The ENI6MA Cypher: A Human-Centric Holographic Proof

by F.D. Rosario

Abstract

This paper presents the Rosario–Wang Proof (RWP) and the ENI6MA cypher as a human-centric cryptographic primitive that replaces stored credentials with per-event, verifiable work. At its core is a secret morphism $\mathcal{M}$—a private map compiled into a pair of "twins" (prover and verifier)—that steers a trajectory on a finite orientation ring Ω when composed with fresh entropy and the agent's choices. The resulting witness is one-time by construction, eliminating replay and neutralizing the value of database compromise.

The central novelty is cognitive: the system converts a high-dimensional family of alphabets into a **foliated manifold** that the human mind can search through fast, intuitive **membership tests**. Rather than recalling a password, the agent answers, round by round, "my symbol is (or is not) present in this zone." These perceptual judgments are easy for rightful users and cryptographically opaque to observers because the underlying geometry is salted, private, and session-specific.

Freshness is enforced by a deterministic, entropy-driven rotation function Υ, which binds each round to time and context. Formally,

$$\Upsilon : (x, T, q, r) \mapsto \sigma_r \in \{0, \ldots, C-1\}, \qquad \omega_{r+1} = \rho_{\sigma_r}\big(\mathcal{M}(\omega_r, s_r)\big),$$

where x is session entropy, T time, q a sealed parameter, r the round index, and ρ a ring rotation on $|\Omega| = C$ orientations. Identical visible inputs thus map to distinct internal states across sessions, collapsing replay at the structural level.

To render the search tractable and auditable, rotated alphabets are partitioned into n balanced **zones** (a contiguous foliation). A private interface morphism $\phi : \mathcal{I} \to \{0, \ldots, n-1\}$ bijects gestures to zones, so that the human's embodied action (tap, arrow, swipe) becomes a zone selection without revealing the mapping itself. The verifier reconstructs the same manifold from

public metadata and accepts iff the observed zone-wise membership matches its recomputation.

Soundness admits a transparent accounting. With witness length L on a ring of size C, a blind forger's chance is bounded by

$$\varepsilon \;\le\; C^{-L} + 2^{-\lambda},$$

the first term for path guessing and the second for entropy collisions (λ bits of session entropy). Because ε decays exponentially in L while verification stays $O(L)$, the system exposes practical knobs for balancing usability and assurance.

We formalize the **holographic collapse**: the verifier's decision reduces to a conjunction of strict membership events across L rounds,

$$\text{ACCEPT} \iff \bigwedge_{i=1}^{L} \mathbf{1}\{\, s_i \in X_i \,\} = 1,$$

where X_i is the emergent, per-round witness for the chosen zone and s_i the committed symbol. No partial credit is possible; either the projected geometry aligns at every step or the proof fails.

Auditability is achieved without leakage. Implementations log deterministic indices for slice origins and domain-separated hash schedules for ring positions, enabling independent reconstruction of the presented manifold while keeping $\mathcal{M}$, ϕ, and the commitment hidden. Thus, regulators can replay the construction; attackers cannot profit from transcripts.

We show how alternating the roles of prover and verifier ("oscillation") upgrades the primitive to **mutual authentication**, forcing a man-in-the-middle to maintain two consistent salted trajectories—impossible without the secret morphism. From the same spatio-temporal seed, twins may derive a session key, binding confidentiality to successful proof.

Because alphabets are modality-agnostic (text, icons, gestures, haptics), ENI6MA accommodates accessibility and operational constraints while preserving formal guarantees. The user learns where their symbolic "family" lives in the projection, not a brittle string; liveness and context binding emerge from Υ rather than second-factor friction.

We position RWP with respect to passwords, biometrics, and classical zero-knowledge. Unlike passwords, there is nothing static to steal; unlike biometrics, there is no universal template to clone; and unlike heavy ZK circuits, verification reduces to constant-time membership checks on an entropy-salted manifold. The result is a compact, keyless substrate for human$\leftrightarrow$AI, AI$\leftrightarrow$AI, and device$\leftrightarrow$device trust.

Finally, we discuss ledger applications: one-time witnesses can be embedded as **proof-of-knowledge** artifacts in block headers, replacing energy or stake with salted, human-verifiable work. Broader implications include secure attestation "in the moment" for critical systems, lawful audit without privacy loss, and a re-framing of identity as **now-work**—performed, proven, and allowed to evaporate.

In sum, the **Rosario contribution** is to bind human pattern recognition to a salted, private geometry so that **perception itself becomes a cryptographic operation**. The marriage of Υ, manifold foliation, and the secret morphism $\mathcal{M}$ yields a primitive that is simple to verify, hard to forge, and naturally aligned with how humans see, search, and decide.

Introduction

Let us consider the perennial failure mode of authentication: persistence. Anything that must be stored—passwords, private keys, biometric templates—can be copied, replayed, or coerced. The ENI6MA cypher and the Rosario–Wang Proof (RWP) address this by eliminating persistence altogether. Identity is not a token to "possess" but **work performed now**: a short, verifiable trajectory on a small ring, recomputable only by a twin that shares a sealed morphism.

The engine of this approach is a **secret morphism** $\mathcal{M}$ that maps orientation states and symbols to new orientations. This morphism, compiled into both twins and never revealed, is woven together with a deterministic salting function Υ that injects entropy, time, and policy context each round. The composition produces a one-time witness W that certifies liveness and context without ever exposing the private geometry that generated it.

We formalize the state evolution as follows. Let Ω be a ring of C orientations and $\mathcal{A} = \{A_1, \ldots, A_m\}$ be user-selectable alphabets (e.g., upper, lower, numeric). In round r, a salt $\sigma_r = \Upsilon(x, T, q, r)$ rotates the ring, and the morphism advances the state using the agent's implicit symbol s_r:

$$\omega_{r+1} = \rho_{\sigma_r}\big(\mathcal{M}(\omega_r, s_r)\big).$$

After L rounds, the path $W = (\omega_1, \ldots, \omega_L)$ is the **holographic witness** to be matched by the verifier.

The cognitive interface is engineered to make the cryptographic act feel natural. Each alphabet is rotated by offsets derived from session entropy and then **foliated** into n contiguous, near-balanced zones. Across alphabets, the zone-wise slices are concatenated into an **emergent witness** X_r that the human inspects. The single question per round is a strict membership test: "Is my committed symbol present in X_r?"

A private interface morphism $\phi : \mathcal{I} \to \{0, \ldots, n-1\}$ maps gestures to zones, so that the user's action selects the witness surface without revealing the gesture→zone permutation. This separation of concerns is intentional: the verifier does not need to know ϕ; it only needs the resulting sequence of zone-wise memberships. Thus, ϕ adds human-facing diversity without entangling the proof logic.

The verifier reconstructs the manifold from public metadata—entropy index, salted schedule, ring size—and checks that the captured memberships align with its recomputation. Acceptance reduces to a conjunction of L indicator events,

$$\text{ACCEPT} \iff \bigwedge_{i=1}^{L} \mathbf{1}\{\, s_i \in X_i \,\} = 1,$$

so that the proof is all-or-nothing. Because Υ differs across sessions, replayed transcripts fail deterministically when recomputed under new (x, T, q).

This structure invites transparent risk accounting. A uniform forger attempting to guess a complete ring path succeeds with probability at most C^{-L}; attempts to collide the salted schedule contribute $2^{-\lambda}$ if λ bits of entropy feed Υ. Hence,

$$\Pr[\text{forge}] \;\le\; C^{-L} + 2^{-\lambda},$$

and designers can dial L and C to meet service-level targets without burdening the user, as verification remains linear in L with constant-time inner steps.

The **holographic collapse** provides conceptual clarity. The high-dimensional alphabet geometry is projected onto a small number of balanced zones, and each round's decision is a one-bit truth about membership within that projection. The verifier's accumulator "collapses" these bits into a single judgment. No distributional leakage is tolerated: foliation is balanced to prevent "hot zones," and symbols preserve case and modality to avoid normalization bias.

We emphasize auditability. Implementations log slice-origin indices and domain-separated hash schedules such that an external auditor can reconstruct each round's manifold and expected zone from the same public seeds. Importantly, neither $\mathcal{M}$ nor ϕ nor the committed secret need ever be disclosed. This yields a rare combination: **lawful transparency without privacy loss**.

The architecture generalizes beyond human↔machine. Because the primitive requires only zone-wise membership over salted projections, the same construction supports AI↔AI and device↔device trust. Alternating challenge roles ("oscillation") upgrades it to **mutual authentication**, and the final salted state can be fed to a KDF to derive ephemeral session keys, binding encryption to successful proof.

Compared to passwords and biometrics, ENI6MA's advantages are structural. There is no static secret to exfiltrate, no template to clone, and no universal replay token. Compared to heavyweight zero-knowledge, the verifier's work is minimal—constant-time membership checks driven by hash schedules and modular arithmetic—yet it preserves the essential zero-knowledge intuition: transcripts reveal nothing reusable.

We close this introduction by situating the contribution. RWP shows that **human pattern recognition can be made formal**: by coupling Υ with manifold foliation and a secret morphism $\mathcal{M}$, perception itself becomes a cryptographic operation. The remainder of the paper (i) develops the formal model; (ii) proves completeness, soundness, and anti-replay; (iii) details audit-friendly engineering; and (iv) explores applications, from access control to proof-of-knowledge ledgers.

In what follows, symbols will be introduced with care: Ω for the orientation ring, $C = |\Omega|$ for its size, $\mathcal{A}$ for alphabets, n for the number of zones, λ for entropy, L for witness length, $\mathcal{M}$ for the secret morphism, ϕ for the interface morphism, and Υ for the salting schedule. This notation anchors both the cognitive intuition—search by membership—and the formalism—proof by salted geometry.

---

1. Novel Paradigm Shift

Traditional cryptography relies on *keys*—long strings of numbers that must be stored, remembered, or protected. These keys are static, and thus vulnerable: once stolen, they can be replayed indefinitely.
Rosario's insight was simple but radical: *the human mind itself can act as a cryptographic search engine*, collapsing an impossibly vast search space into a simple act of recognition.

- **Equation (High-level entropy seed):**

$$\mathcal{E} \in \{0,1\}^{\lambda}, \quad \lambda = 256 \text{ or } 512$$

  Here, $\mathcal{E}$ is the master entropy integer, a huge random number that seeds the system.

- **Key idea:** Instead of memorizing $\mathcal{E}$, the human navigates its *projections* through symbols, alphabets, and zones.

The Problem & the Paradigm Shift — Identity as "Now-Work"

Abstract-level hook. The central vulnerability of today's security is *persistence*: anything that must be stored—passwords, private keys, seeds—can be copied and replayed. The Rosario–Wang Proof (RWP) replaces the *stored* credential with a *one-time witness* that only exists in the present, bound to time and context, and verified by a paired circuit ("twin") that shares a sealed private morphism.

From static possession to ephemeral derivation. Let the session's master entropy be

$$\boxed{\mathcal{E} \in \{0,1\}^{\lambda}} \quad \text{(typically } \lambda \in [256, 512]\text{)}.$$

This is never typed or memorized; it seeds transient operations that *both* twins can regenerate. A coarse time T and a context tag q (policy/scene information) are blended into a temporal nonce:

$$\boxed{n = \mathrm{KDF}(T \parallel q)} \quad \text{(temporal binding)}.$$

Because T and q change across attempts, even identical user gestures produce *different* valid witnesses each time.

Fresh state, fresh geometry. The verifier chunks the entropy (e.g., into 16-bit words) and mixes it with the nonce:

$$\boxed{\chi = \mathrm{Chunk}(\mathcal{E}), \qquad e = \mathrm{Mix}(\chi, n)}.$$

Here, Mix is a constant-time, collision-resistant combiner. Intuitively, e is a *session field* that determines how symbol rings will rotate and how their slices (zones) will be cut.

Holographic witness rather than secret. With a private morphism $\mathcal{M}$ compiled into both twins, the prover's interaction yields an L-step witness (a short trajectory on a small ring), while the verifier computes the same trajectory from $(\mathcal{E}, T, q)$:

$$\boxed{W = \mathrm{Witness}_{\mathcal{M}}(e, P) \in \Omega^L}, \qquad \boxed{W^\star = \mathrm{Recompute}_{\mathcal{M}}(e, P)}.$$

Acceptance is purely a test of equality $W = W^\star$; no reusable secret ever appears on the wire.

Replay collapses by construction. If an adversary replays an old transcript $\langle T, \mathrm{tag}(q), W\rangle$ at a new time T' or altered context q', the verifier's recompute diverges:

$$n' = \mathrm{KDF}(T' \parallel q') \neq n \implies e' \neq e \implies W'^\star \neq W.$$

Thus *stolen receipts do not unlock future doors.* The design converts breach fallout from "keys leaked" to "old receipts leaked."

Risk accounting is auditable. With an orientation ring of size C and witness length L, naive forgery must guess an L-tuple over Ω or collide the mixed state:

$$\boxed{\Pr[\text{forge}] \;\leq\; \epsilon := C^{-L} + 2^{-\lambda}}.$$

Security is a dial: raise L (more steps) or C (more colors/orientations) to drive ϵ down, while λ controls entropy hardness.

Session secrecy from the same seed. The pair can derive a per-session key without additional ceremony:

$$\boxed{k_{\mathrm{sess}} = \mathrm{KDF}(\mathcal{E} \parallel T \parallel q \parallel W)}.$$

This piggybacks confidentiality on the *same* spatio-temporal seed that authenticates presence, avoiding long-lived PSKs.

Operational moral. Identity ceases to be an artifact to *store* and becomes *work performed now*: a synchronized traverse of a tiny ring, predicted by a private geometry and provably unrepeatable outside its moment and context. That single re-framing—*identity as now-work*—is the paradigm shift.

---

2. Alphabets as Rings of Meaning

Rosario replaces a "key" with *alphabets*—rings of symbols. These can be Latin letters, emojis, sounds, or even haptic pulses. Each alphabet is a circular ring that can be rotated.

- **Equation (Alphabet family):**

$$\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \ldots, \alpha_M\}, \quad |\alpha_j| = \text{size of ring } j$$

- Example:
  - Uppercase: S_U = "ABC... Z", size 30.
  - Lowercase: S_L = "abc... z", size 30.
  - Numeric: S_N = "123... 0", size 12.
- **Layman's picture:** Imagine three spinning roulette wheels, one for uppercase, one for lowercase, and one for numbers.

---

2. Alphabets as Rings of Meaning — How the Mind Searches a Foliated Projection

Intuition first. Instead of a password box, RWP shows you *structured projections* of your alphabets—letters, digits, emojis, glyphs—arranged as rotating rings and sliced into colored zones. Your task is not to compute; it is to *recognize membership*: "my secret letter is present in this zone." The human visual system performs this test with remarkable speed and accuracy.

Alphabets as enumerated rings. We formalize the building blocks as user-committed, case-sensitive rings:

$$\boxed{\boldsymbol{\alpha} = \{\alpha_1, \ldots, \alpha_M\}}, \quad |\alpha_j| \in \mathbb{N} \text{ (e.g., } |S_U| = 30, |S_L| = 30, |S_N| = 12).$$

Each α_j is an *ordered* cycle—think of a roulette wheel of symbols.

Möbius rotation from session state. The session field e induces per-round offsets that rotate each ring:

$$\boxed{\Theta_{\alpha_j}^{(r)} = \text{Index}(e, r, j) \bmod |\alpha_j|}, \qquad \boxed{\rho_k(s) = s[k:] \circ s[:k]}.$$

After rotation, the j-th alphabet at round r becomes $\hat{\alpha}_j^{(r)} = \rho_{\Theta_{\alpha_j}^{(r)}}(\alpha_j)$. Rotation preserves content but scrambles positions in a *verifiable* way.

Contiguous foliation into zones (colors). A rotated ring is sliced into n balanced zones (default $n = 6$):

$$\boxed{q = \lfloor |s|/n \rfloor, \quad r = |s| \bmod n, \quad \ell_j = q + \mathbf{1}\{j < r\}},$$

$$\boxed{a_0 = 0,\ a_{j+1} = a_j + \ell_j,\ s_j = s[a_j : a_{j+1}]} \quad (j = 0, \ldots, n-1).$$

Foliation makes *human-auditable* chunks: every symbol lives in exactly one zone per round.

Emergent witnesses per zone. With multiple alphabets, the zone-j slice is a concatenation across rings, a *hyperplane slice* rich enough to catch many plausible symbols:

$$\boxed{W_j^{(r)} = \bigcirc_{m=1}^{M} \alpha_{m,j}^{(r)}}.$$

Here, $\alpha_{m,j}^{(r)}$ is zone j of the m-th rotated ring at round r. This object is *what the human inspects*.

The private morphism: gesture $\to$ zone. The UI binds simple inputs (arrows, taps, swipes) to zone indices through a private, bijective map:

$$\boxed{\phi :\ \mathcal{I} \to \mathcal{Z} = \{0, \ldots, n-1\}}, \qquad \boxed{z_r = \phi(k_r)}.$$

Because ϕ is private and can be diversified per user/device, observed gestures are hard to invert into zone choices without the compiled twin.

Membership as the only cognitive operation. For the i-th symbol of the secret s_i, correctness at round i reduces to a one-bit predicate:

$$\boxed{\mathrm{M}(s_i, X_i) = \mathbf{1}\{\, s_i \in \mathrm{chars}(X_i)\,\}},$$

and the overall acceptance is the strict conjunction:

$$\boxed{\text{ACCEPT} \iff T \geq L \ \wedge \bigwedge_{i=1}^{L} \mathrm{M}(s_i, X_i) = 1}.$$

No scoring, no fuzzy thresholds: either every symbol appeared in the chosen zone when it should have, or the proof fails.

Capacity and tuning without guesswork. The geometry exposes transparent knobs. With ring size $C = n$ for the orientation space and witness length L,

$$\boxed{\mathcal{C}_{\text{guess}} \approx \max\{2^{\lambda}, C^{L}\}}, \qquad \boxed{\epsilon = C^{-L} + 2^{-\lambda}}.$$

Designers can lower C (e.g., accessibility modes) while raising L to keep ϵ fixed; or keep L short for speed and raise C where UI permits. Because foliation is balanced, per-zone symbol frequencies stay near-uniform, sustaining the error model.

Why the mind excels here. A computer would brute-force symbol positions across rotated, sliced rings; a human performs *projective filtering*—a

rapid, parallel scan that answers a yes/no membership query. RWP choreographs the space so that this perceptual act is both *easy for the rightful user* and *hard to counterfeit* without the twins' private morphism and the session's spatio-temporal seed.

Notation recap (for convenience)

- $\mathcal{E}$: session entropy (bits λ).
- T, q: time and context; $n = \mathrm{KDF}(T \parallel q)$.
- $e = \mathrm{Mix}(\chi, n)$: mixed session state.
- α_j: j-th alphabet ring; ρ_k: rotation by k.
- n: number of zones; s_j: j-th slice after foliation.
- W, $W_j^{(r)}$: witness trajectory; zone-j hyperplane witness.
- ϕ: private morphism from input to zone; $z_r = \phi(k_r)$.
- $\epsilon = C^{-L} + 2^{-\lambda}$: conservative per-attempt error.

---

3. Entropy Drives Rotation

Each round, the alphabets rotate unpredictably based on entropy. Rosario invented a *Rosario Modulo Index*—a fractal way of reducing huge entropy values into simple offsets for each alphabet.

- **Equation (Rotation offset):**

$$\Theta_{\alpha_j}^{(r)} = \mathrm{block}_{r,j} \bmod |\alpha_j|$$

  where $\mathrm{block}_{r,j}$ is an entropy-derived slice for round r, alphabet j.

- **Intuition:** This makes the roulette wheels spin differently every time, but in a way that the verifying circuit can always reproduce.

3) Entropy-Driven Offsets and Sampling (Rosario Modulo Index)

Abstract-level introduction.
Let us consider how raw randomness is sculpted into a reproducible yet unpredictable "spin state" that drives the cipher's geometry. Section 3 formalizes an entropy pipeline: we **slice** a large integer, **optionally mix it with time**, **select** blocks deterministically by round and ring, and **reduce** them to per-alphabet

rotation offsets. This chain is the novel contribution that lets a verifier deterministically rebuild the same manifold from public metadata while keeping the private morphism and the user's commitment hidden.

Background and context.
The pipeline begins by writing the session's entropy in a fixed radix and then—if liveness binding is desired—**time-mixing** every slice with a microsecond-resolution coefficient. The governing equation is

$$\tilde{e}_i \;=\; (\tau \cdot e_i) \bmod 10^3,$$

which preserves a three-digit window for human auditing while injecting temporal variability. Here, e_i is the i-th radix-10^3 slice of the base entropy; τ is the time coefficient (e.g., Unix epoch in microseconds); and $\tilde{e}_i$ is the time-mixed slice used downstream. This coupling of entropy to time underwrites structural replay resistance without sacrificing determinism given the same $(\mathcal{E}, \tau)$.

Main exposition: deterministic sampling (Rosario modulo index).
From the (optionally) time-mixed window we choose, for each **round** r and **alphabet coordinate** j, a specific slice via the **Rosario modulo index**:

$$\kappa_{r,j} \;=\; \big((\tau \bmod U) + rM + j\big) \bmod U, \qquad \text{block}_{r,j} \;=\; \tilde{e}_{1+\kappa_{r,j}},$$

where U is the count of usable slices and M is the number of alphabets. Intuitively, $\kappa_{r,j}$ "walks" the window in a round- and ring-aware pattern; $\text{block}_{r,j}$ then names the selected slice. The key property is **determinism given** $(\mathcal{E}, \tau, r, j)$, which makes verifier re-computation straightforward and auditable.

Offset formation (fractal reduction) and rotation.
Each chosen slice is then **reduced modulo the alphabet's size** to obtain a rotation amount:

$$\Theta_{\alpha_j}^{(r)} \;=\; \text{block}_{r,j} \bmod |\alpha_j|, \qquad (\alpha_j)' \;=\; \rho_{\Theta_{\alpha_j}^{(r)}}(\alpha_j).$$

Here, α_j is the j-th alphabet ring; $|\alpha_j|$ its cardinality; ρ_k the Möbius rotation by k positions. The construction supports **nested ("fractal") reductions**, reusing the same slice against multiple moduli to feed different dimensions when needed. The conceptual upshot is that **entropy becomes geometry**—a concrete, per-ring rotation state before foliation.

Canonical serialization and per-round offsets (engineering form).
In the reference ALGO1 framing, the entropy bundle $\text{Entropy} = (i, \tau, \mathbf{m})$ is **serialized** as

$$E_{\text{bytes}} = \text{LE}_{16}(i) \parallel \text{LE}_{64}(\tau) \parallel \Big\|_{k=0}^{L-1} \text{LE}_{16}(m_k),$$

and a simple per-round **offset** is taken as

$$o_r = m_{r \bmod L} \bmod M.$$

This makes offsets computable from fixed-width fields; i indexes the entropy pool; $\mathbf{m} = (m_0, \ldots, m_{L-1})$ are 16-bit chunks; M is the ring size used by the UI

manifold. These equations capture the same spirit as the Rosario index while offering an implementer-friendly path for constant-time code.

Domain-separated seeding (optional) for auditability.
To bind (i, τ) to offsets through a one-way schedule, a **hash-seeded** variant defines

$$s = H(E_{\text{bytes}}), \qquad h_r = H\big(s \,\|\, \text{LE}_{32}(r)\big), \qquad p_r = h_r \bmod M, \quad p'_r = (p_r + o_r) \bmod M.$$

Here, H is a cryptographic hash/PRF; p_r is a ring coordinate derived from h_r; and p'_r incorporates the chunk-based offset o_r. This schedule offers explicit **domain separation** ("mix:…", "k:…") and a clean audit trail: a third party can recompute p'_r from the log to check that the resulting rotations and zone expectations were faithful.

From offsets to logged witnesses.
Once rotations are applied, the system will foliate and concatenate zone slices (Section 4). A run logs, per round t, the **selected witness** X_t and the **origin indices** I_t computed by the index-progression function κ (defined next section). This logging makes the entire process **deterministically replayable** for external audit without ever revealing the private morphism or the static secret. Formally,

$$X_t = W^t_{z_t}, \qquad I_t = \big(\kappa(S_U, n, k^t_U, z_t),\, \kappa(S_L, n, k^t_L, z_t),\, \kappa(S_N, n, k^t_N, z_t)\big).$$

Here, z_t is the zone selected via the agent's private morphism; $k^t_\bullet$ are the round's rotation seeds per alphabet.

Discussion and significance (soundness scaling).
If per-round slices are near-balanced and independent, a **uniform forger** must succeed in a product of membership events:

$$\Pr[\text{ACCEPT}] \;=\; \prod_{i=1}^{L} \frac{|X_i|}{|\Sigma_{\text{tot}}|}.$$

Under the default $M{=}3$ alphabets with sizes $30, 30, 12$, $|\Sigma_{\text{tot}}| = 72$ and $|X_i| = 12$, giving a $(1/6)^L$ envelope—orthogonal to the (separate) security of the embedded morphism. The novelty is that **entropy-driven, time-mixed offsets** push unpredictability into the geometry while leaving the verifier with a simple, auditable recipe.

---

4. Foliation into Hyperplanes

Once rotated, each alphabet ring is sliced into *zones* (colored regions). Think of cutting a pie into six equal slices. These slices across alphabets form **hyperplanes**.

- **Equation (Foliation rule):**

$$s_j = s[a_j : a_{j+1} - 1], \quad j = 0, \ldots, n-1$$

  where n is the number of zones.

- **Analogy:** The system creates a 3D Rubik's Cube made from letters, numbers, and symbols—ever-shifting, but reproducible.

---

4) Manifold Projection (Rotation + Foliation)

Abstract-level introduction.
With offsets in hand, Section 4 translates numbers into **shape**. Two operations—**rotation** and **foliation**—project each alphabet into a segmented, foliated manifold whose **zones** are the canvases where human search happens. The intellectual contribution is to **bind cognition to geometry**: membership in a zone's witness is both easy for the rightful agent to recognize and formally simple for the verifier to check.

Rotation (Möbius shift).
For a string s (alphabet ring) of length $|s|$, rotation by k is

$$\rho_k(s) \;=\; s[k : |s| - 1] \;\circ\; s[0 : k - 1], \qquad 0 \le k < |s|.$$

This bijection preserves multiset content but **re-indexes** symbols, ensuring every starting position is reachable. In practice, the k's are the offsets $\Theta^{(r)}$ from Section 3, so each round presents a **fresh ordering** to the human projector while remaining deterministic to the verifier.

n-way contiguous foliation.
After rotation, the ring is partitioned into n contiguous slices:

$$q = \left\lfloor \frac{|s|}{n} \right\rfloor, \qquad r = |s| \bmod n, \qquad \ell_j = q + \mathbf{1}\{j < r\}, \quad a_0 = 0,\ a_{j+1} = a_j + \ell_j, \quad s_j = s[a_j : a_{j+1} - 1].$$

This guarantees disjoint coverage ("no symbol lost, none duplicated") and near-balance across slices—a necessary condition for clean security accounting and usable visual layout.

Recorded per-slice origin (audit index).
To make slice provenance explicit, the progression function

$$\kappa(s, n, k, j) = (k + j\, q) \bmod |s|$$

records where slice s_j **originates** in the unrotated ring. These indices are logged per round and per alphabet to support deterministic replay and third-party validation of the manifold's construction.

Zone witnesses (multi-alphabet concatenation).
Within a round t, the witness presented for zone j is the **concatenation** across alphabets:

$W_j^t = U_j^t \circ L_j^t \circ N_j^t$ (default three alphabets); general case: $W_j^t = \alpha_{1,j}^t \circ \cdots \circ \alpha_{M,j}^t$.

This unifies modalities (upper, lower, numeric; or icons, tones, haptics) into a single **search surface**. The concatenation preserves slice order and keeps membership tests simple and constant-time.

From rotation to expected zone (engineering view).
In the ALGO1 audit-friendly form, a representative position p_r is derived from a hash schedule and offset; it is then mapped to a **zone id** by dividing the ring into equal segments:

$$z_r^\star \;=\; \left\lfloor \frac{p'_r}{M/6} \right\rfloor \in \{0, \ldots, 5\}, \qquad p'_r = (p_r + o_r) \bmod M.$$

This makes the manifold's segmentation explicit and computable from logs, bridging human selection and verifier expectation with a single arithmetic step.

Verification as membership over a foliated projection.
The system accepts precisely when each committed symbol s_i appears in the corresponding captured witness X_i and enough rounds have been observed:

$$\text{ACCEPT} \iff T \geq L \;\wedge\; \bigwedge_{i=1}^{L} \mathbf{1}\{s_i \in X_i\}.$$

Equivalently, the **accumulator** Λ formed from membership predicates evaluates to 1. This reframes "password matching" as a sequence of **geometric membership** decisions over the projected hyperplanes—simple to check, difficult to forge at scale.

Discussion and significance (human search over alphabets & manifolds).
The novelty lies in the **projective interface**: the mind reduces a high-dimensional, entropically rotated symbol space to a **low-dimensional membership task**—"is my s_i in this zone's witness?"—while the verifier reconstructs the same manifold from $(\mathcal{E}, \tau)$ and logged indices. Rotation scrambles **where** a symbol appears; foliation fixes **how** options are presented. Together they yield a holographically "collapsed" view that is cognitively tractable for humans and algebraically tractable for machines—precisely the joint design target of the manifold projection in ENI6MA.

Conclusion (novel contribution).
By binding per-round offsets to entropy/time (Section 3) and then projecting alphabets through rotation and foliation (Section 4), the scheme achieves a rare synthesis: **auditability without leakage** and **human usability without normalizing away case and structure**. The mathematics is minimal—modular arithmetic and concatenation—yet it scaffolds an interface where secret knowledge is enacted as **zone-wise membership** across a segmented manifold, not exfiltrated as a reusable token.

Symbol key used above (selected)

U, L, N: default uppercase, lowercase, numeric alphabets.
ρ_k: rotation by k. Π_n: n-way foliation into contiguous slices.
κ: index progression for slice origins. X_t: captured witness at round t.
Λ: membership accumulator. M: number/size parameter (context-dependent).

---

5. The Human Mind as a Projective Interface

Here lies Rosario's breakthrough: the human doesn't compute—*they perceive*. The system presents zones (colored, symbol-rich slices). The agent (human) selects the one where their secret symbol "belongs."

- **Equation (Zone morphism):**

$$z_t = \phi(k_t), \quad \phi : \mathcal{I} \to \mathcal{Z}$$

  where ϕ is the private morphism mapping input gestures (e.g. arrow keys, swipes) to zone indices.

- **Intuition:** The human mind collapses a high-dimensional manifold into a single act: *"Yes, my letter is here."*

The Human Mind as a Projective Interface — Theory and Novelty

(1) Conceptual frame.
At the heart of ENI6MA is a simple but profound shift: the human does not compute a password; the human performs a *projective recognition task*. A private morphism ϕ maps an input gesture k_t (e.g., an arrow key, swipe, tap) to a *zone index* z_t on a segmented manifold of symbols:

$$\boxed{z_t = \phi(k_t)}, \qquad \phi : \mathcal{I} \to \mathcal{Z} = \{0, \ldots, n-1\}.$$

This mapping is the "hinge" between cognition and cryptography: it turns a momentary action into a mathematically checkable selection, while keeping the UI layer cleanly separated from the verifier's algebra. The projective interface is thus **human-centric** without sacrificing formal soundness.

(2) Legend glyphs and ergonomic design.
To make ϕ intuitive, ENI6MA specifies a *legend* of six input symbols— / \—that a user can press or enact; the morphism then binds each symbol to exactly one of the six colored zones in the manifold. This gives a visually and kinesthetically coherent vocabulary for selection (e.g., "up" tends to mean "top/zone-1"), reducing cognitive load at the exact moment of proof.

(3) Concrete morphisms (default and reversed).
A canonical (illustrative) mapping m sends arrow keys to spatially adjacent zones and the slash keys to the two remaining zones:

$$m() = 1, \quad m() = 4, \quad m() = 2, \quad m() = 0, \quad m(/) = 5, \quad m(\backslash) = 3.$$

A reversed variant m_r permutes these assignments while preserving the bijection:

$$m_r() = 2, \quad m_r() = 1, \quad m_r() = 3, \quad m_r() = 0, \quad m_r(/) = 5, \quad m_r(\backslash) = 4.$$

Implementations choose one or diversify per agent; in all cases the mapping remains private and ergonomically consistent.

(4) Private morphism as security surface.
Formally, the verifier never needs to *know* ϕ; it only needs the *resulting zone selections* z_t to check the witness. This separation makes ϕ an attack surface with **security through obscurity** value: without the private permutation, adversaries cannot reliably infer zone choices from observed inputs, especially when multiple UI devices or modalities are permitted. The morphism thereby becomes a *tunable, human-facing* layer that preserves the cryptographic core's independence.

(5) Membership, not disclosure.
The human's cognitive act is a *membership decision* over a multi-alphabet witness W_z^t: "is my secret symbol here?" If the committed symbol at round t is s_t, correctness reduces to the predicate

$$\boxed{M(s_t, X_t) = \mathbf{1}\{s_t \in X_t\}}, \qquad X_t := W_{z_t}^t.$$

Nothing about s_t is revealed directly; only the fact that the user *found it* in the appropriate hyperplane slice is conveyed to the verifier.

(6) Determinism and audit without leaking ϕ.
Each round logs the selected witness and its *origin indices*—a tuple I_t that records where the slice arose in each rotated alphabet:

$$\boxed{X_t = W_{z_t}^t}, \qquad \boxed{I_t = \big(\kappa(S_U, n, k_U^t, z_t),\ \kappa(S_L, n, k_L^t, z_t),\ \kappa(S_N, n, k_N^t, z_t)\big)}.$$

These logs allow third-party replay of the manifold construction under $(\mathcal{E}, \tau)$ **without** exposing ϕ or the secret. It is *deterministic for auditors, opaque for attackers.*

(7) Cognitive advantage, quantified.
Because foliation keeps zone sizes balanced, a naive forger's per-round success is approximately the zone fraction. With three alphabets of sizes $30, 30, 12$ and six zones, a typical witness has $|X_t| = 12$ of a total $|\Sigma_{\text{tot}}| = 72$, yielding a uniform bound $\Pr[\text{hit in one round}] \approx 1/6$. Over L rounds, the chance of blind success falls as $(1/6)^L$:

$$\boxed{\Pr[\text{ACCEPT}] = \prod_{i=1}^{L} \frac{|X_i|}{|\Sigma_{\text{tot}}|}}.$$

This connects *usability* (clear visual search) to *soundness* (exponential decay in the forger's odds).

(8) The contribution.
Rosario's novelty is to **bind perception to proof**: a private, ergonomic morphism ϕ over a foliated manifold lets the human *collapse* a high-dimensional symbol geometry into a one-bit membership claim each round. The verification math remains compact and auditable; the interface remains intuitive and device-agnostic. In effect, identity becomes *projective recognition under constraint*, not storage of a brittle secret.

---

6. Holographic Collapse

This is the **holographic principle** in action: from the perspective of the verifier, the human's choice demonstrates knowledge of a trajectory across multiple hyperplanes without ever revealing the secret.

- **Equation (Acceptance rule):**

$$\text{ACCEPT} \iff T \geq L \ \wedge \bigwedge_{i=1}^{L} \mathbf{1}\{s_i \in X_i\}$$

  The verifier accepts if, across T rounds, every secret symbol s_i appears in the chosen witness X_i.

- **Analogy:** It is like watching someone consistently recognize their handwriting in shuffled stacks of paper. You never see the handwriting itself, but their choices prove they know it.

---

6) Holographic Collapse — Theory and Novelty

(1) Collapse as a decision rule.
"Holographic collapse" names the moment the verifier reduces all observed rounds to a *single* cryptographic judgment. Formally, with T observed rounds and a required length L, the acceptance rule is

$$\boxed{\text{ACCEPT} \iff T \geq L \ \wedge \bigwedge_{i=1}^{L} \mathbf{1}\{s_i \in X_i\} = 1.}$$

Equivalently, letting Λ denote the *accumulator*, $\text{ACCEPT} \iff \Lambda = 1$. This expresses collapse as a product of *pure membership events*.

(2) Indicator/accumulator equivalence.
The same logic appears as an indicator $A(s, X_{1:T}) = \mathbf{1}\{T \geq L\} \prod_{i=1}^{L} \mathbf{1}\{s_i \in X_i\}$.

In the one-symbol-per-round setting ($i = R$), $A = 1$ iff $\Lambda = 1$, so the two formulations are interchangeable for implementation and proofs:

$$\boxed{A = 1 \iff \Lambda = 1 \iff \text{ACCEPT.}}$$

This equivalence undergirds the formal completeness and soundness arguments for the protocol.

(3) What collapses: emergent witnesses.
Each X_R is not a static list but an *emergent hyperplane slice*—a concatenation of contiguous pieces from independently rotated alphabets:

$$\boxed{X_R = W_{z_R}^R = \alpha_{1,z_R}^R \circ \cdots \circ \alpha_{M,z_R}^R}, \qquad (\text{e.g., } |U_j^t| = 5, |L_j^t| = 5, |N_j^t| = 2 \Rightarrow |W_j^t| = 12).$$

Emergence ensures content is unpredictable per round while remaining deterministic to reconstruct from logs, which is essential to an auditable collapse.

(4) Geometry that supports collapse.
The geometric pipeline—rotation ρ_Θ, then n-way foliation—produces balanced zones across alphabets. Balance keeps each membership test statistically fair and makes the accumulator a sharp instrument: no zone is bias-favored, so the conjunction does not silently leak structure or skew difficulty.

$$\rho_k(s) = s[k:] \circ s[:k], \qquad \Pi_n : \ s \mapsto (s_0, \ldots, s_{n-1}).$$

The manifold is thus an *even canvas* on which recognition can be trusted to reflect knowledge, not bias.

(5) Soundness as multiplicative decay.
Because each round yields a fresh emergent witness, the probability that a uniform forger passes all L membership tests multiplies:

$$\boxed{\Pr[\text{ACCEPT}] = \prod_{i=1}^{L} \frac{|X_i|}{|\Sigma_{\text{tot}}|}} \approx (1/6)^L \quad \text{(default sizes)}.$$

This gives a transparent dial: increase the witness length L (or adjust zone cardinalities) to push the false-accept rate down exponentially.

(6) Replay resistance within the collapse.
Although collapse is computed over $X_{1:T}$, those witnesses themselves arise from entropy/time-driven rotations and zone expectations that a verifier can recompute: seed $s = H(E_{\text{bytes}})$, digest $h_r = H(s \| \text{LE}_{32}(r))$, position $p_r = h_r \bmod M$, rotated $p'_r = (p_r + o_r) \bmod M$, expected zone $z_r^\star = \lfloor p'_r/(M/6) \rfloor$. Collapse then checks that each observed $z(w_r)$ matches $z_r^\star$. Replays at a different (E, τ) fail deterministically.

(7) Novel contribution: collapse as *proof by recognition.*
Conventional proofs bind a secret to algebraic constraints; here, the *recognition act itself*—membership across emergent hyperplanes—*is* the constraint. The human "holographically collapses" a high-dimensional manifold to a one-bit truth per round, and the verifier composes these bits into an all-or-nothing

judgment. No partial credit, no graded scores—either the geometry aligns at every step, or it does not.

(8) Implementation clarity and audit trail.
Practically, collapse costs $O(R)$ operations (one hash, simple arithmetic, and a membership/equality check per round). Systems emit an *audit event* (entropy index, verification id, boolean result, timestamp), optionally HMAC-tagged for integrity. This places the "holographic collapse" on solid operational footing: fast to verify, easy to persist, and straightforward to replay for regulators or courts—without ever exposing the private morphism or the secret itself.

Notation collected (used above)

- $\mathcal{I}$: input gesture set; $\mathcal{Z} = \{0, \ldots, n-1\}$: zones.
- ϕ: private morphism $\mathcal{I} \to \mathcal{Z}$; $z_t = \phi(k_t)$.
- W_j^t: zone-j witness at round t; $X_t = W_{z_t}^t$: selected witness.
- $M(s, X)$: membership predicate; Λ: accumulator; ACCEPT: final decision.
- ρ_k: rotation; Π_n: foliation; $|\Sigma_{\text{tot}}|$: total symbol count.

---

7. Cognitive Geometry: Searching the Manifold

The real marvel is cognitive: the human brain effortlessly searches a foliated projection. While computers would grind through combinatorial explosion, the brain perceives membership almost instantly.

- **Mathematical analogy:** The brain performs a mapping:

$$\text{Mind} : \Omega^M \to \mathbb{Z}_n$$

  reducing a multi-alphabet manifold into a yes/no membership test.

- **Significance:** Rosario reframes identity as *trajectory recognition across manifolds*, not possession of a static key.

Cognitive Geometry: Searching the Manifold — Theory and Novelty

(1) Balanced canvases for perception.
RWP engineers the symbol space so that what the human sees each round—a *foliated projection* into colored zones—is statistically balanced. Foliation guarantees that every zone contains approximately the same number of symbols from

each alphabet, preventing "easy" zones and thereby keeping visual search honest and security-relevant. This balance is not ornamentation; it is a cryptographic condition that ensures a yes/no recognition carries the right evidentiary weight.

(2) From high-dimensional structure to a projective stage.
Formally, the alphabets live in a higher-dimensional configuration whose *projection* is rendered as the round's interface. A linear map $f : \mathbb{R}^d \to \mathbb{R}^n$ with $d > n$ delivers this projection while approximately preserving distances,

$$f : \mathbb{R}^d \to \mathbb{R}^n, \qquad d_{\text{proj}}\big(f(\alpha_i), f(\alpha_j)\big) \approx d(\alpha_i, \alpha_j),$$

so that *nearby* symbols in the latent manifold remain *nearby* in the interface. This preserves the geometry that human vision relies on when scanning for membership.

(3) Gestalt proximity as a cryptographic ally.
Human search efficiency is grounded in *Gestalt* sensitivity to proximity. RWP captures this with an explicit proximity kernel,

$$P(d_{ij}) = e^{-\gamma d_{ij}}, \qquad G_{ij} = \frac{P(d_{ij})}{\sum_{k \neq i} P(d_{ik})},$$

which models the probability that items i and j will be perceived as belonging to the same local group after projection. By keeping perceptual neighborhoods coherent, the system makes "is my symbol here?" a natural, low-load visual act while still maintaining rigorous, auditable mathematics underneath.

(4) Mind→zone: the projective decision.
The mind's computation is deliberately simple: choose a zone. This is formalized by a private morphism ϕ that maps an input gesture to a zone index z_R each round,

$$z_R = \phi(k_R), \qquad \phi : \mathcal{I} \times \mathcal{Z} \to \{1, \ldots, n\},$$

providing a clean hinge between embodied action and the verifier's algebra. The morphism is private to the agent; multiple ergonomic instantiations exist, and the factorial number of possible configurations adds an extra (human-facing) layer of difficulty for attackers.

(5) Constructing the *single witness* surface.
Once a zone z is chosen, the system presents a *single composite surface*—the zone-z witness W_z^R—obtained by concatenating the contiguous slice from each rotated alphabet in that zone:

$$W_z^R = \alpha_{1,z}^R \circ \alpha_{2,z}^R \circ \cdots \circ \alpha_{M,z}^R.$$

This construction merges modalities (e.g., upper, lower, numeric) into one inspection target per round, which is exactly what the mind excels at scanning. It is the mathematical reduction of a high-dimensional ensemble to a *single private witness* presented for recognition.

(6) Membership as the invariant of understanding.
Recognition is encoded as a strict membership predicate—case-sensitive and

modality-aware—so that *knowledge* is "my committed symbol p_i is present in this round's witness X_R." Formally,

$$\mathrm{M}(p_i, X_R) = \text{true} \iff p_i \in X_R,$$

with no normalization that might blur categories (e.g., "A" $\neq$ "a"). This sharp predicate is the algebraic image of the gestalt percept: a single bit that the verifier can check deterministically.

(7) Accumulating cognition into a proof.
The verifier composes these membership bits across rounds into one judgment via a logical conjunction (the accumulator Λ):

$$\Lambda = \bigwedge_{R=1}^{n} \bigwedge_{i=1}^{|P|} \mathbf{1}\{p_i \in x_i^R\}.$$

Equivalently stated in the ALGO1 check: for every round r, the observed zone id must match the expected zone id computed from the entropy-seeded schedule. Either *all* recognitions align with the reconstructed manifold, or the proof fails—*holographic collapse* as a binary verdict.

(8) Provenance and audit of the projection.
To make this cognition auditable, each captured witness X_t is paired with an index triple (or M-tuple) I_t that records the exact rotation origins for the slices used:

$$I_t^{(\text{general})} = \big((k_U^t + q_U j) \bmod |S_U|,\ (k_L^t + q_L j) \bmod |S_L|,\ (k_N^t + q_N j) \bmod |S_N|\big).$$

In the default six-zone setting the slice strides are $(5, 5, 2)$ for $|S_U|$=30, $|S_L|$=30, $|S_N|$=12. These records let a third party *replay the manifold* from the entropy/time seeds and verify that the presented witness truly corresponds to the chosen zone.

(9) Why the projection is fresh each time.
The geometry the mind searches is not static; it is regenerated from session entropy, optionally mixed with time, and sampled deterministically by the Rosario modulo index:

$$\tilde{e}_i = (\tau \cdot e_i) \bmod 10^3, \qquad \kappa_{r,j} = ((\tau \bmod U) + rM + j) \bmod U, \qquad \Theta_{\alpha_j}^{(r)} = \mathrm{block}_{r,j} \bmod |\alpha_j|.$$

This pipeline ensures that even if a transcript is captured, its manifold will *not* recur at a new time or context. The mind performs the same act; the canvas is newly spun.

(10) Gestalt proximity → faster, safer search.
Because distance relations are preserved through projection and zones are balanced, the human uses proximity (clustered cues, color/shape coherence) to locate the secret's neighborhood rapidly. That perceptual advantage does not translate into attacker advantage: balance prevents biased "hot zones," and the verifier's accumulator still demands unanimous success across rounds. The user's brain saves time; the protocol does not cede ground.

(11) The single private witness per round.
Crucially, all of that geometry is *collapsed* for the human into one private surface $X_R = W^R_{z_R}$ at a time—the round's witness. Transport to the validator is minimal (zone ids), and verification reduces to equality/membership checks computed from a hash-seeded schedule:

$$s = H(E_{\text{bytes}}), \quad h_r = H(s \| \text{LE}_{32}(r)), \quad p_r = h_r \bmod M, \quad p'_r = (p_r + o_r) \bmod M, \quad z^\star_r = \left\lfloor \frac{p'_r}{M/6} \right\rfloor.$$

Thus the human's *gestalt decision* becomes a constant-time predicate on the verifier's side, with a clean audit trail tying every slice to its origin.

(12) Novel contribution.
Rosario's advance is to formalize an interface where *proximity-driven perception*—a core human faculty—is harnessed as a cryptographic primitive. By preserving distances under projection, balancing the foliation, and reducing the search to a *single composite witness* per round, RWP turns a cognitively natural act ("I see my symbol here") into a mathematically tight proof of knowledge, complete with deterministic reconstruction, strict membership semantics, and a conjunctive accumulator that composes perception into certainty.

Key symbols used.
f: projection \$ \mathbb{R}^{\text{d!\to!\mathbb{R}}}\$; d_{proj}: projected distance; P, G: proximity kernel and normalized grouping score; ϕ: private morphism; W^R_z: zone-z witness; M: membership; Λ: accumulator; I_t: logged origin indices; $\tilde{e}_i, \kappa_{r,j}, \Theta^{(r)}$: time-mix, index schedule, and rotation offsets.

---

8. Conclusion: A New Edifice of Security

Rosario's contribution to science is twofold:

1. **Mathematical:** The Rosario Modulo Index and manifold foliations create a deterministic yet unpredictable cryptographic space.
2. **Cognitive:** He discovered how the *human perceptual system* can act as a holographic collapse operator—reducing high-dimensional entropy into a provable, projective act of knowledge.

This changes the paradigm: identity is no longer something you *hold*, but something you *prove by recognition*. The alphabets and manifolds are the canvas; the mind is the painter that collapses possibility into truth.

Secret Morphism as a Cryptographic Primitive

At the heart of ENI6MA is a **secret morphism**—a compile-time private map $\mathcal{M}$ shared only by a pair of "entangled" verifier/prover circuits. Given fresh entropy, time, and the agent's symbol choices, $\mathcal{M}$ deterministically steers a short trajectory on a finite ring of orientations, yielding a one-time **holographic witness** W that the verifier can recompute but no observer can reuse. This reframes identity from a stored secret to **per-event, spatio-temporal work** with built-in replay resistance and zero-knowledge-like transcripts.

There are two distinct "private maps":

(i) The hologram morphism $\mathcal{M}$. This is the cryptographic engine, compiled into both twins and never exposed. It maps the current ring state and a symbol selection to the next ring state, and—when iterated with a rotation—produces the witness path. Formally,

$$\mathcal{M}:\ \Omega \times A_1 \times \cdots \times A_m \to \Omega, \qquad \Pi_{k+1} = \rho_k \circ \mathcal{M}\big(\Pi_k(\omega_0), s_k\big),$$

with Ω a ring of C orientations, A_j user-chosen alphabets, s_k the round-k symbol, and ρ_k a per-round rotation.

(ii) The interface morphism ϕ. A private, bijective map that sends UI inputs to one of n zones (hyperplanes) each round:

$$\phi:\ \mathcal{I} \times \mathcal{Z} \to \{1, \ldots, n\},$$

inducing $n!$ possible input→zone configurations (e.g., $6! = 720$). This adds human-centric obscurity on top of the cryptographic core.

(a) Fresh state. Each session draws high-entropy x, chunks it to χ, and mixes in a temporal nonce $n = \mathrm{KDF}(T \parallel q)$ (timestamp T, in-circuit prime q) to form state e. Per round, the ring rotates by $\rho_i(\omega) = \omega \oplus (\chi_i \bmod C)$. Fresh x, n ensure identical inputs traverse different valid paths across sessions (structural anti-replay).

(b) Private update. The twin circuits apply $\mathcal{M}$ to the running state and selected symbol s_k; the Möbius-style self-composition Π interleaves $\mathcal{M}$ with ρ_k, producing the next coordinate on Ω. Iterating L times yields $W = (\omega_1, \ldots, \omega_L)$.

(c) Prove/verify. The prover sends $\langle T, \mathrm{tag}(q), \{w_i\}\rangle$, where w_i encodes ω_i. The verifier, holding the same $\mathcal{M}$, recomputes e from (T, q) and accepts iff its $W^\star$ equals the submitted W. Because freshness changes e, stale transcripts fail.

(d) Acceptance rule. In the multi-alphabet, foliated view, acceptance is the conjunction of per-round membership checks,

$$\mathrm{ACCEPT} \iff T \geq L \ \wedge \bigwedge_{i=1}^{L} \mathbf{1}\{\, s_i \in \mathrm{chars}(X_i)\,\} = 1,$$

which is the "direct proof" accumulator in the protocol.

Let C be ring size and L witness length. For an adversary without $\mathcal{M}$, the best offline strategy is to guess a full path on Ω or collide the mixed state; the per-attempt error is

$$\epsilon \;=\; C^{-L} + 2^{-\lambda},$$

with λ the session-entropy bits. The protocol runs in $O(L)$ with constant-time inner steps (one $\mathcal{M}$ lookup, one rotation), giving auditable tuning of usability vs. assurance.

Keyless authentication. No reusable secret is ever stored or transmitted; only one-time witnesses exist on the wire and in logs, turning data breaches into "receipts leaked," not "keys leaked."

Structural anti-replay and liveness. Fresh n and entropy remap the same input sequence to a new path; an eavesdropped transcript cannot be replayed.

Passive zero-knowledge view. Because $\mathcal{M}$ never leaves the twins and W is one-time, transcripts reveal nothing beyond acceptance.

Mutual authentication ("oscillation"). Alternating challenges force a man-in-the-middle to keep both directions consistent—impossible without $\mathcal{M}$. Session keys can be ratcheted from the same spatio-temporal seed.

Human-centric hardening via ϕ. The private input→zone map ϕ adds $n!$ combinatorial uncertainty atop $\mathcal{M}$, especially valuable in human-in-the-loop deployments.

The **secret morphism** $\mathcal{M}$ is a private, compile-time geometry that, when coupled with entropy, time, and a minimal interface morphism ϕ, yields a **cryptographic primitive** with three rare properties: (i) **keyless** by construction, (ii) **anti-replay** by design, and (iii) **privacy-preserving** under passive observation. Its mathematics are simple to audit yet difficult to subvert, offering a tunable, high-assurance substrate for human↔AI and AI↔AI authentication alike.

Concrete Contribution

Rosario-Wang Proof (RWP) & Cypher — A Concise Synthesis

The RWP Proof reimagines authentication as an act of **pattern discovery** rather than password recall. Its cypher constructs a private geometry—defined by a secret morphism—across a family of high-dimensional alphabets and then asks the human (or agent) to perform a brief, guided search that collapses those dimensions into a one-time, verifiable trace. Identity is thus expressed not as possession of a static secret but as per-event work: a transient trajectory through a finite projection space that only the intended twins (prover and verifier, compiled from the same binary) can reconstruct.

At the core lies a **morphism** $\mathcal{M}$ that acts as a private map between enumerated sets: the ring of orientations Ω and the user-selectable alphabets $\mathcal{A} = \{A_1, \ldots, A_m\}$. Iterated under fresh rotations, $\mathcal{M}$ turns a short sequence of user choices into a compact witness path W on Ω. Because $\mathcal{M}$ is sealed into both twins and never leaves them, no reusable secret traverses the wire. The only artifact ever observed is W, which is **one-time by construction**; it certifies liveness and context without revealing the private geometry that produced it.

The novel contribution is the **human-machine division of labor**. High-dimensional alphabets are projected into a **segmented, foliated interface**—think of layered slices of a manifold—whose purpose is to make a difficult cryptographic search feel like a simple perceptual task. The human mind is exceptionally good at visual and categorical membership tests ("does this symbol belong here?"). Rosario's insight is to cast the cryptographic step as precisely this kind of micro-judgment, so that the prover's perceptual system supplies the selection signal while the twin circuits supply the unforgeable mapping.

A small but decisive function knits this together: Υ. Formally, one may view

$$\Upsilon : (x, T, q, r) \mapsto \sigma_r \in \{0, \ldots, C-1\},$$

where x is session entropy, T the timestamp, q a sealed per-circuit parameter, r the round index, and σ_r a rotation (or "salt") on the orientation ring Ω of size C. Each round's state is rotated by σ_r before $\mathcal{M}$ is applied. Because Υ injects **fresh, per-event randomness** and context, the same visible interaction never yields the same internal path twice. Replay becomes structurally futile: even "perfect" copies of yesterday's witness fail today.

In use, the interface shows the prover a **foliated projection**: discrete zones that each correspond to a latent equivalence class within the alphabets. The human performs a rapid **membership search**—"which zone contains the character family consistent with my commitment?"—and taps that zone. This selection, when composed with Υ and $\mathcal{M}$, advances the hidden state by one step on Ω. After a small number of rounds, the accumulated steps form the witness W. To the prover, the task is a short series of intuitive recognitions; to an attacker without $\mathcal{M}$, the same clicks are **cryptographically opaque**.

The **holographic collapse** is the geometrical intuition behind verification. A large, combinatorial alphabet space is folded onto a **low-dimensional orientation ring**, and only the correct composition of (i) the user's membership picks, (ii) the round salts σ_r, and (iii) the private morphism $\mathcal{M}$ yields the precise path W the verifier expects. The verifier, possessing the same $\mathcal{M}$ and computing the same σ_r via Υ, reconstructs $W^\star$ locally and accepts if $W = W^\star$. No external observer can invert this collapse because the preimage depends on sealed structure and fresh salts.

Security arises from three mutually reinforcing properties. **Keylessness:** because no long-term secret is ever revealed or stored in the clear, breaches yield only spent witnesses—receipts, not keys. **Anti-replay by design:** Υ binds each round to time and session entropy, ensuring that identical perceptual inputs map to distinct internal states across sessions. **Cognitive shielding:** the membership test is semantically meaningful to the intended user yet semantically void to an eavesdropper; the visible sequence looks like benign UI clicks, while the hidden transition system—$\mathcal{M}$ under salted rotation—remains unreachable.

From an adversarial standpoint, the best generic attack is to **guess a complete path** on the ring or to find a collision in the salted state evolution. If Ω has size C and the witness uses L rounds, blind guessing succeeds with probabil-

ity C^{-L}; salted state collisions add a further term on the order of $2^{-\lambda}$, where λ is the session-entropy budget feeding Υ. The system therefore exposes a **linear usability knob** (choose L) with **exponential security returns**, while the compute cost for honest parties remains $O(L)$.

Protocol flow is intentionally minimal. At start, both twins derive the per-session salts $\sigma_1, \ldots, \sigma_L$ from Υ. The prover completes L micro-rounds of membership selection; the verifier recomputes the salted trajectory and checks equality. For **mutual authentication**, the roles alternate ("oscillation"), forcing a man-in-the-middle to sustain two consistent hidden trajectories—impossible without the same morphism and salts. If desired, the twins ratchet a **session key** from the final salted state, binding encryption to the very act of successful proof.

Rosario's cypher is **human-centred by construction**. Because alphabets are modular (letters, glyphs, gestures, icons), deployments can be adapted for accessibility and task environment—glove-friendly gestures for field use, high-contrast glyphs for low-vision, or silent micro-motions for covert contexts. Training is light: users learn to recognize where "their" family lives within the projection, not to memorize strings. Error tolerance can be tuned via the acceptance rule (e.g., allowing Hamming-bounded deviations), preserving dignity and speed without undermining assurance.

Crucially, the Upsilon-driven search reframes common failure modes of passwords and biometrics. There is **nothing static to steal**, no universal template to clone, and no replayable challenge response. Even perfect shoulder-surfing only reveals yesterday's path, which is uncorrelated with today's salted manifold. Because Υ blends time and entropy into each round, the system delivers **liveness** and **context binding** "for free," without second-factor frictions.

In sum, the Rosario Proof's novelty is not only mathematical; it is **architectural and cognitive**. By turning high-dimensional alphabets into a perceptual search task and binding that search to salted, sealed dynamics, it upgrades the humble act of pattern recognition into a **cryptographic primitive**. The result is a compact, auditable mechanism that is fast enough for everyday use, strong enough for adversarial environments, and flexible enough to serve human$\leftrightarrow$AI, AI$\leftrightarrow$AI, and device$\leftrightarrow$device trust without the liabilities of stored secrets.

Looking ahead, the same witness transcripts can serve as **ledger artifacts**—a proof-of-knowledge substrate in which block headers carry salted witness commitments rather than energy expenditure or stake. More generally, wherever we need to certify "the right mind was present and working at this moment," the cypher supplies a disciplined way to bind cognition, time, and entropy into a single, verifiable act—and then let it evaporate. This, finally, is the ethos of the system: **do the work, prove the work, leave no residue.**