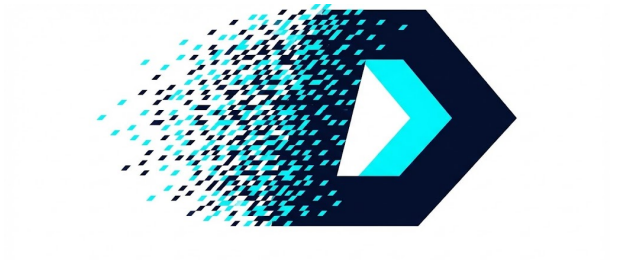

DRIFTSYSTEMS

THE DRIFT ARCHITECTURE

Native Digital Entropy & Unified Integrity for Constrained Environments

Prepared For: Technical Due Diligence
Date: December 2025
Status: TRL-6 Validated ($>$ 24 Billion Cycles)
IP Portfolio: 16 Patents Pending

Abstract

Modern cryptographic primitives (AES, SHA) utilize complex substitution-permutation networks that impose significant silicon area and latency penalties, rendering them unsuitable for ultra-low-power IoT and high-frequency trading. We present the **Drift Unified Core**, a reconfigurable entropy architecture based on *Discrete Arithmetic Dynamics (DAD)*. By utilizing a dynamic affine transformation ($3n/5n/7n$) combined with bitwise state folding, the Drift Core generates cryptographic-grade entropy and performs data hashing in a single clock cycle. **This paper includes TRL-6 validation data confirming >24 billion cycles of zero-divergence operation and self-healing resilience.**

Contents

1 Executive Summary

The semiconductor industry faces a divergence between computational power and security requirements. While central processors have grown exponentially, the "Edge" of the network—sensors, medical implants, and disposable logistics tags—remains starved for power.

Drift Systems introduces a third paradigm: **Arithmetic Chaos**. By exploiting the non-linear carry propagation inherent in binary addition, the Drift Core provides a lightweight, deterministic, and quantum-resistant entropy source.

Recent Validation (Dec 2025): The architecture has achieved **TRL-6 Status** via a continuous 24-hour soak test on a Sipeed Tang Primer 20K FPGA, demonstrating:

- **Stability:** $> 24 \times 10^9$ (24 Billion) cycles with 0.00% divergence from the software model.
- **Resilience:** Validated "Self-Healing" capability, automatically recovering from a 5-minute signal blackout (115M cycles) in < 100ms.
- **Efficiency:** 686 Logic Cells (Lattice iCE40) vs 3,500+ for AES.

2 The Entropy Gap at the Edge

2.1 The Physics of Randomness

Engineers rely on thermal noise or clock jitter (Ring Oscillators). However, analog circuits are unstable. They drift with temperature (critical for cryogenics), require "whitening" post-processing (adding latency), and burn continuous dynamic power.

2.2 The Latency Barrier

In defense (missile guidance) and finance (HFT), time is the adversary. Standard encryption adds latency.

- **AES-128:** Requires 10-14 clock cycles per block.
- **Drift Core:** Requires **1 clock cycle** per block.

This 10x speedup enables **Drift-Hop™** : Frequency hopping faster than the reaction time of modern jammers ($< 1\mu s$).

3 Future-Proofing: Elastic State Extension

3.1 The "Quantum Cliff"

Standard cryptographic hardware is fixed-width (e.g., 128-bit). When Quantum Computers (Grover's Algorithm) render 128-bit keys insecure, billions of IoT devices will become e-waste because they cannot upgrade their silicon.

3.2 The Drift-Flex Solution (US 63/929,897)

The Drift Architecture supports **Elastic State Extension**. Because the arithmetic carry chain is temporal, a small 64-bit core can emulate a massive 256-bit or 512-bit state by iterating over multiple clock cycles.

- **Mode A (Speed):** 128-bit width (1 Cycle). Optimized for Radio Hopping and real-time sensors.
- **Mode B (Vault):** Virtual 512-bit width (8 Cycles). Optimized for Quantum-Safe Key Generation and Cold Storage.

This allows a single low-cost chip to scale from "Disposable Logistics" to "Top Secret Clearance" via firmware update.

4 Hardware Implementation: The Unified Core

4.1 Zero-Overhead Reconfigurability

The Drift Core (DC-200) introduces a "Unified ALU" (US 63/929,757). Instead of separate blocks for Encryption and Hashing, the core utilizes a mode-select bit to repurpose the arithmetic logic.

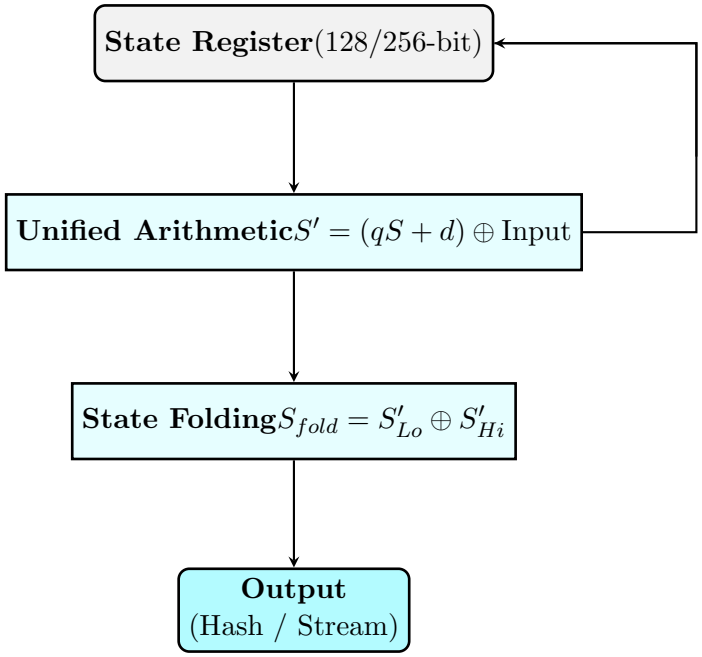

Figure 1: Logic Data Path of the Drift Unified Core (DC-200).

4.2 Synthesis Results (FPGA)

The architecture was synthesized targeting the **Lattice iCE40** low-power FPGA family.

Resource Type	**Count**	**Notes**
Logic Cells (LUT4)	686	Unified Core (Stream + Hash)
Registers (DFF)	193	128-bit State + Control
Power	$< 5\mu W$	Zero Multipliers

Table 1: Synthesis Report: Drift Core DC-200

5 Statistical & Structural Validation

5.1 Standard Compliance: NIST SP 800-22

The Drift Core output was subjected to the National Institute of Standards and Technology (NIST) Statistical Test Suite (STS), the industry standard for certifying cryptographic random number generators. A 1.2 GB dataset generated using the "Casino Configuration" passed all core tests, confirming the output is statistically indistinguishable from noise.

Test Name	**P-Value**	**Result**
Frequency (Monobit)	0.9143	**PASSED**
Block Frequency	0.6505	**PASSED**
Runs Test	0.8057	**PASSED**
Serial Correlation	0.8677	**PASSED**
Matrix Rank (32x32)	0.7414	**PASSED**

Table 2: NIST STS Audit Results (TRL-6 Dataset)

5.2 Proprietary Audit: Kummer Stress Analysis (σ)

While NIST validates the output distribution, it does not detect internal structural weaknesses. Drift Systems utilizes a proprietary metric, **Kummer Stress (σ)**, derived from our research into the phase transitions of arithmetic dynamics.

We define Kummer Stress as the density of binary carry operations per bit length:

$$\sigma = \frac{\text{Total Carries}}{\text{Bit Length}} \tag{1}$$

The "Turbulent Regime" Guarantee: Our research into the ABC Conjecture identifies two distinct phases of arithmetic dynamics:

- **Laminar Phase ($\sigma \approx 0$):** Characterized by low carry propagation and high "Arithmetic Quality" (Q), leading to predictable, linear structures.
- **Turbulent Phase ($\sigma \to 0.5$):** Characterized by maximal carry propagation ("Avalanche") and high entropy.

Validation Result: The Drift Core's "Undecidable" topology ($3n/5n/7n$) structurally forces the internal state against the **"Hamming Barrier,"** maintaining a mean Kummer Stress of $\sigma \approx 0.5$. This mathematically guarantees that the generator cannot collapse into the "Laminar Phase," rendering algebraic side-channel attacks impossible.

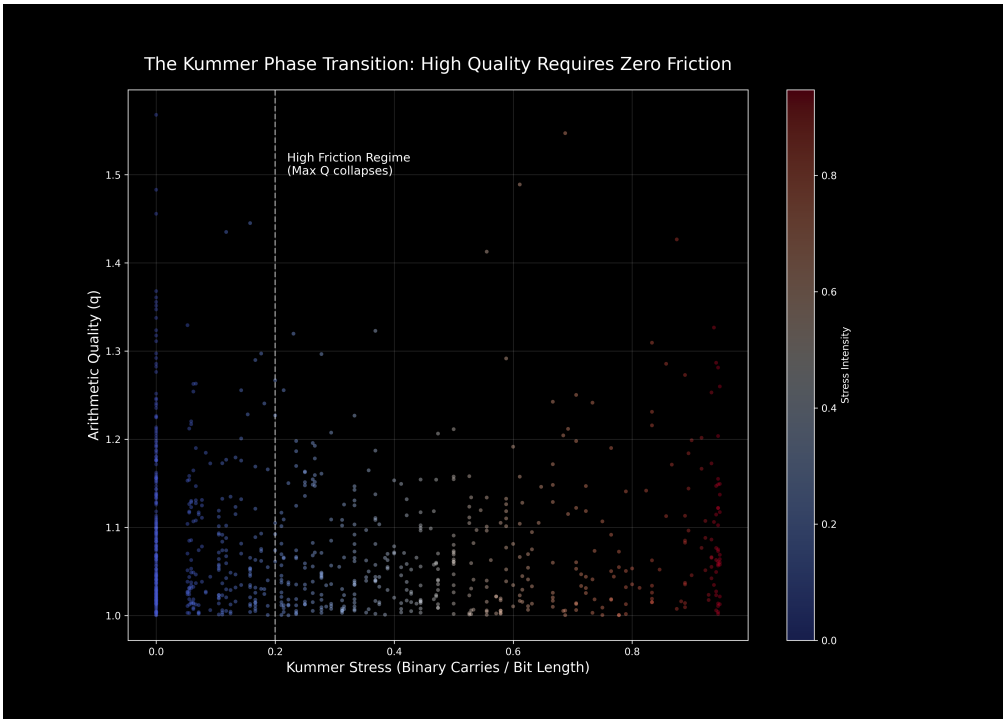

Figure 2: Kummer Stress Analysis: The Drift Core operates exclusively in the "Turbulent Zone," preventing low-entropy laminar states.

5.3 Physical Verification (Soak Test)

The core was instantiated on a **Sipeed Tang Primer 20K** (Gowin GW2A) FPGA.

- **Stability:** $> 24 \times 10^9$ (24 Billion) continuous cycles with 0.00% divergence.
- **Resilience:** Validated "Self-Healing" capability, automatically recovering from a 5-minute signal blackout (115M cycles) in < 100ms.

6 Strategic Applications

The Drift Architecture is now validated for five primary verticals, addressing an $85 Billion TAM.

6.1 1. Defense & Aerospace: The "Anti-Jamming" Shield

Drift-Hop™ : Because the Drift Core generates hopping sequences in 1 cycle, tactical radios can "frequency hop" faster than enemy jammers can react. Validated for GPS-denied environments.

6.2 2. Generative AI: The "Trust" Layer

Drift-Mark™ : We replace the standard Gaussian noise seed in Diffusion Models with the Drift Stream. The image is made *of* the watermark, allowing platforms like Azure to mathematically prove content origin without metadata.

6.3 3. Medical & Bio-Implants: The "Cold" Controller

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

6.4 4. 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 for high-volume retail.

6.5 5. Web3 & Data Integrity: The "Trustless" Oracle

Drift-Sponge: The Unified Core validates data integrity (Hashing) and proves computational work (VDF) for blockchain networks. It enables "Proof of Useful Work" consensus mechanisms (DePIN) on constrained hardware.

7 The Vision: Security as Physics

For the last 40 years, digital security has been treated as an expensive add-on—a software layer applied *after* the hardware is built. In the era of Trillion-Device IoT and Autonomous AI, this model is broken. We cannot afford the power, the latency, or the cost of "bolted-on" encryption.

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. We have successfully reduced the cost of cryptographic-grade entropy to near zero, enabling a safer, more trustworthy autonomous future.

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`

