Kinematic Footprints for Auditable True Random Number Generators

Replacing early opaque cryptographic whitening with two-layer geometric trajectory verification

shahiN Noursalehi
(mixoftix@gmail.com)

Abstract—Conventional True Random Number Generators (TRNGs) rely on immediate cryptographic whitening—such as linear-feedback shift registers (LFSRs) or hash functions—to condition raw physical noise into uniform bitstreams. While effective at removing statistical bias, the strict avalanche property of cryptographic whiteners destroys structural visibility, making it difficult to audit the underlying physical process or detect partial hardware degradation without opaque statistical post-processing. In this paper, we present a human-auditable TRNG architecture implemented on an 8-bit ATmega328P microcontroller coupled with four asynchronous 8 MHz Pierce crystal oscillators and a 74HC74 dual D flip-flop. Rather than masking raw oscillator jitter behind an early black-box whitener, our system maps physical jitter into the initial conditions and mid-flight aerodynamic wind vectors of an embedded 2D rigid-body die-drop physics engine. Furthermore, we introduce a novel "Kinematic Footprint" verification framework that decomposes drop trajectories into a two-layer acceptance law: Stage 1 inspects the collision-free initial free-fall segment to verify entropy-source health against weakened pre-drop shuffles, while Stage 2 evaluates post-impact parabolic rebound angles and signed lateral drift across both multi-bounce terrestrial drops and zero-impact orbital regimes. Optimized via monotonic velocity projections into a 40-byte, inverse-trigonometric-free routine in volatile SRAM, this architecture provides a self-contained defense against replay states and hardware faults prior to final Key Derivation Function (KDF) extraction.

INDEX TERMS:
True Random Number Generator (TRNG), hardware security, metastability, rigid-body physics simulation, dynamical systems, health testing, key derivation, cryptographic entropy.

I. INTRODUCTION

Cryptographic key generation—particularly for offline, air-gapped asymmetric key pairs and cryptocurrency seed material—depends fundamentally on the unpredictability and integrity of the underlying entropy source. Recent high-profile cryptographic failures have demonstrated that flaws in pseudo-random number generators (PRNGs), uninitialized entropy pools, or silently degraded hardware noise sources can collapse a nominal 256-bit keyspace into a trivially searchable subset.

In standard TRNG architectures (e.g., NIST SP 800-90B compliant designs [1]), raw physical noise is fed directly into a conditioning stage such as a cryptographic hash function or block cipher. While mathematically sound for uniformity, early cryptographic conditioning introduces an auditability trade-off: because a single bit change at the input completely scrambles the output (the avalanche effect), an external auditor cannot visually or geometrically distinguish between a healthy multi-oscillator entropy source and a degraded source whose output is merely being masked by a strong hash.

Conversely, purely mechanical entropy sources such as physical dice throws are intuitively auditable by humans, yet classical mechanics research—notably Diaconis et al. [2] and Kapitaniak et al. [3]-has shown that realistic, low-energy

die throws obey deterministic trajectories that retain a measurable statistical bias toward their initial bottom orientation, particularly on high-damping surfaces.

To combine the physical unpredictability of silicon jitter with the structural transparency of classical mechanics, this work proposes a transparent physical conditioning pipeline:
1. A multi-crystal oscillator and flip-flop metastability stage harvests raw hardware entropy.
2. An embedded 2D rigid-body physics engine acts as a non-avalanche, auditable mixing medium driven by live mid-flight hardware jitter ("crystal wind").
3. A two-sided Kinematic Footprint health test inspects the physical trajectory before passing oversampled outcomes into a standard cryptographic KDF extractor.

Related Work and Literature Distinction:
Prior hardware TRNG research has addressed entropy monitoring and dynamical mixing along two primary tracks, neither of which provides human-auditable geometric state inspection. First, standardized online health-testing frameworks—most notably NIST SP 800-90B [1] and BSI AIS 20/31 [4]—mandate continuous statistical watchdogs (such as Repetition Count Tests, Adaptive Proportion Tests, and total-failure monitors) alongside stochastic entropy bounds. While effective at flagging stuck-at-zero or heavily biased digital bitstreams, these scalar bit-frequency counters operate blindly on post-digitized symbols and offer no physical insight into intermediate mechanical or circuit trajectories. Second, chaos-based TRNG architectures [6] exploit continuous-time nonlinear analog oscillators (such as Chua circuits) or discrete chaotic maps to amplify physical noise, yet they typically digitize analog voltages immediately into XOR or LFSR scramblers—reintroducing the exact black-box avalanche opacity that prevents visual auditing. In contrast, our architecture embeds a discrete-time 2D rigid-body mechanical simulation perturbed mid-flight by asynchronous crystal oscillator wind, preserving continuous geometric trajectory footprints (Kinematic Footprints) that can be verified via lightweight trajectory divergence before final KDF extraction.

Consequently, the Kinematic Footprint bridges a longstanding divide in hardware entropy conditioning: through multi-bounce corner discontinuities and mid-flight crystal wind perturbations, it achieves input sensitivity comparable to a cryptographic hash's avalanche effect—where microscopic physical variations drive the die onto completely different resting faces—while simultaneously preserving full geometric auditability across the intermediate trajectory.

Table I contrasts the structural and operational trade-offs between early-stage cryptographic hash conditioning and the proposed rigid-body physics conditioning approach.

TABLE I

COMPARISON OF RIGID-BODY PHYSICS CONDITIONING VS. CRYPTOGRAPHIC HASH WHITENING		
Feature	**Physics Simulator (Decent Dice)**	**Cryptographic Hash (SHA-256)**
Output Uniformity	Depends on physical energy & bounce count (can show bias at low energy)	Mathematically uniform across the full 256-bit space
Input Quality Visibility	Transparent: Weak/low-energy inputs visibly fail to randomize	Opaque: Masks weak inputs by making even a bad seed look uniform
Runtime Jitter Harvesting	Samples live execution timing across thousands of variable branches	Runs once in microseconds on static inputs
Compute Cost per Outcome	High (thousands of floating-point & collision steps)	Extremely low (~1 microsecond)
Primary Strength	Studying physical chaos, mechanical bias, and timing jitter	Condensing raw entropy into uniform cryptographic keys

II. HARDWARE ENTROPY SOURCE ARCHITECTURE

The hardware platform ("Personal TRNG") is constructed using discrete, inspectable off-the-shelf components to eliminate opaque black-box silicon:

- Microcontroller: ATmega328P operating on its internal 8 MHz RC oscillator.

- Oscillator Array ("Shutter System"): Four independent 8 MHz fundamental-mode quartz crystals biased into their linear regions via 10 MOhm feedback resistors across unbuffered 74HC04 CMOS hex inverters. Operating without external discrete load capacitors allows natural stray PCB and pin capacitance tolerances to separate the four oscillation frequencies slightly, preventing injection locking.

- Metastability & Phase-Jitter Capture: Pairs of asynchronous oscillator outputs drive the Data (D) and Clock (CLK) inputs of a 74HC74 dual D flip-flop. Because the free-running oscillators drift continuously relative to one another, rising CLK edges periodically violate the flip-flop's setup and hold time windows, driving the bistable latch into metastability and resolving thermal noise into hardware interrupt triggers (INT0 and INT1).

Additional PCB-level metastability and clock-coupling mechanisms of the v1.0 hardware layout are detailed in Appendices A and B.

III. AERODYNAMIC PHYSICS CONDITIONING & RUNTIME JITTER

Instead of routing captured jitter directly into a cryptographic hash, the firmware uses harvested entropy to parameterize a 2D rigid-body square die simulation (extending the open-source Decent Dice model).

A. Initial Parameter Randomization

Before each drop, hardware jitter randomizes the die's initial drop height, angular orientation (theta), initial angular velocity (omega), surface material coefficients (restitution, kinetic friction, adhesion), and environmental parameters (ambient temperature T, relative humidity, and altitude h). Effective gravitational acceleration g(h) is scaled using the inverse-square Earth-radius relation:

$$g(h) = g_0 * (R_E / (R_E + h))^2 \quad (1)$$

where g_0 = 9.81 m/s^2 and R_E = 6371 km.

B. Mid-Flight "Crystal Wind" & Aerodynamic Coupling

A key limitation of offline physics simulations is that once initial conditions are fixed, trajectory integration becomes deterministic and replayable. To inject continuous non-determinism during execution without calling software PRNGs mid-flight, all four crystal oscillator outputs are wired directly to GPIO port pins (PINC.0–PINC.3) and sampled asynchronously during numerical integration steps as a four-directional wind vector W = (W_x, W_y):

$$W_x = (PINC.0 - PINC.1) * W_{scale}$$
$$W_y = (PINC.2 - PINC.3) * W_{scale} \quad (2)$$

To couple these discrete logic gusts into physically authentic rigid-body forces rather than additive noise, the engine computes local air density rho(h, T) from simulated altitude h and temperature T (in Kelvin) via the barometric-ideal gas approximation:

$$rho(h, T) = rho_0 * (T_0 / T) * exp(-h / H_s) \quad (3)$$

where rho_0 = 1.225 kg/m^3, T_0 = 288.15 K, and H_s = 8.5 km is the atmospheric scale height. Thus, near sea level (h -> 0), crystal wind exerts full aerodynamic coupling, whereas in high-altitude low-pressure regimes (rho -> 0), wind forces naturally vanish.

At each integration step, the instantaneous projected cross-sectional width A(theta) of the rotating square die of side length L (varying from L at theta = 0 deg to L*sqrt(2) at theta = 45 deg) is given by:

$$A(theta) = L * (|cos(theta)| + |sin(theta)|) \quad (4)$$

Defining relative air velocity as v_rel = (v_rel,x, v_rel,y) = (V_x - W_x, V_y - W_y) with magnitude |v_rel| = sqrt(v_rel,x^2 + v_rel,y^2), the quadratic aerodynamic drag force vector F_drag = (F_drag,x, F_drag,y) is computed as:

$$F_{drag,x} = -0.5 * rho(h, T) * C_d * A(theta) * |v_{rel}| * v_{rel,x}$$
$$F_{drag,y} = -0.5 * rho(h, T) * C_d * A(theta) * |v_{rel}| * v_{rel,y} \quad (5)$$

where C_d is the bluff-body drag coefficient. Simultaneously, angular rotation omega induces a perpendicular Magnus lift force F_magnus = (F_magnus,x, F_magnus,y) proportional to (omega x v_rel):

$$F_{magnus,x} = -C_m * \rho(h, T) * A(\theta) * \omega * v_{rel,y}$$
$$F_{magnus,y} = +C_m * \rho(h, T) * A(\theta) * \omega * v_{rel,x} \quad (6)$$

where C_m is the Magnus lift coefficient. The resulting linear accelerations a_x = (F_drag,x + F_magnus,x) / m and a_y = -g(h) + (F_drag,y + F_magnus,y) / m update V_x and V_y at each step. Because corner-impact collision branching causes each loop iteration to execute in a variable number of CPU cycles, sampling PINC mid-flight couples real-time oscillator phase drift directly into the die's velocity vectors, breaking deterministic replayability whenever the hardware wind jumper is enabled.

IV. KINEMATIC FOOTPRINT HEALTH TESTING

In handwritten biometric signature verification (such as Dynamic Time Warping [7]), authenticity requires two simultaneous conditions: the macro-geometry of the stroke must conform to a valid physical motion envelope, while micro-variations between consecutive signatures must remain non-zero (preventing exact replay forgery).

Because our physics conditioner preserves geometric continuity rather than enforcing a cryptographic avalanche, every drop trajectory decomposes naturally at discrete floor impacts t_1, t_2, ..., t_N (where minimum corner height min(y_vert) <= 0) into two fundamental kinematic regimes:

1. Initial Free-Fall Curve (S_0 on [0, t_1)): A single downward descent from release height y_0 to the first corner collision at t_1.
2. Post-Impact Rebound ("Shooting") Arcs (S_k on [t_k, t_{k+1}) for k = 1, ..., N): A sequence of upward ballistic launches following each impact, where the die rises against gravity, reaches a local apex defined by zero vertical velocity (V_y = 0), and falls back to the subsequent impact t_{k+1}.

A. Governing Ballistic & Apex Equations

Within each flight segment S_k, vertical velocity V_y(t) and position (x(t), y(t)) evolve under gravity g(h) and instantaneous aerodynamic acceleration a_aero(t) = (F_drag + F_magnus) / m:

$$V_y(t) = V_y(t_k^+) - g(h)*(t - t_k) + \int_{t_k}^{t} a_{aero,y}(\tau)\, d\tau \quad (7)$$

$$y(t) = y(t_k) + V_y(t_k^+)*(t - t_k) - 0.5*g(h)*(t - t_k)^2 + \int_{t_k}^{t} \int_{t_k}^{u} a_{aero,y}(\tau)\, d\tau\, du \quad (8)$$

$$x(t) = x(t_k) + V_x(t_k^+)*(t - t_k) + \int_{t_k}^{t} \int_{t_k}^{u} a_{aero,x}(\tau)\, d\tau\, du \quad (9)$$

where V_x(t_k^+) and V_y(t_k^+) denote the post-impact rebound velocities immediately after collision k. For every shooting arc k >= 1 with upward launch velocity V_y(t_k^+) > 0, the trajectory reaches its peak elevation at apex time t_apex,k where vertical velocity vanishes:

$$V_y(t_{apex,k}) = 0 \implies t_{apex,k} \approx t_k + V_y(t_k^+) / (g(h) - a_{avg,y}) \quad (10)$$

Evaluating (8) at t_apex,k yields the apex height y_apex,k = y(t_apex,k), which directly reflects kinetic energy dissipation across consecutive bounces (effective restitution e_eff ≈ sqrt(y_apex,k / y_apex,k-1)), while lateral displacement Delta_x_k = x(t_{k+1}) - x(t_k) captures cumulative mid-flight crystal wind drift.

B. Kinematic Footprint Sequence & Empirical Trace

We define the die's Kinematic Footprint Sigma as the ordered sequence of arc footprints across the drop:

$$\Sigma = \{ f_0, f_1, \ldots, f_N \}$$
$$f_0 = (t_1, \Delta x_0, V_y(t_1^-), \omega(t_1^-))$$
$$f_k = (\Delta t_k, y_{apex,k}, \Delta x_k, \omega_k) \quad \text{for } k = 1, \ldots, N \quad (11)$$

where f_0 characterizes the initial free-fall curve and each f_k captures the duration Delta_t_k = t_{k+1} - t_k, apex height (V_y = 0), lateral drift, and angular rate of the k-th shooting arc.

Table II presents an empirical Kinematic Footprint extracted directly from an ATmega328P hardware simulation trace (32-bit single-precision profile, metal die on carpet at h = 11,297 km, g(h) ≈ 1.2787 m/s^2, settling at t = 7.5761 s with lateral rest position X = -2.9753 m). Notably, between arcs f_2 and f_3, high rotational kinetic energy (omega_2 = +95.09 rad/s) converts back into vertical translational impulse on impact, elevating y_apex,3 (0.4690 m) above y_apex,2 (0.3672 m) before decaying into rapid micro-settling chatter (t >= 7.2867 s).

TABLE II

EMPIRICAL KINEMATIC FOOTPRINT SEQUENCE EXTRACTED FROM ATMEGA328P TELEMETRY						
Arc ID	**Regime Type**	**Flight Window (s)**	**Duration Delta_t (s)**	**Apex Height y_apex (m)**	**Lateral Drift Delta_x (m)**	**Spin omega (rad/s)**
f_0	Initial Free-Fall (S_0)	[0.0000, 1.6314)	1.6314	1.7308 (Release y_0)	0.0000	-9.8186
f_1	Rebound Arc 1 (S_1)	[1.6334, 3.6713)	2.0379	0.6923 (at t=2.6439s)	-1.6218	-64.9065
f_2	Rebound Arc 2 (S_2)	[3.6713, 5.1182)	1.4469	0.3672 (at t=4.3932s)	+0.0954	+95.0896
f_3	Rebound Arc 3 (S_3)	[5.1182, 6.7695)	1.6513	0.4690 (at t=5.9456s)	-1.3100	+5.4751
f_4	Rebound Arc 4 (S_4)	[6.7970, 7.2303)	0.4333	0.0607 (at t=7.0069s)	-0.1021	+12.1571

TABLE III

EXPLICIT BALLISTIC PARABOLA EQUATIONS FOR REBOUND ARCS f_1 THROUGH f_4 (g = 1.2787 m/s^2)			
Arc ID	**Launch Speed v_k & Angle alpha_k**	**Explicit Parabolic Trajectory Equation y(x)**	**Lateral Domain x (m)**
f_1	v_1 = 1.5287 m/s, alpha_1 = 2.1180 rad (121.35 deg)	y(x) = 0.0269 + (x - 0.0002)*tan(2.1180) - [g / (2 * 1.5287^2 * cos^2(2.1180))] * (x - 0.0002)^2	[-1.6216, 0.0002]
y = 0.0269 + (x - 0.0002)*tan(2.1180) - (g / (2 * 1.5287^2 * cos(2.1180)^2)) * (x - 0.0002)^2 {-1.6216 <= x <= 0.0002}			
f_2	v_2 = 0.9311 m/s, alpha_2 = 1.5000 rad (85.94 deg)	y(x) = 0.0303 + (x + 1.6216)*tan(1.5000) - [g / (2 * 0.9311^2 * cos^2(1.5000))] * (x + 1.6216)^2	[-1.6216, -1.5262]
y = 0.0303 + (x + 1.6216)*tan(1.5000) - (g / (2 * 0.9311^2 * cos(1.5000)^2)) * (x + 1.6216)^2 {-1.6216 <= x <= -1.5262}			
f_3	v_3 = 1.3191 m/s, alpha_3 = 2.2165 rad (127.00 deg)	y(x) = 0.0352 + (x + 1.5262)*tan(2.2165) - [g / (2 * 1.3191^2 * cos^2(2.2165))] * (x + 1.5262)^2	[-2.8362, -1.5262]
y = 0.0352 + (x + 1.5262)*tan(2.2165) - (g / (2 * 1.3191^2 * cos(2.2165)^2)) * (x + 1.5262)^2 {-2.8362 <= x <= -1.5262}			
f_4	v_4 = 0.3576 m/s, alpha_4 = 2.2909 rad (131.26 deg)	y(x) = 0.0325 + (x + 2.8529)*tan(2.2909) - [g / (2 * 0.3576^2 * cos^2(2.2909))] * (x + 2.8529)^2	[-2.9550, -2.8529]
y = 0.0325 + (x + 2.8529)*tan(2.2909) - (g / (2 * 0.3576^2 * cos(2.2909)^2)) * (x + 2.8529)^2 {-2.9550 <= x <= -2.8529}			

C. Two-Layer Verification Architecture: Source Health vs. Conditioning Q.C.
Prior to KDF extraction, the firmware evaluates the extracted Kinematic Footprint Sigma = {f_0, f_1, ..., f_N} through a strict two-layer verification gate that separates entropy-source health testing from physics-conditioning quality control:

1. Stage 1 — Initial Free-Fall Gate Health(f_0) (TRNG Source Integrity): Evaluates the collision-free initial descent segment f_0 = (t_1, Delta_x_0, V_y(t_1^-), omega_0) before any floor impact occurs. By comparing consecutive free-fall durations |t_1^(m) - t_1^(m-1)|, initial angular velocities |omega_0^(m) - omega_0^(m-1)|, and descent wind drift |Delta_x_0^(m) - Delta_x_0^(m-1)| against hardware transition watchdogs on PINC.0–PINC.3, Stage 1 verifies that the hardware TRNG and pre-drop shuffle injected fresh, non-collapsed physical perturbations prior to impact.

2. Stage 2 — Post-Impact Rebound Gate V >= min(1, K) (Conditioning Q.C.): Evaluates the post-impact rebound arcs f_1, ..., f_K (where K = min(N_m, N_{m-1}, 4) is the number of shared rebound arcs) to verify that the rigid-body physics conditioner and mid-flight crystal wind properly propagated and amplified entropy into valid, non-degenerate trajectories without numerical saturation or collision-solver limit cycles.

Table IV summarizes this functional division of responsibility between Stage 1 (Source Health) and Stage 2 (Conditioning Q.C.).

TABLE IV

TWO-LAYER KINEMATIC VERIFICATION ARCHITECTURE: SOURCE HEALTH VS. CONDITIONING Q.C.			
Verification Layer	**Trajectory Scope**	**Core Engineering Question Answered**	**Specific Threats & Faults Mitigated**
Stage 1: Entropy Source Health Check Health(f_0)	Segment f_0 (Collision-Free Initial Free-Fall, t < t_1)	Did the hardware TRNG and pre-drop shuffle inject fresh, non-collapsed physical perturbations before the drop began?	- Stalled hardware timers or frozen PRNG/TRNG seeds - "Small-Offset Masking" attacks (Table VIII), where collapsed initial offsets would otherwise be hidden by post-impact collision chaos - Stalled crystal oscillator pins (PINC.0–PINC.3)
Stage 2: Physics Conditioner Q.C. V >= min(1, K)	Segments f_1, ..., f_K (Post-Impact Rebound Arcs)	Did the rigid-body physics engine and mid-flight crystal wind propagate and amplify that entropy into valid, non-degenerate rebound trajectories?	- Collision-solver limit cycles (identical rebounds despite differing f_0 inputs) - Numerical overflow or stuck-GPIO wind saturation (c_k > 0.850) - Deterministic replay during multi-bounce flight - Automatically passes zero-impact orbital sessions (K = 0 ==> 0 >= 0) without artificial bounce floors

Analytical Sensitivity of Kinematic Parameters:

Comparing the empirical values across Tables II and III reveals a clear hierarchy in parameter sensitivity for distinguishing consecutive drop sessions, summarized in Table V. While the initial free-fall segment f_0 (t_1 = 1.6314 s, Delta_x_0 = 0) acts primarily as a deterministic baseline determined by release height y_0 and gravity g(h), post-impact rebound angles alpha_k and signed lateral displacements Delta_x_k exhibit the highest inter-session divergence. Specifically, in parabolic trajectories near vertical launch (such as arc f_2, where alpha_2 = 1.5000 rad = 85.94 deg), the cos^2(alpha_k) term in the denominator of y(x) approaches zero, amplifying sub-degree corner-impact perturbations and mid-flight crystal wind gusts (W_x) into large sign-reversing shifts in lateral drift (Delta_x_1 = -1.6218 m vs. Delta_x_2 = +0.0954 m). Coupled with violent spin inversions across impacts (omega_k shifting from -64.91 to +95.09 rad/s), the ordered sequence of launch angles and signed lateral drifts provides a compact, high-sensitivity fingerprint of physical randomness.

TABLE V

DISCRIMINATIVE POWER RANKING OF KINEMATIC FOOTPRINT PARAMETERS			
Rank	**Footprint Parameter**	**Value Range in Session**	**Physical Mechanism & Discriminative Role**
1 (Highest)	Launch Angle alpha_k & Lateral Drift Delta_x_k	alpha_k in [85.94, 131.26] deg Delta_x_k in [-1.6218, +0.0954] m	Sign-Reversing Sensitivity: tan(alpha_k) and cos^2(alpha_k) diverge rapidly near 90 deg (f_2 at 85.94 deg vs. f_1 at 121.35 deg); tiny impact shifts flip Delta_x_k sign and directly capture mid-flight crystal wind (W_x).
2 (High)	Post-Impact Spin omega_k	-64.91 -> +95.09 -> +5.48 rad/s	Rotational-Translational Coupling: Corner collisions invert both magnitude and sign of omega_k; a 1 deg impact shift alters rotational energy transfer on subsequent bounces.
3 (Medium-High)	Apex Height y_apex,k & Launch Speed v_k	y_apex in [0.0607, 0.6923] m v_k in [0.3576, 1.5287] m/s	Non-Monotonic Energy Exchange: In f_2 -> f_3, stored spin (+95.09 rad/s) converts back into vertical lift (0.3672 m -> 0.4690 m), forming a distinct energy-decay signature.
4 (Baseline)	Arc Duration Delta_t_k	0.4333 s to 2.0379 s	Macro-Envelope Anchor: Scales with v_k*sin(alpha_k)/g(h); verifies macro ballistic bounds, though less sensitive to horizontal wind gusts than Delta_x_k.
5 (Lowest)	Free-Fall Curve f_0	t_1 = 1.6314 s, Delta_x_0 = 0.0000 m	Initial Condition Baseline: Governed almost solely by release height y_0 and gravity g(h) prior to corner chaos; serves as a sanity check rather than a uniqueness metric.

D. Per-Arc Kinematic Divergence & Regime-Adaptive Acceptance Law

Rather than computing a simple arithmetic mean across all bounces—which can allow a single extreme numerical outlier to be masked by low-divergence settling hops—Stage 2 evaluates each shared rebound arc f_k (k = 1, ..., K) individually. Comparing session Sigma^(m) against Sigma^(m-1), we compute the per-arc normalized divergence score c_k combining launch-angle and signed lateral-drift differences:

```
c_k = w_alpha * ( |Delta_alpha_k| / pi )
    + w_x     * ( |Delta_x_k^(m) - Delta_x_k^(m-1)| / L_ref )        (12)
```

where |Delta_alpha_k| = atan2(|sin(alpha_k^(m) - alpha_k^(m-1))|, cos(alpha_k^(m) - alpha_k^(m-1))) is the shortest angular separation in [0, pi], L_ref = 2.0 m is the characteristic lateral chamber scale, and w_alpha = 0.6, w_x = 0.4 weight angular sensitivity and signed wind drift.

An individual rebound arc f_k is classified as chaotically valid if and only if c_k falls within the two-sided "Goldilocks" acceptance band:

```
tau_low <= c_k <= tau_high                                        (13)
```

with calibrated per-arc thresholds tau_low = 0.030 and tau_high = 0.850:

- Lower Replay Guard (c_k < 0.030): Rejects arcs whose launch angles differ by less than ~5 deg and lateral drifts match within ~6 cm, indicating a stalled timer, replayed seed, or degenerate collision-solver limit cycle.

- Valid Chaotic Arc (0.030 <= c_k <= 0.850): Confirms genuine mid-flight oscillator perturbation within physically bounded aerodynamic limits.

- Upper Fault Guard (c_k > 0.850): Rejects arcs exhibiting unphysical lateral saturation from a stuck GPIO wind pin or arithmetic corruption.

Setting tau_low conservatively at 0.030 avoids censoring natural coincidences in which two independent drops occasionally rebound at similar angles—preventing artificial selection bias in the post-Q.C. distribution—while tau_high = 0.850 accommodates full left-to-right directional reversals without permitting unphysical wind saturation or floating-point overflow. Table VI summarizes the physical and cryptographic calibration criteria behind both thresholds.

TABLE VI

CALIBRATION RATIONALE FOR KINEMATIC Q.C. BOUNDARY THRESHOLDS (tau_low = 0.030, tau_high = 0.850)		
Boundary Limit	**Calibration Criterion**	**Physical & Cryptographic Justification**
Lower Threshold tau_low = 0.030	1. Anti-Censorship & Selection-Bias Prevention 2. Settling-Hop Tolerance 3. Limit-Cycle & Replay Guard	Prevents false rejection of legitimate drops that occasionally rebound at similar angles (e.g., c_2 = 0.1067 in Table VII), avoiding statistical bias. Accommodates late, low-energy rebound arcs (such as f_4) whose smaller flight windows naturally exhibit tighter trajectory dispersion. Requires simultaneous angular (< ~5 deg) and lateral (< ~6 cm) similarity to trigger rejection, isolating stalled timers or degenerate collision loops.
Upper Threshold tau_high = 0.850	1. Full Directional Reversal Headroom 2. Stuck-GPIO Wind Saturation 3. 32-Bit Arithmetic Overflow Protection	Permits legitimate opposite-direction rebounds across the chamber (such as c_1 = 0.7367 in Table VII, where Delta_x reverses from -1.62 m to +1.21 m). Rejects unphysical unidirectional lateral drift (> 3.5 m) caused by a crystal wind pin (PINC.0–PINC.3) becoming shorted or stuck at a static logic level. Flags non-Newtonian velocity spikes, energy gain (e > 1), or single-precision floating-point corruption on the 8-bit microcontroller.

Let V = sum_{k=1}^{K} I(tau_low <= c_k <= tau_high) denote the count of chaotically valid post-impact rebound arcs (where the empty sum evaluates to V = 0 when K = 0). To unify terrestrial multi-bounce drops (K >= 1) and zero-impact low-gravity orbital drops (K = 0, such as Geostationary Orbit at h ≈ 35,786 km where g(h) ≈ 0.224 m/s^2 and a 4 m drop requires t_1 ≈ 5.98 s to reach the floor, potentially expiring T_sim before first impact) under a single branch-free algebraic law, the complete session acceptance verdict is defined as:

$$\text{Session Verdict} = \text{Health}(f_0) \ \text{AND} \ [\, V \geq \min(1, K) \,] \qquad (14)$$

Equation (14) enforces two strict requirements without arbitrary minimum bounce floors:

- Multi-Bounce Surface Regime (K >= 1): Since min(1, K) = 1, the session passes if and only if Stage 1 Health(f_0) passes AND at least one rebound arc clears the acceptance band (V >= 1). If differing f_0 inputs yield identical

rebound arcs across all impacts (V = 0), the session is rejected as a physics-conditioning fault.

- Zero-Impact Orbital Regime (K = 0): Since min(1, 0) = 0, the Stage 2 inequality reduces automatically to V >= 0 (always satisfied), allowing valid orbital free-fall sessions to pass cleanly based on Stage 1 Health(f_0) dispersion alone.

Table VII illustrates the Stage 2 per-arc evaluation between two empirical ATmega328P sessions (Session 1 vs. Session 2, where K = 4 and V = 4 >= 1).

TABLE VII

PER-ARC KINEMATIC DIVERGENCE & REGIME-ADAPTIVE Q.C. EVALUATION BETWEEN TWO EMPIRICAL ATMEGA328P LOGS						
Arc ID	**Session 1 (alpha_1, Delta_x_1)**	**Session 2 (alpha_2, Delta_x_2)**	**|Delta_alpha_k|**	**|Delta_x Diff|**	**Per-Arc Score c_k**	**Arc Q.C.**
f_1	2.1180 rad (121.35°), -1.6218 m (L)	1.2274 rad (70.33°), +1.2113 m (R)	0.8906 rad (51.03°)	2.8331 m	0.7367	PASS
f_2	1.5000 rad (85.94°), +0.0954 m (R)	1.1312 rad (64.82°), +0.2766 m (R)	0.3688 rad (21.13°)	0.1812 m	0.1067	PASS
f_3	2.2165 rad (127.00°), -1.3100 m (L)	0.5331 rad (30.54°), +0.1402 m (R)	1.6834 rad (96.45°)	1.4502 m	0.6115	PASS
f_4	2.2909 rad (131.26°), -0.1021 m (L)	0.4876 rad (27.94°), +0.0130 m (R)	1.8033 rad (103.32°)	0.1151 m	0.3674	PASS
STAGE 2 CONDITIONING Q.C. VERDICT (K = 4): Valid Arcs V = 4 >= min(1, 4) ==> STAGE 2 PASS						

E. Embedded 8-Bit Optimization & Memory Footprint

To execute the two-layer Kinematic Footprint gate efficiently on resource-constrained 8-bit microcontrollers (such as the ATmega328P without a hardware floating-point unit), two implementation optimizations eliminate inverse trigonometric overhead and non-volatile memory wear:

1. Inverse-Trigonometric Elimination via Monotonic Velocity Projection:

In software floating-point libraries, evaluating atan2() for every rebound arc incurs substantial flash footprint and execution latency. Because every valid upward rebound launch satisfies $V_y(t_k^+) > 0$, the launch angle α_k is strictly bounded within $(0, \pi)$. Over this open interval, the normalized horizontal velocity projection

$$\cos(\alpha_k) = V_x(t_k^+) / \sqrt{V_x(t_k^+)^2 + V_y(t_k^+)^2} \qquad (15)$$

is strictly monotonic, mapping smoothly from +1 (0 deg, pure rightward launch) through 0 (90 deg, pure vertical launch) to -1 (180 deg, pure leftward launch). Consequently, replacing the angular separation term $|\Delta\alpha_k| / \pi$ in (12) with the normalized cosine difference

$$\Delta_{\cos,k} = |\cos(\alpha_k^{(m)}) - \cos(\alpha_k^{(m-1)})| / 2 \qquad (16)$$

preserves full directional and angular sensitivity across (0, pi) using only a single division, subtraction, and scaling shift—eliminating all transcendental atan2() evaluations from the Q.C. loop.

2. Regime-Adaptive Horizon & 40-Byte Volatile SRAM Footprint:
For any shared rebound count K >= 0 (including K = 0 zero-impact orbital drops and K = 1..4 terrestrial bounce sessions), storing the collision-free free-fall pair (t_1, omega_0) alongside up to four pairs of 32-bit single-precision rebound descriptors (cos(alpha_k), Delta_x_k) requires exactly 40 bytes of volatile SRAM (10 single-precision floats). Keeping the trajectory baseline strictly in volatile SRAM avoids non-volatile EEPROM wear and ensures zero persistent state remnants upon power-off, while cold-boot startup is naturally validated against the zero-initialized SRAM baseline (Prev_T1 = 0, Prev_W0 = 0).

Listing 1 presents the complete 40-byte BASCOM-AVR implementation of the two-layer Stage 1 Health(f_0) and Stage 2 V >= min(1, K) verification routine executed on the ATmega328P.

LISTING 1
40-BYTE ATMEGA328P TWO-LAYER KINEMATIC VERIFICATION ROUTINE (BASCOM-AVR)

```
' 40 bytes in volatile SRAM (zeroized automatically on power-off)
Dim Curr_T1 As Single , Curr_W0 As Single
Dim Prev_T1 As Single , Prev_W0 As Single
Dim Curr_CosAlpha(4) As Single , Curr_Dx(4) As Single
Dim Prev_CosAlpha(4) As Single , Prev_Dx(4) As Single

Function Evaluate_Kinematic_QC(Byval K As Byte) As Byte
  Local I As Byte , Valid_Arcs As Byte
  Local Dt1 As Single , Dw0 As Single
  Local Diff_A As Single , Diff_X As Single , C_Score As Single

  ' Stage 1: TRNG Entropy Source Health Check — Health(f_0)
  Dt1 = Abs(Curr_T1 - Prev_T1)
  Dw0 = Abs(Curr_W0 - Prev_W0)
  If Dt1 <= 0.005 And Dw0 <= 0.050 Then
    Evaluate_Kinematic_QC = 0   ' Fail Stage 1: collapsed pre-drop shuffle/source
    Exit Function
  End If

  ' Stage 2: Physics Conditioner Quality Control — V >= min(1, K)
  Valid_Arcs = 0
  For I = 1 To K
    Diff_A = Abs(Curr_CosAlpha(I) - Prev_CosAlpha(I)) * 0.5
    Diff_X = Abs(Curr_Dx(I) - Prev_Dx(I)) * 0.5
    C_Score = (0.6 * Diff_A) + (0.4 * Diff_X)

    If C_Score >= 0.030 And C_Score <= 0.850 Then
      Incr Valid_Arcs
    End If
  Next I

  ' K = 0 (orbital free-fall) passes automatically; K >= 1 requires Valid_Arcs >= 1
  If (K = 0) Or (Valid_Arcs >= 1) Then
    Evaluate_Kinematic_QC = 1   ' Pass: Source Health AND Conditioning Q.C.
  Else
    Evaluate_Kinematic_QC = 0   ' Fail Stage 2: all rebound arcs frozen or saturated
  End If
End Function
------------------------------------------------------------
```

V. CRYPTOGRAPHIC EXTRACTION & SECURITY CONSIDERATIONS

Consistent with NIST SP 800-90B/90C design principles, this architecture separates raw entropy generation from cryptographic extraction:

A. Raw Entropy vs. Uniform Randomness: Physical and aerodynamic biases (such as minor asymmetries in bounce damping) mean that individual simulated die outcomes (1–6) do not possess full log2(6) = 2.585 bits of min-entropy. Therefore, raw die sequences must never be used directly as cryptographic keys.

B. Oversampling & KDF Conditioning: To achieve a 256-bit security level (e.g., for secp256k1 private key generation), the system oversamples 160 to 200 validated drops (providing >350 bits of conservative min-entropy) and passes the concatenated sequence through a standardized, peer-reviewed Key Derivation Function (such as HKDF-SHA256, PBKDF2-HMAC-SHA512, or BIP-39) inside a trusted offline environment.

C. Resilience Against Manipulated Initial Offsets ("Small-Offset Masking"):
A subtle adversarial scenario arises if a compromised or degraded pre-drop shuffle routine supplies only microscopic initial parameter offsets while mid-flight crystal wind is disabled. Because corner collisions act as nonlinear chaotic amplifiers, even tiny initial perturbations can cause post-impact rebound arcs (f_1, ..., f_K) to diverge onto distinct resting faces—potentially satisfying the Stage 2 rebound gate (V >= min(1, K)) despite severe entropy collapse in the initial parameter shuffle.

Because post-impact trajectories already contain collision-amplified chaos, inspecting rebound arcs alone cannot isolate pre-drop shuffle degradation. Instead, Stage 1 anchors initial-shuffle verification directly on the collision-free initial free-fall segment f_0 = (t_1, Delta_x_0, V_y(t_1^-), omega_0), where zero impact discontinuities have occurred:

1. Free-Fall Shuffle Dispersion Gate Health(f_0): In the Decent Dice protocol, each drop draws symmetric timer-driven perturbations across eight physical channels: drop-height offset Delta_y_0 in [-0.01, +0.01] m, initial spin offset Delta_omega_0 in [-0.8, +0.8] rad/s, altitude offset Delta_h in [-25, +25] km, initial angle offset Delta_theta_0 in [-1.5, +1.5] deg, simulation-time offset Delta_T in [-1.0, +1.0] s, and contact-material offsets (Delta_e in [-0.02, +0.02], Delta_mu in [-0.03, +0.03], Delta_a in [-0.015, +0.015]). During collision-free descent (t < t_1), variations in release height y_0 + Delta_y_0 and altitude-scaled gravity g(h + Delta_h) directly govern time-to-impact t_1 ≈ sqrt(2*y_0 / g(h)), while Delta_omega_0 directly governs initial angular rate omega_0. Prior to evaluating post-impact rebounds, Stage 1 verifies non-trivial dispersion between consecutive free-fall footprints f_0^(m) and f_0^(m-1) across |t_1^(m) - t_1^(m-1)| and |omega_0^(m) - omega_0^(m-1)| (alongside descent wind drift |Delta_x_0^(m) - Delta_x_0^(m-1)|). If a manipulated

shuffle routine collapses initial offsets below legitimate protocol bounds, consecutive free-fall trajectories become nearly identical, immediately failing Stage 1 before post-impact amplification can mask the fault.

Table VIII demonstrates the detection capability of the combined two-layer gate across a healthy multi-session pair (Session 1 vs. Session 2 from Table VII), a simulated "Small-Offset Masking" fault where pre-drop shuffle offsets are suppressed by two orders of magnitude, and a zero-impact Geostationary Orbit (GEO, K = 0) session.

TABLE VIII

TWO-LAYER SECURITY EVALUATION ACROSS TERRESTRIAL, ADVERSARIAL, AND ORBITAL REGIMES					
Evaluation Scenario	**Free-Fall Time Diff $\lvert t_1^{(m)} - t_1^{(m-1)} \rvert$**	**Free-Fall Spin Diff $\lvert omega_0^{(m)} - omega_0^{(m-1)} \rvert$**	**Stage 1: Health(f_0)**	**Stage 2: V >= min(1, K)**	**Combined Final Session Verdict**
Healthy Empirical Pair (Session 2 vs. Session 1)	$\lvert 4.8152 - 1.6314 \rvert$ = 3.1838 s	$\lvert +8.8670 - (-9.8186) \rvert$ = 18.6856 rad/s	PASS (Full Shuffle)	V = 4 >= 1 (Table VII PASS)	PASS (Authentic Physical Chaos)
Adversarial Weak-Shuffle ("Small-Offset Masking")	0.0002 s (Collapsed Offsets)	0.0040 rad/s (Collapsed Offsets)	FAIL (Source Fault)	V = 3 >= 1 (Masked by Chaos)	FAIL (Blocked at Stage 1 Pre-Gate)
Zero-Impact Orbital Drop (GEO, h ≈ 35,786 km, K=0)	$\lvert 6.1204 - 5.8910 \rvert$ = 0.2294 s	$\lvert -4.1200 - (+3.7500) \rvert$ = 7.8700 rad/s	PASS (Valid Descent)	V = 0 >= 0 (Orbital Pass)	PASS (Valid GEO Orbital Session)

2. Continuous Mid-Flight Crystal Wind Injection: Enabling the hardware PINC.0–PINC.3 wind jumper injects fresh asynchronous oscillator phase jitter on every integration step—including during the initial free-fall descent—ensuring that live physical entropy continuously steers the die even if pre-drop initial conditions are tightly constrained.

D. Hardware Fail-Stop Interlock & Magnitude-Free Jitter Conditioning

Beyond software shuffle manipulation, physical TRNGs face hardware-level oscillator faults and upper-register stagnation when mapping raw timer captures into simulation parameters. Our architecture addresses both layers without introducing statistical selection bias:

1. Direct Four-Crystal Flip-Flop Fail-Stop Interlock: In our architecture, two independent 8 MHz Pierce oscillators directly drive the Data (D1, D2) inputs of the 74HC74 dual D flip-flop while the remaining two independent 8 MHz oscillators directly drive its Clock (CLK1, CLK2) inputs, with the flip-flop outputs triggering hardware external interrupts INT0 and INT1 on the ATmega328P. Because there is no intermediate combinational masking, the failure of any single crystal immediately collapses entropy harvesting into a

hard fail-stop: if either clock-driving oscillator stalls, its corresponding 74HC74 latch receives no rising CLK edges and ceases generating interrupts; likewise, if either data-driving oscillator stalls at a static logic level, the latched flip-flop output stops toggling, halting edge-triggered interrupt execution across the hardware.

2. Branchless Magnitude-Free Jitter Conditioning (MFE-31): When latching 32-bit hardware timer-counter registers upon asynchronous INT0/INT1 interrupts, high-frequency phase jitter concentrates in the lower-order bits while the most significant bits (MSBs) frequently stagnate due to bounded interrupt intervals—causing severe macro-scale skewing if mapped directly into floating-point physics parameters. Rather than discarding valid physical samples, our firmware conditions raw 32-bit timer captures through the Magnitude-Free Entropy Extractor (MFE-31) [8]. Executing a constant-time, branchless 32-step circular bit rotation (X <- ROTL32(X, 1 - X_31)) followed by linear MSB magnitude subtraction (L = X - 2^31), MFE-31 promotes active lower-register jitter into a uniform 31-bit integer block without conditional branches, timing side-channels, or statistical censoring before parameterizing the physics engine.

VI. CONCLUSION

By replacing opaque initial whitening with an auditable 2D rigid-body physics engine driven by live crystal wind, Personal TRNG achieves transparent entropy conditioning without sacrificing cryptographic sensitivity. Decomposing drop trajectories into an initial free-fall segment followed by post-impact parabolic rebound arcs enables a compact 40-byte Kinematic Footprint evaluated through a two-layer verification law: Stage 1 (Health(f_0)) verifies TRNG entropy-source integrity prior to impact, while Stage 2 (V >= min(1, K)) enforces physics-conditioner quality control across both multi-bounce terrestrial drops and zero-impact orbital regimes. Optimized via monotonic velocity projections into an inverse-trigonometric-free routine in volatile SRAM on an 8-bit ATmega328P microcontroller, this architecture provides a self-contained defense against deterministic replay, weak pre-drop shuffles, and hardware faults prior to final KDF extraction.

ACKNOWLEDGMENT

This whitepaper was developed with the assistance of Google Gemini, whose mathematical formulation support, adversarial security analysis, and embedded 8-bit optimization feedback helped refine the two-layer Kinematic Footprint verification framework and make its hardware-software architecture clear and accessible for practitioners.

APPENDIX A
RESISTIVE DISPLAY-BUS LOADING AND SLEW-RATE METASTABILITY ENHANCEMENT

In the open-source Personal TRNG v1.0 hardware layout (https://github.com/mixoftix/personal_trng_pcb), two free-running 8 MHz Pierce crystal oscillators (74HC04) connect directly to the Data (D1, D2) inputs of the 74HC74 dual D flip-flop, while all four crystal outputs are wired directly to ATmega328P port pins PINC.0–PINC.3 as the hardware Shutter System. Simultaneously, the firmware drives a common-anode 7-segment display through eight PORTB lines connected to 470 Ohm current-limiting resistors, with two tap traces routed directly ahead of the 470 Ohm resistors into the 74HC74 Clock (CLK1, CLK2) inputs.

This shared resistive display-bus topology enhances flip-flop metastability through two physical effects:

1. Elevated Low-State Voltage Divider & Slew-Rate Modulation (dV/dt): Because the 7-segment display is common-anode (tied to +5 V V_CC), driving a PORTB pin LOW sinks ~6.8 mA through the LED forward drop (~1.8 V), the 470 Ohm resistor, and the microcontroller's internal NMOS pull-down resistance (R_on ≈ 25–35 Ohm). This forms a resistive voltage divider at the tap node ahead of the 470 Ohm resistor that elevates the logic-low pedestal (V_OL ≈ 0.20–0.35 V) and couples LED junction capacitance into the rising-edge transition (0 -> 1) when segments turn off. Crossing the CMOS switching threshold (~2.5 V) with a modulated dV/dt increases transition aperture uncertainty inside the 74HC74 master-slave latch, promoting thermal-noise-dominated metastability resolution.

2. Dynamic Multiplexing Load Modulation: As the firmware updates 7-segment status digits during operation, simultaneous sink currents across the eight PORTB lines modulate internal ground bounce and edge timing at the CLK tap nodes prior to flip-flop capture.

APPENDIX B
MCU INSTRUCTION-PIPELINE AND PORT-BUS CLOCK JITTER COUPLING

Because the 74HC74 Clock (CLK1, CLK2) inputs are tapped from the ATmega328P PORTB display lines while two asynchronous 8 MHz crystal oscillators directly drive the Data (D1, D2) inputs, every rising clock edge presented to the flip-flop incorporates live execution jitter from the microcontroller's processing domain (implemented in the open-source AVR-BASCOM firmware at https://github.com/mixoftix/personal_trng_firmware):

1. Asynchronous RC-to-Crystal Beat Drift: The ATmega328P operates on its uncalibrated internal 8 MHz RC oscillator, which exhibits continuous thermal and supply-voltage frequency drift relative to the quartz-stabilized 8 MHz Pierce oscillators on the D inputs.

2. Branch-Dependent Execution & Peripheral Switching Jitter: Because conditional collision branches in the rigid-body HRNG physics loop, 115200-baud UART transmission routines, and 7-segment display refresh cycles alter instruction cycle counts and internal PORTB switching activity in real time, subtle phase jitter from the MCU's execution pipeline directly modulates the arrival timing of CLK edges at the 74HC74—creating a coupled hardware-software entropy feedback loop between physics computation and flip-flop sampling.

APPENDIX C
EXPERIMENTAL VALIDATION ROADMAP (ONGOING BENCHMARKS)

While this whitepaper establishes the mathematical formulation, two-layer acceptance law, and 40-byte ATmega328P reference implementation of the Kinematic Footprint framework, large-scale empirical validation is currently underway for the companion full-length paper across four targeted benchmark suites:

1. NIST SP 800-90B Min-Entropy & Restart Testing (1,000,000+ Samples): Applying the official NIST SP 800-90B Non-IID and IID entropy estimators alongside 1,000 x 1,000 cold-restart tests on both raw die outcomes (1–6) and two-layer Q.C.-validated sequences to empirically bound per-drop min-entropy and verify the conservative >350-bit entropy margin across 160–200 oversampled drops.

2. Fault-Injection Detection Matrix (True/False Rejection Rates): Harvesting 1,000-drop hardware logs across four controlled operating regimes—(i) Healthy Baseline, (ii) Manipulated Pre-Drop Shuffle ("Small-Offset Masking"), (iii) Stuck-GPIO Crystal Wind Pin (PINC.0–PINC.3), and (iv) Single-Crystal Oscillator Stall—to quantify exact True Positive Rejection Rates and False Rejection Rates for Stage 1 Health(f_0) and Stage 2 $V \geq \min(1, K)$.

3. Empirical Distribution of Per-Arc Divergence Scores (c_k): Constructing a 1,000+ drop histogram of per-arc divergence scores c_k to verify that healthy multi-bounce trajectories cluster well inside the [0.030, 0.850] acceptance band without boundary clipping at $\tau_{low} = 0.030$, empirically confirming zero statistical censorship bias.

4. Comparative 2D Ballistic Trajectory Visualizations: Generating side-by-side (x, y) parabolic trajectory plots comparing a Healthy Multi-Bounce Drop, a Small-Offset Masking fault (collapsed f_0 descent), and a Stuck-Pin Wind Saturation fault ($c_k > 0.850$) to provide direct visual benchmarks of geometric auditability.

REFERENCES

[1] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the Entropy Sources Used for Random Bit Generation," NIST Special Publication 800-90B, Jan. 2018.
[2] P. Diaconis, S. Holmes, and R. Montgomery, "Dynamical bias in the coin toss," SIAM Review, vol. 49, no. 2, pp. 211–235, 2007.
[3] M. Kapitaniak, J. Strzalko, J. Grabski, and T. Kapitaniak, "The three-dimensional dynamics of the die throw," Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 22, no. 4, p. 047504, Dec. 2012.
[4] W. Killmann and W. Schindler, "A Proposal for: Functionality Classes for Random Number Generators," Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Germany, Tech. Rep. AIS 20 / AIS 31, Version 3.0, 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e_2023.pdf
[5] M. Bakiri, C. Guyeux, J.-F. Couchot, and A. K. Oudjida, "Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses," Computer Science Review, vol. 27, pp. 135–153, Feb. 2018.
[6] Z. Wang et al., "A Survey on True Random Number Generators Based on Chaos," Discrete Dynamics in Nature and Society, vol. 2019, Art. no. 2545123, Dec. 2019.
[7] H. Sakoe and S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition," IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 26, no. 1, pp. 43–49, Feb. 1978.
[8] s. Noursalehi, "Magnitude-Free Entropy Extractor (MFE-31): A minimalist linear extractor for jitter-based entropy sources," Curiosity Lab, Tech. Rep., Oct. 2026. [Online]. Available: https://mixoftix.net/essays/Magnitude_Free_Entropy_Extractor.pdf