Holographic Entanglement for Keyless Proof of Knowledge

A formalization of the ENI6MA cypher as an interactive proof with holographic witnesses

by F. Dylan Rosario , Tony Zirnoon, Dr. Lin Wang

Abstract

We propose a treaty of "informational entanglement" that unifies spatio-temporal entropy and attestation into a keyless authentication primitive. Two compiled *twins*—provable/verifiable clones sharing a sealed private morphism $\mathcal{M}$—transform fresh session entropy x, timestamp T, and contextual inputs q into a one-time *holographic witness* W, realized as an ephemeral trajectory on a discrete orientation ring Ω via per-round rotations ρ_i and a Möbius-style combiner Π. Identity is recast as per-event, per-context *work*: the credential is not a stored secret but the ability to reproduce, *now*, the trajectory that the twins' private geometry predicts. This yields structural replay resistance through a temporal nonce $n = \mathrm{KDF}(T \parallel q)$, bilateral liveness and mutual authentication by oscillating challenge–response, and optional session keys derived from the same spatio-temporal seed. We give conservative, auditable security parameters with per-attempt error $\epsilon = C^{-L} + 2^{-\lambda}$ (ring size C, rounds L, entropy λ), constant-time $O(L)$ execution, and a passive zero-knowledge view of transcripts. The construction supports PII-minimizing attribute proofs and spans human↔AI and AI↔AI settings without PKI lifecycle burden. We discuss engineering constraints—trusted time, robust entropy, white-box/side-channel hardening (e.g., TEEs, diversification, constant-time tables)—that make the guarantees bite in practice. By replacing reusable secrets with spatio-temporally bound witnesses, the framework shifts breach economics from "keys leaked" to "receipts leaked," collapsing phishing and credential stuffing while enabling measurable, accessibility-aware risk tuning.

We present a keyless authentication primitive in which a prover derives an ephemeral **holographic witness** from (i) user-chosen alphabets, (ii) a private morphism ("hologram") known only to prover and verifier, and (iii) a high-entropy session state mixed with a temporal nonce. The verifier holds an **entangled circuit** (a compiled twin of the prover's circuit) that deterministically checks the witness without ever storing a reusable secret in plaintext. We formalize the construction, give axioms, lemmas, and a security theorem establishing

completeness, anti-replay, and soundness bounds of roughly C^{-L} (for C colors and witness length L), augmented by entropy-based protection. We sketch a zero-knowledge simulator for passive eavesdroppers and analyze performance and deployability.

Keywords: keyless authentication, informational entanglement, spatio-temporal attestation, holographic witness, replay resistance, zero-knowledge, mutual authentication, side-channel hardening.

Introduction

Below is a consolidated theoretical and conceptual expansion of the provided text body—organized to answer **why**, **how**, **what**, **benefits**, **feature set**, **capabilities**, and **who benefits**—in **eight focused paragraphs** spanning the model, construction, axioms, security claims, complexity, protocol, implementation, and primitive mapping.

The model formalizes a **keyless** authentication substrate where the reusable "secret" never appears on the wire or at rest as plaintext. By elevating the user's chosen **alphabets** $\mathcal{A}$, the **orientation ring** Ω with tunable size C, and a compile-time-private **hologram** $\mathcal{M}$, the system encodes cognition and policy into a **holographic witness** $W \in \Omega^L$. Sessions are individualized by high-entropy draws $x \leftarrow \{0,1\}^\lambda$ and a **temporal nonce** $n = \mathrm{KDF}(T \parallel q)$, ensuring fresh, context-specific proofs. The "why" is twofold: (i) eliminate **replay** and **surveillance** value from captured transcripts; (ii) remove brittle lifecycle burdens of static keys/passwords by compiling state into **entangled twins** that only recognize correct, one-time witnesses. This reframes identity proofs as **per-event attestations** bound to time and context—useful for human logins, AI↔AI channels, and provenance. The model's structure also exposes clean tuning knobs—(C, L, λ)—linking usability and security with auditable error bounds. In short, the model turns identity from "stored secret" into a **fresh derivation problem** solved jointly by entropy, time, and a private morphism.

2) System realizes keyless authentication.
Each session draws x, forms 16-bit chunks χ, derives $n = \mathrm{KDF}(T \parallel q)$, and mixes to $e = \mathrm{Mix}(\chi, n)$. The **rotation** $\rho_i(\omega) = \omega \oplus (\chi_i \bmod C)$ advances the ring state, while the **Möbius combiner** $\Pi_{k+1} = \rho_k \circ \mathcal{M}(\Pi_k(\omega_0), s_k)$ twists state through $\mathcal{M}$ under a symbol selector s_k. The prover emits **witness indices** $w_i \in \{0, \ldots, C-1\}$ with $(T, \mathrm{tag}(q))$; the verifier recomputes e and the same W deterministically from shared $\mathcal{M}$ and accepts iff $W^\star = W$. Because n and x are fresh, **identical keystrokes** or UI gestures across sessions map to **different valid trajectories** on Ω, nullifying replays. The construction scales to **oscillating** agent pairs (entangled twins) by repeating this exchange with fresh (T_r, q_r) each round, optionally deriving ratcheted session keys. Implementation-wise, the compile step "burns" $\mathcal{M}$ and tables into per-user binaries with multi-dimensional transforms to resist extraction, keeping only black-box acceptance observable.

3) The assurance envelope.

A1 guarantees **min-entropy** in x and unpredictability of Mix; A2 asserts that $\mathcal{M}$ is confined inside the twins; A3 ensures **temporal uniqueness** of n; A4 gives **determinism** (binding) for honest parties and **pseudorandomness** of W for any mismatched morphism; A5 bounds white-box leakage to black-box I/O. Together they define a crisp envelope: outsiders cannot predict e or W; any transcript is **one-time**; acceptance depends on a morphism **never exported** in the clear. Practically, these axioms allow you to treat captured transcripts as **non-credentialized artifacts** (no reuse value), treat servers as **non-custodians** of user secrets (reduced breach liability), and justify simulator-based privacy claims (passive zero-knowledge). They also clarify where engineering must be strongest: entropy sources, compile/burn hygiene, and side-channel suppression. In audits, these axioms translate to testable controls: RNG tests, code attestations, constant-time lookups, and policy isolation.

4) Security theorem

Completeness (L1) follows from shared $\mathcal{M}$ and deterministic pipelines—honest runs always accept. **Anti-replay (L2)** hinges on freshness of n, so replays of att mismatch the recomputed e and fail. **Soundness (L3)** yields a guess-bound $\Pr[\text{forge}] \leq C^{-L} + 2^{-\lambda}$: either the attacker guesses an L-tuple on Ω or finds a collision in the mixed state. **Passive ZK-IP (Thm 1)** says an eavesdropper's view is **simulatable**, as $\mathcal{M}$ never leaves the twin and W is one-time; hence transcripts leak nothing beyond acceptance. **Mutual entanglement (L4)** extends this to bilateral challenge–response: a MiTM cannot **sustain the oscillation** in both directions without $\mathcal{M}$. Operationally, these claims imply that keyloggers, cameras, or packet captures do not produce re-usable credentials; stolen databases of transcripts do not enable replay; and service providers can validate **liveness** without hoarding secrets.

5) The capability & tuning.

Per-round cost is constant-time: one rotation, one $\mathcal{M}$ lookup, and a combine; total work is $O(L)$ plus $O(|\chi|)$ for mixing—compatible with the **"AES-class"** throughput target. The **state space** is $\max\{2^{\lambda}, C^{L}\}$, so security scales by increasing λ (entropy) or (C, L) (combinatorial witness space). Define $\epsilon = C^{-L} + 2^{-\lambda}$; for $C = 6, L = 6, \lambda = 512$, $\epsilon \approx 1.6 \times 10^{-5}$ (dominated by 6^{-6}). Raising L to 8 drops the dominant term to $6^{-8} \approx 1.7 \times 10^{-6}$; or keep L fixed and increase C in accessibility-permitting contexts. This tunability is a **feature**: mobile or kiosks may run $(C = 3, L = 7)$ for usability, whereas server-to-server channels can push $(C = 6, L \geq 8)$. Because transcripts are one-time, **online** rate-limits and lockouts complement ϵ to bound practical risk. Architects thus get a clean **budgeting calculus**: pick (C, L, λ) to meet target FAR/FRR and adversary cost curves.

6) Protocol & engineering safely.

The pseudocode describes a minimal **Prove**/**Verify** API; production systems extend it with admission control, telemetry, and recovery. Admission binds to time via T and to device posture via **attestation** (e.g., TEE reports), refusing clients with unknown measurements. Telemetry stores (σ, ctx) rather than secrets, enabling **audits** without privacy exposure. **Build hygiene** operationalizes A5: reproducible builds, SBOMs, signed provenance, per-user diver-

sification, constant-time tables for $\mathcal{M}, \rho$, and fuzzing of parsers/state machines. **Side-channel** risks are handled by fixed-size records, jitter padding, and uniform error envelopes; **DoS** is mitigated with cheap pre-filters and bounded work per attempt. Recovery avoids static backups: escrow is a **process** gated by external attestations and a separate morphism, preserving keylessness even under account restoration or inheritance.

7) Performance Results.
Core features include **surveillance-resilient login**, **mutual AI↔AI entanglement** with ratcheting keys, **selective attestations** that prove predicates without PII, **duress synonyms** that silently branch server policy, **escrow gating** for recovery without stored secrets, and **per-user compiled artifacts** that raise extraction cost and shrink blast radius. Capabilities extend to **context binding** (every token is married to ctx), **unlinkability by default** (fresh n), and **federation** (same primitives under OIDC/SAML, PAM/SSH, CI/CD registries). Benefits accrue across the stack: users shed password resets and OTP fatigue; merchants and banks reduce PCI/PII scope and replay fraud; DevOps eliminates key sprawl; compliance gains high-integrity, low-PII logs; and security teams get liveness with **no custodial secrets**. Because the witness path is $O(L)$ with constant-time inner loops, these gains arrive **without latency penalties** typical of heavyweight ZK systems.

8) The stakeholder benefits.
Individuals (journalists, executives, at-risk users) gain **coercion resistance** and privacy-preserving authentication; **enterprises** gain **secretless SSO**, hardened CI/CD, and lower breach liability; **SaaS/Cloud** providers ship **signed, diversified clients** that self-prove liveness; **OT/IoT/Edge** adopts **entangled channels** resilient to interception; **finance & healthcare** use **PII-free attestations** to cut onboarding friction and regulatory exposure; and **public sector** deploys identity without stockpiling sensitive data. Standards bodies and auditors benefit from the **axiomatized** envelope (A1–A5) and measurable error ϵ, enabling policy to reference parameters rather than implementation folklore. In short, any environment where **replay, surveillance, or secret custody** is the limiting factor stands to gain: the platform converts identity from a stored liability into **fresh, verifiable work**—fast to compute, hard to fake, and easy to audit.

We present our treaste on "entanglement," where spatio-temporal entropy, and attestation as a single conceptual edifice provide uncrackable security. Our thesis is that identity can be recast as per-event, per-context *work* that two "twins" can verify but nobody else can reuse. In this view, the credential is not a possession but a trajectory—an ephemeral path through a small, discrete orientation space—shaped by fresh entropy, time, and a sealed morphism inside the twins.

We begin with the definition of entanglement yet immediately remove the suggestion of quantum mystique. The relevant entanglement is informational: two circuits compiled from the same binary share a private morphism $\mathcal{M}$ and therefore a private geometry. When they encounter the same stimulus—fresh session entropy x, a timestamp T, and contextual inputs q—they compute con-

gruent trajectories on an orientation ring Ω. To an outsider, the outputs appear as a scatter of indices; to the twins, they are coordinates in a shared chart. This is how a statement can be "made anywhere": not by violating physics, but by ensuring both parties can reconstruct the *same* one-time witness W from the *same* spatio-temporal seed.

The vehicle of information transfer is a holographic overlay: multiple streams—entropy chunks, time, and user symbols—are superposed by $\mathcal{M}$ and then folded by per-round rotations ρ_i into a Möbius-like loop Π. Each round maps the current ring position and symbol choice to a new position; the L positions compose the witness. Because the mix depends on T and high-entropy state, identical keystrokes or gestures land on *different* valid trajectories across sessions. Thus the transcript of a prior success is not a credential but a fossil; its shape explains the acceptance that already happened, while refusing to unlock a future door.

Time is not an afterthought but a constitutive dimension of the proof. A temporal nonce $n = \mathrm{KDF}(T \parallel q)$ couples the wall clock to the circuit's internal algebra—optionally salted by an in-circuit prime—to guarantee that the same nominal input produces a different mixed state e whenever the clock or context changes. Attestation then becomes spatio-temporal: the question "are you you?" is replaced by "can you produce *now*, under this context, the witness our geometry predicts?" The arrow of time is thereby enlisted as a cryptographic ally; replay is not merely discouraged by policy but invalidated by construction.

To transform a private trajectory into a portable claim, the twins bind it to context. The prover emits a one-time witness and a context tag (login, payment, deploy), and optionally computes a MAC or hash-based token over (T, q, W, ctx). These tokens are not keys and do not expose secrets; they are receipts that say "the right work was done at the right time in the right context." In richer modes, attributes D (eligibility, limits, roles) can be folded through $\mathcal{M}$ to produce PII-free attestations: the verifier learns that the attribute is held, not what the attribute contains.

Mutual authentication is achieved by *oscillation*. Each twin alternates challenge and verification, forcing the adversary to sustain consistency in both directions under fresh entropy. A man-in-the-middle lacking $\mathcal{M}$ can forward messages but cannot maintain the bilateral constraint that each side imposes. From the oscillation transcript, both parties may KDF ephemeral session keys, ratcheting if desired. Thus session secrecy and liveness are by-products of the same geometry that already ensures non-replay.

The security envelope is explicit and tunable. Let C be the ring's cardinality and L the number of rounds. Guessing a full witness requires work on the order of C^L; independent entropy protects against shortcutting the mix, contributing a 2^λ term. The conservative per-attempt error is $\epsilon = C^{-L} + 2^{-\lambda}$. This is not cosmic numerology but an auditable budget: accessibility can be improved by lowering C, provided L is raised to keep ϵ below target risk. Because each round is constant-time—one morphism lookup, one rotation, one combine—the latency scales linearly in L, enabling "dial-a-risk" deployments without architectural upheaval.

From a systems perspective, the replacement of secrets with witnesses changes

the economics of compromise. Servers no longer curate evergreen credentials; they store attestations bound to context, time, and entropy. Breach fallout thus shifts from "all keys exposed" to "historical receipts leaked." Phishing collapses because there is nothing durable to steal; credential stuffing collapses because acceptance depends on the present tense of the proof. Operational controls—rate limits, lockouts, sharding of verifiers—compose cleanly atop the formal error bound to produce defense in depth.

Human factors enter through the geometry rather than in spite of it. The ring can be three, four, or six orientations; alphabets can be textual, symbolic, gestural; synonym inputs can map to duress behaviors at the server without changing the on-wire distribution. Because each of these choices has a mathematical shadow—each alters C, L, or the mix—they can be tuned consciously. Accessibility ceases to be a bolt-on and becomes a first-class design parameter whose security consequences are not guessed at but measured.

The "universal entropy" and "mind–circuit resonance" is rooted in the described framework. If a human and a compiled twin consult the same ambient randomness and the same clock, their shared morphism lets them agree privately on a witness no third party can reuse. The romance is not in faster-than-light messaging but in the elegance with which cognition, time, and computation are braided into a proof that only the rightful pair can regenerate. The novelistic flourish—characters "speaking anywhere"—thus reduces to a precise and falsifiable claim: identity is enacted, not carried.

None of this absolves engineering of its ordinary sins. The assumption that compiled code leaks at most black-box I/O is a working premise, not a theorem; hostile devices motivate TEEs, build attestation, code diversification, and side-channel suppression. Time must be trustworthy; clocks drift and can be spoofed, so verifiers should bind acceptance to attested time or verifiable delay. Entropy must be real; embedded systems should be audited for RNG quality and seeded carefully. These caveats are not decorations; they are the scaffolding that makes the mathematics bite.

For machine interlocutors—agents, services, autonomous systems—the geometry is especially congenial. The twins' oscillation replaces certificate lifecycles and PSK sprawl with per-round derivations; session keys fall out naturally; provenance becomes an accumulation of one-time receipts rather than a registry of immortal secrets. The same primitive harmonizes human–AI and AI–AI interactions, enabling ecosystems in which attestation is cheap, replay is structurally impotent, and privacy is a default property of transcripts.

At the level of epistemology, the scheme distinguishes *knowledge* from *evidence* with unusual clarity. Knowledge is the latent ability to reproduce W under the correct spatio-temporal conditions; evidence is the transient act of doing so now. Because the evidence is one-time, it cannot be warehoused as knowledge by an adversary. The proof is of the *capacity* to align with a private geometry in the present, not of possession of an artifact from the past. For a philosophical novel, this is fertile ground: identity as performance, truth as synchronization, trust as agreement on a path through a finite space.

The practical moral is simple and radical: stop storing what you do not need,

and stop sending what you cannot revoke. Compile twins that share $\mathcal{M}$; bind attestation to time and context; select C, L, λ to meet a measured error budget; instrument the usual defenses; and treat side channels as first-class citizens. If you do, the usual threats are bent out of shape: transcripts become harmless, stolen databases become inert, and the only thing that matters is whether the twins can dance the same short dance at the same moment.

In closing, the lecture returns to story. Imagine a world in which every meaningful interaction—unlocking a door, signing a contract, dispatching a drone—is a brief, choreographed traverse of a ring that only the rightful pair can predict. The choreography is different each time; observers can listen and learn nothing usable; the partners separate, leaving behind only a receipt that says "we danced here, then." Whether written as a chronicle or a technical manual, the core remains the same: entanglement, in this sense, is the art of making *now* the only key that ever fits.

---

1. Model and Notation

Alphabets. Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be user-selectable alphabets (e.g., LAT, Han, emoji). Let $|A_j| = a_j$.
Orientation/Color ring. Let $\Omega = \{\uparrow, \rightarrow, \downarrow, \leftarrow, \backslash, /\}$ with $|\Omega| = C \in \{3, 4, 6\}$.
Entropy. Each session samples $x \leftarrow \{0,1\}^\lambda$ (typ. $\lambda = 512$). Write the 16-bit chunk stream as $\chi = (\chi_1, \chi_2, \ldots)$, $\chi_i \in \{0, \ldots, 2^{16}-1\}$.
Temporal nonce. Let T be a coarse timestamp and q a session prime ($\approx$512 bits) from a CSPRNG seeded inside the circuit; define $n = \mathrm{KDF}(T \parallel q)$.
Private hologram. A secret morphism

$$\mathcal{M} : \Omega \times A_1 \times \cdots \times A_m \to \Omega$$

committed at compile time; only the paired circuits know $\mathcal{M}$.
Rotation. Per round i, define ring rotation

$$\rho_i(\omega) = \omega \oplus (\chi_i \bmod C),$$

where $\oplus$ is modular addition on the Ω ring.
Möbius loop combiner. Define a twisted self-composition (one-sided "Möbius" wrap):

$$\Pi_{k+1} = \rho_k \circ \mathcal{M}\big(\Pi_k(\omega_0), s_k\big), \quad \Pi_0 = \mathrm{id},$$

with symbol selector $s_k \in A_1 \times \cdots \times A_m$ (from UI or defaults).
Password. Minimal password P can be a single symbol p repeated L times (E2).
Holographic witness. The L-step witness is

$$W = (\omega_1, \ldots, \omega_L), \qquad \omega_i = \Pi_i(\omega_0) \in \Omega,$$

optionally compressed to **witness indices** $w_i \in \{0, \ldots, C-1\}$.

---

2. Construction

Setup. Choose $(\mathcal{A}, C, L, \lambda)$. Compile the **entangled circuit** pair $(\mathsf{Prov}, \mathsf{Ver})$ with shared $\mathcal{M}$ and code-generated tables; the compile step performs multi-dimensional obfuscating transforms (E8–E9).

Prove (per session).

1. Sample x, derive χ, compute $n = \mathrm{KDF}(T \parallel q)$.
2. Mix: $e = \mathrm{Mix}(\chi, n)$.
3. Compute witness $W = \mathrm{Witness}(\mathcal{M}, e, P)$ using ρ_i and Π_i.
4. Send challenge/attestation $\mathsf{att} = (T, \mathrm{tag}(q), \{w_i\}_{i=1}^{L})$.

Verify. Deterministically recompute e and W from $(T, \mathrm{tag}(q))$ and $\mathcal{M}$; accept iff W matches.

Anti-replay. Any replay with stale (T, q) fails because n (hence e) differs (E6).

---

3. Axioms

A1 (Entropy). x has min-entropy λ; Mix is collision-resistant and unpredictable given transcripts.
A2 (Hologram secrecy). $\mathcal{M}$ is unavailable to adversaries outside $\mathsf{Prov}/\mathsf{Ver}$.
A3 (Temporal uniqueness). With overwhelming probability, n is unique per session.
A4 (Binding). For fixed $(\mathcal{M}, e, P)$, the mapping to W is deterministic; for $\mathcal{M}' \neq \mathcal{M}$ the induced distribution on W is pseudorandom over Ω^L.
A5 (White-box hardness). The compiled binary leaks at most black-box I/O behavior relevant to acceptance (E8–E9).

---

4. Lemmas and Theorems

Lemma 1 (Completeness). If Prov and Ver share $\mathcal{M}$ and follow the protocol on the same (x, T, q, P), then Ver accepts with probability 1.
Proof. Determinism of ρ_i, Π_i and shared $\mathcal{M}$ implies identical W.

Lemma 2 (Anti-Replay). Replaying a prior att at a later time is rejected except with negligible probability.
Proof. By A3, n changes when T or q changes, altering e and W. Collisions are negligible by A1.

Lemma 3 (Soundness bound). For an adversary without $\mathcal{M}$, the best offline forgery against a fresh session succeeds with probability

$$\Pr[\text{forge}] \leq C^{-L} + 2^{-\lambda}.$$

Proof sketch. Without $\mathcal{M}$, A4 yields W indistinguishable from uniform over Ω^L; guessing W costs C^L. Collisions in e add at most $2^{-\lambda}$.

Theorem 1 (Holographic ZK-IP, passive). Under A1–A5, the transcript viewed by an eavesdropper reveals no information about $\mathcal{M}$ or P beyond acceptance.

Proof sketch (simulator). Given public $(T, \text{tag}(q))$ and an oracle for accept/reject, a simulator samples $W^\star \leftarrow \Omega^L$ until acceptance (expected C^L tries) or uses rejection-sampling with a trapdoor to match the distribution induced by A4. Since $\mathcal{M}$ never leaves the circuits and W is one-time (A3), transcripts are simulatable.

Lemma 4 (Mutual entanglement / oscillation). Let two compiled twins Drago, Boros share $\mathcal{M}$. In the bidirectional challenge–response loop with fresh nonces, both sides remain synchronized and authenticated each round; a man-in-the-middle without $\mathcal{M}$ cannot sustain the oscillation beyond negligible probability.

Proof sketch. Each side both verifies and issues a fresh challenge keyed by its locally mixed e. Any splice breaks equality of W on at least one edge, failing verification.

---

5. Equations (size, work, and error)

State-space (parameterized). With $\lambda = 512$, the session entropy space is 2^λ. Effective search complexity for naive guessing is

$$\mathcal{C}_{\text{guess}} \approx \max\{2^\lambda, C^L\}.$$

Error exponent. Define $\epsilon = C^{-L} + 2^{-\lambda}$. For $C = 6, L = 6, \lambda = 512$,

$$\epsilon \leq 6^{-6} + 2^{-512} \approx 1.6 \times 10^{-5} \text{ (dominated by } 6^{-6}).$$

Cost. Per round: one rotation, one $\mathcal{M}$ lookup, constant-time combine; total $O(L)$ plus $O(|\chi|)$ mixing. Claimed empirical speed is "as fast as AES" (E15).

---

6. Protocol Pseudocode (agent $\leftrightarrow$ agent)

```
parameters: C, L, , alphabets , private hologram
compile: (Prov, Ver) ← CompileTwin(, , C, L, )

function Prove(P):
```

```
  x ← {0,1}^ ;  ← Chunk16(x)
  T ← Now() ; q ← PrimeGen()
  n ← KDF(T || q); e ← Mix(, n)
  W ← []
   ← id;  ← 0
  for i in 1..L:
     ← _i( ( (), s_i ) ) ;  ← _i
    W.append(Index())                // witness index w_i
  send ⟨T, tag(q), W⟩

function Verify(T, tag(q), W):
  q' ← RecoverPrime(tag(q))
  n ← KDF(T || q'); e ← Mix(', n)    // ' from verifier's entropy twin
  recompute W* with  as above
  return (W* == W)
```

---

7. Discussion, Implications, Limitations

- **No reusable secret in the clear.** Secrets are embedded via $\mathcal{M}$ in compiled twins; transcripts are one-time (E1, E6, E8–E9).
- **Accessibility.** C is tunable (e.g., $C = 3$ for color-blind modes; E12).
- **Mutual authentication & session keys.** The oscillating twin protocol (E5) yields bilateral liveness; session keys can be KDF'd from (T, q, x).
- **Replay resistance.** Timestamp+prime mixing prevents stale matches (E3, E6).
- **Parameter selection.** Increase L or C to push ϵ below target risk.
- **White-box caveat.** A5 is an assumption; hostile device extraction remains a practical threat—harden via TEEs, code randomization, and anti-side-channel controls.
- **Claimed astronomical space.** Transcript claims (E2, "10^{720}") are modeled as parameterized security; formal bounds above are conservative and auditable.

The design's first-order property is that **no reusable secret ever exists in the clear**—not on the wire, not at rest. The only thing that ever leaves a device is a one-time **witness** W derived from fresh entropy and a temporal nonce; the **private morphism** $\mathcal{M}$ that binds cognition/policy to verification remains compiled inside the entangled twins. Practically, this means transcripts have no "replay" value and stored databases of past sessions don't translate into

credentials. In the formal write-up, this is captured explicitly: "Secrets are embedded via $\mathcal{M}$ in compiled twins; transcripts are one-time (E1, E6, E8–E9)."

Mechanistically, every session samples entropy x, derives a nonce $n = \mathrm{KDF}(T \parallel q)$, mixes to state $e = \mathrm{Mix}(\chi, n)$, and then advances an **orientation ring** Ω via per-round rotation ρ_i interleaved with the private morphism $\mathcal{M}$ (the "Möbius" loop). The L iterates of this twisted composition produce the witness coordinates $(\omega_1, \ldots, \omega_L)$, optionally emitted as indices w_i. Because x and n are fresh each time, *the same human inputs map to different valid trajectories across sessions*, which is the crux of surveillance and replay resistance.

Beyond one-sided proofs, the **oscillating twin protocol** extends this into bilateral liveness and optional key agreement. Two compiled clones (sharing $\mathcal{M}$) alternate verify→challenge steps; a man-in-the-middle without $\mathcal{M}$ cannot sustain the oscillation in both directions. Each side can KDF a per-round key from its fresh inputs (x, T, q), ratchet them if desired, and bind channel tokens to context with a MAC—cleanly replacing long-lived PSKs with witnesses.

Replay resistance is structural, not policy-based: reusing an old attestation $\langle T, \mathrm{tag}(q), W \rangle$ will mismatch the verifier's recomputed e whenever T or q changes (which they do by construction). This is the formal content of Anti-Replay (L2) and the "entropy–time mixing" primitive (P1), and it matches the demonstrated behavior where identical keystrokes produced different accepted paths while replays failed.

Accessibility and UX are tunable rather than hard-wired: the ring cardinality C can be $3, 4$, or 6 (e.g., grayscale-friendly for color-blind users), alphabets are user-selectable, and synonym passwords enable duress policies without changing the on-wire distribution. These choices let deployments meet users where they are while keeping a clear handle on the security envelope tied to C and L.

On the assurance and performance axes, the **auditable knobs** are explicit. Naïve search scales as $\max\{2^\lambda, C^L\}$; per-attempt error is $\epsilon = C^{-L} + 2^{-\lambda}$; per-round compute is constant-time (one $\mathcal{M}$ lookup, one rotation, one combine), yielding total $O(L)$ plus mixing. For example, $C{=}6, L{=}6, \lambda{=}512$ gives $\epsilon \approx 1.6 \times 10^{-5}$, dominated by 6^{-6}, with "AES-class" throughput claimed for practical implementations.

Finally, the "**astronomical space**" assertion sometimes stated informally (e.g., 10^{720}) is normalized in this treatment as **parameterized security** under the (C, L, λ) model. The **formal bounds are intentionally conservative and auditable**, aligning stakeholder decisions with measurable error rather than folklore.

Implications

Operational: Eliminating reusable secrets changes breach economics. Servers and logs hold **attestations bound to context** (e.g., $\sigma = \mathrm{MAC}_k(T \parallel q \parallel W \parallel \mathrm{ctx})$), *not* passwords/keys, reducing custodial liability and replay fraud exposure. Audit trails remain high-integrity without stockpiling PII, and admission

control can bind acceptance to trustworthy time and device posture.

Security program: Phishing and credential stuffing **collapse** because there's nothing reusable to phish or stuff; key-rotation fire drills fade; and SOCs gain liveness signals tied to fresh entropy and time. Parameter profiles (C, L) can be segmented by device class to balance cognitive load and risk, while duress policies add safety without on-wire identifiers.

Machine-to-machine: For AI↔AI or service↔service links, **entangled twins** remove PKI lifecycle pain (issuance/rotation/escrow) by turning identity into per-round derivations with optional ratchets. The same primitive can underlay PSK-style channels (e.g., provide an external PSK derived from witnesses), preserving low-latency handshakes with strong non-replay and forward secrecy characteristics.

Compliance & auditability: The axioms (A1–A5) **translate into testable controls**—RNG tests for entropy, build attestation and SBOMs for "burn" hygiene, and constant-time lookups for $\mathcal{M}, \rho$. On the privacy front, the **passive ZK** simulator argument ensures transcripts reveal nothing beyond acceptance, which helps satisfy least-privilege and data-minimization policies.

Scale & deployment: Per-user compiled artifacts ("burn") deliver diversity and limit blast radius, while **cross-platform** toolchains (ARM/x86/Apple/RISC/MIPS, WASM/JVM/CLR) make it feasible to standardize identity across endpoints, clouds, and CI/CD. The same approach yields **secretless pipelines** where build agents authenticate by witness rather than long-lived keys.

Human factors: Because C and the alphabet schema are adjustable, teams can **tune accessibility** (e.g., C=3 grayscale) without abandoning formal bounds; the same UX works from mobile to desktop without hardware tokens or OTP fatigue. This alignment of ergonomics and math helps sustain adoption without eroding security.

Risk budgeting: Concrete, **conservative error accounting**—$\epsilon = C^{-L} + 2^{-\lambda}$—lets architects target FAR/FRR and adversary cost curves and then **reinforce** with online defenses (rate-limits, lockouts, verifier sharding). The result is a tractable budgeting calculus rather than guesswork.

Limitations

White-box caveat: Assumption A5 states that compiled twins leak at most black-box I/O relevant to acceptance; in practice, **hostile-device extraction remains a threat**. Deployments should treat A5 as a *design assumption* to be strengthened with **TEEs/attestation**, code diversification/randomization, constant-time tables, and **side-channel suppression** (uniform envelopes, jitter control).

Time trust & clocks: Anti-replay leans on **temporal uniqueness** (A3). Clocks that drift or can be spoofed erode this guarantee. The manuscript explicitly advises binding T to a **trusted clock** (or even a verifiable delay path) across platforms; engineering must therefore address time attestation and skew handling in adversarial networks.

Accessibility vs. security tradeoffs: Lowering C improves accessibility but shrinks the combinatorial space C^L. Projects should publish **parameter guidance** (e.g., C=6, $L\geq$8 for $\epsilon \leq 10^{-6}$) and automate linting so UX accommodations don't silently weaken targets. This is consistent with the formal error bound and the paper's parameter-profile guidance.

Entropy sources & mixing: A1 requires high min-entropy and unpredictable mixing. Embedded or offline contexts with weak RNGs risk increased collision/replay windows. Audits should therefore include **RNG testing**, seed-lifecycle review, and negative-testing of the Mix/KDF pipeline under constrained entropy.

Interoperability gaps: While the Prove/Verify core is minimal and portable, robust rollouts depend on **admission control**, **telemetry schemas**, and **context labels** to prevent cross-channel confusion or transcript interleaving. Standardized artifacts (SBOMs, signed provenance) and API contracts mitigate these risks, but they require disciplined productization.

Threat model scope: The current security theorem **sketches passive zero-knowledge**; it does not claim a full active-adversary ZK proof. The oscillation lemma limits MiTM sustainment without $\mathcal{M}$, but formalizing active ZK (and richer concurrency properties) remains future work and should be called out in security claims.

Performance claims & side channels: The text cites "**AES-class**" throughput under constant-time inner loops; delivering that in practice depends on careful table design, compiler behavior, and side-channel controls. Systems should also plan for **DoS resilience** (verifier throttling/sharding) since low-latency acceptance paths are attractive flood targets.

---

9. Core Primitive Concepts (extracted from transcript)

P1 — Entropy–Time Mixing (E-Mix). Each session derives a nonce from a timestamp T and an in-circuit prime q ($\approx$512-bit) to prevent replay:

$$n = \mathrm{KDF}(T \parallel q), \qquad e = \mathrm{Mix}(\chi, n), \quad \chi \in \{0,1\}^{\lambda}.$$

Rosario: "append … a timestamp … can never be replayed … reacts upon the current time and a 512-bit prime generated inside of the circuit."

P2 — Private Hologram Morphism. A committed morphism $\mathcal{M}$ maps multi-alphabet symbols and ring states to ring states:

$$\mathcal{M} : \Omega \times A_1 \times \cdots \times A_m \to \Omega.$$

Described as a "second-layer hologram on top of your password" bound to a private map.

P3 — Möbius Loop Integrator. A twisted composition that "loops back on itself at each dimensional space," modeled as

$$\Pi_{k+1} = \rho_k \circ \mathcal{M}(\Pi_k(\omega_0), s_k), \quad \Pi_0 = \mathrm{id},$$

driving witness coordinates on the orientation ring Ω.

P4 — Rotation Ring. With $\Omega = \{\uparrow, \rightarrow, \downarrow, \leftarrow, \backslash, /\}$ and $|\Omega| = C$, per-round rotation

$$\omega_{k+1} = \rho_k(\omega_k) = \omega_k \oplus (\chi_k \bmod C).$$

Rosario demonstrates repeated logins with identical keystrokes but changing valid trajectories.

P5 — Entangled Twin Circuits (oscillation). Two compiled clones (e.g., *Drago*, *Boros*) maintain symmetric challenge↔response "oscillation" and cannot be sustained by a MiTM lacking $\mathcal{M}$.

P6 — Multi-Password Synonyms & Duress. Multiple passcodes map to distinct policy outcomes (normal, duress/decoy, etc.), e.g., a hidden "hockey" duress code. Formalize $\mathcal{S} = \{P^{(1)}, \ldots, P^{(r)}\}$ and a policy $\pi : \mathcal{S} \to \{\mathsf{allow}, \mathsf{duress}, \mathsf{revoke}, \mathsf{escrow}\}$.

P7 — Alphabet Schema & Accessibility. User selects alphabets (LAT, Han, emoji, suits) and color cardinality $C \in \{3, 4, 6\}$ to tune difficulty and accessibility.

P8 — Per-User Compiled Binary ("burn"). Password+map are compiled into a unique artifact; binaries exist for ARM/x86/Apple/RISC/MIPS/PowerPC/WASM/JVM/CLR and are deployable across devices and clouds.

P9 — Trusted-Contact Recovery (conditional access). Optional "dead-man"/escrow flow gates access to a trusted contact only upon verified conditions (e.g., certified medical proof).

P10 — Transaction Attestation. "Every transaction gets signed with a unique piece of entropy and a proof," targeting AES-like throughput.

---

10. Use-Case Patterns and Formal Adaptations

UC-1: Surveillance-Resilient Login (human↔service).
Protocol: Prover computes witness $W = (\omega_1, \ldots, \omega_L)$ from e and $\mathcal{M}$; verifier recomputes and accepts iff W matches. Identical keystrokes replayed later fail because $n = \mathrm{KDF}(T \parallel q)$ changes.
Claimed behavior demonstrated live with a keylogger and replay failure.

UC-2: Agent↔Agent Entangled Channel (AI↔AI).
Bidirectional loop with fresh (T, q) each round:

$$\text{Round } r: \ (T_r, q_r) \mapsto e_r \mapsto W_r, \quad \text{accept} \wedge \text{issue next challenge.}$$

Observed oscillation and AES-class throughput.

UC-3: PII Attestation without Disclosure.
Let user data D (SSN, mother's name) be attested via

$$\tau = \mathsf{H}(\mathcal{M}(e, \mathrm{Enc}(D)) \parallel \mathrm{ctx}),$$

returned to a third-party verifier for match without revealing D. *Motivation given via retail credit-application identity-theft risk.*

UC-4: Coercion Resistance (Duress).
Multiple passwords with policy π emit different transcripts and server actions; e.g., $\pi(P^{(\mathrm{duress})}) = \mathsf{allow\_decoy} \parallel \mathsf{trace}$. *Duress "hockey" example and policy discussion.*

UC-5: Recovery & Inheritance.
Conditional release to trusted contact TC if and only if $\mathsf{Attest}_{\mathrm{doctor}}(\mathrm{coma/death}) = 1$ and a secondary challenge is solved by TC. *Transcribed as micro-AI policy gating escrow.*

UC-6: Cross-Platform & Cloud Rollout.
Burn once, deploy many: mobile (Android/iOS), OS (Linux/macOS/Windows), cloud (CF/AWS/GCP), containers; binaries are signed, relocatable, and API-exposed.

UC-1: Surveillance-Resilient Login (human↔service)

Why. Traditional logins leak reusable secrets to shoulder-surfing, keyloggers, cameras, and RDP capture. The holographic scheme replaces a static secret with a one-time **witness** $W = (\omega_1, \ldots, \omega_L)$ derived from session entropy $x \in \{0,1\}^\lambda$, a temporal nonce $n = \mathrm{KDF}(T \,\|\, q)$, and a private morphism $\mathcal{M}$. Because W is bound to (T, q), identical keystrokes produce different valid trajectories across sessions, invalidating replays. Conceptually, this turns "typing a password" into solving a per-session micro-puzzle on the Ω ring.

How. The prover mixes $\chi = \mathrm{Chunk16}(x)$ with n to form $e = \mathrm{Mix}(\chi, n)$. Per round i, the state rotates $\omega_{i+1} = \rho_i(\omega_i) = \omega_i \oplus (\chi_i \bmod C)$, and the Möbius integrator Π updates via $\Pi_{i+1} = \rho_i \circ \mathcal{M}(\Pi_i(\omega_0), s_i)$. The witness indices $w_i = \mathrm{Index}(\omega_i)$ form the transcript sent to the verifier, which deterministically recomputes $W^\star$ from $(T, \mathrm{tag}(q))$ and accepts iff $W^\star = W$. Because n is fresh, any recorded W is stale.

What (features). Tunable color cardinality $C \in \{3, 4, 6\}$ and mixed alphabets $A_1, \ldots, A_m$ adjust cognitive load and throughput. Multiple **synonym passwords** map to policies (normal, duress, escrow), yet the public distribution of accepting transcripts remains simulatable. Latency is $O(L)$ with constant-time table operations; authentication tokens $\sigma = \mathsf{MAC}_k(T \parallel q \parallel W \parallel \mathrm{ctx})$ bind context without revealing $\mathcal{M}$ or P. Audit logs retain (σ, ctx) only.

Benefit & capability. Resistance to surveillance and replay arises from one-time entropy and private morphism secrecy. No plaintext secrets reside server-side; breach blast-radius shrinks to per-session artifacts. Accessibility modes (e.g., $C = 3$ grayscale) broaden usability; duress routes add safety. Soundness per attempt is $\epsilon \le C^{-L} + 2^{-\lambda}$; with $C = 6, L = 6, \lambda = 512$, $\epsilon \approx 1.6 \times 10^{-5}$ (dominated by 6^{-6}).

Who benefits. High-risk individuals (journalists, executives), enterprises consolidating SSO, and public-sector operators needing login under observation. Helpdesks benefit from fewer resets; compliance teams reduce exposure to credential-stuffing and keylogger claims. Developers gain a single UX that scales from mobile to desktop without hardware tokens.

Engineering notes. Choose L for target FAR/FRR; rate-limit and lockout at the verifier; bind T to a trusted clock. Harden binaries with TEEs and code randomization (assumption of white-box hardness). Provide fallbacks (recovery, offline codes) under policy π. Ensure constant-time lookups for ρ_i and $\mathcal{M}$, and encrypt telemetry at rest.

UC-2: Agent↔Agent Entangled Channel (AI↔AI)

Why. Machine-to-machine links inherit the pain of PKI: key issuance, rotation, escrow, and revocation. Entangled twins replace static keys with per-round holographic witnesses, removing long-lived secrets from the attack surface. This aligns with ephemeral, autoscaled, or serverless topologies where identity must prove *liveness* as well as *possession*.

How. Two compiled clones share $\mathcal{M}$. In round r, each side samples (T_r, q_r), derives e_r and W_r, verifies peer's W_r, and issues the next challenge:

$$(T_r, q_r) \xrightarrow{\text{KDF}} n_r \xrightarrow{\text{Mix}} e_r \xrightarrow{\mathcal{M},\rho} W_r, \quad \text{accept} \wedge \text{challenge}_{r+1}.$$

Derive a session key per round $k_r = \mathsf{KDF}(x_r, T_r, q_r)$ and optionally ratchet $K_{r+1} = \mathsf{HKDF}(K_r \parallel k_r)$. A MiTM lacking $\mathcal{M}$ cannot sustain both directions.

What (features). Mutual liveness and forward secrecy (keys never repeat; transcripts are one-time). Channel-binding via $\sigma_r = \mathsf{MAC}_{K_r}(W_r \parallel \text{ctx}_r)$. Concurrency support through context labels to avoid transcript interleaving. Stateless bootstrap—no CA, CRL, or OCSP—while remaining compatible with TLS offload if desired (use W_r as external PSK).

Benefit & capability. Ultra-low-latency handshakes (no multi-round PKI ceremony) with post-quantum plausibility: breaking requires learning $\mathcal{M}$ or guessing W_r. Works in edge/IoT, swarms, drones, satellites, factory floors, and mesh networks with intermittent links. Graceful resynchronization by rolling r and replay-protecting with (T_r, q_r).

Who benefits. Platform teams managing microservice fleets, telecom edge nodes, OT/SCADA integrators, defense systems with contested spectrum, and SaaS vendors seeking secretless mutual auth. MSPs avoid mass key rollovers; SecOps gains verifiable liveness traces without key escrow.

Engineering notes. Implement QUIC streams with per-stream ratchets; cache short-term acceptance windows to absorb jitter. Gate CPU with DoS-aware puzzles if unauthenticated traffic spikes. Export-controlled environments can ship offline trust bundles (code signatures) without distributing keys.

UC-3: PII Attestation without Disclosure

Why. Identity flows often leak sensitive data (SSNs, names, addresses) to third parties, inflating breach risk and compliance burden. Replace transfer of D with a cryptographic **attestation** that proves possession/consistency relative to context while keeping D private.

How. Encrypt D locally, combine with e under $\mathcal{M}$, and hash with context:

$$\tau = \mathsf{H}(\mathcal{M}(e, \mathrm{Enc}(D)) \parallel \mathrm{ctx}).$$

The verifier either recomputes τ inside an entangled circuit holding the same $\mathcal{M}$, or checks equality against a pre-registered τ family (salted by ctx). Because e is per-session, tokens are non-replayable across contexts.

What (features). Selective disclosure by partitioning D into attributes with separate τ_i and contexts ctx_i ("over-18", "is-resident", "last-4 match"). Non-transferability via device binding and freshness n. Expiry and revocation by context versioning. Auditable consent: store $(\tau, \mathrm{ctx}, \sigma)$ without revealing D.

Benefit & capability. Retail credit checks, SIM-swap defenses, e-prescriptions, and KYC can verify predicates instead of pulling raw PII. Consumers reduce the number of data custodians; enterprises lower GDPR/CCPA footprint and breach liability. Fraud teams compare tokens across merchants without building shadow data lakes.

Who benefits. Banks and fintechs (account opening), healthcare portals (age/coverage proof), government e-services (eligibility), and marketplaces (seller identity) gain faster onboarding with fewer false positives. Users retain dignity and privacy while achieving higher acceptance rates.

Engineering notes. Protect against dictionary attacks on small attribute domains by salting/peppering and rate-limiting. Anchor time-sensitive contexts (e.g., "current address") with validity windows. Provide dispute workflows (reissue τ upon correction of D) without exposing prior D. Consider CBOR/COSE envelopes for device-portable attestations.

UC-4: Coercion Resistance (Duress)

Why. Users may be forced to authenticate under threat. Systems should enable *plausible compliance* while initiating protective responses. Static secrets make signaling impossible without tipping off the coercer; holographic synonyms enable silent branching.

How. Define a set of passwords $\mathcal{S} = \{P^{(1)}, \ldots, P^{(r)}\}$ with policy $\pi : \mathcal{S} \to \{\mathsf{allow}, \mathsf{allow\_decoy}, \mathsf{trace}, \mathsf{revoke}, \mathsf{escrow}\}$. All $P^{(j)}$ yield accepting witnesses W under $\mathcal{M}$, but server-side actions diverge invisibly to observers. By transcript simulability, an eavesdropper cannot distinguish which $P^{(j)}$ was used beyond ϵ.

What (features). Decoy environments seeded with synthetic data; throttled capabilities; covert telemetry σ^{duress} to SOC; progressive slow-walk of sensitive operations; geofenced allow-lists; and "quiet lock" that completes UX while

isolating assets. Time-delayed confirmations require out-of-band approval to finalize.

Benefit & capability. Users can comply under pressure while signaling risk to guardians or SOCs. Organizations investigate from safe remove, tag the session for forensics, and preserve evidentiary chains. Assets remain shielded behind decoys, reducing harm even if the coercer continues operating.

Who benefits. Journalists/defenders in hostile regions, executives subject to kidnap risks, domestic-violence survivors, and field operatives. Enterprises with high-value back-office systems and banks with teller/branch workflows gain protective redundancy without harming regular UX.

Engineering notes. Carefully govern π to avoid accidental triggers; log minimally to prevent coercer learning. Train staff on decoy procedures; test with red teams. Provide legal/ethics reviews for tracing and law-enforcement integrations. Ensure decoy content cannot be trivially fingerprinted.

UC-5: Recovery & Inheritance

Why. Seed phrases and static backup codes are brittle: they're either lost or exfiltrated. Recovery should be conditional, attestable, and privacy-preserving, reflecting real-world events (incapacity, death) without custodial takeover.

How. Define an escrow policy where access is granted iff external attestations hold and a trusted contact TC solves a secondary challenge. The gate composes predicates $g = \bigwedge_j \mathrm{Attest}_j$ (e.g., medical/death certificate) with a fresh witness W_{TC} under $\mathcal{M}_{\mathrm{escrow}}$. Optionally split control among contacts using thresholding (e.g., Shamir over independent TC_k) with each share guarded by a witness.

What (features). Time-locks ("not before" T_0), grace periods, and revocation channels. Audit-friendly proof artifacts ($\sigma_{\mathrm{escrow}}, \mathrm{ctx}$) without exposing user secrets. Programmable scopes (read-only vs. transfer), and expiry requiring re-attestation. Emergency break-glass that opens a decoy state while launching out-of-band confirmations.

Benefit & capability. Families and estates avoid catastrophic lockouts; DAOs and SMEs can structure continuity without centralized custodians. Compliance teams satisfy fiduciary and probate requirements while preserving user privacy. Recovery becomes a *process*—not a stored secret—reducing theft incentives.

Who benefits. Consumers (wallets, cloud vaults), enterprises (admin accounts, HSM roots), clinicians (patient portals), and regulated industries managing dormant assets. Legal counsel gets verifiable logs for probate and disputes.

Engineering notes. Standardize attestation formats (e.g., digitally signed medical certificates). Maintain rotating rosters of TC with periodic liveness checks. Simulate edge cases (false attestations, contact compromise) and layer duress-aware flows. Bind recovery artifacts to jurisdictional requirements and data minimization.

UC-6: Cross-Platform & Cloud Rollout

Why. Security architectures fail if they don't ship everywhere users compute. Per-user **burned** binaries deliver uniqueness and defense-in-diversity across ARM/x86/Apple/RISC/MIPS, WASM/JVM/CLR, containers, and FaaS, minimizing monoculture risk and easing integration.

How. The build pipeline compiles twins with embedded $\mathcal{M}$ and per-user parameters, applying multi-dimensional code transforms and signing the artifact. Distribution uses standard channels (mobile SDKs, package repos, container registries). Verification keys sign releases; SBOMs accompany artifacts for supply-chain transparency.

What (features). Portable SDKs, offline mode, tenant isolation, policy packs, and APIs that expose attestations σ while keeping $\mathcal{M}$ sealed. Optional FIPS-validated primitives in the mixing/KDF/MAC layer. Integrations for HSMs/TEEs provide sealed storage for runtime material like q.

Benefit & capability. CI/CD pipelines become **secretless**: build agents authenticate via witnesses, not long-lived keys. Multi-cloud failover retains identity without re-provisioning. Field devices operate disconnected with local acceptance caches and reconcile upon connectivity. Performance targets match "AES-class" throughput by keeping per-round work constant.

Who benefits. App developers needing a single auth substrate across platforms, MSPs managing fleets, cloud providers offering value-add identity services, and enterprises consolidating legacy auth stacks. Users enjoy consistent UX across phone, laptop, and kiosk.

Engineering notes. Treat white-box hardness as an assumption—reinforce with attestation (e.g., enclave measurements), anti-tamper and JIT randomization. Use reproducible builds, signed provenance (SLSA), and per-tenant namespaces. Telemetry must be privacy-preserving; tune C, L per device class to balance security and UX.

Synthesis

Across all six use-cases, the common spine is a **holographic witness** derived from fresh entropy x, temporal nonce $n = \mathrm{KDF}(T \parallel q)$, and a private morphism $\mathcal{M}$. This yields (i) per-session non-replayability, (ii) no reusable server-side secrets, (iii) simulatable public transcripts, and (iv) tunable error $\epsilon \leq C^{-L} + 2^{-\lambda}$. The result is a unifying **keyless** paradigm spanning human logins, AI-to-AI channels, selective attestations, duress-aware operations, conditional recovery, and mass deployment—without sacrificing speed or accessibility.

---

11. Feature Formalizations

F1 — Witness Error Bound (per attempt).
With $|\Omega| = C$ and length L,

$$\epsilon_{\text{forge}} \leq C^{-L} + 2^{-\lambda}.$$

Increasing C (color count) or L (steps) tightens error; choosing multiple passwords multiplies the adversary's uncertainty over π.

F2 — Policy Algebra.
Let $\pi : \mathcal{S} \to \mathcal{A}$ with $\mathcal{A} = \{\mathsf{allow}, \mathsf{duress}, \mathsf{revoke}, \mathsf{escrow}\}$. Server action is

$$\text{act} = \pi(P) \parallel f(W, \text{ctx}),$$

binding high-level outcomes to cryptographic acceptance.

F3 — Attestation Token (transaction signing).
Issue $\sigma = \mathsf{MAC}_k(T \parallel q \parallel W \parallel \text{ctx})$ where $k = \mathsf{KDF}(x, T, q)$ never leaves the circuits; logs store (σ, ctx) for audit without leaking P or $\mathcal{M}$. *Matches "unique entropy + proof" semantics and audit integrations.*

---

12. Lemmas and Security Notes

Lemma 5 (Coercion-Policy Indistinguishability). Under A1–A5, an eavesdropper cannot distinguish which $P^{(j)} \in \mathcal{S}$ produced an accepting transcript beyond ϵ_{forge}. *Sketch:* transcripts are one-time and simulatable; π influences server-side action, not the public distribution of W.

Lemma 6 (Escrow Gating Correctness). If escrow predicates are satisfied and TC answers the secondary challenge, recovery succeeds with probability 1; otherwise negligible. *Relies on unique n and the independence of secondary challenge.*

Note (White-Box Risk & Build Hygiene). Rosario's "burn/compile" step implies per-user obfuscation; still pair with TEEs, anti-tamper, and constant-time tables for $\mathcal{M}, \rho$.

Mathematical Treatments

Lemma 5 — Coercion-Policy Indistinguishability (CPI)

Why. Coercion changes the threat model: an adversary can force a user to authenticate, observe the full on-wire transcript, and later punish deviations. We require that switching among synonym passwords $P^{(j)} \in \mathcal{S}$ (e.g., *normal*, *duress*, *decoy*) be unobservable on the public channel. Formally, define game

CPI where the adversary chooses $j_0 \neq j_1$, receives a single accepting transcript produced under one of $\{P^{(j_0)}, P^{(j_1)}\}$, and must guess the index. CPI asks that the adversary's distinguishing advantage be negligible beyond the baseline forgery error ϵ_{forge}.

How. Under A1–A5, transcripts are one-time: $n = \text{KDF}(T \parallel q)$ and fresh x force a new mixed state e every session. The witness distribution $W \in \Omega^L$ is independent of which $P^{(j)}$ was used, because the private morphism $\mathcal{M}$ binds the acceptance relation while server-side policy π branches *after* verification. Let View_j denote the public transcript when $P^{(j)}$ authenticates. Then

$$\Delta_{\text{TV}}\big(\mathsf{View}_{j_0}, \mathsf{View}_{j_1}\big) \;\leq\; \epsilon_{\text{forge}} + 2^{-\lambda} + \delta_{\text{side}},$$

where δ_{side} upper-bounds out-of-model leakage (timing, traffic shaping). Hence the CPI advantage

$$\text{Adv}^{\mathsf{CPI}}_{\mathcal{A}} \;\triangleq\; \left|\Pr[b' = b] - \tfrac{1}{2}\right| \;\leq\; \tfrac{1}{2}(\epsilon_{\text{forge}} + 2^{-\lambda} + \delta_{\text{side}}).$$

What (features). CPI enables (i) **synonym passwords** $\mathcal{S}$ with a policy algebra $\pi : \mathcal{S} \to \{\mathsf{allow}, \mathsf{allow\_decoy}, \mathsf{trace}, \mathsf{revoke}, \mathsf{escrow}\}$; (ii) **decoy sessions** that complete UX normally; (iii) **covert alerts** (σ^{duress}) emitted to SOC without observable protocol differences; (iv) **graceful degradation** (rate caps, minimal scopes) that are indistinguishable from benign server variance; and (v) **multi-session CPI**, where a polynomial number of accepting transcripts still remain indistinguishable, via a hybrid/simulator argument.

Benefit & capability. Users can comply under coercion while silently invoking containment actions; organizations obtain **plausible deniability** guarantees that are cryptographically auditable. CPI composes with rate-limits and lockouts without breaking indistinguishability, because those controls are triggered by server-local state, not by View_j. The security reduction ties CPI to (a) unforgeability of fresh W and (b) black-box simulability of the transcript, yielding a clear attack budget: to break CPI the adversary must either forge W (cost $\approx C^L$) or extract $\mathcal{M}$ (white-box attack, covered below).

Who benefits. High-risk individuals (journalists, activists), branch banking, high-value ops (trading floors, datacenter NOCs), and any line of business facing social engineering or physical duress. Legal/risk teams benefit from formal CPI statements when designing duty-of-care and escalation SOPs.

Engineering notes. Keep δ_{side} small: constant-time verification paths; fixed-length records; jitter padding; identical HTTP/2 or QUIC priorities; uniform error messages; and bounded server think-time. Log duress outcomes only in shielded backends. Periodically red-team CPI to catch *implicit* side channels (A/B infrastructure differences, CDN routing, CDN cache hits).

Lemma 6 — Escrow Gating Correctness

Why. Recoverability and inheritance cannot rely on static secrets; those are lost or stolen. Correctness must reflect *real-world predicates* (e.g., certified incapacity, death) and *fresh agency* by a designated trusted contact (TC). The protocol should guarantee: if predicates hold and TC solves a secondary challenge, recovery **must** succeed; otherwise, attempts **must** fail except with negligible probability.

How. Model escrow as a guarded state machine. Let $g = \bigwedge_{i=1}^{m} \mathsf{Attest}_i$ be external, signed predicates (e.g., $\mathsf{Attest}_{\text{doctor}} = \text{true}$). Let $\mathcal{M}_{\text{escrow}}$ be a distinct morphism compiled into an escrow twin; generate a fresh nonce $n' = \text{KDF}(T' \parallel q')$ and require a TC witness W_{TC} of length L'. **Completeness**: if $g = 1$ and $\mathsf{Verify}_{\mathcal{M}_{\text{escrow}}}(W_{\text{TC}}) = 1$, the machine transitions to **Released**. **Soundness**: if $g = 0$ or W_{TC} is incorrect, the probability of release is $\leq C^{-L'} + 2^{-\lambda}$. With t-of-n contacts, replace the single W_{TC} by independent witnesses W_k and threshold verification; independence preserves the same bound against any coalition smaller than t.

What (features). (i) **Predicate modularity:** multiple attestations with issuers, validity windows, and revocation lists; (ii) **Secondary challenge diversity:** separate alphabets, color cardinality C', and length L' to isolate escrow surface from primary auth; (iii) **Time controls:** "not-before" T_0, grace periods, and human-in-the-loop delays; (iv) **Scope restriction:** recovery can expose only a subset of capabilities (read-only, transfer-only); (v) **Audit artifacts:** $\sigma_{\text{escrow}} = \mathsf{MAC}_{k'}(g \parallel T' \parallel W_{\text{TC}} \parallel \text{ctx})$ for court-grade provenance without revealing secrets.

Benefit & capability. Users and organizations avoid catastrophic lockouts while removing honey-pot backups. Attackers cannot pre-compute recovery because predicates are world-anchored and challenges are fresh. Executors and compliance teams obtain non-repudiation via σ_{escrow}. Threshold designs distribute trust; periodic liveness checks prevent dormant takeover.

Who benefits. Consumers (wallets, vaults), SMEs (admin break-glass), DAOs (governance continuity), healthcare (patient proxies), and regulated finance (estate/probate). Legal teams gain a cryptographic basis for *intent* and *authority*, while security teams retire sticky notes and insecure backup vaults.

Engineering notes. Standardize attestations (X.509/COSE-signatures; issuer PKI). Maintain **independence** between primary and escrow morphisms and parameter sets (C, L) vs. (C', L'). Enforce anti-rollback (monotone counters; signed state). Simulate edge cases: forged attestations, compromised TC, partial thresholds, and jurisdictional conflicts.

Note — White-Box Risk & Build Hygiene (from "burn/compile")

Why. Per-user compilation and obfuscation raise the bar but do not, by themselves, defeat a determined white-box adversary armed with dynamic instrumentation, micro-architectural probes, or firmware-level access. The goal is to minimize extractable *useful* information (e.g., $\mathcal{M}$) and shrink the exploit window via rapid, diversified, attestable artifacts.

How. Treat the toolchain as a *security-critical* pipeline: reproducible builds; hermetic dependencies; SBOM emission; provenance per SLSA; artifact signing; and policy-gated promotion. On device, anchor secrets to TEEs (SGX/TDX/SEV-SNP/ARM-CCA), measure the binary (PCR, REPORT), and gate protocol participation on remote attestation. Make critical paths constant-time; randomize layout and in-memory encodings; and apply coverage-guided fuzzing + concolic testing on parsers and state machines.

What (features). (i) **Binary diversification:** per-user instruction-set shuffling, opaque predicates, control-flow flattening, basic-block reordering; (ii) **Exploit mitigations:** CFI, CET/shadow stacks, pointer-auth (PAC), hardened allocators, W^X; (iii) **Anti-tamper/anti-debug:** anti-hook trampolines, JIT re-encryption, entropy-tied decryption of hot code, crash-resistant telemetry; (iv) **Side-channel guards:** constant-time tables for $\mathcal{M}, \rho$; masking; noise injection; fixed-rate I/O; (v) **Supply-chain posture:** SBOM diffs, vulnerability gates, staged canaries, rollback prevention.

Benefit & capability. Increases attacker *cost* and *time-to-extract*, localizes fallout (each binary is unique), and enables rapid revocation/rotation on compromise. Measurement-based admission lets services refuse stale or repacked clients. For regulated sectors, provenance + SBOM improve audit readiness and incident response.

Who benefits. Platform owners, ISVs, and integrators distributing clients to heterogeneous devices (mobile, desktop, IoT). SOCs gain higher-fidelity alerts (attestation failures, integrity drift). End-users inherit stronger protections without extra hardware, and procurement teams can demand verifiable supply-chain artifacts.

Engineering notes. Model residual leakage explicitly:

$$\mathrm{Adv}_{\mathrm{extract}} \;\le\; \mathrm{Adv}_{\mathrm{wb\text{-}anal}} \;+\; \mathrm{Adv}_{\mathrm{sc}} \;+\; \mathrm{Adv}_{\mathrm{fault}},$$

and budget monitoring accordingly. Keep hot paths tiny; prefer table-free arithmetic where possible; instrument hardware performance counters for anomaly detection; and periodically *re-burn* with fresh diversity seeds.

---

13. Implementation & Deployment

Pipeline. Onboard → select alphabets/C → set $\mathcal{S}$ (incl. duress) → create hologram map → self-test → burn → deploy per-arch → expose API. *Console and architecture listings shown live.*

Accessibility. Offer $C = 3$ (grayscale) and mnemonic recording of the map; test mode verifies mastery before burn.

---

14. Applications & Integrations

- **Proof of Humanity / Identity Layer** for data provenance systems; issue per-event σ with context binding.
- **Voice/retail checkout** without PII leak; third-party verifier sees proofs only.
- **Consumer/enterprise**: phone, bank, OS login; dockerized services with signed binaries.

14.A1. Proof of Humanity / Identity Layer (for data provenance)

Why. Provenance systems need to assert that *some* accountable human (or approved agent) created or approved an artifact without leaking long-lived identifiers or PII. Passwords and static keys fail under replay and surveillance; biometrics create irrevocable identifiers. A **holographic witness** W derived from fresh entropy x and nonce $n = \mathrm{KDF}(T \parallel q)$ yields *per-event*, non-replayable proofs, transforming identity from a static secret into a one-time attestation.

How. For each event with context ctx (e.g., document hash, camera sensor ID, capture location/time), the agent computes

$$\sigma = \mathsf{MAC}_k(T \parallel q \parallel W \parallel \mathrm{ctx}), \quad k = \mathsf{KDF}(x, T, q),$$

and publishes (σ, ctx) alongside the artifact or its hash. Verifiers (holding the entangled circuit) recompute W from $(T, \mathrm{tag}(q))$ and accept iff σ verifies. Because x, T, q are fresh, linkability across events is policy-controlled rather than an inherent side effect.

What (feature set). (i) **Unlinkable pseudonyms** via rotating (T, q) and scoped ctx; (ii) **Selective disclosure** by separating provenance channels (capture vs. edit vs. approve); (iii) **Revocation** using context versioning and deny-lists over ctx; (iv) **Ledger anchoring** by committing σ to a transparency log without publishing $\mathcal{M}$ or W; (v) **Rate controls** per pseudonym to deter Sybil behaviors; (vi) **Federation** across domains by bridging ctx namespaces.

Benefit & capability. Platforms obtain cryptographic provenance without handling raw identity; creators gain proof-of-authorship that is portable yet

privacy-preserving; auditors can verify continuity of control over time. Attackers can neither replay old σ (fresh n) nor cheaply forge new W (cost $\approx C^L$). The privacy surface is tunable: one can enable *unlinkability by default* and opt into linkable channels where accountability is required.

Who benefits. Newsrooms, research datasets, supply-chain imaging, digital art, and AI-generated content pipelines that must distinguish "who attested this" from "who *is* this." Regulators and standards bodies gain a neutral, cryptography-first substrate to implement provenance policies without mandating central identity vaults.

Engineering notes. Normalize ctx (CBOR) to avoid canonicalization bugs; pad records to constant length; implement batch verification for high-throughput feeds; publish public transparency proofs (Merkle roots) while keeping $\mathcal{M}$ sealed. Expose opt-in *linkability tokens* derived as $t = \mathsf{H}(k \parallel \text{scope})$ to support abuse-mitigation without de-anonymizing events.

14.A2. Voice / Retail Checkout (no PII leakage)

Why. Call centers and points-of-sale routinely solicit PII (SSNs, ZIP codes, birthdays) that are easy to overhear, store, and breach. Friction is high; fraud vectors multiply. The objective is to bind a customer to an account and a transaction **without** transferring secrets—only proofs.

How. The customer's device (or kiosk) computes a holographic witness W and produces a merchant-verifiable token

$$\tau = \mathsf{H}\big(\mathcal{M}(e, \mathrm{Enc}(D)) \parallel \mathrm{ctx}\big), \quad \mathrm{ctx} = \mathrm{merchantID} \parallel \mathrm{basket} \parallel T,$$

where D is account material stored locally (encrypted) and $e = \mathrm{Mix}(\chi, \mathrm{KDF}(T \parallel q))$. The merchant receives τ (e.g., via DTMF, QR, NFC, ultrasonic) and checks it using an entangled verifier. No PII crosses the channel; τ is context-bound and non-replayable.

What (feature set). (i) **Scoped consent** (amount, merchant, validity window) bound into ctx; (ii) **Duress variants** that authorize decoy/limited spend while flagging risk; (iii) **Offline mode** creating time-locked τ with delayed settlement; (iv) **Chargeback-resistant receipts** by logging $(\tau, \mathrm{ctx}, \sigma)$; (v) **Multi-factor composition** (device posture, geofence) folded into ctx without extra user steps.

Benefit & capability. Merchants reduce PCI scope and fraud by verifying proofs, not secrets. Customers enjoy faster checkout and smaller attack surfaces—nothing to overhear or scrape. Because τ is one-time and context-specific, replay at a different merchant or for a different basket fails; phishing yields no reusable artifact.

Who benefits. Retailers (in-store, curbside), subscription call centers, delivery and gig-economy apps, and telcos. Issuing banks and PSPs gain stronger non-repudiation while minimizing PII handling. Accessibility improves (voice or color-reduced modes) without sacrificing security.

Engineering notes. For low-entropy attributes (e.g., ZIP), add pepper and enforce per-account rate limits; publish SDKs with constant-time primitives; provide fallbacks to card rails with the same UI flow. Bind dispute workflows to (τ, ctx) rather than raw PII; instrument duress policies to avoid adversary detection (same protocol envelope, uniform timing).

14.A3. Consumer & Enterprise: Phone, Bank, OS Login; Dockerized Services

Why. Users juggle passwords, OTPs, and device-bound authenticators; enterprises manage keys for CI/CD, registries, and microservices. Static secrets propagate risk and operational toil. A single **keyless** substrate should secure human logins and machine pathways while preserving speed and UX.

How. *Phone/OS:* a local entangled verifier (PAM/Pluggable Auth Module on Linux; Credential Provider on Windows; LoginWindow plugin on macOS; mobile SDKs) checks W offline, then issues a short-lived SSO token. *Bank/web:* remote verifier repeats the check and mints OIDC/SAML assertions. *Dockerized services:* per-user/per-tenant **burned** binaries authenticate to registries and CI by emitting W-bound σ, replacing long-lived access keys.

What (feature set). (i) **Adapters** for OIDC/SAML/SCIM, PAM/GSSAPI, and SSH certificates; (ii) **TEE/TPM binding** for q and clock trust; (iii) **Duress & recovery policies** π integrated with admin workflows; (iv) **Remote attestation** gates workload participation; (v) **Secretless CI/CD**: build, push, and deploy via witnesses instead of tokens; (vi) **Parameter profiles** (C, L) per device class to balance security with cognitive load.

Benefit & capability. Phishing and credential stuffing collapse: there's no reusable secret to steal. Helpdesks see fewer resets; SOCs gain high-fidelity liveness trails (σ, ctx) without collecting PII. DevOps eliminates key rotation emergencies; supply-chain posture improves through SBOMs, signed provenance, and workload attestation. Latency remains near "AES-class" since per-round work is constant time.

Who benefits. Consumers logging into phones, laptops, and banks; enterprises consolidating identity across endpoints and clouds; SaaS vendors distributing signed clients; regulated industries needing attestable access without key escrow. Legal/compliance benefits from auditable, privacy-preserving logs.

Engineering notes. Treat white-box defenses as layers: TEEs + diversification + constant-time tables for $\mathcal{M}, \rho$. Enforce uniform network envelopes to suppress side channels; throttle and shard verifiers to mitigate DoS. Offer *break-glass* flows bound to escrow morphisms and external attestations. Provide formal parameter guidance (e.g., $\epsilon \leq 10^{-7}$ via $C = 6, L = 8$) and automated policy linting to prevent misconfiguration.

Synthesis

All three integrations share the same cryptographic spine: a **holographic witness** W computed from fresh entropy and a **private morphism** $\mathcal{M}$, producing one-time tokens (σ, τ) *bound to context*. This yields surveillance-resistant authentication, non-transferable attestations, and secretless automation—while keeping UX fast and accessible and placing organizations on firmer, auditable security footing.

---

15 Holographic Entanglment

Theoretical concepts

1) "Entanglement" as a security primitive

- **Our claim.** The human mind can "entangle" with a pre-committed circuit so that both can read the *same* ambient entropy and privately agree on an answer that nobody else can know; the mind can "make a statement at any point in the universe," and the paired circuit interprets that same entropy *at that moment* to co-attest a fact.
- **Operational picture.** Two compiled, symmetric "twin" circuits (e.g., Drago/Boros) are cloned from the same binary and "oscillate" messages only they can sustain; Dylan describes this as "completely entangled" communication resistant to interception.
- **Formalization.** The paper renders this metaphor as **entangled circuits** that share a private morphism $\mathcal{M}$ and verify a one-time **holographic witness** W; there is no reusable secret in the clear, and transcripts are one-time.
- **Security meaning.** Mutual "entanglement" becomes a **bidirectional challenge–response oscillation**: a MiTM without $\mathcal{M}$ cannot keep both directions consistent over rounds.
- **Takeaway.** "Entanglement" here is **informational**, not physical quantum entanglement: a compile-time shared private map $\mathcal{M}$ and synchronized derivations create a closed verification loop that others can observe but not *continue* without the map.

2) Information transfer via "holographic overlay," rotations, and Möbius looping

- **Our claim.** Instead of sweeping a full stochastic space, the system applies a **"holographic overlay"** of multiple information streams and **projects**

them into a space "that can be attested to."

- **Demonstrated behavior.** Identical keystrokes (e.g., "up, right, ...") replayed later fail; the colored "pad" is a one-time pad whose rotation remaps the same password to a *different* valid trajectory each session.
- **Formalization.** The "overlay" is the **private hologram morphism** $\mathcal{M} : \Omega \times A_1 \times \cdots \times A_m \to \Omega$ acting on an **orientation ring** Ω with per-round **rotation** ρ_i. The **Möbius combiner** $\Pi_{k+1} = \rho_k \circ \mathcal{M}(\Pi_k(\omega_0), s_k)$ "loops back on itself" to generate the witness coordinates.
- **Attacker's view.** Without $\mathcal{M}$, observed witnesses look pseudorandom and are one-time; replays fail when the verifier recomputes on new mixed state.

3) Spatio-temporal entropy: turning *time* into anti-replay

- **Our claim.** Each statement is bound to *when* it was made: the attesting value is extended with a **timestamp** and reacts to a **512-bit in-circuit prime**, so "this piece of entropy can never be replayed."
- **Formalization.** A **temporal nonce** $n = \mathrm{KDF}(T \parallel q)$ is mixed with high-entropy session state x to produce e; per session, the prover emits witness indices with $(T, \mathrm{tag}(q))$, and the verifier recomputes deterministically.
- **Interpretation.** This casts "space-time" talk into a precise rule: **fresh time + in-circuit prime** $\to$ fresh state $\to$ new trajectory on Ω. It is *time-scoped attestation* rather than location-based magic.

4) Attestation as "fresh, verifiable work"

- **Our claim.** "Every transaction gets signed with a unique piece of entropy and a proof."
- **Formalization (provenance).** The paper instantiates *per-event* attestations: derive W from (T, q) inside the twins and bind an external context to produce signatures (e.g., $\sigma = \mathsf{MAC}_k(T \,\|\, q \,\|\, W \,\|\, \mathrm{ctx})$).
- **PII-free proofs.** For attributes D, produce non-transferable tokens $\tau = \mathsf{H}(\mathcal{M}(e, \mathrm{Enc}(D)) \parallel \mathrm{ctx})$ that verify without revealing D.
- **Meaning.** "Attestation" = **context-bound, one-time proof of liveness/possession** derived from entropy and time inside an entangled circuit, not a static credential.

5) State space & the "cosmic scale" claim

- **Our claim.** Using a trivial human password (even a single character repeated), the rotational space is touted as "10^{720}," i.e., vastly exceeding the "10^{100}" scale often used to dramatize infeasibility.
- **Formalization.** The paper reframes this as tunable search complexity $\mathcal{C}_{\text{guess}} \approx \max\{2^{\lambda}, C^{L}\}$ and error $\epsilon = C^{-L} + 2^{-\lambda}$, with concrete budgets (e.g., C=6, L=6, λ=512 $\Rightarrow$ $\epsilon \approx 1.6\times10^{-5}$).
- **Meaning.** The "astronomical" rhetoric maps to **auditable parameters** (C, L, λ): raise L or C to push ϵ below target risk while keeping constant-time per-round cost.

6) Entanglement as Encryption

- We illustrate a language outlining **consciousness** and **universal entropy** motivates an intuition for *non-extractable* knowledge sharing, but the implementation grounds it in standard cryptographic levers: **fresh entropy**, **time-mixing**, a **private morphism** sealed in compiled twins, and **deterministic recomputation** at the verifier.
- The result is not quantum signaling; it's a **keyless interactive proof** with one-time witnesses and **oscillating** mutual checks. The "entanglement" metaphor is realized as **shared $\mathcal{M}$ + synchronized derivations** that outsiders can't replay or extend.

We presented here in our treaste on "entanglement," that spatio-temporal entropy, and attestation as a single conceptual edifice provide uncrackable security. Our thesis is that identity can be recast as per-event, per-context *work* that two "twins" can verify but nobody else can reuse. In this view, the credential is not a possession but a trajectory—an ephemeral path through a small, discrete orientation space—shaped by fresh entropy, time, and a sealed morphism inside the twins.

We begin with the definition of entanglement yet immediately remove the suggestion of quantum mystique. The relevant entanglement is informational: two circuits compiled from the same binary share a private morphism $\mathcal{M}$ and therefore a private geometry. When they encounter the same stimulus—fresh session entropy x, a timestamp T, and contextual inputs q—they compute congruent trajectories on an orientation ring Ω. To an outsider, the outputs appear as a scatter of indices; to the twins, they are coordinates in a shared chart. This is how a statement can be "made anywhere": not by violating physics, but by ensuring both parties can reconstruct the *same* one-time witness W from the *same* spatio-temporal seed.

The vehicle of information transfer is a holographic overlay: multiple streams—entropy chunks, time, and user symbols—are superposed by $\mathcal{M}$ and then folded by per-round rotations ρ_i into a Möbius-like loop Π. Each round maps the current

ring position and symbol choice to a new position; the L positions compose the witness. Because the mix depends on T and high-entropy state, identical keystrokes or gestures land on *different* valid trajectories across sessions. Thus the transcript of a prior success is not a credential but a fossil; its shape explains the acceptance that already happened, while refusing to unlock a future door.

Time is not an afterthought but a constitutive dimension of the proof. A temporal nonce $n = \mathrm{KDF}(T \parallel q)$ couples the wall clock to the circuit's internal algebra—optionally salted by an in-circuit prime—to guarantee that the same nominal input produces a different mixed state e whenever the clock or context changes. Attestation then becomes spatio-temporal: the question "are you you?" is replaced by "can you produce *now*, under this context, the witness our geometry predicts?" The arrow of time is thereby enlisted as a cryptographic ally; replay is not merely discouraged by policy but invalidated by construction.

To transform a private trajectory into a portable claim, the twins bind it to context. The prover emits a one-time witness and a context tag (login, payment, deploy), and optionally computes a MAC or hash-based token over (T, q, W, ctx). These tokens are not keys and do not expose secrets; they are receipts that say "the right work was done at the right time in the right context." In richer modes, attributes D (eligibility, limits, roles) can be folded through $\mathcal{M}$ to produce PII-free attestations: the verifier learns that the attribute is held, not what the attribute contains.

Mutual authentication is achieved by *oscillation*. Each twin alternates challenge and verification, forcing the adversary to sustain consistency in both directions under fresh entropy. A man-in-the-middle lacking $\mathcal{M}$ can forward messages but cannot maintain the bilateral constraint that each side imposes. From the oscillation transcript, both parties may KDF ephemeral session keys, ratcheting if desired. Thus session secrecy and liveness are by-products of the same geometry that already ensures non-replay.

The security envelope is explicit and tunable. Let C be the ring's cardinality and L the number of rounds. Guessing a full witness requires work on the order of C^L; independent entropy protects against shortcutting the mix, contributing a 2^λ term. The conservative per-attempt error is $\epsilon = C^{-L} + 2^{-\lambda}$. This is not cosmic numerology but an auditable budget: accessibility can be improved by lowering C, provided L is raised to keep ϵ below target risk. Because each round is constant-time—one morphism lookup, one rotation, one combine—the latency scales linearly in L, enabling "dial-a-risk" deployments without architectural upheaval.

From a systems perspective, the replacement of secrets with witnesses changes the economics of compromise. Servers no longer curate evergreen credentials; they store attestations bound to context, time, and entropy. Breach fallout thus shifts from "all keys exposed" to "historical receipts leaked." Phishing collapses because there is nothing durable to steal; credential stuffing collapses because acceptance depends on the present tense of the proof. Operational controls—rate limits, lockouts, sharding of verifiers—compose cleanly atop the formal error bound to produce defense in depth.

Human factors enter through the geometry rather than in spite of it. The

ring can be three, four, or six orientations; alphabets can be textual, symbolic, gestural; synonym inputs can map to duress behaviors at the server without changing the on-wire distribution. Because each of these choices has a mathematical shadow—each alters C, L, or the mix—they can be tuned consciously. Accessibility ceases to be a bolt-on and becomes a first-class design parameter whose security consequences are not guessed at but measured.

The speculative rhetoric of "universal entropy" and "mind–circuit resonance" finds a sober landing in this framework. If a human and a compiled twin consult the same ambient randomness and the same clock, their shared morphism lets them agree privately on a witness no third party can reuse. The romance is not in faster-than-light messaging but in the elegance with which cognition, time, and computation are braided into a proof that only the rightful pair can regenerate. The novelistic flourish—characters "speaking anywhere"—thus reduces to a precise and falsifiable claim: identity is enacted, not carried.

None of this absolves engineering of its ordinary sins. The assumption that compiled code leaks at most black-box I/O is a working premise, not a theorem; hostile devices motivate TEEs, build attestation, code diversification, and side-channel suppression. Time must be trustworthy; clocks drift and can be spoofed, so verifiers should bind acceptance to attested time or verifiable delay. Entropy must be real; embedded systems should be audited for RNG quality and seeded carefully. These caveats are not decorations; they are the scaffolding that makes the mathematics bite.

For machine interlocutors—agents, services, autonomous systems—the geometry is especially congenial. The twins' oscillation replaces certificate lifecycles and PSK sprawl with per-round derivations; session keys fall out naturally; provenance becomes an accumulation of one-time receipts rather than a registry of immortal secrets. The same primitive harmonizes human–AI and AI–AI interactions, enabling ecosystems in which attestation is cheap, replay is structurally impotent, and privacy is a default property of transcripts.

At the level of epistemology, the scheme distinguishes *knowledge* from *evidence* with unusual clarity. Knowledge is the latent ability to reproduce W under the correct spatio-temporal conditions; evidence is the transient act of doing so now. Because the evidence is one-time, it cannot be warehoused as knowledge by an adversary. The proof is of the *capacity* to align with a private geometry in the present, not of possession of an artifact from the past. For a philosophical novel, this is fertile ground: identity as performance, truth as synchronization, trust as agreement on a path through a finite space.

The practical moral is simple and radical: stop storing what you do not need, and stop sending what you cannot revoke. Compile twins that share $\mathcal{M}$; bind attestation to time and context; select C, L, λ to meet a measured error budget; instrument the usual defenses; and treat side channels as first-class citizens. If you do, the usual threats are bent out of shape: transcripts become harmless, stolen databases become inert, and the only thing that matters is whether the twins can dance the same short dance at the same moment.

In closing, the lecture returns to story. Imagine a world in which every meaningful interaction—unlocking a door, signing a contract, dispatching a drone—is

a brief, choreographed traverse of a ring that only the rightful pair can predict. The choreography is different each time; observers can listen and learn nothing usable; the partners separate, leaving behind only a receipt that says "we danced here, then." Whether written as a chronicle or a technical manual, the core remains the same: entanglement, in this sense, is the art of making *now* the only key that ever fits.

Theoretical concepts

1) "Entanglement" as a security primitive

- **Our claim.** The human mind can "entangle" with a pre-committed circuit so that both can read the *same* ambient entropy and privately agree on an answer that nobody else can know; the mind can "make a statement at any point in the universe," and the paired circuit interprets that same entropy *at that moment* to co-attest a fact.
- **Operational picture.** Two compiled, symmetric "twin" circuits (e.g., Drago/Boros) are cloned from the same binary and "oscillate" messages only they can sustain; Dylan describes this as "completely entangled" communication resistant to interception.
- **Formalization.** The paper renders this metaphor as **entangled circuits** that share a private morphism $\mathcal{M}$ and verify a one-time **holographic witness** W; there is no reusable secret in the clear, and transcripts are one-time.
- **Security meaning.** Mutual "entanglement" becomes a **bidirectional challenge–response oscillation**: a MiTM without $\mathcal{M}$ cannot keep both directions consistent over rounds.
- **Takeaway.** "Entanglement" here is **informational**, not physical quantum entanglement: a compile-time shared private map $\mathcal{M}$ and synchronized derivations create a closed verification loop that others can observe but not *continue* without the map.

2) Information transfer via "holographic overlay," rotations, and Möbius looping

- **Our claim.** Instead of sweeping a full stochastic space, the system applies a **"holographic overlay"** of multiple information streams and **projects** them into a space "that can be attested to."
- **Demonstrated behavior.** Identical keystrokes (e.g., "up, right, ...") replayed later fail; the colored "pad" is a one-time pad whose rotation remaps the same password to a *different* valid trajectory each session.

- **Formalization.** The "overlay" is the **private hologram morphism** $\mathcal{M} : \Omega \times A_1 \times \cdots \times A_m \to \Omega$ acting on an **orientation ring** Ω with per-round **rotation** ρ_i. The **Möbius combiner** $\Pi_{k+1} = \rho_k \circ \mathcal{M}(\Pi_k(\omega_0), s_k)$ "loops back on itself" to generate the witness coordinates.
- **Attacker's view.** Without $\mathcal{M}$, observed witnesses look pseudorandom and are one-time; replays fail when the verifier recomputes on new mixed state.

3) Spatio-temporal entropy: turning *time* into anti-replay

- **Our claim.** Each statement is bound to *when* it was made: the attesting value is extended with a **timestamp** and reacts to a **512-bit in-circuit prime**, so "this piece of entropy can never be replayed."
- **Formalization.** A **temporal nonce** $n = \mathrm{KDF}(T \parallel q)$ is mixed with high-entropy session state x to produce e; per session, the prover emits witness indices with $(T, \mathrm{tag}(q))$, and the verifier recomputes deterministically.
- **Interpretation.** This casts "space-time" talk into a precise rule: **fresh time + in-circuit prime** $\to$ fresh state $\to$ new trajectory on Ω. It is *time-scoped attestation* rather than location-based magic.

4) Attestation as "fresh, verifiable work"

- **Our claim.** "Every transaction gets signed with a unique piece of entropy and a proof."
- **Formalization (provenance).** The paper instantiates *per-event* attestations: derive W from (T, q) inside the twins and bind an external context to produce signatures (e.g., $\sigma = \mathsf{MAC}_k(T \,\|\, q \,\|\, W \,\|\, \mathrm{ctx})$).
- **PII-free proofs.** For attributes D, produce non-transferable tokens $\tau = \mathsf{H}(\mathcal{M}(e, \mathrm{Enc}(D)) \parallel \mathrm{ctx})$ that verify without revealing D.
- **Meaning.** "Attestation" = **context-bound, one-time proof of liveness/possession** derived from entropy and time inside an entangled circuit, not a static credential.

5) State space & the "cosmic scale" claim

- **Our claim.** Using a trivial human password (even a single character repeated), the rotational space is touted as "10^{720}," i.e., vastly exceeding the "10^{100}" scale often used to dramatize infeasibility.

- **Formalization.** The paper reframes this as tunable search complexity $\mathcal{C}_{\text{guess}} \approx \max\{2^{\lambda}, C^{L}\}$ and error $\epsilon = C^{-L} + 2^{-\lambda}$, with concrete budgets (e.g., C=6, L=6, λ=512 $\Rightarrow \epsilon \approx 1.6\times10^{-5}$).
- **Meaning.** The "astronomical" rhetoric maps to **auditable parameters** (C, L, λ): raise L or C to push ϵ below target risk while keeping constant-time per-round cost.

6) Where the metaphor ends and the system begins

- We present a language showing that **consciousness** and **universal entropy** motivates an intuition for *non-extractable* knowledge sharing, but the implementation grounds it in standard cryptographic levers: **fresh entropy**, **time-mixing**, a **private morphism** sealed in compiled twins, and **deterministic recomputation** at the verifier.
- The result is not quantum signaling; it's a **keyless interactive proof** with one-time witnesses and **oscillating** mutual checks. The "entanglement" metaphor is realized as **shared $\mathcal{M}$ + synchronized derivations** that outsiders can't replay or extend.

---

1) Contribution

The central contribution is a unifying **keyless authentication** primitive in which the "secret" never exists as a static value at rest or in flight. Instead, every session derives a **holographic witness**—a short trajectory on a finite orientation ring—from fresh entropy and a **private morphism** burned into two **entangled circuits** (prover/verifier). Under axioms A1–A5, the construction delivers **completeness**, **anti-replay**, and a **soundness** bound with tunable error $\epsilon = C^{-L} + 2^{-\lambda}$. A passive zero-knowledge simulator argument captures the privacy of on-wire transcripts. In short: the system replaces reusable secrets with per-event, per-context *work* that is easy for the twins to verify and hard to fake.

Structurally, the model's building blocks are simple and auditable: **alphabets** chosen by the user, a C-ary **orientation/color ring** Ω, fresh **entropy** x, a **temporal nonce** $n = \mathrm{KDF}(T \parallel q)$, and the **private hologram morphism** $\mathcal{M}$. These generate a per-round **rotation** ρ_i and a "**Möbius**" self-composition Π whose iterates $(\omega_1, \ldots, \omega_L)$ constitute the witness W. Because T and q are fresh, identical inputs (keystrokes, symbols, gestures) traverse different valid paths across sessions, breaking replay. This reframes identity as *per-event attestation* bound to time and context rather than possession of a long-lived secret.

The assurance envelope is explicit. **A1** demands high min-entropy and unpredictable mixing; **A2** constrains $\mathcal{M}$ to the twins; **A3** ensures nonce uniqueness per session; **A4** binds honest parties deterministically while making mismatched maps look pseudorandom; **A5** caps white-box leakage to black-box I/O. On these axioms rest **L1** (completeness), **L2** (anti-replay), **L3** (soundness), and **L4** (mutual entanglement). The result is that outsiders cannot turn captured transcripts into credentials, and a MiTM cannot sustain the bidirectional "oscillation" without the private morphism.

Security-to-performance economics are favorable and tunable. The attacker's naive work is $\max\{2^{\lambda}, C^{L}\}$; per-attempt error is $\epsilon = C^{-L} + 2^{-\lambda}$; per-round cost is constant-time (one rotation, one $\mathcal{M}$ lookup, one combine), so end-to-end work is $O(L) + O(|\chi|)$. For example, with $C{=}6, L{=}6, \lambda{=}512$, $\epsilon \approx 1.6 \times 10^{-5}$, dominated by 6^{-6}, and increasing L or C tightens the bound without changing asymptotic cost. These knobs let architects budget usability vs. assurance (e.g., lower C for accessibility, higher L server-side).

From an engineering standpoint, **per-user compiled artifacts** ("burned" twins) localize blast radius and raise extraction cost, while **constant-time** lookups and uniform envelopes suppress timing/traffic side channels. Build hygiene (reproducible builds, SBOMs, signed provenance) operationalizes A5; device-level posture and **remote attestation** can gate participation for hostile environments. Telemetry stores proofs and contexts—not secrets—improving auditability without expanding PII custody.

Threat-modeling is transparent about residual risks. A5 is an assumption: sufficiently privileged white-box adversaries still motivate TEEs, diversification, anti-tamper, and side-channel controls. Those mitigations, paired with rate-limits and lockouts, keep practical risk aligned with the stated ϵ and expected adversary cost. Operationally, the scheme renders stolen transcript databases and keylogger captures largely worthless, while enabling **coercion-resistant** experiences (synonym passwords and duress policy) without on-wire distinguishers.

Finally, the paradigm is broad: human↔service logins hardened against surveillance, **AI↔AI entanglement** with ratcheted keys, **PII-free attestations** for onboarding and payments, and **secretless CI/CD** and fleet auth. Axiomatization (A1–A5) and explicit error bounds make the system policy-friendly and audit-ready. Future work: formalize active ZK (beyond passive), quantify side-channel envelopes, standardize context schemas, and publish conformance tests and proofs to cement interoperability and independent verification.

2) Glossary & Appendix

- **Entangled circuits / twins.** Compiled clones sharing a sealed $\mathcal{M}$ that can sustain a bilateral oscillation and verify each other's one-time witnesses; the "entanglement" is informational, not physical.
- **Holographic witness W.** A trajectory on the ring Ω produced by iter-

ated $\mathcal{M}$ and rotations; transmitted as witness indices.

- **Temporal nonce** n**.** $n = \mathrm{KDF}(T \parallel q)$ binds proofs to time with an in-circuit prime to defeat replay.
- **Möbius loop** Π**.** Twisted self-composition ensuring the state "loops back on itself," matching the demo narrative.
- **Attestation.** A per-event, context-bound proof (e.g., σ, τ) derived from W, not a reusable identifier or secret.
- "Second-layer hologram ... attest at any moment in space-time ... conscious mind can entangle ... look at a piece of entropy ... only you and that circuit know the answer."
- "Two symmetric twins ... oscillate ... completely entangled ... cannot be intercepted."
- One-time pad rotation demo (replay fails).
- "Holographic overlay ... projecting into a space that can be attested to ... append a timestamp ... reacts with 512-bit prime."
- "Every transaction gets signed with a unique piece of entropy and a proof."
- "10^720" scale claim tied to rotations and a trivial password.

(We formalizes each idea into alphabets $\mathcal{A}$, ring Ω, private morphism $\mathcal{M}$, temporal nonce n, witness W, and oscillating twin protocol with measurable error $\epsilon = C^{-L} + 2^{-\lambda}$.)

Witness, Orientation Ring, and Alphabets. The **holographic witness** $W = (\omega_1, \ldots, \omega_L)$ is an ordered list of ring positions $\omega_i \in \Omega$, optionally sent as indices $w_i \in \{0, \ldots, C-1\}$. The ring Ω is a finite set of C orientations (e.g., six arrows), and visible **alphabets** A_j are user-selectable symbol sets whose selections steer $\mathcal{M}$. These elements shape both usability and the combinatorial space C^L.

Entropy, Temporal Nonce, Mix, and Rotation. Each session draws high-entropy x, is chunked into 16-bit values χ, and combined with a **temporal nonce** $n = \mathrm{KDF}(T \parallel q)$ to form a mixed state e. Per round, the ring rotates by $\rho_i(\omega) = \omega \oplus (\chi_i \bmod C)$. Fresh x and n guarantee that equal inputs lead to different valid trajectories across time, underpinning anti-replay.

Hologram Morphism and Möbius Loop. The private morphism $\mathcal{M} : \Omega \times A_1 \times \cdots \times A_m \to \Omega$ is compiled into both twins and never leaves them. The "Möbius" combiner $\Pi_{k+1} = \rho_k \circ \mathcal{M}(\Pi_k(\omega_0), s_k)$ twists state through $\mathcal{M}$ given the symbol selector s_k, yielding the next witness point. This pairing encodes cognition/policy into verifiable but non-reusable artifacts.

Entangled Circuits, Attestation, and Verification. *Entangled twins* are the compiled prover/verifier pair sharing $\mathcal{M}$. A prover emits $\langle T, \mathrm{tag}(q), \{w_i\}\rangle$, and the verifier deterministically recomputes e and $W^\star$ from the same inputs,

accepting iff $W^\star = W$. Because n changes with T or q, replays fail except with negligible probability; multi-round "oscillation" builds mutual liveness.

Axioms and Lemmas (Index).
• **A1–A5:** entropy/mix unpredictability; hologram secrecy; temporal uniqueness; binding/pseudorandomness; white-box hardness.
• **L1–L4:** completeness, anti-replay, soundness bound $\Pr[\text{forge}] \le C^{-L} + 2^{-\lambda}$, and mutual entanglement.
These are the scaffolding for **Theorem 1 (Passive ZK-IP)**: transcripts reveal nothing beyond acceptance.

Complexity, Error, and Cost. The attacker's baseline search is $\mathcal{C}_{\text{guess}} \approx \max\{2^\lambda, C^L\}$. Error per attempt is $\epsilon = C^{-L} + 2^{-\lambda}$; with C=6, L=6, λ=512, $\epsilon \approx 1.6 \times 10^{-5}$. Runtime per round is constant-time (one rotation, one $\mathcal{M}$ lookup, combine); protocol work is $O(L) + O(|\chi|)$.

Operational Terms (Policy & Deployment).
• **Context** ctx: binds proofs to use-cases (e.g., login, payment).
• **Attestation tokens** σ, τ: MACs over (T, q, W, ctx) or $\mathcal{M}(e, \text{Enc}(D))$ used for transaction or attribute proofs.
• **Duress policy** π: maps synonym passwords to invisible server actions (allow, decoy, trace, revoke).
• **Burn/compile**: per-user diversified artifacts and supply-chain hardening (SBOM, signed provenance).

3) Bibliography & References

Information Theory, Entropy, and Mixing (for A1 and §1–2).
Shannon's seminal work and modern texts ground entropy and coding; standard KDF/MAC primitives (e.g., HKDF, HMAC) inform nonce derivation and attestation tokens. Suggested anchors: C. E. Shannon, "A Mathematical Theory of Communication," *BSTJ* (1948); T. Cover & J. Thomas, *Elements of Information Theory* (Wiley, 2006). For constructions: H. Krawczyk & al., "HMAC: Keyed-Hashing for Message Authentication," RFC 2104; H. Krawczyk, "HKDF," RFC 5869; NIST SP 800-108 (KDF in Key Establishment). These justify the entropy-mix and MAC-based tokens used where σ and τ are introduced. (Anchor in text at definitions of n=KDF($T \parallel q$) and transaction tokens.)

Interactive Proofs and Zero-Knowledge (for §4 Lemmas/Theorems).
Foundational IP/ZK theory underpins completeness, soundness, and transcript simulability: S. Goldwasser, S. Micali, C. Rackoff (1985); O. Goldreich, S. Micali, A. Wigderson (GMW, 1986/1991); O. Goldreich, *Foundations of Cryptography* Vol. 1–2 (2001/2004). Fiat-Shamir (1986) is relevant if non-interactive variants are later considered. These references map directly onto L1–L4 and Theorem 1 (Passive ZK-IP).

Provable Security & Practice (for MAC/KDF bindings and context).
M. Bellare & P. Rogaway (1993–2000s) on the practice of provable security and concrete reductions; Katz–Lindell, *Introduction to Modern Cryptography* (CRC)

for modern MAC/KDF analyses; Boneh–Shoup, *A Graduate Course in Applied Cryptography* (2017 draft book) for accessible modern treatments. These sources align with the paper's concrete ϵ accounting and operational binding of ctx.

White-Box, Obfuscation, and Program Protection (for A5). Foundational limits: Barak et al., "On the (Im)possibility of Obfuscating Programs" (CRYPTO 2001). Applied defenses: Chow et al., "White-Box Cryptography and an AES Implementation" (SAC 2002); Collberg et al., "A Taxonomy of Obfuscating Transformations" (2007). These motivate treating A5 as an assumption and pairing with platform defenses and build hygiene. (Cite where A5 and the build/attestation guidance appear.)

Trusted Execution & Remote Attestation (for deployment notes). Standards and vendor docs for attested execution: Intel SGX/TDX SDM, AMD SEV-SNP, ARM CCA; IETF RATS architecture (RFC 9334) for attestation flows. These ground the recommendation to bind T and device posture to a trustworthy clock/enclave and to gate participation based on measurements and reports. (Anchor where admission control and attestation are discussed.)

Time-Binding and Delay (for A3 hardening). To make A3 robust across platforms, reference secure time sources and, where appropriate, **verifiable delay functions**: D. Boneh et al., "Verifiable Delay Functions" (CRYPTO 2018). Complement with NTP/PTP hardening literature for reliable T under partial compromise. This supports the implementation tip to bind T to a trusted clock or VDF.

Usability, Accessibility, and Human Factors (for Ω, C, alphabets). Guides for color/shape coding and cognitive load—W3C WCAG (contrast, color-blind accessibility), C. Ware, *Information Visualization*—support parameterization ($C \in \{3, 4, 6\}$) and multi-alphabet UX. These references justify tuning C for accessibility while keeping L and ϵ within targets. (Anchor where accessibility and parameter selection are discussed.)