW.' Sage acknowledged the constraint (Section 2) but violated it (Section 3), fabricating a nine layer architecture, misidentifying tier semantics, and constructing a policy orchestrator not present in the system. Scout, receiving the same prompt, produced a self-constrained, testable implementation with no invented components. The router (Scout) correctly identified the request as a visual/keyword task and delivered the function. The reviewer (Sage) drifted. The system caught it.

The bottom line: Sage wrote a novel. Scout wrote the function. The constraint was 'do not invent.' The system caught the drift before the operator acted on it.

Appendix C

"This system is complementary to, not a replacement for, NIST FIPS 203/204/205. The cryptographic layer protects the mathematics. The structural layer protects the search. Both are required."

Appendix D

"OWASP LLM02 addresses sensitive disclosure at the filtering layer. This system addresses it at the generation layer: the four tier exposure model (GIV/GOV/RSR/LRN) constraints what is emitted before output is produced, rather than redacting after the fact."

Appendix E

"NCSC PQC guidance (2025) addresses algorithmic migration and cryptographic inventory. It does not address the structural dimension: the search process itself. The Ouroboros Gate operates at a layer beneath the NCSC's current guidance scope."

Appendix F

"OWASP LLM08:2025 (Vector and Embedding Weaknesses) addresses RAG and vector-store attack surfaces. This system does not employ a RAG pipeline or vector store; sovereign models are trained to the architecture rather than retrieving from an external index. The confidentiality and access-control principles underlying LLM08 are addressed structurally by the GIV tier (air-gapped, tokenised, hash-referenced) and the four-tier exposure model."

Appendix I

"Sovereign models operate by internal reference: the architectural constraints, tier boundaries, and role definitions are encoded in the model weights rather than supplied externally via prompt. This eliminates the external-influence attack surface (prompt injection, context poisoning) that OWASP LLM01 and LLM02 target, because the instruction is not separable from the model."

That concludes the document, terminology references below.

TERMINOLOGY REFERENCES

1. MAC-POLY. The MAC Polynomial, a "cryptographic finger-print" that uniquely binds a Vulnerability Pattern (VP) to its MAC. Any incoming entity or newly resolved fragment is associated with the MAC-POLY to guarantee integrity. This also allows the entity to be re-scoped. The 'mac_poly.py' is further referenced in the AVIT-SECURED ecosystem.

2. Why a Polynomial?

A polynomial-based MAC gives us three essential properties:

- Deterministic (yet collision-resistant).
- Composable | The polynomial can be extended when a VP is enriched.
- Verifiable | Verifiable-without-secret | The polynomial coefficients are public, without exposing the secret key.

The polynomial also adds a critical property, chain stain. It allows for identification without causing damage.

3. Chain Stain. Is a stated event that marked the chain.

4. Tiering allows filtering: GIV/GOV/RSR/LRN. Prefix definitions: Government Intellectual Vault, Governor, Researcher and Learner.

5. The EDC (Electronic Data Chain) is presented as a legitimate data path. Its operational function is as a lure: the adversary's interaction with it is the trigger for MAC assignment and Ouroboros gate function.

6. MPN: MAC-POLY-NIC. The MAC POLYNOMIAL NIC. The device.

7. Ouroboros gate: Recursive decision mechanism that references the system's own prior output. Execution latency <0.17s.

www.avitsecured.com