DRIFT SYSTEMS

THE DRIFT PRIMER

The Case for Native Digital Chaos in the Post-Quantum Era

Prepared For: Strategic Partners & Technical Review

Date: December 2025

Status: TRL-6 Validated (24B+ Cycles)

IP Portfolio: 16 Patents Pending

Contents

1 The Entropy Crisis

The industry is currently trapped between two inadequate paradigms for generating entropy.

Analog TRNGs rely on physical phenomena like thermal noise or oscillator jitter. While statistically random, they suffer from inherent physical latency (waiting for entropy to accumulate) and environmental bias (temperature drift), rendering them unreliable for high-speed, precision control loops.

Conversely, standard **Digital CSPRNGs** (like AES-CTR) provide robust security but impose a heavy computational tax. They rely on complex S-Box substitutions and matrix multiplications that require over 3,500 logic gates and multiple clock cycles to initialize. This architecture generates significant dynamic power heat—a "Thermal Tax"—that is prohibitive for cryogenic environments, bio-implants, and energy-starved edge devices.

There is currently no primitive that delivers cryptographic-grade entropy with the **zero-latency speed** of a simple logic gate and the **near-zero thermal profile** required by next-generation hardware.

The Drift Thesis

The industry needs Native Digital Chaos. We generate cryptographic-grade entropy using the inherent physics of digital logic—Shift and Add—without the overhead of multipliers or analog circuitry.

2 Discrete Arithmetic Dynamics (DAD)

The core innovation of Drift Systems is the rejection of "simulated" randomness in favor of **Native Digital Chaos**. We utilize the inherent non-linear properties of binary addition to generate entropy.

2.1 The Core Mechanism

The Drift Engine operates on a 128-bit (or 256-bit) state register. It generates a stream of non-repeating, high-entropy numbers by cycling through three distinct atomic operations in a single clock cycle:

1. **THE PUSH (Expansion):** The state S is subjected to an affine transformation ($qS + d$). The multiplication by an odd integer (e.g., $q = 3$) creates a **Carry Chain Avalanche**.
2. **THE SQUEEZE (Drift):** We prevent short cycles via Forced Drift. By restricting the division step, we guarantee the internal trajectory wants to grow to infinity.

3. **THE FOLD (Mixing):** Since infinite growth is impossible on a finite chip, we Fold the overflow back into the lower bits, creating a non-linear trapdoor.

2.2 The Unified Core (Stream + Hash)

Unlike legacy chips that require separate blocks for Encryption (AES) and Hashing (SHA), the Drift Core is **Reconfigurable**.

- **Stream Mode:** The core generates infinite entropy for encryption.
- **Sponge Mode (Hash):** The core absorbs external data (via XOR injection) and mixes it using the arithmetic carry chain.
- **Benefit:** A single 686-gate circuit performs both functions, reducing silicon area by 50%.

3 The Trust Architecture: Provable Math

For a new cryptographic primitive, trust is paramount. Users must know that the generator does not hide ”Dark Corners” (unreachable states) or ”Backdoors” (secret cycles). We address this via two fundamental mathematical proofs.

3.1 1. Provable Ergodicity (Dynamic Covering Systems)

We utilize a **Dynamic Covering System** (Erdős Covering). The transition function $f(S)$ is not static; it changes based on the residue of the state modulo a set of primes. We mathematically prove that the union of these transition rules covers the entire integer set $\mathbb{Z}$. There are no ”Orphan States.” The generator is structurally forced to visit the entire state space (Ergodicity), making hidden backdoors algebraically impossible.

3.2 2. Computational Irreducibility (Conway Maps)

We utilize **Undecidable Dynamics** based on the Generalized Collatz Problem. The ”Conway Core” switches between multipliers $(3n, 5n, 7n)$ based on the state’s modulo properties. This system is **Tur-

ing Complete**. Predicting the state at $t + k$ without running k steps is equivalent to solving the Halting Problem. The stream is **Computationally Irreducible**, making it a perfect Verifiable Delay Function (VDF).

4 Metrics & Validation (TRL-6)

4.1 1. The Silicon Footprint (686 Gates)

Industry Standard (AES-128): Requires $\approx$ 3,500 to 10,000 gates.
Drift Core (DC-100): Synthesizes to **686 Logic Cells**.
Impact: The Drift Core is **5x smaller** than the smallest AES implementation.

4.2 2. Physical Validation (Soak Test 2025)

On December 4, 2025, the Drift Core achieved TRL-6 via a continuous hardware soak test.

- **Stability:** $> 24,000,000,000$ (24 Billion) cycles with **0.00% Divergence**.
- **Resilience:** Validated ”Self-Healing” capability. During a simulated ”Signal Blackout” (Host LOS), the core continued blind operation for 115 million cycles. Upon reconnection, the software shadow model automatically re-synchronized in < 100ms.

5 Strategic Applications

5.1 Defense & Aerospace: The ”Anti-Jamming” Shield

Drift-Hop™: Tactical radios hop frequencies in 1 clock cycle (Zero Latency), faster than enemy jammers can react (”Look-through” capability).

5.2 Medical & Bio-Implants

Bio-Drift™: Zero-Multiplier architecture reduces dynamic power draw to $< 5\mu W$, enabling secure authentication for pacemakers without heating tissue.

5.3 Logistics: "The Internet of Disposables"

Drift-Tag™: A printed electronics label that changes its digital identity every time it is scanned, making supply chain cloning mathematically impossible.

5.4 Web3 & Data Integrity: The "Trustless" Oracle

Drift-Sponge: The Unified Core validates data integrity (Hashing) and proves computational work (VDF) for blockchain networks.

- **Validation:** In TRL-6 testing, the core demonstrated a **50% Avalanche Effect**, proving that a single bit-flip in the input completely rewrites the output state within 20 cycles. This enables "Hardware Hashing" on devices too small for SHA-256.

6 The Vision: Security as Physics

Drift Systems Inc. proposes a new paradigm: **Security as Physics.** By embedding the Drift Core into the fundamental logic gates of the semiconductor, we transform security from a "Computational Task" into a "Physical Property" of the chip.

Join the Pilot Program

Drift Systems Inc. is currently selecting strategic partners for early access to the Drift Core IP (Verilog/SystemC) and the Drift-Mark AI SDK.

Contact:
Lukas Cain, Systems Architect
licensing@driftsystems.io
https://driftsystems.io

Contact: Lukas Cain — lukas@driftsystems.io
US Patent Pending. Export Controlled Technology (EAR99).