HOLogram

Human Obfuscation Layer

L’AI vede un riflesso, non l’originale

Whitepaper

Versione 1.0 (Marzo 2026) - BaffiSan

info@hologramprotocol.org

www.hologramprotocol.org

Indice

Abstract 1
1. Introduzione 1
2. Il problema 1
3. Architettura 1
4. Funzionamento 2
5. Sicurezza 2
6. Compliance 2
7. Ecosistema & HOLoToken 2
8. Hash / Notarizzazione 3
9. Conclusione 3

Abstract

I segnali comportamentali generati durante l'interazione digitale—ritmo di digitazione, traiettorie del puntatore, dinamica dello scroll—consentono l'identificazione dell'utente anche in assenza di cookie, login o fingerprinting tradizionale. HOLogram introduce uno Human Obfuscation Layer: uno strato locale che offusca, normalizza e riduce la granularità di tali segnali prima che raggiungano gli script di pagina o sistemi di AI, preservando la naturalità d'uso e riducendo la riconducibilità. Il protocollo opera interamente in locale, non conserva dati, non manipola l'intenzione dell'utente, e nasce come standard aperto sostenuto da un sistema reputazionale non finanziario (HOLoToken) basato su Proof-of-Contribution. Obiettivo: riconoscere il diritto a non essere identificati dal proprio comportamento.

1. Introduzione

La biometria comportamentale è una firma unica, stabile e difficilmente modificabile che emerge da come scriviamo, muoviamo il puntatore e scorriamo le pagine. Le soluzioni esistenti (VPN, modalità privata, difese anti-fingerprinting del dispositivo) non schermano la dinamica del gesto umano. HOLogram si interpone tra l'utente e la pagina come strato di protezione comportamentale, riducendo la fedeltà dei segnali senza alterare il contenuto o l'intenzione. È human-centric, local-only, trasparente (HUD minimale) e aperto a implementazioni e varianti.

2. Il problema

Gli eventi ad alta frequenza (tastiera, puntatore, scroll) sono raccolti silenziosamente via script e, combinati con modelli, consentono re-identificazione, correlazione cross-site e inferenze indesiderate (es. indecisione, stress). L'utente resta esposto perché la sua firma comportamentale è intrinseca e ricompare in ogni sessione. Serve uno strato intermedio che trasformi la forma del comportamento mantenendo la funzione dell'interazione.

3. Architettura

1. ShadowDOM Input Vault — isola gli eventi di input (keydown/keyup/keypress) e rilascia verso la pagina eventi normalizzati (input/change) senza micro-tempi tipografici.
2. Pointer & Scroll Normalizer — applica campionamento, quantizzazione e smoothing controllato a movimenti e scroll, mantenendo plausibilità umana ma riducendo unicità.
3. Persona Mixer (session-consistent) — assegna a ogni sessione una persona sintetica con parametri entro range plausibili e parzialmente sovrapposti, per evitare sia correlazione tra sessioni sia fingerprinting dell'offuscamento.
4. Behavioral Differential Privacy Engine — applica rumore calibrato e stabilizzazione per ridurre la sensibilità dell'output a micro-variazioni dell'input (ultima barriera matematica).
5. Behavioral Privacy Budget — misura e controlla quanta informazione comportamentale è esposta; attiva escalation (più smoothing/quantizzazione, meno frequenza) al calare del budget; si rigenera gradualmente (idle/eventi a bassa intensità) e si azzera al reset di sessione. Il costo evento considera tipo, frequenza, complessità geometrica ed entropia.

6. Exposure HUD — mostra livello di protezione, stato del budget e attività dei moduli.

Flusso: Input → Vault → Normalizer → Persona Mixer → DP Engine → Privacy Budget → Output proiettato al sito.

4. Funzionamento

- Acquisizione: intercetto degli eventi prima della pagina (nessun salvataggio).
- Normalizzazione: riduzione frequenza, quantizzazione, smoothing, omogeneizzazione dei tempi.
- Personalizzazione: persona sintetica coerente nella sessione, variabile tra sessioni.
- Protezione: DP Engine + escalation del Privacy Budget.
- Emissione: la pagina riceve segnali plausibilmente umani, non la firma comportamentale reale.
- Chiusura: reset completo; nessuno stato persiste.

5. Sicurezza

Obiettivi: ridurre riconducibilità; mantenere usabilità; impedire che l'offuscamento diventi impronta; nessuna telemetria; resistenza al rilevamento. Minacce: fingerprinter lato pagina; correlazione cross-site; sistemi anti-bot aggressivi; avversari mirati. Difese: Vault (niente micro-tempi), Normalizer (downsampling/quantizzazione/smoothing), Persona Mixer (variabilità session-consistent entro range plausibili), DP Engine (rumore/stabilizzazione), Privacy Budget (controllo esposizione), HUD (trasparenza). Limiti: non anonimizza rete; non copre fingerprinting non comportamentale; possibili profili "compatibilità" per app altamente temporizzate.

6. Compliance

HOLogram non tratta dati personali: non raccoglie, non conserva, non trasmette, non profila. È local-only, zero-retention, non manipolativo e neutrale. Il sistema reputazionale HOLoToken è non finanziario (non trasferibile, non scambiabile, nessun valore economico) e misura solo il merito tecnico dei contributori (HRL/HCS), senza relazione con l'identità dell'utente protetto. Nota non vincolante: l'architettura riflette i principi generali delle principali normative europee sui diritti digitali, senza generare trattamenti o basi giuridiche.

7. Ecosistema & HOLoToken

Protocollo aperto con reference implementation, specifica HLP, test di conformità HCT e processo RFC. Varianti e fork sono benvenuti se trasparenti e compatibili con una versione HLP, con possibilità di rientro nel trunk tramite RFC. HOLoToken (HRL/HCS) assegna badge/ruoli/permessi in base ai contributi (codice, sicurezza, test, docs, i18n…), con policy versionate, anti-gaming e auditabilità. Nessun aspetto economico.

8. Hash / Notarizzazione

Ogni versione è distribuita con SHA-256, pubblicata su GitHub (commit/tag), IPFS (CID) e, facoltativamente, timestamping distribuito. Storico versioni in HASHES.txt, tag immutabili, catena verificabile (v1.0 → hash → CID). Paternità sotto pseudonimo BaffiSan attestata da hash + pubblicazioni pubbliche + eventuale firma dei commit. Verifica aperta alla community.

9. Conclusione

HOLogram non modifica ciò che l'utente fa, ma come il comportamento viene esposto. Proietta verso il web un ologramma del gesto reale: funzionale, naturale, non riconducibile. È un protocollo deterministico, AI-free, locale, pensato per evolvere come standard aperto. Missione: **proteggere la libertà comportamentale come diritto digitale**.