EPEX / EchoPulse: Master Technical Reference

Document 1.0 | Core Lineage, Comprehensive Document Directory, and Repository Map

Author: Tom Wartenberg, System Architect
Target Audience: Technical Auditors, Cryptographers, and Core Developers
Status: Final V1.0 Repository Directory Mapping

1. Technical Lineage & The Architectural Pivot

The Embedded Procedural Expansion Engine (EPEX) repository preserves the complete, transparent record of an iterative cryptographic engineering lifecycle. The project originally launched under the name **EchoPulse**, exploring a high-risk hypothesis: whether asymmetric trapdoor-like structures could naturally emerge from the bitwise feedback loops of a highly customized symmetric Addition-Rotation-XOR (ARX) permutation network.

To verify this, the 16-bit word variant of the EchoPulse v5.2 core was subjected to an exhaustive state-space sweep over all 4.29 billion permutations. The analysis yielded mathematical proof of **perfect bijectivity** (zero inversion failures). Because a pure bijection cannot compress or funnel state entropy at a single-round level, the inherent trapdoor hypothesis was invalidated. Additionally, mapping the quadratic Simon-style AND gate revealed a silent set of exactly 2,207 states, aligning perfectly with the Lucas Number L(16), confirming a highly rigid combinatorial structure.

Rather than introducing artificial mathematical flaws to force asymmetric behavior, the architecture was pivoted. The verified strength of the symmetric block was repurposed as a hyper-fast, seekable, deterministic Extendable Output Function (XOF) to solve the **SRAM bottleneck in Post-Quantum Cryptography (PQC)**. By wrapping this engine around standardized Learning With Errors (LWE) problems, public matrices are transformed from static data blocks in RAM into a stateless, register-resident procedural generator function.

2. Core System Architecture (v1.0 Baseline)

The operational pipeline of the EPEX streaming framework bypasses traditional memory materialization through a specialized register-only data path:

- **Keyed Counter-Mode Injection (Strategy-1):** Spatial coordinate parameters (row and column indices) are mapped bijectively and XOR-injected alongside a compact master seed directly into the 32-bit CPU register state, neutralizing prior coordinate-aliasing vulnerabilities.
- **Permutation Core:** A 6-round ARX sequence (Constants: `A=0x9E37, ROT_BOOL=1, ROT_X=7, ROT_Y=11`) processes the state entirely within local CPU registers, requiring zero intermediate heap or stack cache buffers.
- **Coefficient Extraction:** The scrambled state yields a truncated 1-byte coefficient matching the LWE modulus ceiling (***q=256***), which is used instantly in vector multiplication and evaporated from the register.

3. Comprehensive Project Directory & Document Map

Because each phase of the project was documented at the exact time of execution, the repository contains a cumulative 23-document audit trail. This directory maps those artifacts logically to guide external reviewers and technical auditors.

ARTIFACT ID / RANGE	TECHNICAL FOCUS	REVIEW PURPOSE & REFERENCE
Document 0.1	Executive Summary (Groq Baseline)	High-level management summary, commercial value proposition, and SPRIND/NLnet grant funding context.
Document 1.0	Master Technical Reference	This document. Serves as the primary entry point, lineage record, and complete repository guide.
Documents 2 – 12	Early Symmetric Foundations	Exhaustive bijectivity mapping, Lucas Number L(16) combinatorial verification, and MSB carry saturation tracking.
Document 13	Matrix-Free Streaming Crate	Codebase architecture and mathematical equivalence proofs for eliminating the 1,024-byte static array.
Document 14	Statistical Distinguishability	Empirical validation suites tracking output uniformity, spatial correlation, and ciphertext variance.
Documents 15 – 16	Embedded Hardware Validation	Cycle-accurate profiling and bare-metal compilation logs for target microcontrollers.
Documents 17 – 17.5	Defect Identification & Repair	Analysis of Phase-5 vulnerabilities (dead high seed bits and coordinate aliasing) and the design of the Strategy-1 fix.
Documents 18 – 21	Post-Repair Cryptanalysis Suite	Phase-6 adversarial testing. Includes automated SMT solver runs (Z3), lag-1 autocorrelation testing, and cross-seed stability audits.
Document 22	Bare-Metal Hardware Benchmark	Deterministic footprint analysis on ARM Cortex-M4 confirming the ~2.18 KB Flash size and 0-byte core static SRAM.

ARTIFACT ID / RANGE	TECHNICAL FOCUS	REVIEW PURPOSE & REFERENCE
Document 23	32-Bit Technical Roadmap	Forward-looking feasibility study for Axis A lane widening (v2.0 scaling from 16-bit to native 32-bit registers).

4. Validated Engineering Constraints & Boundaries

To maintain strict academic honesty, the EPEX framework explicitly defines its operational boundaries:

- **Footprint Research Status:** The current codebase uses structural toy parameters (***n=m=32, q=256***) to prove the matrix-free thesis. It is not intended for production secrets until the overlying LWE noise budgets are formally scaled.
- **The Birthday Ceiling:** The internal 16-bit lane configuration limits state collision resistance per coordinate to the birthday bound of ~2^16. This structure is secure against the tested output distinguishers but requires the Axis A 32-bit widening outlined in Document 23 to scale to production-grade cryptographic margins (~2^32 collision resistance).