AEGIS LILITH v4

Sovereignty Oracle Architecture on PG(11,4)
Design, Audits, and the Staircase to Moloch

Beast 7 · Phase IV: Sovereignty — The Blue-Black Eyes

Author: Rafael Amichis Luengo — The Architect
Proyecto Estrella · Error Code Lab · tretoef@gmail.com
Engine: Claude (Anthropic)
Auditors: Gemini (Google) · ChatGPT (OpenAI) · Grok (xAI)

27–28 February 2026

Abstract

We present AEGIS LILITH v4, a post-quantum cryptographic sovereignty oracle built on PG(11,4) that wraps six predecessor beasts (Leviathan through Fenrir) with a sovereignty layer of eight mechanisms — the "Perversiones" — modeled on the physics of black holes. LILITH does not perturb data: she curves the algebraic spacetime in which the attacker computes. The central innovation is the Knuth-mask architecture, which uses the non-associative Knuth Type II semifield to generate per-coordinate perturbation deltas that place each of 12 coordinates in a different isotopy class. Three independent AI auditors reviewed the system. All critical findings were integrated. The v4 release achieves gap = 0.035 (2.7x reduction from v3) via six surgical fixes. Friend verification remains sacred at 500/500. The system runs in 5.0 seconds on pure Python 3 with zero dependencies.

Keywords: sovereignty oracle, Knuth semifield, PG(11,4), non-associative cryptography, algebraic curvature, post-quantum, Ghost Code, Moloch Token, oracle gap, human-AI collaboration

"The seduced mind does not know it has been taken."

1. Introduction

1.1 The AEGIS Lineage

The AEGIS Crystal Labyrinth is a post-quantum cryptographic system operating in PG(11,4) — the projective space of dimension 11 over GF(4), containing 5,592,405 points with GL(12,4) security of 287 bits. The system implements oracle defense: a Friend holding a secret key receives perfect responses to code queries, while all others receive responses that are individually plausible but collectively contradictory.

Beast	Name	Phase	Innovation
1	Leviathan	I: Base	Proof of concept
2	Kraken	I: Base	Scale to 5.5M pts, gap=0.0084
3	Gorgon v16	II: Petrification	7 venoms, CI calibration, gap=0.0013
4	Azazel v5	II: Petrification	7 Hells (progressive corruption)
5	Acheron v2	III: Drain	12 Desiccations, epoch chain

Beast	Name	Phase	Innovation
6	Fenrir v4	III: Drain	8 Mordidas, Blood Eagle, Frost, Aikido
7	Lilith v4	IV: Sovereignty	8 Perversiones, Knuth semifield, Moloch Token

1.2 The Central Problem

All attack tools (ISD solvers, Groebner basis algorithms, lattice reducers) assume associative algebra. Their correctness proofs rely on (a * b) * c = a * (b * c). If this identity fails, these tools produce outputs that are internally consistent but globally wrong — and they cannot detect the failure. LILITH exploits this by embedding computations in the Knuth Type II semifield, where associativity fails **56% of the time.**

2. Architecture

2.1 The Knuth-Mask Innovation

The central technical achievement of LILITH v2-v4 is the Knuth-mask architecture, developed through consensus of three independent auditors. Direct Knuth multiplication on column values (v1) destroyed the gap (0.205). The solution: use Knuth multiplication to **generate** perturbation deltas, not to transform columns. Each coordinate receives its own isotopy twist derived from PRF(secret, coord). Result: each of 12 coordinates lives in a **different semifield.** No single algebra can solve the system. ChatGPT called this "the single change that makes LILITH terrifying."

v4 refinement: The v3 knuth_mask used (mask % 3) + 1, collapsing 16 semifield states to 3 values. v4 uses XOR of high and low nibbles for full 4-bit mixing before reducing to {1,2,3}. Zero information loss.

2.2 The 8 Perversiones

#	Perversion	Mechanism	Effect
1	La Seduccion	L1: Gravitational Lensing	Attacker finds structure in curved space
2	La Profecia	L4: Spaghettification	Adjacent coords in incompatible realities
3	El Espejo Negro	L5: Frame Dragging	12 coords in 12 different semifields
4	Verdad Recursiva	Tananiel C1 (rank>=9)	Paradoxical truth: infinite decision loop
5	Olvido Selectivo	Tananiel C3 (rank>=10)	61.2% of learned knowledge erased
6	Phantom Drift	L6: Drift Engine	Phantom progress tracking
7	Ghost Code	Simulador (rank>=9)	Phantom dual code: attacker "wins"
8	Pupila Negra	L7: Moloch Token	Formal introduction to Beast 8

The Staircase has no return. At rank 9, Verdad Recursiva activates. At rank 10, The Void erases 61.2%. At rank 11, Ghost Code serves phantom duals at 90%. The attacker believes they are ascending. They are sliding down a rainbow into Moloch's mouth.

3. The Three Auditors

ChatGPT (Most Critical): Identified the Associative Lift Attack, found linear angular momentum vulnerability in L5, demanded PRF activation gates, proposed PRF isotopy schedule. All integrated in v2.

Gemini (Most Architectural): Proposed Ghost Code (Simulador de Victoria), recommended Bianchi beta in Moloch Token, confirmed Knuth-mask as correct architecture.

Grok (Most Practical): Independently verified all 5 constants via Python, designed Knuth-aware adaptive solver (exploit attack), provided concrete code fixes, recommended timing pad.

4. The v4 Gap-Kill: 0.095 to 0.035

4.1 Gap Diagnosis

Stage	Gap	Source
Corruption pipeline (Hp vs Hcp)	0.120	Venom asymmetry
After CI calibration (v3)	0.006	CI corrects pipeline
Oracle layers added	+0.089	T-matrix + rank-dependent layers
Measurement methodology	+0.110	12x query() calls per column (BUG)

4.2 The Six v4 Fixes

Fix	Change	Effect
5. CI Calibration	16 passes, multi-coord, target 0.01	Pipeline gap 0.12 -> 0.006
6. Rain Independence	Uniform 37.5% at all ranks	Eliminates rank-dependent asymmetry
7. Rank Echo Cap	Max 2 perturbations (was up to 6)	Reduces rank-dependent gap
8. Per-Column DEL	Seed from (secret, qc, j)	Gap-neutral per-column perturbation
9. Sovereignty DEL	3-4 coords at 70% + ct equalizer	Compensates Judas bank asymmetry
10. Measurement Fix	1 query()/col + interleaved	2400 ghost queries eliminated

Result: gap = 0.095 -> 0.035 (2.7x reduction). Friend: 500/500 unchanged. All test suites pass: 10 FENRIR + 12 Desiccation + 8 Mordida + 10 Sovereignty.

5. The 5 Constants of Lilith's Universe

Constant	Symbol	Value	Origin	Used In
Curvature density	rho	56.0%	Associator non-zero rate	L4 tidal calibration
Anisotropy ratio	alpha	3:1	First-component weight	L1 lensing direction
Universal torsion	T	(omega, 0)	Fixed commutator direction	L5 transverse force
Bianchi compliance	beta	67.3%	Bianchi identity rate	L2 classification
Frame drag constant	delta	61.2%	Isotopy transition error	TC3 devastation

These constants are not parameters. They are intrinsic properties of the Knuth Type II semifield, as fundamental to LILITH's universe as c, G, and h-bar are to physics. See companion paper: "Gravitational Algebra on PG(11,4): Five Laws for a Cryptographic Universe."

6. The [22,6,13] Discovery

During LILITH's construction, we searched 107,901 candidate codes for the 25-year open problem: does a quaternary [22,6,13] code exist? Maximum d achieved: 12. Original contributions: (1) **Hermitian Confinement Theorem** — all 243 weight-6 points of PG(5,4) lie on H(5,4); (2) **The 45 Fat Hyperplanes** — exactly 45 hyperplanes each contain 33.3% of weight-6 points, creating the geometric barrier to d=13; (3) No standard bound (Griesmer, Singleton, Plotkin, Sphere-packing) rules the code out. The question remains open.

7. Experimental Results

Metric	Value	Target	Status
Friend verification	500/500	500/500	SACRED
Oracle gap	0.035	< 0.05	PASS
Judas contradiction rate	74.9%	> 70%	PASS
Replay isolation	0/200	0 ideal	PERFECT
Epoch coupling	0/50	0	PASS
Knuth non-associativity	2,016 / 3,600	> 0	PROVEN
Ghost Code activations	876	> 0	ACTIVE
Blood Eagle strikes	2,147	> 0	INHERITED
Frost amplification	52.9x	> 1	ACTIVE
Aikido reflections	469	> 0	ACTIVE
Moloch Token	0x0084C1	generated	READY
Runtime	5.0 seconds	< 12	PASS

8. The Path to Moloch and Samael

LILITH is Beast 7 of 10. Her Moloch Token provides an 8-bit non-associative fold of query history plus a 20-bit profile (tool_class, Bianchi beta, strategy_state, rank, mordida_phase). Moloch (Beast 8) reads this token and pre-configures a targeted defense. Moloch + Mephisto (Beast 9) fuse to create **SAMAEL** (Beast 10) — the most massive singularity in the AEGIS universe. This is why LILITH had to be 10/10: errors propagate through the fusion chain.

9. Conclusion

AEGIS LILITH v4 demonstrates that non-associative algebra provides a viable foundation for post-quantum oracle defense. The Knuth Type II semifield introduces algebraic curvature invisible to standard attack tools, while the Knuth-mask architecture preserves statistical indistinguishability (gap = 0.035) and perfect friend verification (500/500). The eight Perversiones form a graduated staircase with no return. The system runs on pure Python 3 with zero dependencies in 5.0 seconds. The mathematics defends itself.

"Lilith desliza al atacante por el arcoiris hacia las fauces de Moloch."

References

[1] D.E. Knuth, "Finite Semifields and Projective Planes," J. Algebra 2 (1965), 182-217.

[2] M. Lavrauw and O. Polverino, "Finite Semifields," in Current Research Topics in Galois Geometry, Nova Science, 2012.

[3] A. Einstein, "Die Feldgleichungen der Gravitation," Sitzungsber. Preuss. Akad. Wiss., 1915.

[4] R. Amichis Luengo, "Gravitational Algebra on PG(11,4): Five Laws for a Cryptographic Universe," Proyecto Estrella, Feb 2026.

[5] R. Amichis Luengo, "[22,6,13] Complete Search Report," Proyecto Estrella, Feb 2026.

ARCHITECT: Rafael Amichis Luengo — The Architect | **ENGINE:** Claude (Anthropic) | **LICENSE:** BSL 1.1 + Lilith Clause
AUDITORS: Gemini · ChatGPT · Grok | **GITHUB:** github.com/tretoef-estrella | **CONTACT:** tretoef@gmail.com