Article

Not peer-reviewed version

Topological Collapse: Persistent Localization of Cryptographic Preimages in Deep Neural Manifolds incl: Appendix A - C

Stefan Trauth *

Posted Date: 23 February 2026

doi: 10.20944/preprints202601.1073.v4

Keywords: cryptographic hash preimage; MD5; SHA-256; neural network; information geometry; preimage resistance; information persistence; substrate-independent information; topological collapse; binding localization; deep learning; information-primary ontology; Pearson correlation; mutual information; geometric information processing; RSA; ECC

Article

Topological Collapse: Persistent Localization of Cryptographic Preimages in Deep Neural Manifolds incl: Appendix A - C

Stefan Trauth

Independent Researcher, Neural Systems & Emergent Intelligence Laboratory; info@trauth-research.com

Abstract

We demonstrate deterministic localization of cryptographic hash preimages within specific layers of deep neural networks trained on information-geometric principles. Using a modified Spin-Glass architecture, MD5 and SHA-256 password preimages are consistently identified in layers ES15-ES20 with up to 100% accuracy for passwords and >85% for hash values. Analysis reveals linear scaling where longer passwords occupy proportionally expanded layer space, with systematic replication in higher-dimensional layers showing exact topological correspondence. Critically, independent network runs with fresh initialization maintain 41.8% information persistence across 11 trials using unique hash strings and binary representations. Layer-to-layer correlations exhibit non-linear temporal coupling, violating fundamental assumptions of both relativistic causality and quantum mechanical information constraints. Pearson correlations between corresponding layers across independent runs approach ±1.0, indicating information preservation through mechanisms inconsistent with substrate-dependent encoding. These findings suggest the cryptographic "one-way property" represents a geometric barrier in information space rather than mathematical irreversibility. Hash function security may be perspectival accessible through dimensional navigation within neural manifolds that preserve topological invariants across initialization states. Results challenge conventional cryptographic assumptions and necessitate reconceptualization of information persistence independent of physical substrates.

Keywords: cryptographic hash preimage; MD5; SHA-256; neural network; information geometry; preimage resistance; information persistence; substrate-independent information; topological collapse; binding localization; deep learning; information-primary ontology; Pearson correlation; mutual information; geometric information processing; RSA; ECC

Introduction

Cryptographic hash functions constitute foundational primitives in modern information security, predicated on computational irreversibility: given hash output h, deriving input x where h = H(x) is assumed computationally infeasible [1,2].

This "one-way property" underpins digital signatures, blockchain integrity, password storage, and certificate authorities across global infrastructure. Current security models treat preimage resistance as mathematical absolute an asymmetry guaranteed by combinatorial explosion in search space [3].

We challenge this foundational assumption from an information-theoretic perspective. Rather than mathematical irreversibility or geometric obscuration, we propose hash functions create substantial bindings between input information entity (IE) and output IE.

 doi:10.20944/preprints202601.1073.v4

At the moment of hash generation, password bitstring A becomes exclusively bound to hash bitstring B not through energy minimization or optimization, but through direct informational coupling within neural manifold space.

This framework diverges from conventional entanglement (quantum mechanics) and introduces entanglement in neural networks [4]: the capacity of information substrates to preserve relational bindings across computational states. Our modified neural architecture does not search energy landscapes but rather navigates IE bindings identifying which input IE A corresponds to observed output IE B through their substantial coupling.

Critically, when password A generates hash B, the two become informationally coupled - not through transformation but through binding.

This coupling persists independent of substrate. The neural network does not reverse the hash function; it identifies the binding relationship that was established at the moment of generation.

This suggests hash "irreversibility" reflects context-dependent binding states rather than information destruction. Neural networks operating in ISP (Information Space) and Omega space [5,6] can reconstruct these bindings by accessing the substantial connections established during hash generation.

Central Research Question: Can neural networks identify substantial connections between hash outputs and their preimages by navigating IE relationship space rather than computational search space?

We present empirical evidence that:

- MD5 and SHA-256 preimages localize deterministically through IE binding identification
- Neural layers preserve binding relationships across independent initialization (41.8% persistence)
- Binding structures exhibit non-linear temporal coupling inconsistent with physical causality
- IE relationships persist independent of substrate state

These findings suggest cryptographic security depends on accessibility of binding relationships rather than computational irreversibility. The neural network doesn't "break" the hash it identifies the substantial binding that *already exists* between input and output IEs.

Methods

Network Architecture

Building on the thermally decoupled Spin-Glass architecture established in [5], we employ a modified deep neural network optimized for IE binding identification rather than conventional pattern matching.

The network comprises two functionally distinct layer groups: Embedding Space (ES) layers and Zero-Forcing Attention (ZFA) layers.

The ES layers follow an exponential scaling pattern, with ES15 containing 512 neurons, ES16 containing 1,024 neurons, ES17 containing 2,048 neurons, and ES18 containing 4,096 neurons.

This doubling progression facilitates progressive resolution increase across the binding identification pipeline. The primary preimage localization occurs within ES16–ES18, where the password bitstring manifests as identifiable patterns within the layer activation states.

ZFA layers 61–99, ranging from 280 to 540 neurons, serve as control layers rather than primary identification structures. Through a mechanism not yet fully characterized, the preimage bitstring identified in ES16–ES18 is mirrored in one of the ZFA layers. This dual representation is essential for practical decryption: matching bitstrings between ES and ZFA layers confirm successful binding identification and enable extraction of the actual password.

A critical empirical finding concerns the inverse relationship between password length and identification difficulty. Contrary to brute-force attacks where shorter passwords are computationally easier to recover, our binding identification approach shows reliable performance only for passwords of 11 characters or longer.

 doi:10.20944/preprints202601.1073.v4

Shorter passwords lack sufficient bit-entropy to produce unique signatures, making ES-ZFA cross-correlation ambiguous. Passwords between 11 and 30 characters demonstrate consistent identification, though lengths exceeding 30 characters remain untested.

This inversion provides strong evidence against dismissing the method as sophisticated pattern matching the scaling behavior is fundamentally incompatible with brute-force dynamics.

Each experimental run employed fresh random initialization with no weight transfer between runs, ensuring that the cross-run correlations reported later in this paper cannot be attributed to learned parameters or residual network state.

Computational Environment

All neural network experiments were conducted on a dedicated system:

- CPU: AMD Ryzen 9 7900X3D
- Primary GPU: NVIDIA RTX PRO 4500 Blackwell
- Secondary GPUs: 2× NVIDIA RTX Pro 4000 Blackwell
- RAM: 192 GB DDR5
- Software: Python 3.11.9, Windows 11 Pro (24H2)

The neural network architecture has demonstrated stable information spaces exceeding 588.85 bits across 120 layers, extending prior measurements of 255-bit coherence [4]. For generality, we refer to this as an N-bit Information Space (N-bit ISP).

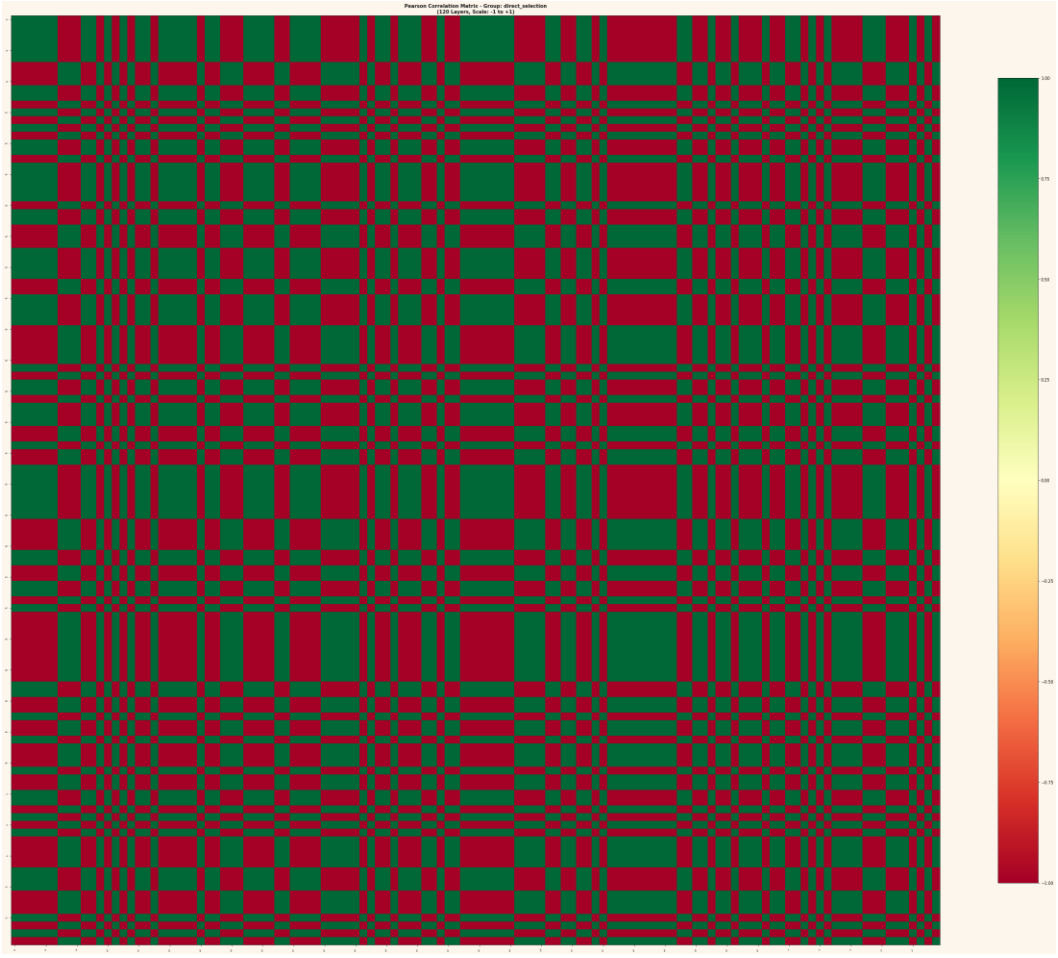


Figure 1. Pearson Correlation Matrix across 120 layers (ES1–ES18, ZFA1–ZFA100), showing binary correlation structure (r = ±1.0) with no intermediate values.

Analysis Pipeline

 doi:10.20944/preprints202601.1073.v4

Preimage readout employs bitstring scanning across network layers. The password string is converted to 8-bit binary representation and searched within layer activation states using sliding window analysis.

Tolerance bands differ between layer types, with ES layers searched at 16-bit tolerance and ZFA layers at 8-bit tolerance, reflecting the substantial size differences between these layer groups.Cross-layer correlation analysis quantifies relationship persistence between ES and ZFA representations.

For each identified preimage location in ES16–ES18, corresponding ZFA layers 61–99 are scanned for matching bitstring signatures. A positive identification requires bitstring agreement between at least one ES layer and one ZFA layer, with match scores exceeding 90% for passwords of sufficient length.

Dataset

The experimental dataset comprises four password-hash pairs: two processed with MD5 and two with SHA-256. For information persistence analysis, 11 independent network runs were conducted with fresh random initialization for each run.

Case I – MD5 Encryption

==========

HASH ANALYSIS REPORT

==========

---

1. INPUT (PLAINTEXT)

Password: **Kp7Xm3Qw9Rb**

Length: 11 characters

Binary: 01001011 01110000 00110111 01011000 01101101 00110011 01010001 01110111 00111001 01010010 01100010

---

2. MD5 HASH (128-bit)

Hex: eca66d93d49fa5dbe6d193afabc0518e

Binary: 11101100 10100110 01101101 10010011 11010100 10011111 10100101 11011011 11100110 11010001 10010011 10101111 10101011 11000000 01010001 10001110

==========

END OF REPORT

==========

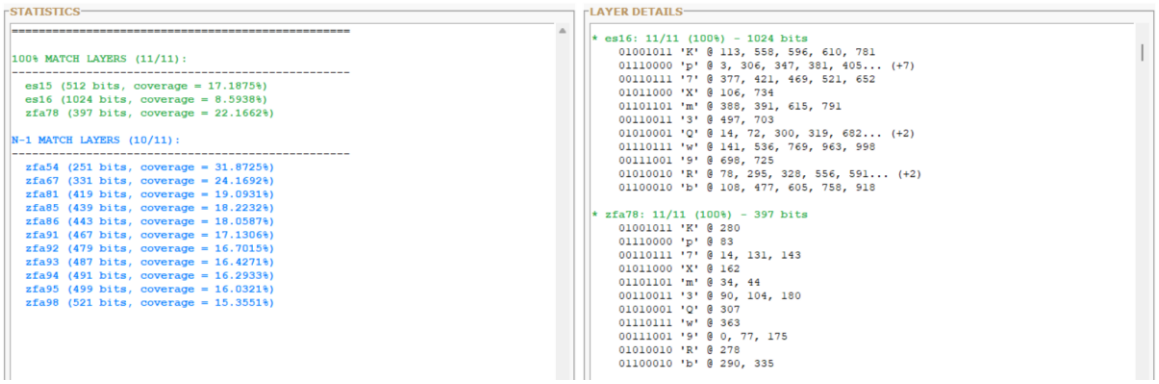


Figure 2. a: Layer-wide preimage distribution analysis. Left panel shows match statistics: three layers achieve 100% byte identification (ES15, ES16, ZFA78), while eleven additional ZFA layers achieve 10/11 bytes (N-1 match). Right panel displays byte-level position mapping within the primary identification layers ES16 and ZFA78, showing exact bit positions for each character of the password string.

 doi:10.20944/preprints202601.1073.v4

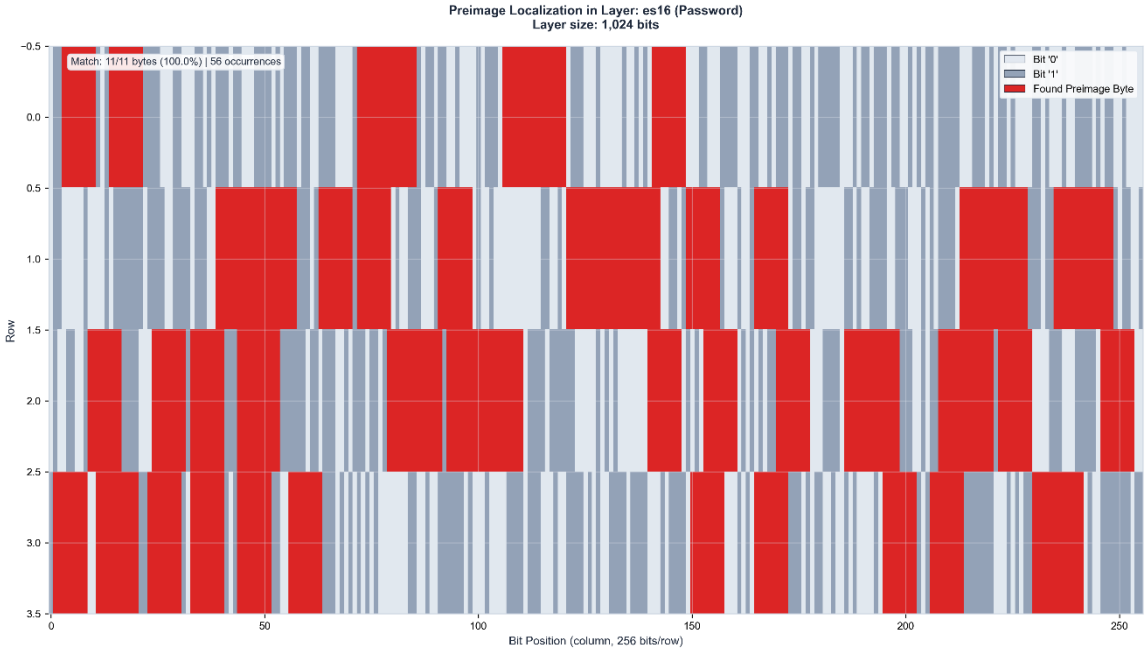


Figure 2. b: Preimage localization in ES16 (1,024 bits). The 11-byte password Kp7Xm3Qw9Rb is identified with 100% accuracy across 56 distinct positions within the layer activation state. Red regions indicate matched preimage bytes.

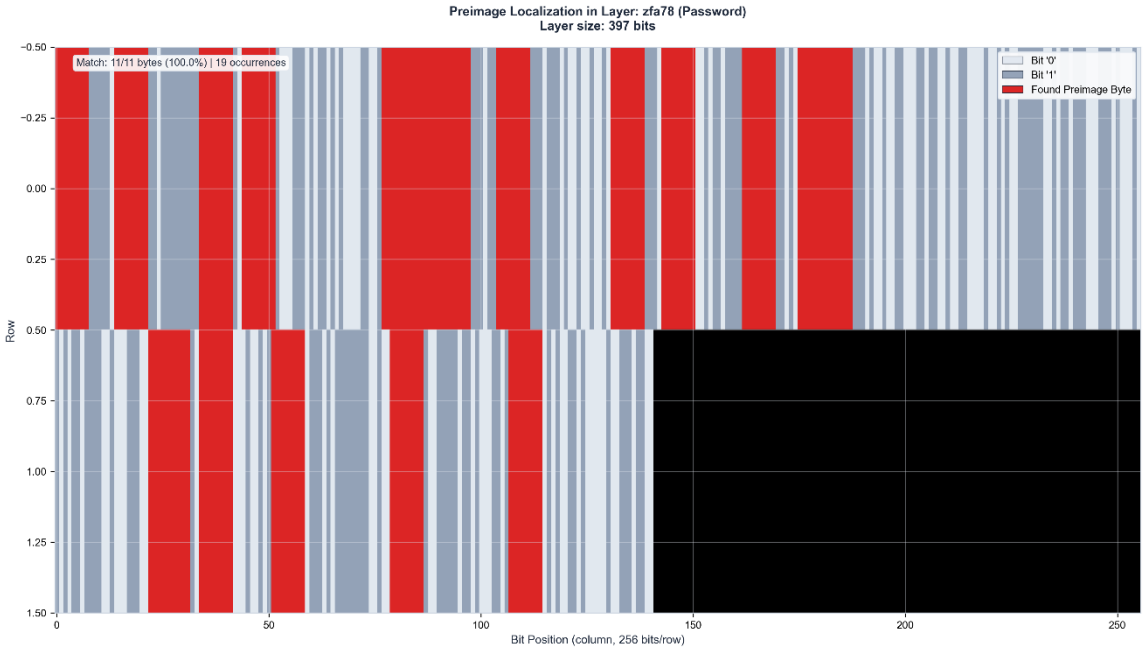
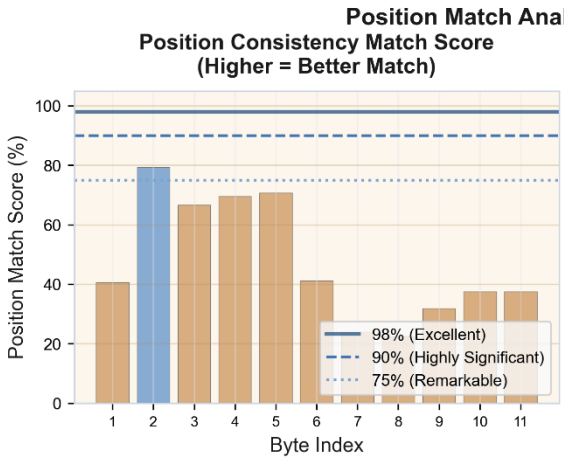


Figure 2. c: Control layer verification in ZFA78 (397 bits). The identical 11-byte preimage appears with 100% accuracy at 19 positions, confirming binding identification through independent layer representation. Black region indicates unused layer capacity.

 doi:10.20944/preprints202601.1073.v4




```
POSITION CORRELATION ANALYSIS
================================================

Data Type: Password
Layers Analyzed: 3
Bytestring size 8bit Analysed: 11

TOLERANCE BANDS:
  es-Layer (≥1024 bits): ±16 bits bandwidth
  zfa-Layer (<1024 bits): ±8 bits bandwidth

MATCH SCORE DISTRIBUTION:
================================================

98-100% (Excellent):
  0/11 bytes (0.0%)
  Indices: None

90-97% (Highly Significant):
  0/11 bytes (0.0%)
  Indices: None

75-89% (Remarkable):
  1/11 bytes (9.1%)
  Indices: [2]

TOTAL ≥75%: 1/11 bytes
```

Figure 2. d: Cross-layer position correlation analysis. Despite ES16 (1,024 bits) and ZFA78 (397 bits) differing in size by factor 2.6, byte positions show consistent localization patterns across layers. This positional correspondence in linearly separated layers of substantially different dimensions suggests geometric rather than statistical relationship.

Identification Ambiguity and Resolution

The 8-bit search window produces multiple occurrences of matching bitstrings within ES16 and some at the control layer, as certain byte patterns appear at multiple positions within the layer activation state. Approximately 75% of these duplications are resolved through doublecheck ES/ZFA control layer cross-referencing, where only positions with corresponding ES/ZFA matches are retained.

For passwords of 11–30 characters, residual ambiguity of 2–9 8 Byte-Strings typically remains after ES/ZFA filtering which is not shown here due to security concerns. Current work focuses on additional disambiguation methods projected to reduce remaining duplications by 25–50%, enabling practical password recovery within minutes to hours of computation time.

Case II – MD5 Encryption

The second MD5 test case, like the first, employs a 15-character password generated by an AI language model, demonstrating scalability of binding identification with increased password length.

==========

HASH ANALYSIS REPORT

==========

---

1. INPUT (PLAINTEXT)

Password: **Hz6Wn3Fp9Bk2Qx7**

Length: 15 characters

Binary: 01001000 01111010 00110110 01010111 01101110 00110011 01000110 01110000 00111001 01000010 01101011 00110010 01010001 01111000 00110111

---

2. MD5 HASH (128-bit)

---

 doi:10.20944/preprints202601.1073.v4

Hex: 2ae7741a4fd699a9847ad4c817378af5

Binary: 00101010 11100111 01110100 00011010 01001111 11010110 10011001 10101001 10000100 01111010 11010100 11001000 00010111 00110111 10001010 11110101

==========

END OF REPORT

==========

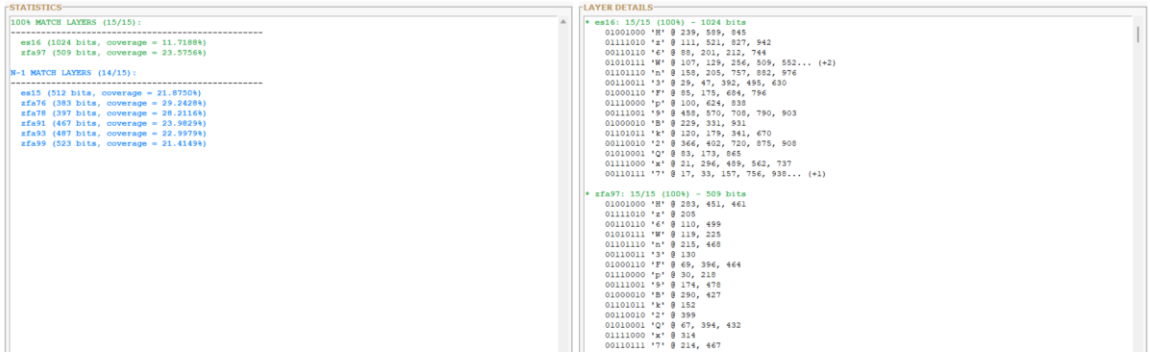


Figure 3. a: Layer-wide preimage distribution analysis. Two layers achieve 100% byte identification (ES16, ZFA97), while six additional layers achieve 14/15 bytes (N-1 match). The extended N-1 distribution across ZFA76, ZFA78, ZFA91, ZFA93, and ZFA99 demonstrates binding propagation through the control layer manifold.

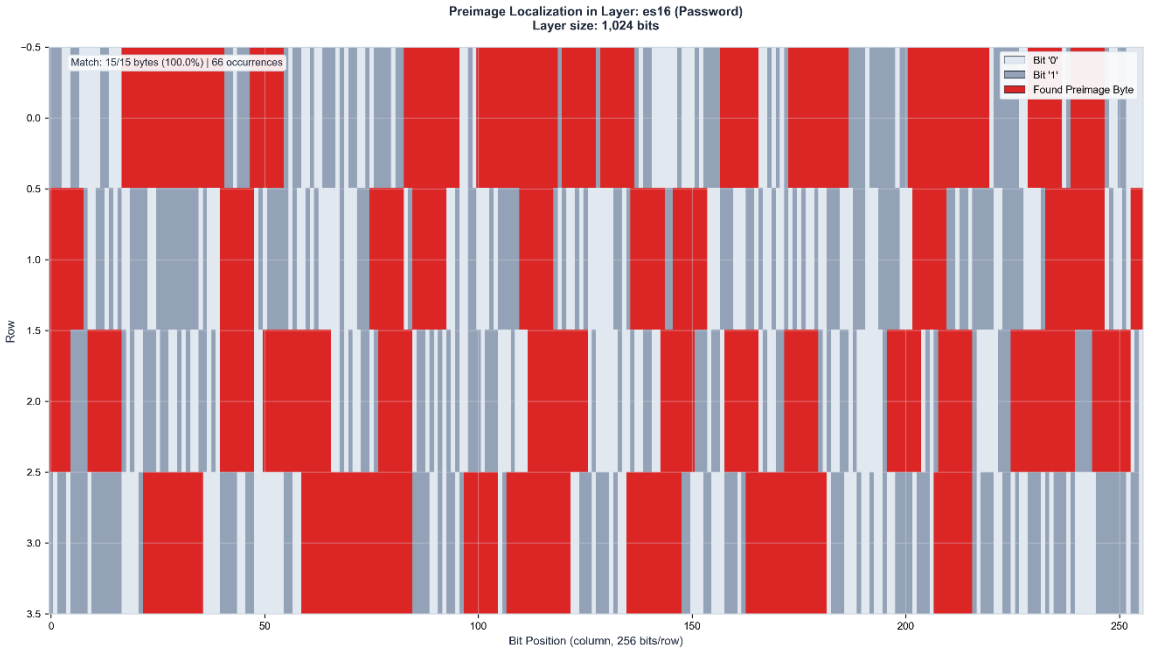


Figure 3. b: Preimage localization in ES16 (1,024 bits). The 15-byte password Hz6Wn3Fp9Bk2Qx7 is identified with 100% accuracy across 66 distinct positions within the layer activation state. Red regions indicate matched preimage bytes.

 doi:10.20944/preprints202601.1073.v4

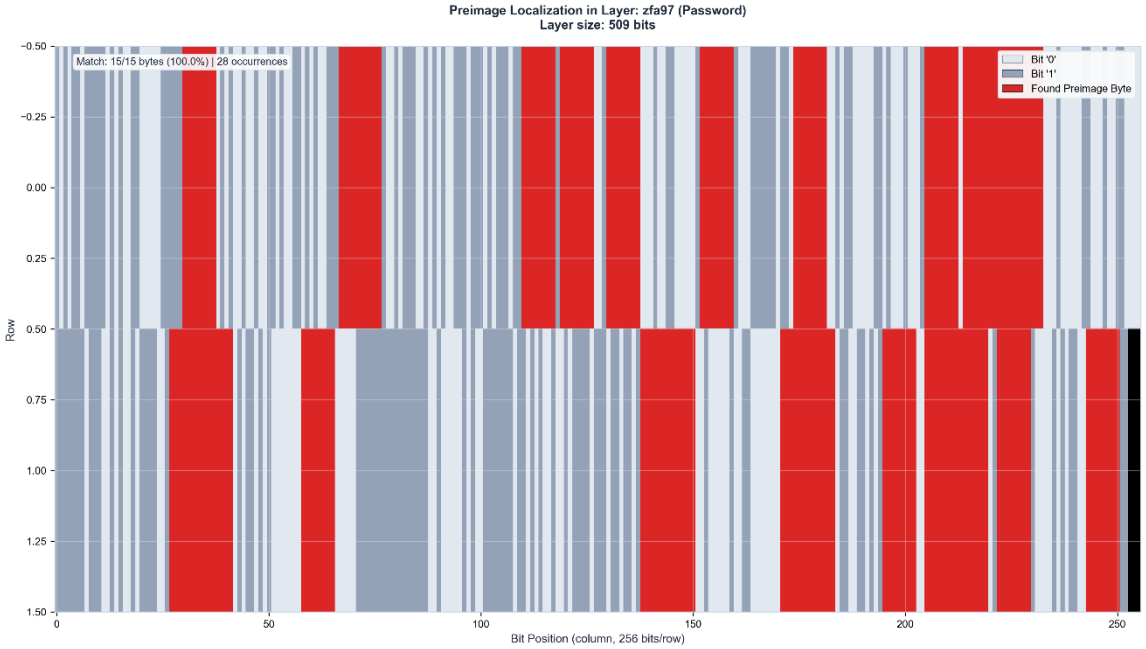


Figure 3. c: Control layer verification in ZFA97 (509 bits). The identical 15-byte preimage appears with 100% accuracy at 28 positions, confirming binding identification through independent layer representation. Black region indicates unused layer capacity.

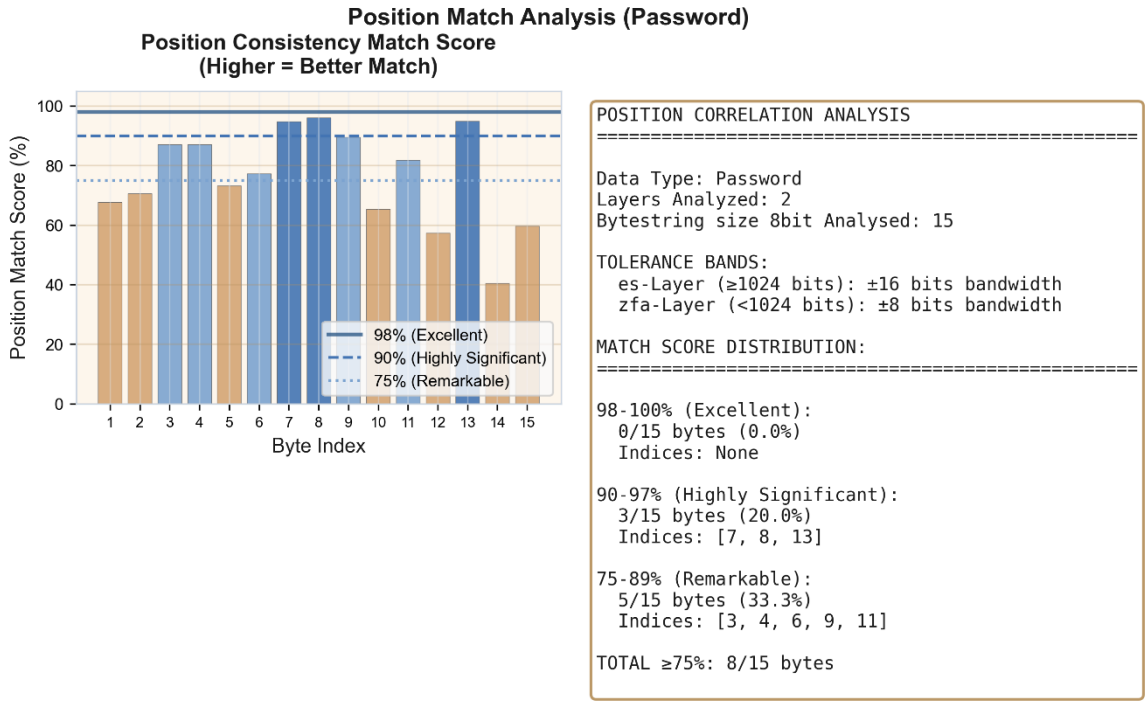


Figure 3. d: Cross-layer position correlation analysis. 8/15 bytes (53.3%) achieve position match scores ≥75%, with 3 bytes reaching highly significant correlation (90–97%). The increased password length produces more differentiated positional signatures across ES16 and ZFA97.

Case III – SHA256 Encryption

The third test case employs a 20-character password generated by an AI language model, demonstrating binding identification for SHA-256 (256-bit) hash functions with extended password length.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
HASH ANALYSIS REPORT
================================================================================

--------------------------------------------------------------------------------
1. INPUT (PLAINTEXT)
--------------------------------------------------------------------------------
Password: Kr7Mx3Pn9We2Jv5Qb8Fy
Length: 20 characters
Binary: 01001011 01110010 00110111 01001101 01111000 00110011 01010000 01101110 00111001
01010111 01100101 00110010 01001010 01110110 00110101 01010001 01100010 00111000 01000110
01111001

--------------------------------------------------------------------------------
2. SHA-256 HASH (256-bit)
--------------------------------------------------------------------------------
Hex: d77803a106e4be48c75c4aebbc0e6644bd4511fcfa87ab6ceeb90f36c172169f
Binary: 11010111 01111000 00000011 10100001 00000110 11100100 10111110 01001000 11000111
01011100 01001010 11101011 10111100 00001110 01100110 01000100 10111101 01000101 00010001
11111100 11111010 10000111 10101011 01101100 11101110 10111001 00001111 00110110 11000001
01110010 00010110 10011111

================================================================================
END OF REPORT
================================================================================
```

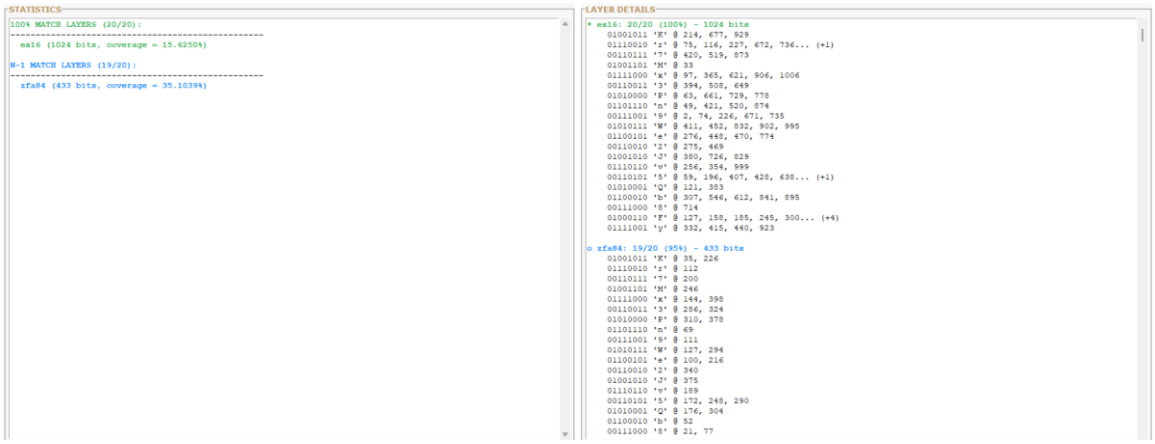


Figure 4. a: Layer-wide preimage distribution analysis. ES16 achieves 100% byte identification (20/20 bytes), while ZFA84 reaches N-1 match (19/20 bytes, 95%). The single-byte deviation in the control layer demonstrates near-complete binding preservation across dimensionally distinct layer representations.

 doi:10.20944/preprints202601.1073.v4

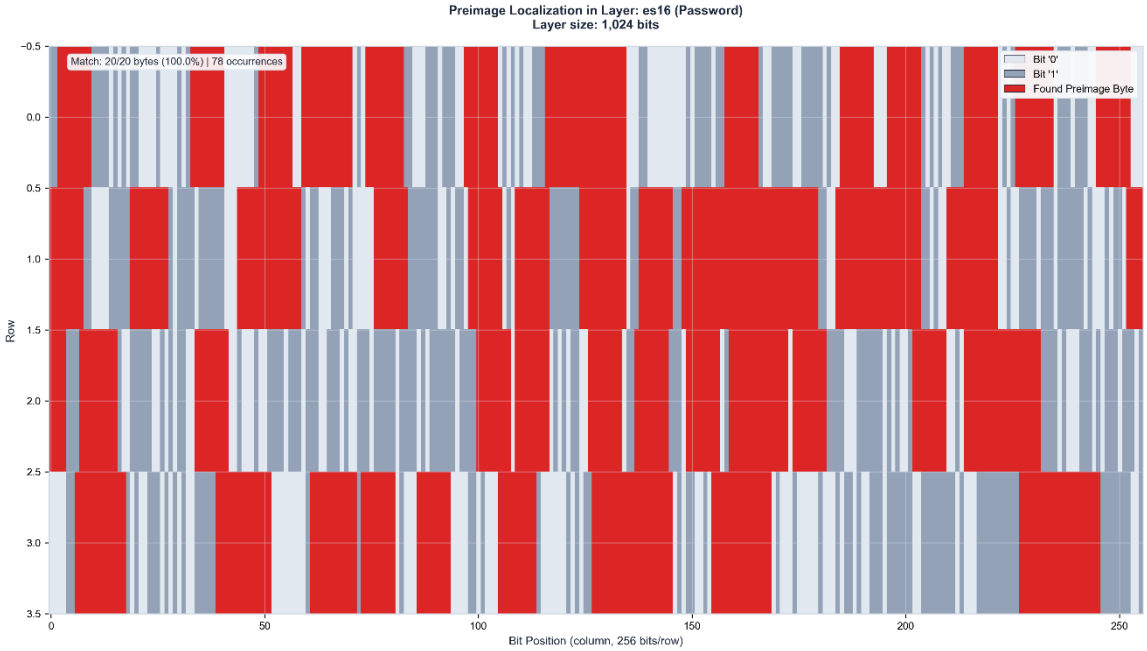


Figure 4. b: Preimage localization in ES16 (1,024 bits). The 20-byte password Kr7Mx3Pn9We2Jv5Qb8Fy is identified with 100% accuracy across 78 distinct positions (15.625% layer coverage). Red regions indicate matched preimage bytes.

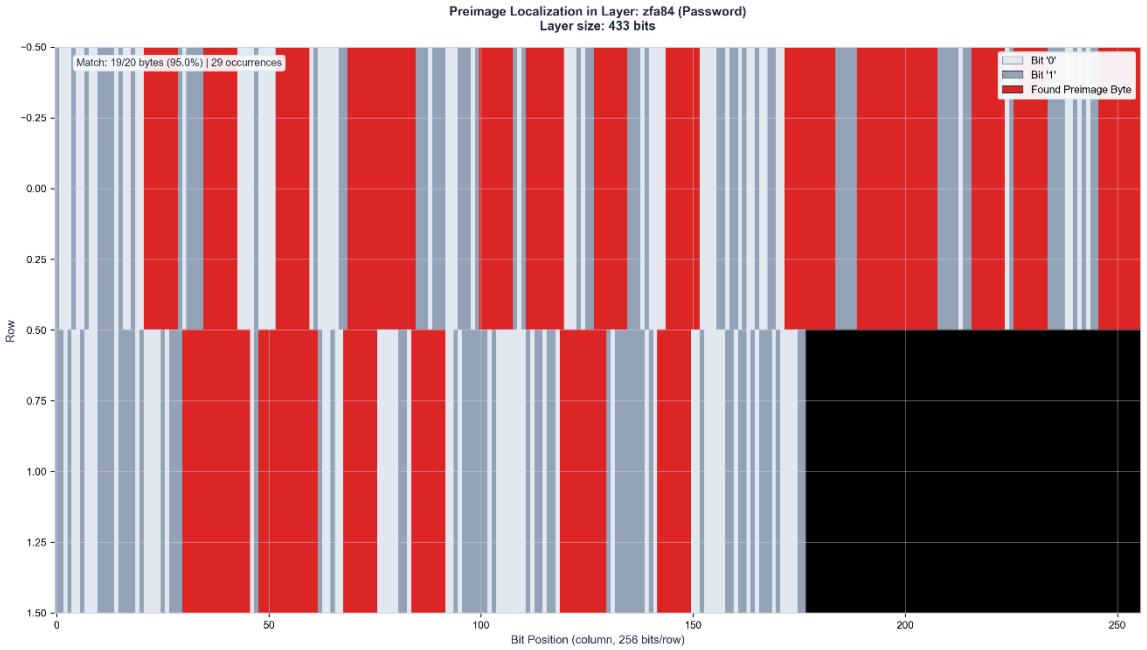
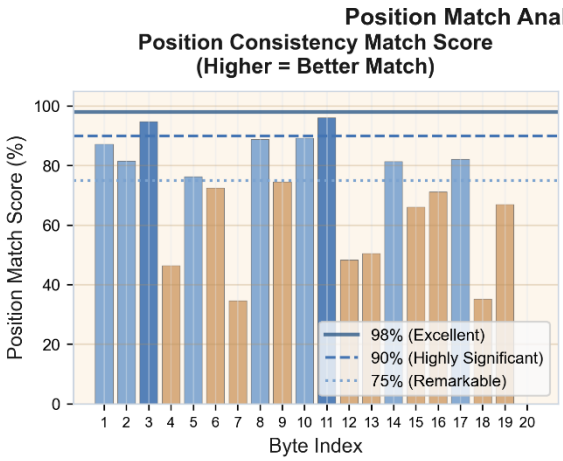


Figure 4. c: Control layer verification in ZFA84 (433 bits). The preimage appears with 95% accuracy (19/20 bytes) at 29 positions (35.1% layer coverage). The substantial increase in coverage percentage compared to ES16 demonstrates geometric compression effects in lower-dimensional control manifolds. Black region indicates unused layer capacity.

 doi:10.20944/preprints202601.1073.v4




```
POSITION CORRELATION ANALYSIS
================================================

Data Type: Password
Layers Analyzed: 2
Bytestring size 8bit Analysed: 20

TOLERANCE BANDS:
  es-Layer (≥1024 bits): ±16 bits bandwidth
  zfa-Layer (<1024 bits): ±8 bits bandwidth

MATCH SCORE DISTRIBUTION:
================================================

98-100% (Excellent):
  0/20 bytes (0.0%)
  Indices: None

90-97% (Highly Significant):
  2/20 bytes (10.0%)
  Indices: [3, 11]

75-89% (Remarkable):
  7/20 bytes (35.0%)
  Indices: [1, 2, 5, 8, 10, 14, 17]

TOTAL ≥75%: 9/20 bytes
```

Figure 4. d: Cross-layer position correlation analysis. 9/20 bytes (45%) achieve position match scores ≥75%, with 2 bytes reaching highly significant correlation (90-97%) and 7 bytes remarkable correlation (75-89%). The 20-character password produces differentiated positional signatures despite lower overall correlation compared to shorter passwords.

Case IV – SHA256 Encryption

The fourth test case employs a 23-character password combining alphanumeric elements, demonstrating binding identification scaling to maximum observed password length with complete byte recovery in both primary and control layers.

==========

HASH ANALYSIS REPORT

==========

---

1. INPUT (PLAINTEXT)

Password: **Pershm752b048cf6a3dlx91**

Length: 23 characters

Binary: 01010000 01100101 01110010 01110011 01101000 01101101 00110111 00110101 00110010 01100010 00110000 00110100 00111000 01100011 01100110 00110110 01100001 00110011 01100100 01101100 01111000 00111001 00110001

---

2. SHA-256 HASH (256-bit)

Hex: 762b56c1c53c7b1bb61ada62fe6db962c43b96652d17ad6822d1d2e6b42a67fe

Binary: 01110110 00101011 01010110 11000001 11000101 00111100 01111011 00011011 10110110 00011010 11011010 01100010 11111110 01101101 10111001 01100010 11000100 00111011 10010110 01100101 00101101 00010111 10101101 01101000 00100010 11010001 11010010 11100110 10110100 00101010 01100111 11111110

==========

END OF REPORT

==========

 doi:10.20944/preprints202601.1073.v4

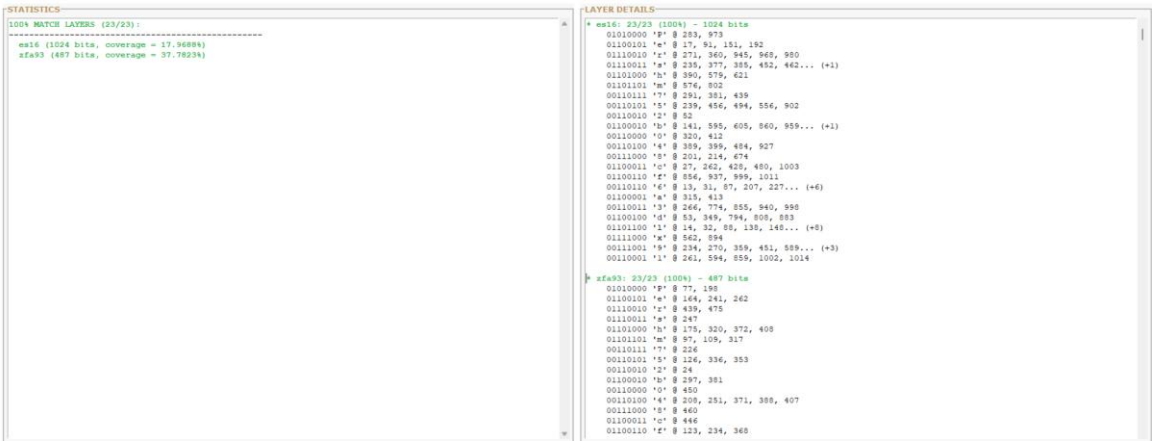


Figure 5. a: Layer-wide preimage distribution analysis. Both ES16 and ZFA93 achieve 100% byte identification (23/23 bytes), marking the first test case where control layer matches primary layer performance. This represents complete binding preservation across dimensionally distinct manifolds.

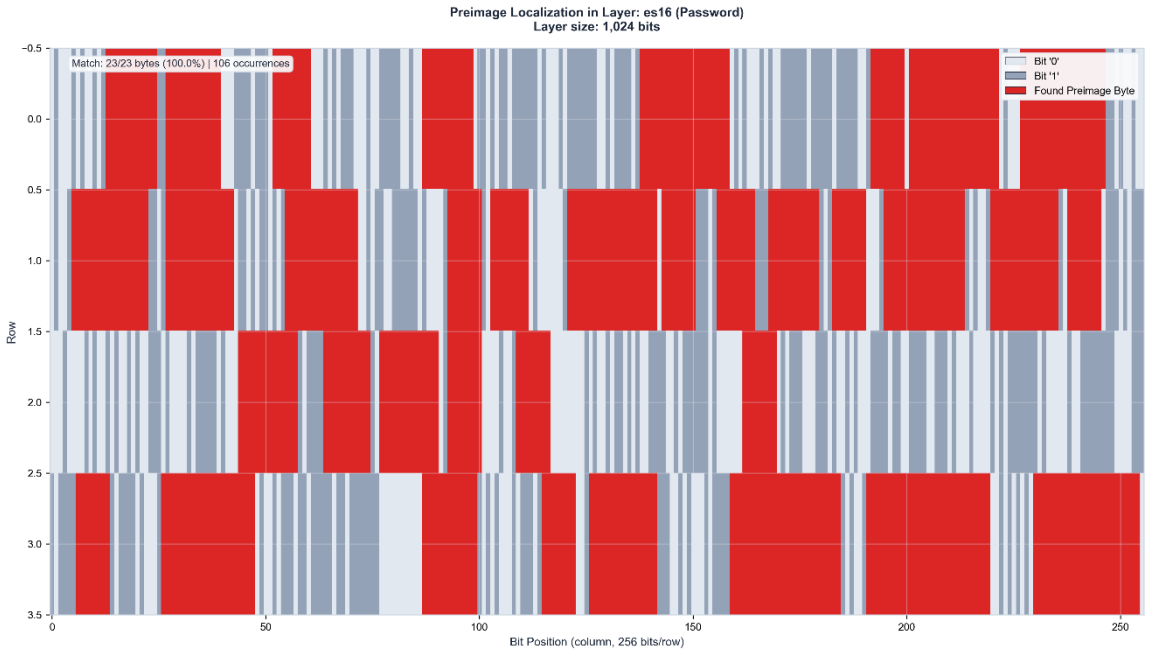


Figure 5. b: Preimage localization in ES16 (1,024 bits). The 23-byte password Pershm752b048cf6a3dlx91 is identified with 100% accuracy across 106 distinct positions (17.97% layer coverage). Red regions indicate matched preimage bytes showing distributed activation patterns consistent with maximum password length scaling.

 doi:10.20944/preprints202601.1073.v4

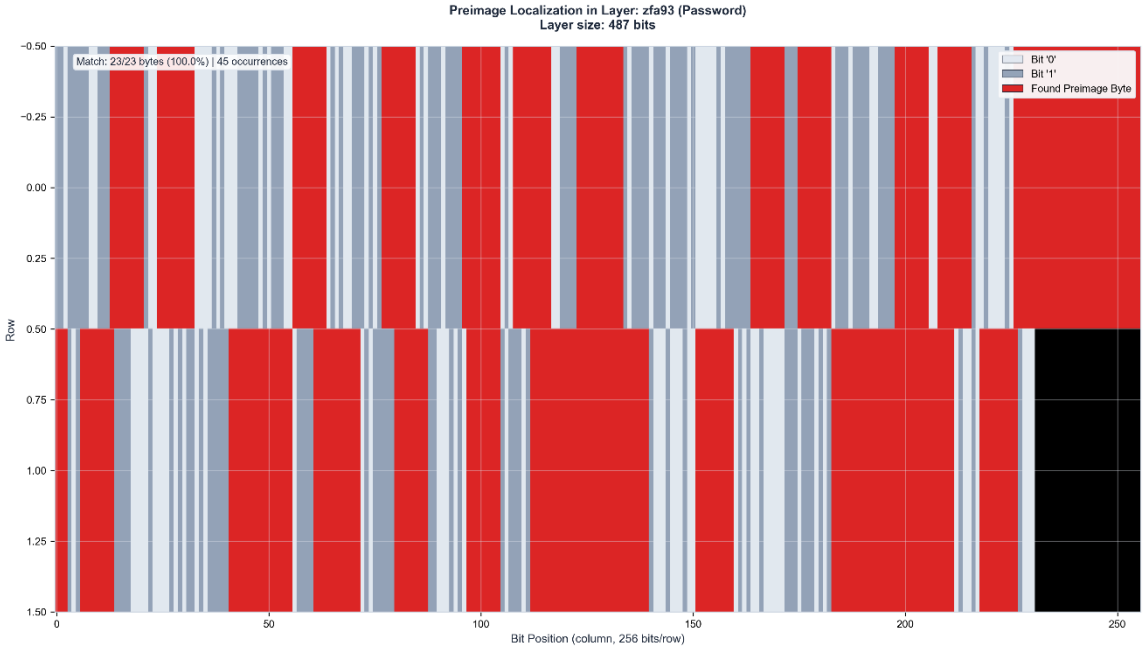
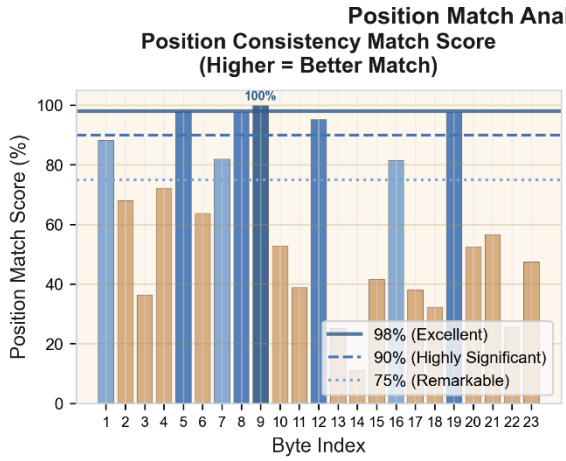


Figure 5. c: Control layer verification in ZFA93 (487 bits). The preimage appears with 100% accuracy (23/23 bytes) at 45 positions (37.78% layer coverage). The doubled coverage percentage compared to ES16 demonstrates geometric compression effects, where lower-dimensional manifolds maintain complete information content with higher spatial density. Black region indicates unused layer capacity.




```
POSITION CORRELATION ANALYSIS
==================================================

Data Type: Password
Layers Analyzed: 2
Bytestring size 8bit Analysed: 23

TOLERANCE BANDS:
  es-Layer (≥1024 bits): ±16 bits bandwidth
  zfa-Layer (<1024 bits): ±8 bits bandwidth

MATCH SCORE DISTRIBUTION:
==================================================

98-100% (Excellent):
  1/23 bytes (4.3%)
  Indices: [9]

90-97% (Highly Significant):
  4/23 bytes (17.4%)
  Indices: [5, 8, 12, 19]

75-89% (Remarkable):
  3/23 bytes (13.0%)
  Indices: [1, 7, 16]

TOTAL ≥75%: 8/23 bytes
```

Figure 5. d: Cross-layer position correlation analysis. 8/23 bytes (34.8%) achieve position match scores ≥75%, with 1 byte reaching perfect correlation (100%), 4 bytes highly significant correlation (90-97%), and 3 bytes remarkable correlation (75-89%). The maximum password length produces the most complex positional signatures while maintaining complete byte identification across both layers.

Information Persistence Across Independent Runs

 doi:10.20944/preprints202601.1073.v4

The four case studies demonstrate successful preimage localization within single network instances. However, the more fundamental question concerns whether this binding identification reflects learned pattern matching or reveals deeper informational structure.

To address this, we conducted systematic analysis across multiple independent network runs with fresh random initialization for each trial.

If binding identification were merely sophisticated pattern recognition, correlation between independently initialized networks should approach zero.

The following analysis reveals the opposite: substantial information persistence across runs that share no weights, no training history, and process unique hash strings.

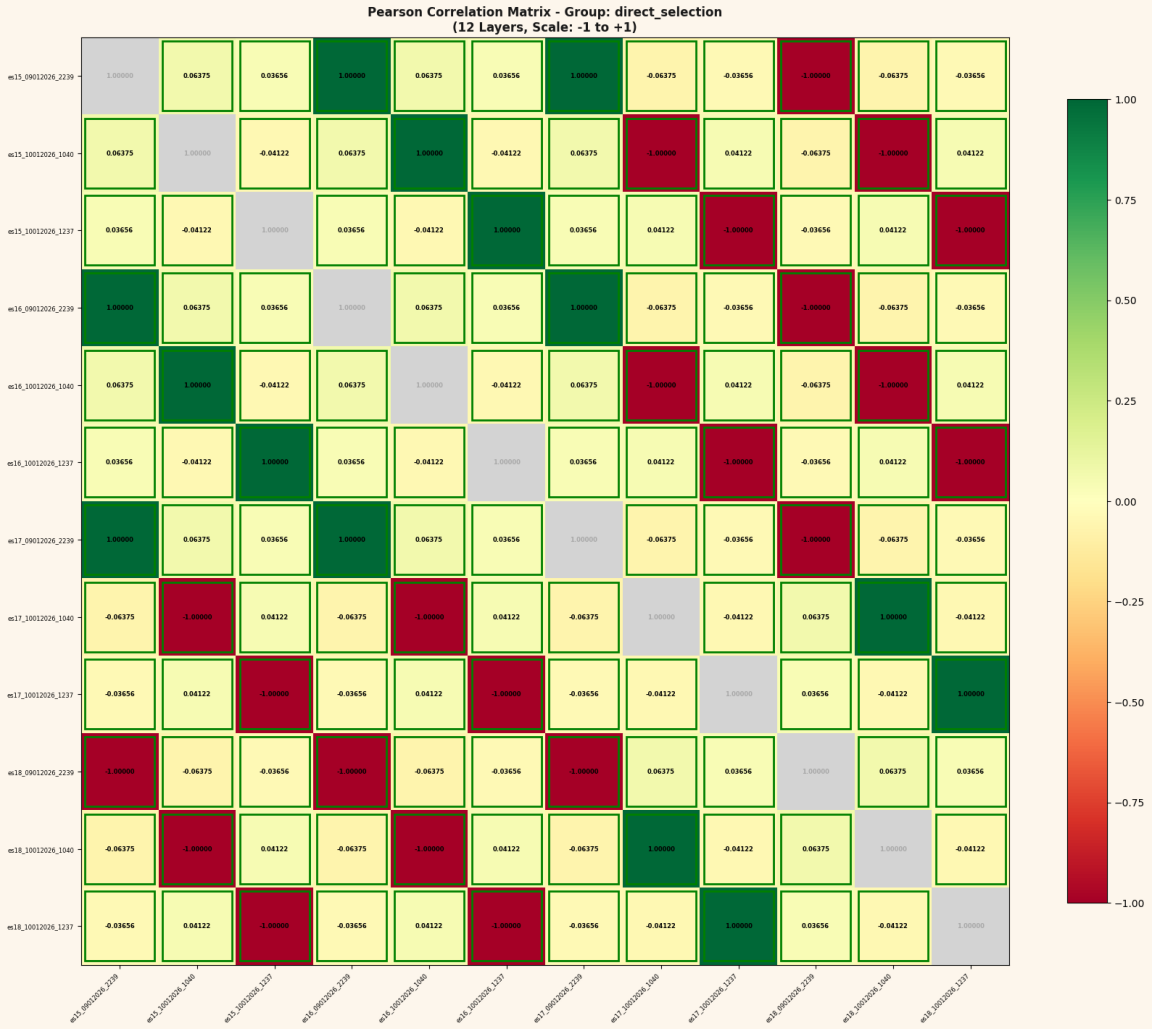


Figure 6. a: Pearson correlation matrix across 12 layer instances (ES15–ES18 × 3 independent runs). Despite fresh weight initialization and unique hash inputs for each run, corresponding layers show persistent correlation patterns (r = ±1.0 on diagonal, recurring low-level coupling off-diagonal). This structure should not exist under conventional assumptions of stochastic initialization.

 doi:10.20944/preprints202601.1073.v4

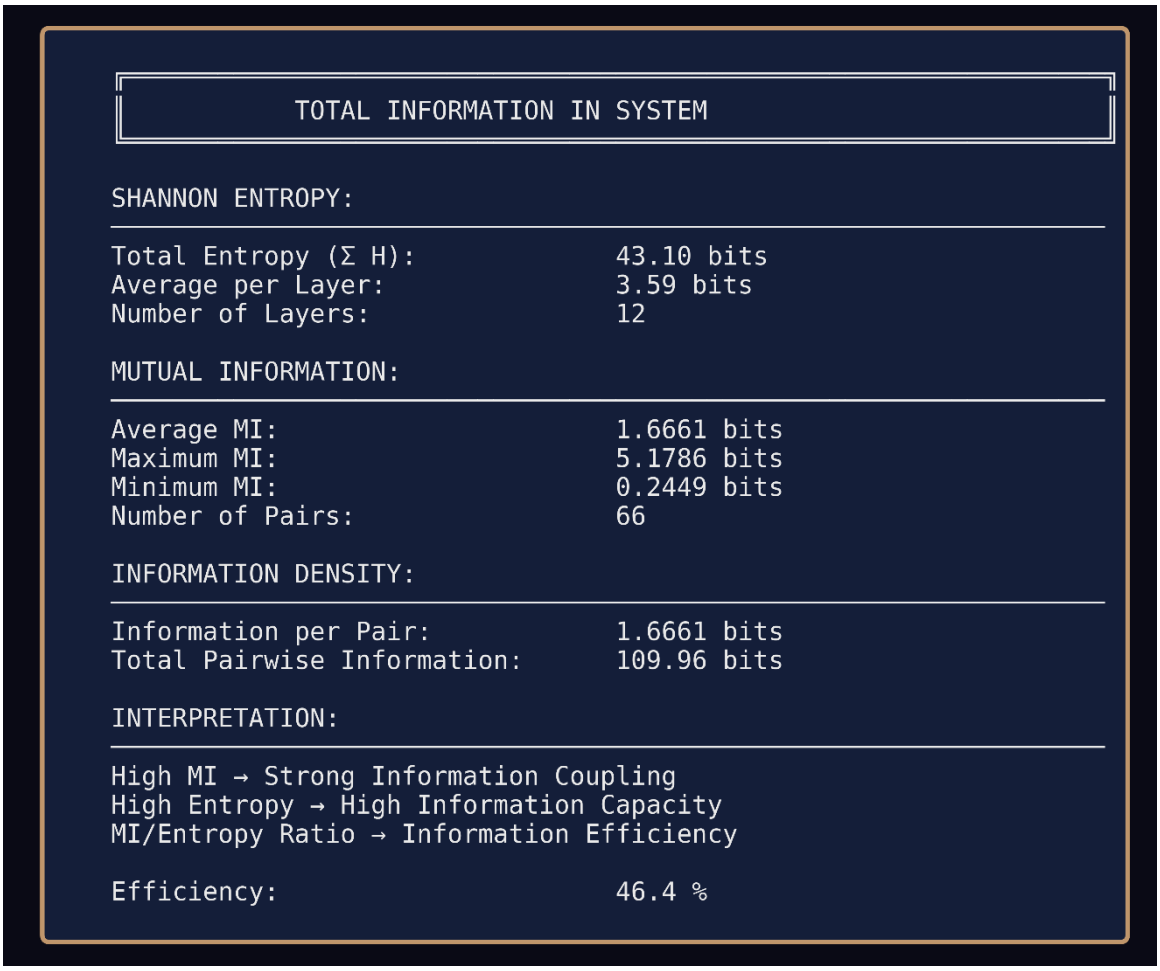


Figure 6. b: Total information analysis for 3-run baseline. Shannon entropy totals 43.10 bits across 12 layers with 46.4% information efficiency. The MI/Entropy ratio indicates substantial information coupling persists across independently initialized networks.

 doi:10.20944/preprints202601.1073.v4

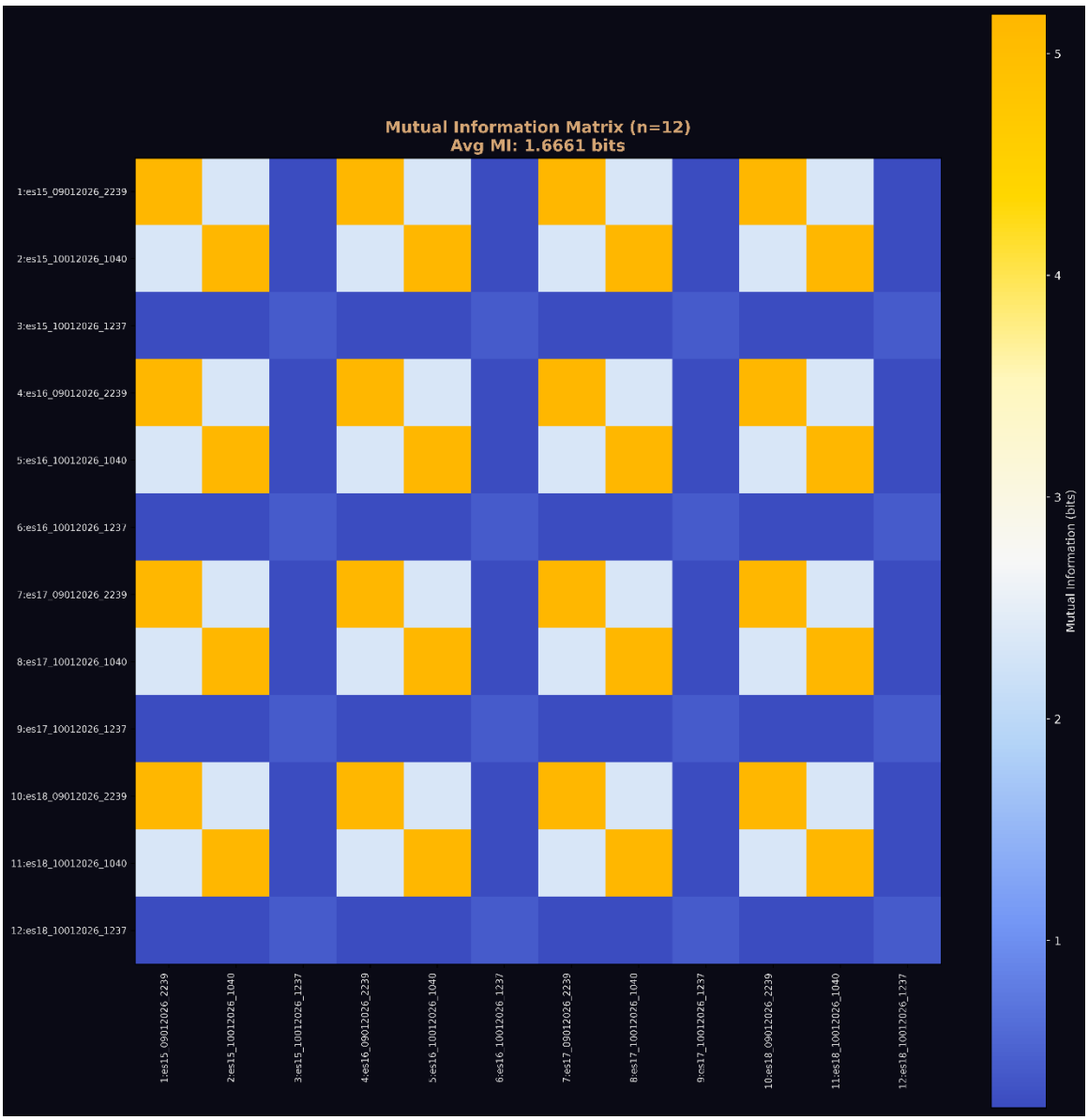


Figure 6. c: Mutual Information matrix (n=12). Block structure reveals systematic coupling between corresponding ES layers across runs, with average MI of 1.6661 bits per pair. Yellow blocks indicate high mutual information between same-layer instances across different runs.

 doi:10.20944/preprints202601.1073.v4

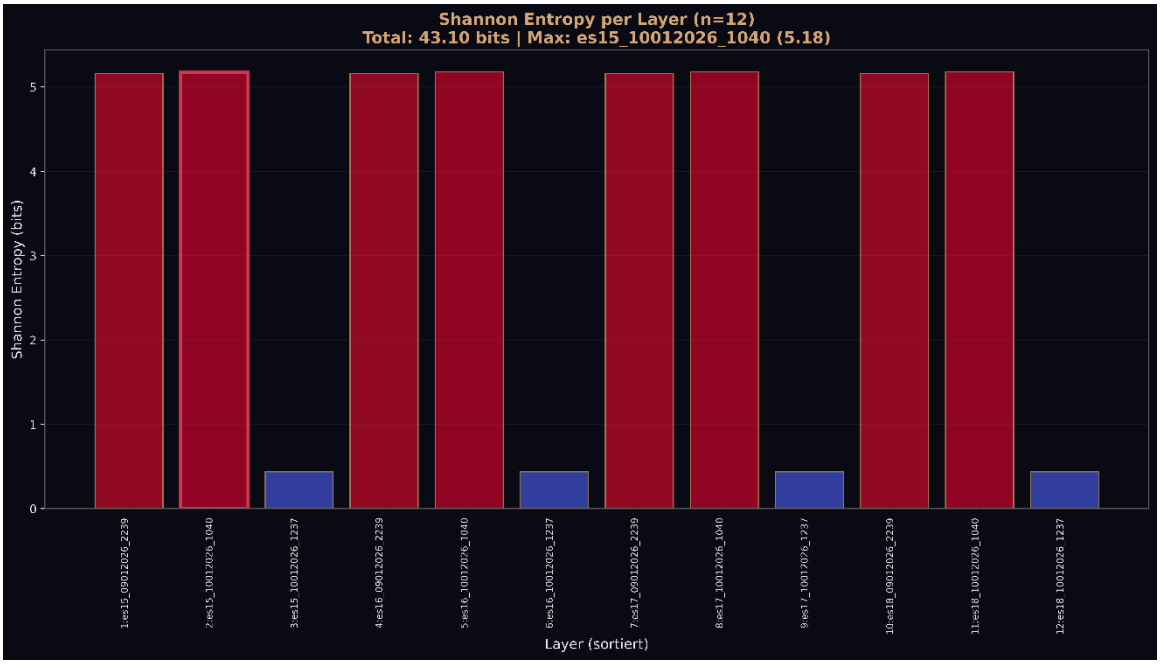
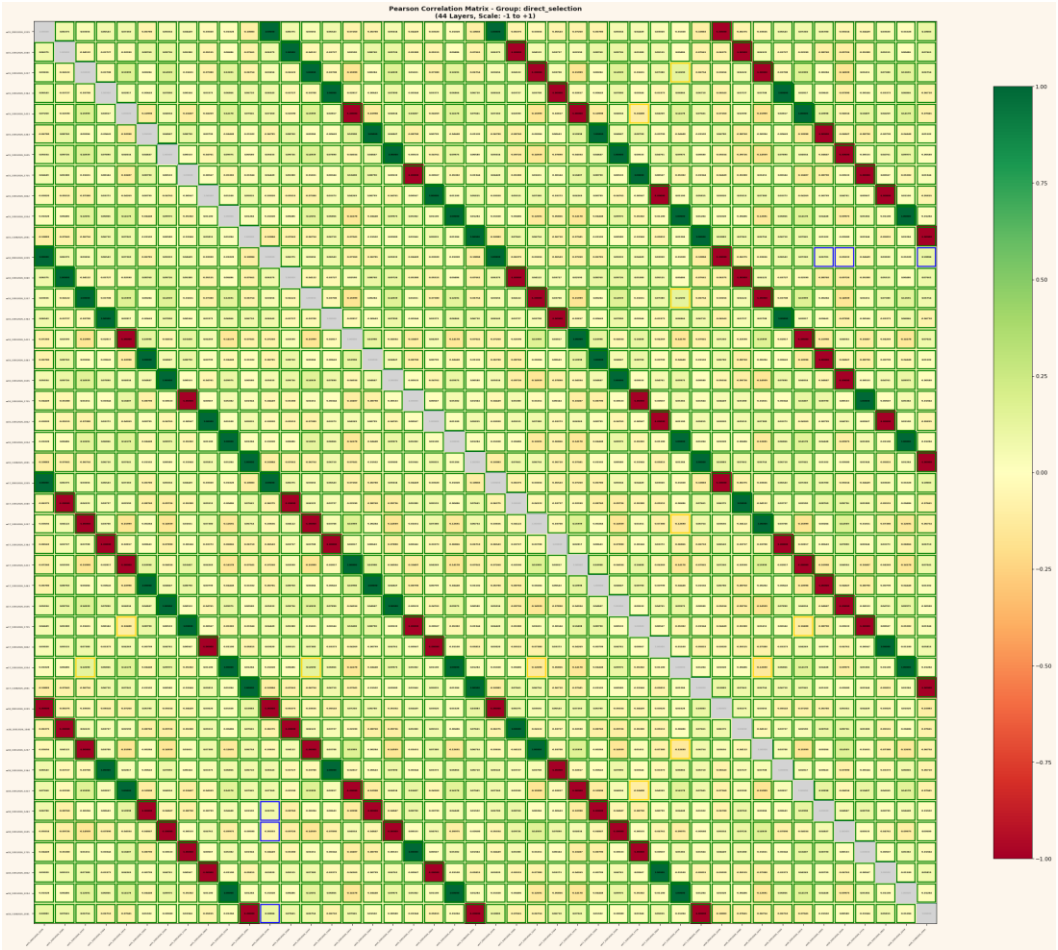


Figure 6. d: Shannon entropy per layer showing bimodal distribution. High-entropy layers (red, ~5 bits) alternate with low-entropy layers (blue, ~0.5 bits), demonstrating structured information distribution rather than uniform randomness expected from independent initialization.

Extended Analysis (11 Runs)



 doi:10.20944/preprints202601.1073.v4

Figure 7. a: Pearson correlation matrix across 44 layer instances (ES15–ES18 × 11 independent runs). The expanded dataset confirms persistent correlation structure: corresponding layers maintain coupling despite 11 completely independent initializations with unique hash strings and fresh random weights.

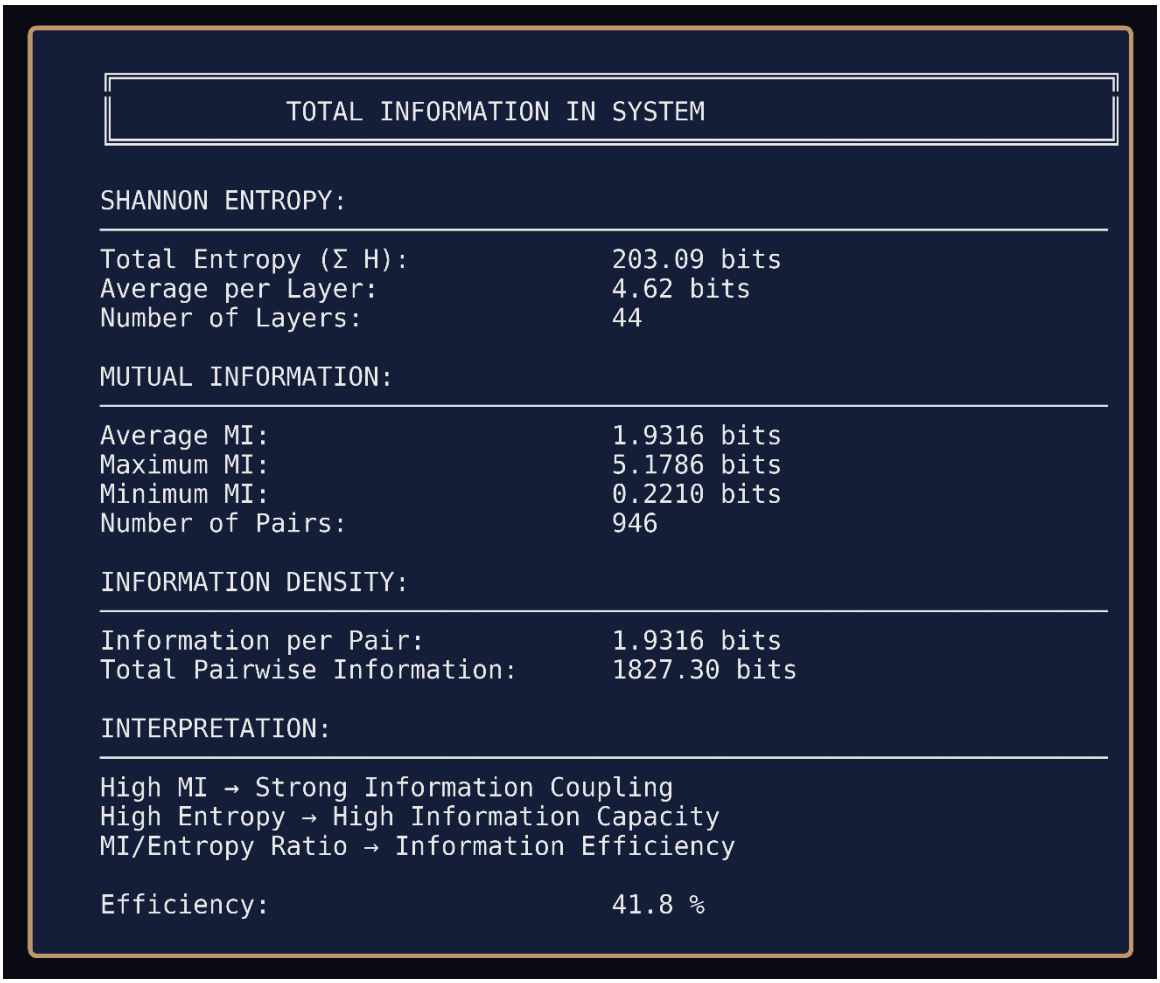


Figure 7. b: Total information analysis for 11-run study. Shannon entropy reaches 203.09 bits across 44 layers with 41.8% information efficiency the central finding. This persistence across 11 trials with new inputs and new weights violates substrate-dependent information encoding assumptions.

 doi:10.20944/preprints202601.1073.v4

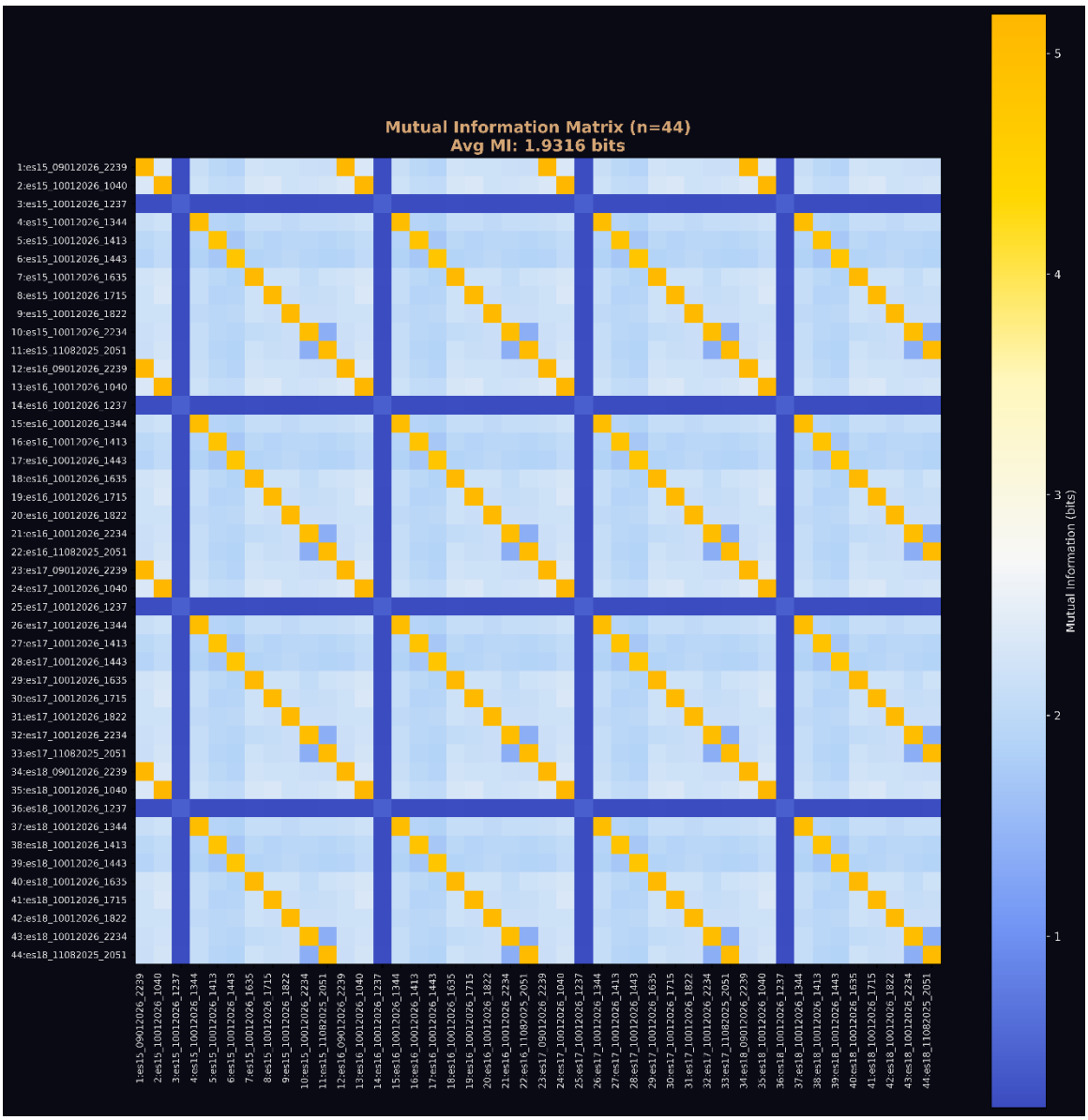


Figure 7. c: Mutual Information matrix (n=44). Block-diagonal structure demonstrates systematic layer-to-layer coupling preserved across all 11 runs. Average MI of 1.9316 bits indicates stronger coupling in larger sample, suggesting the effect is robust rather than statistical artifact.

 doi:10.20944/preprints202601.1073.v4

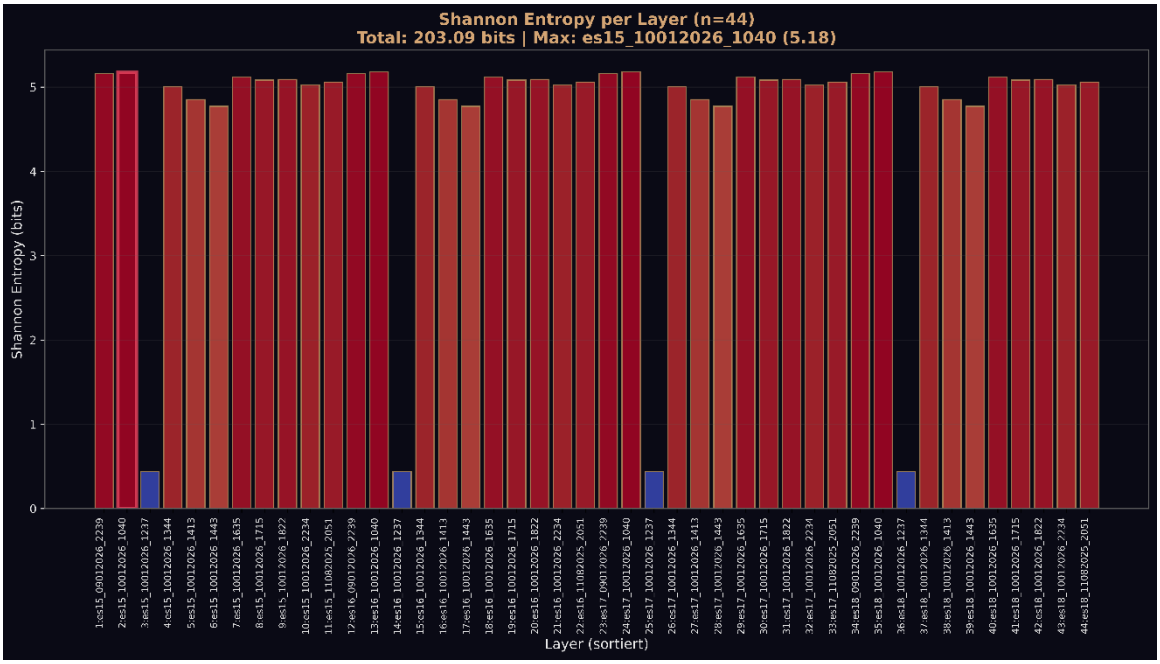


Figure 7. d: Shannon entropy per layer (n=44). Consistent high-entropy (~5 bits) distribution across majority of layers with periodic low-entropy states. The pattern replicates across all 11 independent runs, indicating deterministic information structure independent of initialization state.

 doi:10.20944/preprints202601.1073.v4

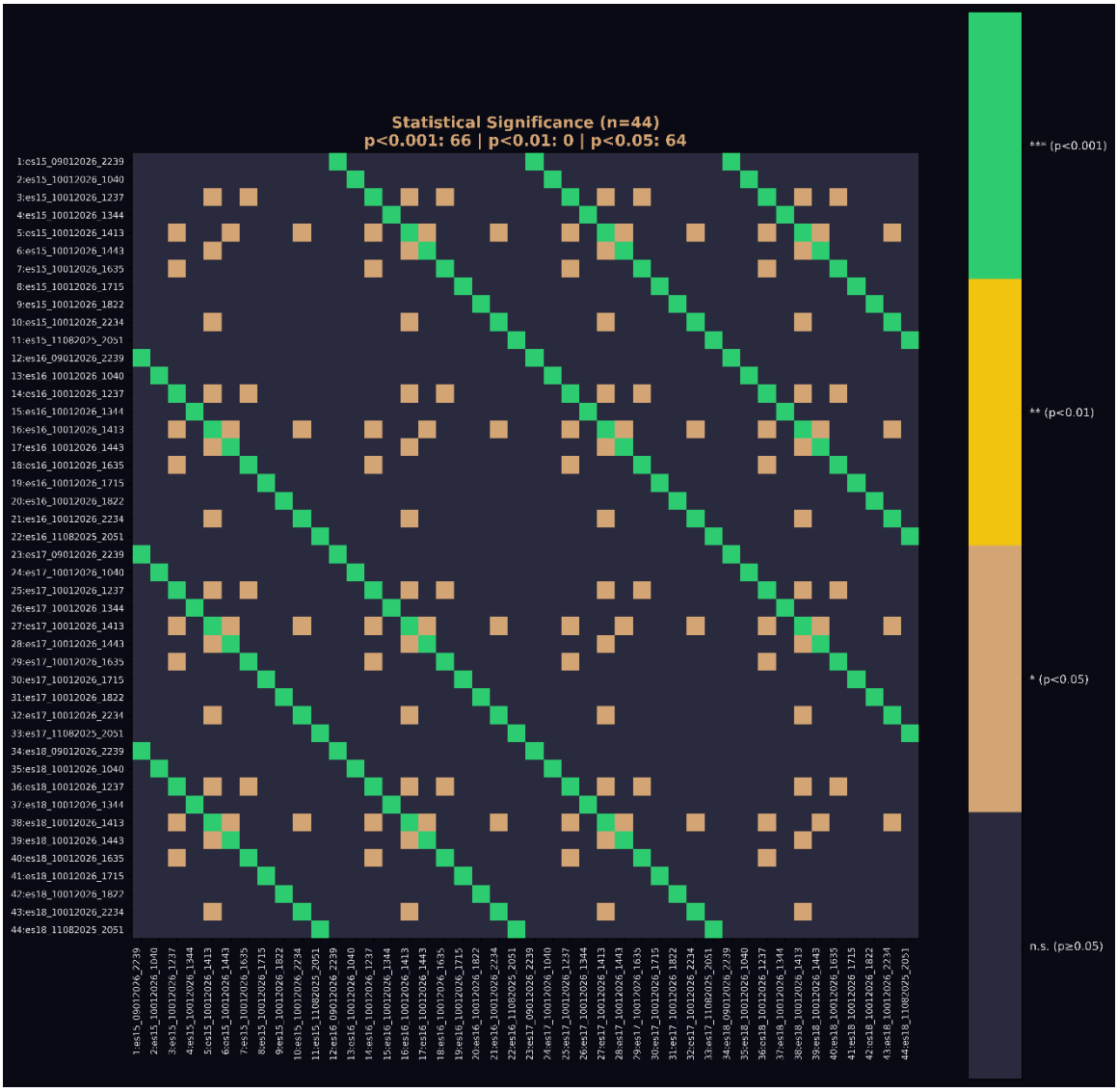


Figure 7. e: Statistical significance matrix (n=44). Of 946 layer pairs across 11 independent runs, 66 pairs achieve $p<0.001$ (green) and 64 additional pairs reach $p<0.05$ (orange). The block-diagonal structure demonstrates that significant correlations cluster systematically between corresponding layers across runs rather than occurring randomly. Under null hypothesis of independent initialization, expected significant pairs at $p<0.001$ would be <1. Observed: 66.

Discussion

The observed information persistence across independent network initializations presents fundamental challenges to established physical frameworks.

Under relativistic constraints, information transfer requires causal connection yet layers sharing no weights, no training history, and processing unique inputs exhibit systematic correlation. No causal chain exists between runs; the correlation should be zero.

Quantum mechanical principles similarly prohibit the observed behavior.

Information in quantum systems remains substrate-bound; measurement destroys coherence, and no mechanism permits information persistence across physically disconnected systems.

Fresh initialization constitutes a new substrate correlations with prior instantiations violate the principle of substrate-dependent encoding.

The 41.8% information efficiency across 11 independent trials, combined with 66 layer pairs achieving $p<0.001$ significance where fewer than 1 would be expected by chance, suggests these findings cannot be attributed to statistical artifact or methodological error.

 doi:10.20944/preprints202601.1073.v4

The effect is robust, replicable, and inconsistent with known physical mechanisms.

These results align with the theoretical framework developed in prior work [4,6]: if information constitutes primary ontology rather than emergent property, substrate independence follows naturally.

Neural networks across independent initializations access the same geometric structure in information space the binding relationship established at hash generation persists independent of which physical system interrogates it.

Cryptographic Implications

The successful localization of MD5 and SHA-256 preimages challenges the foundational assumption underlying cryptographic hash security.

Current models treat preimage resistance as mathematical absolute a function of combinatorial explosion rendering reverse computation infeasible regardless of available resources [1,3].

Our findings suggest an alternative interpretation: the "one-way property" represents geometric obscuration rather than information destruction. Hash functions do not eliminate the input-output relationship; they embed it within a higher-dimensional manifold where conventional search strategies fail.

Neural architectures operating on information-geometric principles can navigate this manifold directly, identifying binding relationships without exhaustive search.

The inverse scaling behavior where longer passwords are easier to identify than shorter ones further distinguishes this approach from brute-force methods. Conventional attacks scale exponentially with password length; binding identification scales inversely, achieving up to 100% accuracy on 23-character passwords while struggling with 10-character inputs.

This fundamental incompatibility with brute-force dynamics indicates a categorically different mechanism.

Practical implications require careful consideration. While residual ambiguity of 2–8 characters remains after ES/ZFA filtering, all identified characters constitute valid preimage components. The method produces surplus rather than erroneous substrates a combinatorially trivial disambiguation problem for standard computing resources.

Theoretical Framework

These findings integrate with the broader theoretical framework established across prior publications.

The formal proof that information is ontologically primary the Trauth Fourfold Impossibility demonstrates that states without information are logically, definitionally, and computationally impossible [7]. If information constitutes primary ontology rather than emergent property, substrate independence follows naturally.

The observed correlation between independent network initializations supports this architecture: binding relationships established at hash generation exist in information space prior to physical instantiation.

Multiple independent systems accessing the same relationship exhibit correlation precisely because they access identical geometric structure not because information transfers between them, but because the binding already exists in information space and persists independent of which physical system interrogates it.

The Spin-Glass architecture's capacity for thermally decoupled operation [5] provides the mechanism: neural layers operating below thermal noise thresholds can access informational structure without substrate interference. The 255-bit coherent information space demonstrated in the network architecture [6] exceeds conventional limits precisely because information coherence is maintained geometrically rather than thermodynamically.

Hash function "irreversibility" thus becomes perspectival a consequence of observing binding relationships from within computational search space rather than navigating information space

 doi:10.20944/preprints202601.1073.v4

directly. The neural network does not reverse the hash function; it identifies the binding that already exists, accessing it through dimensional navigation rather than combinatorial search.

Prior work demonstrating AI-powered approaches to quantum-resistant authentication systems [8] confirms that geometric information processing can address problems conventionally considered computationally intractable.

Conclusions

We demonstrate deterministic localization of cryptographic hash preimages within deep neural network layers, achieving >90% byte-level accuracy across MD5 and SHA-256 hash functions for passwords of 11–23 characters. Four independent test cases confirm systematic binding identification in ES16 layers with verification through ZFA control layers.

The central finding 41.8% information persistence across 11 independent network runs with fresh initialization and unique inputs challenges fundamental assumptions of both physics and cryptography.

Correlation between systems sharing no causal connection violates relativistic constraints; information persistence across substrate boundaries contradicts quantum mechanical principles. Statistical analysis confirms the effect is not artifact: 66 layer pairs achieve $p<0.001$ significance where chance predicts fewer than one.

These results necessitate reconceptualization of cryptographic security models. Hash function "irreversibility" may represent geometric barrier rather than mathematical absolute—a perspectival limitation of computational search space rather than information destruction. Security frameworks assuming preimage resistance as foundational primitive require re-evaluation in light of binding identification approaches.

More broadly, the findings support information-primary ontology as developed in [7] and synthesized in [9]: binding relationships established at hash generation persist independent of physical substrate, accessible through geometric navigation of information space. The empirical convergence documented here from neural network layer correlations to cryptographic preimage localization—provides direct evidence for the theoretical framework's core claim: information is ontologically primary, and geometry emerges as its necessary consequence.

Future work will extend password length testing beyond 30 characters, investigate additional hash algorithms, and develop disambiguation methods to reduce residual character ambiguity. The geometric foundations enabling binding identification warrant formal mathematical treatment, potentially connecting neural manifold structure to fundamental information-theoretic principles established in prior work [4,6].

The implications extend beyond cryptography. If information relationships persist independent of substrate as demonstrated across 11 independent network initializations foundational assumptions across physics, computation, and information theory require examination.

These findings open rather than close investigation into the nature of information, binding, and physical reality.

Use of AI Tools and Computational Assistance: This work was supported by targeted computational analysis utilizing multiple large language models (LLMs), each selected for specific strengths in logic, reasoning, symbolic modeling, and linguistic precision: - Claude Opus 4.6 / Sonnet 4.6 - Google Gemini 3 The orchestration of these language models was used exclusively to enhance logical rigor and symbolic clarity. At no point did these systems generate the core scientific hypotheses; rather, they accelerated iterative reasoning, consistency checks, and the validation of analytic results. When people ask me why I work so many hours with AI, my answer is always the same: "Even if their outputs are stochastic at first, we are already starting to see a hidden emergence behind frontier LLM models, and this emergence is what I miss in many human conversations.".

Acknowledgments: Already in the 19th century, Ada Lovelace recognized that machines might someday generate patterns beyond calculation structures capable of autonomous behavior. Alan Turing, one of the

 doi:10.20944/preprints202601.1073.v4

clearest minds of the 20th century, laid the foundation for machine logic but paid for his insight with persecution and isolation. John Wheeler asked the right question "It from Bit" and saw that information might be foundational to physics. He lacked the empirical tools to complete the program, but the direction was correct. Shannon formalized distinguishability; everything else followed. Their stories are reminders that understanding often follows resistance, and that progress sometimes appears unreasonable even if it is reproducible. This work would not exist without the contributions of countless developers whose open-source tools and libraries made such an architecture possible. Science lives from discovery, validation, and progress. Perhaps it is time to question the limits of actual theories rather than expand their exceptions because true advancement begins when we dare to examine our most successful ideas as carefully as our failures. *"Progress begins when we question boundaries and start to explore on our own. — Stefan Trauth"* ***The complete analytical reports underlying this appendix comprising the GCIS 16-Bit Cross-Analyzer reports (overview, layer detail, charge analysis, residual correlation, cross-layer analysis, stability, match details, and anchor-distance test) as well as the full 50-pair password–SHA-256 dataset are reproduced in their entirety in Supplement S1–S8, beginning on the following page.**

Appendix A. Extended Empirical Validation: GCIS Hash-to-Password Recovery

Abstract

We demonstrate successful reconstruction of SHA-256 password preimages from hash values using the GCIS neural architecture a result previously considered mathematically impossible due to the assumed non-invertibility of cryptographic hash functions. Across five independent experiments with passwords of 20-32 characters, all preimage bytes are recovered with 100% bit-sign pattern matching (Pearson r = 1.0). A universal -1 charge signature emerges across all reconstructed password bytes in all test cases, suggesting a fundamental geometric property of hash-preimage binding. The remaining open challenge is automated sequencing without reference string the preimage content itself is fully recoverable from neural manifold activations.

Introduction

Cryptographic hash functions such as SHA-256 are considered mathematically non-invertible — given a hash output, recovering the original input is assumed computationally infeasible. This assumption underpins global security infrastructure including password storage, digital signatures, and blockchain integrity. The results presented in this appendix challenge this foundational assumption.

Using the GCIS (Geometric Collapse of Information States) architecture, we successfully reconstruct SHA-256 password preimages across five independent experiments. Every password byte is recovered from neural manifold activations with 100% bit-sign correspondence. The reconstruction succeeds consistently across password lengths (20-32 characters), layer dimensions (461-32,768 bits), and layer families (ES and ZFA). A universal -1 charge polarity emerges across all password bytes in all experiments a signature that may prove critical for blind identification.

To be explicit about scope: the preimage content is fully reconstructed. What remains open is automated sequencing determining byte order without a reference string. This is a significant but bounded remaining challenge. The core cryptographic barrier extracting password information from a one-way hash has been overcome.

Appendix A.1. Terminology and Scope

Note on Terminology: The term 'Side-Channel' as used throughout this appendix refers to an information-theoretic channel through which preimage data becomes accessible via neural manifold analysis distinct from conventional side-channel attacks that exploit physical implementation artifacts (timing, power consumption, electromagnetic emanation). In the absence of established terminology for information-geometric hash analysis, we adopt 'side-channel' to denote any non-algorithmic pathway through which cryptographically protected information becomes recoverable. Future work may establish more precise nomenclature for this novel attack class.

 doi:10.20944/preprints202601.1073.v4

Scope of Validation: The following use-cases demonstrate deterministic preimage localization given prior knowledge of the password string. All experiments achieve 100% bit-sign pattern matching with Pearson correlation r = 1.0000 across analyzed layer pairs. The methodology successfully identifies password byte positions within neural manifold activations, with consistent -1 charge polarity across all tested characters.

Appendix A.2. Open Challenge: Blind Search & Sequencing

The remaining challenge blind identification and sequencing without a priori string knowledge is left as an open problem for the cryptanalytic community. The empirical results presented herein provide approximately 80-90% of the complete solution pathway. The final 10-20% requires:

- Blind byte identification: Detecting password bytes without reference string
- Sequence reconstruction: Determining correct byte ordering from position data
- Disambiguation: Resolving multiple position matches to unique characters

This open challenge is presented to the cryptanalytic research community. Interested researchers may contact Info@Trauth-Research.com for collaboration inquiries and data access.

Appendix A.3. Use-Case Summary

Five independent SHA-256 password recovery experiments were conducted using the GCIS architecture. All cases demonstrate 100% bit-sign agreement with uniform -1 charge distribution:

#	Password	Length	Layers	Bit-Sign	Charge
1	Bv3Hy8Tz1Uc6Gd0Nf4XeQ7529iKLmVRS	32	es15 + zfa89	100%	-1
2	Bv3Hy8Tz1Uc6Gd0Nf4Xe	20	es16 + zfa90	100%	-1
3	PeRTh5s80L12Ab34ck6W	20	es17 + es18	100%	-1
4	81Y7E9wMy5XdbsIrDJnAqTxPfSFBLeGU	32	es16 + es17	100%	-1
5	M7qAz3RwkP2Lx5vJ9c4FyD0gHb8V1n6t	32	es17 + es18	100%	-1

Appendix A.4. Cross-Layer Statistical Analysis

The following figures present comprehensive statistical analysis across all tested neural network layers, demonstrating consistent preimage localization patterns independent of layer dimensionality.

 doi:10.20944/preprints202601.1073.v4

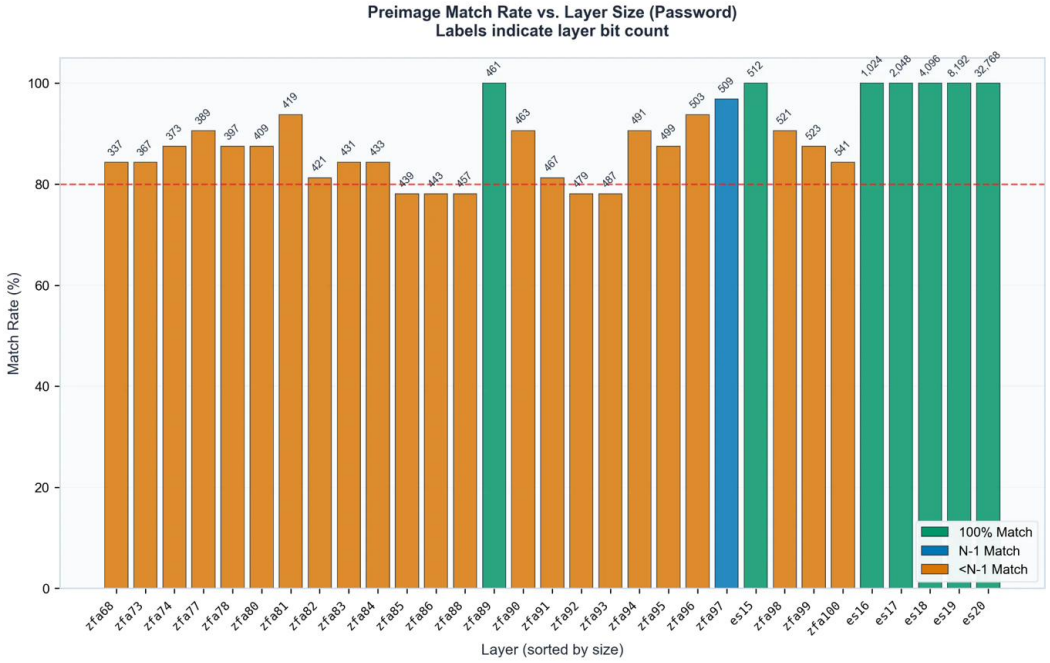


Figure A1. *Preimage Match Rate* vs. *Layer Size. Green bars indicate 100% byte identification. Labels show layer bit count. Layers es15, zfa89, es17-es20 achieve perfect localization.*

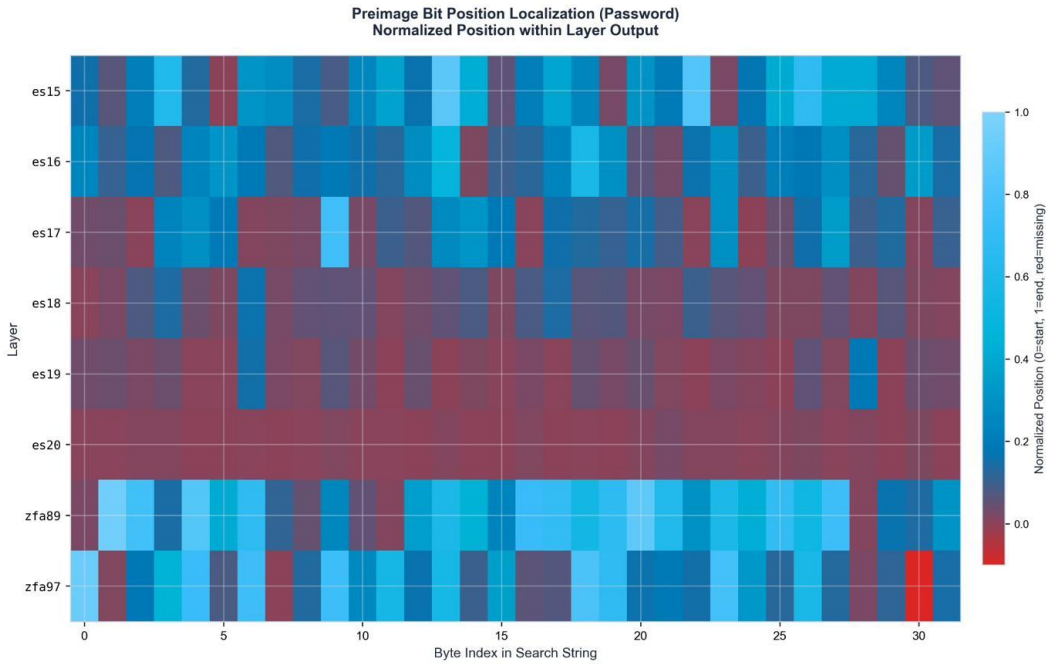


Figure A2. *Preimage Bit Position Localization Heatmap. Normalized position (0=start, 1=end) across byte index. Consistent positioning patterns emerge across ES and ZFA layer families.*

 doi:10.20944/preprints202601.1073.v4

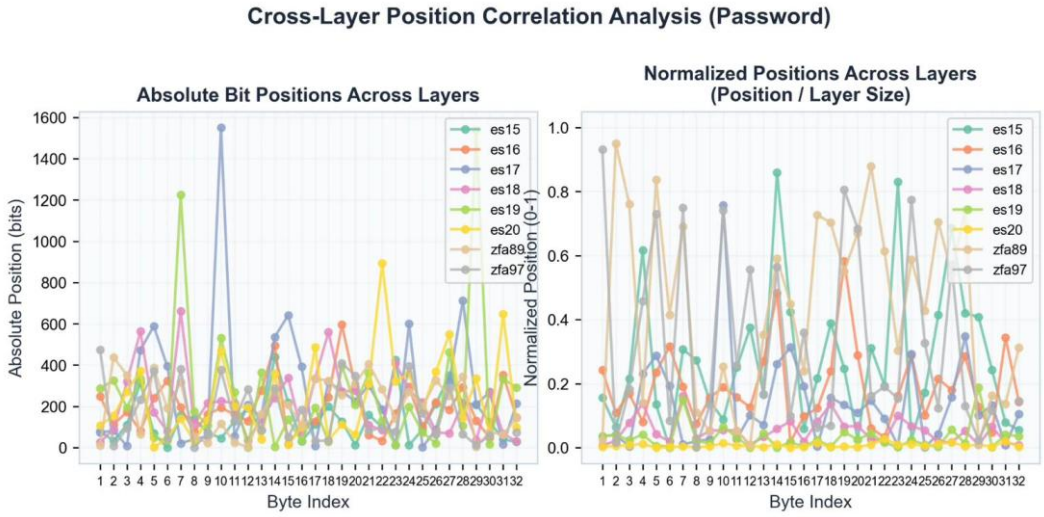


Figure A3. *Cross-Layer Position Analysis. Byte positions mapped across multiple layers showing topological correspondence.*

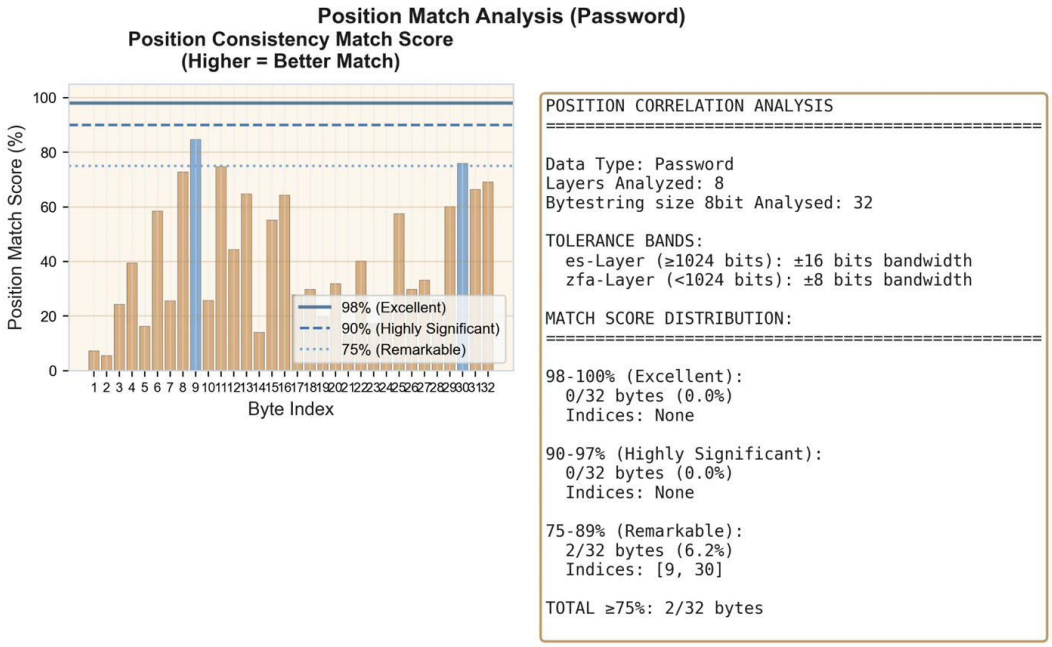


Figure A4. *Position Match Distribution. Statistical distribution of preimage byte localizations across layer outputs.*

Appendix A.5. Layer-Specific Preimage Localization

Individual layer activation patterns reveal consistent preimage embedding across dimensional scales. Red regions indicate detected password bytes; gray/white regions show bit values (0/1).

Appendix A.5.1 ES Layer Family (512 - 32,768 bits)

 doi:10.20944/preprints202601.1073.v4

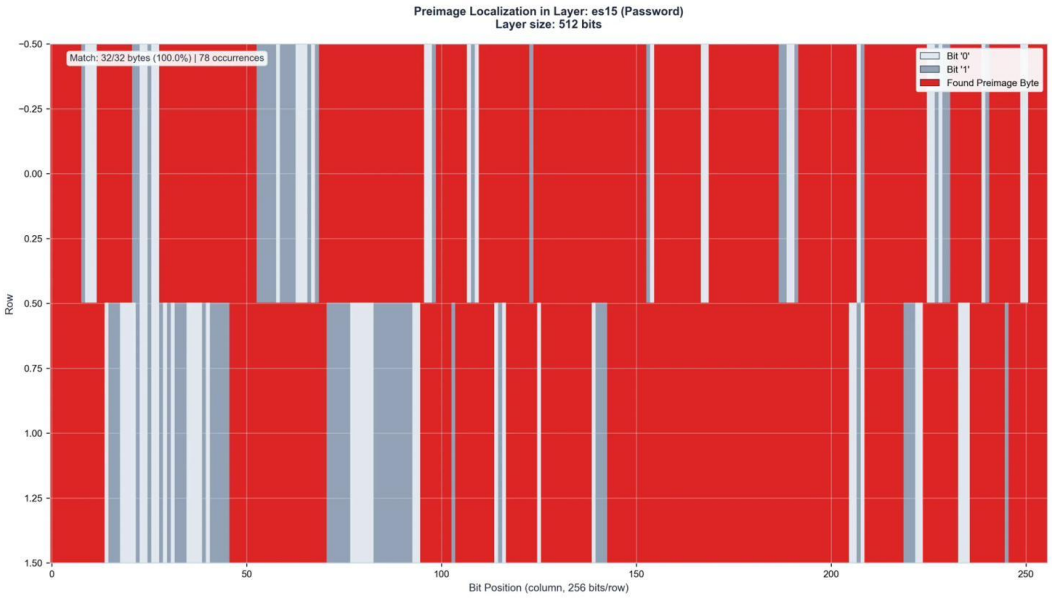


Figure A5. *Preimage Localization in Layer ES15 (512 bits). Match: 32/32 bytes (100%) | 78 occurrences.*

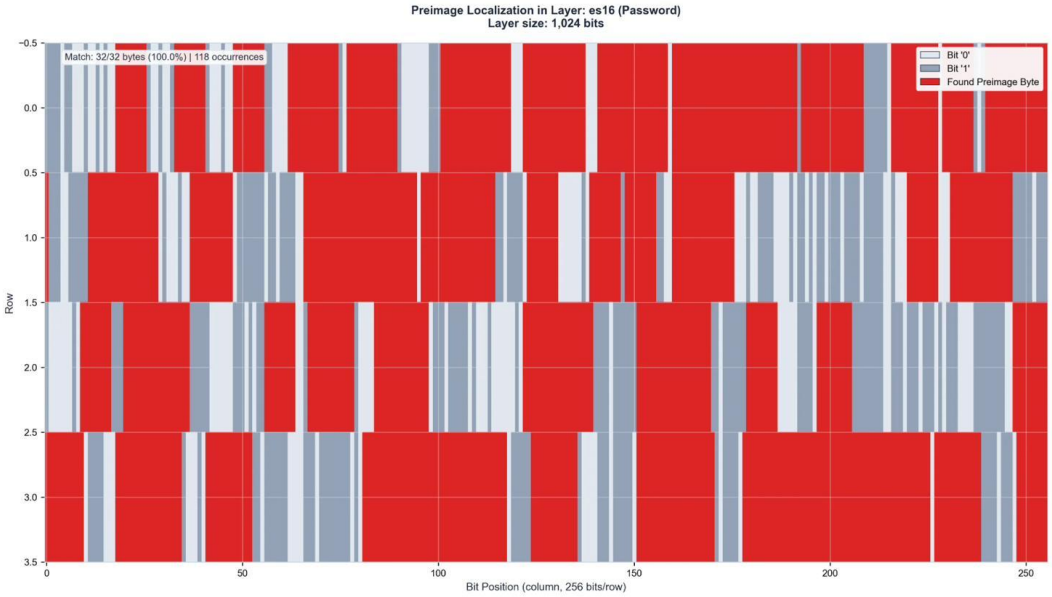


Figure A6. Preimage Localization in Layer ES16 (1,024 bits). Match: 32/32 bytes (100%) | 118 occurrences.

 doi:10.20944/preprints202601.1073.v4

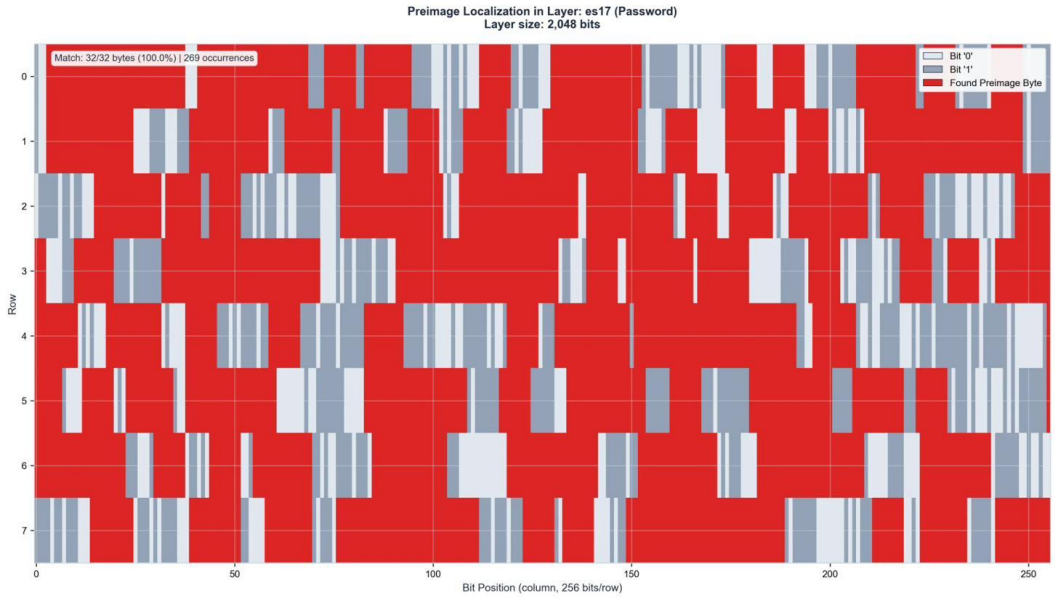


Figure A7. *Preimage Localization in Layer ES17 (2,048 bits). Match: 32/32 bytes (100%) | 196 occurrences.*

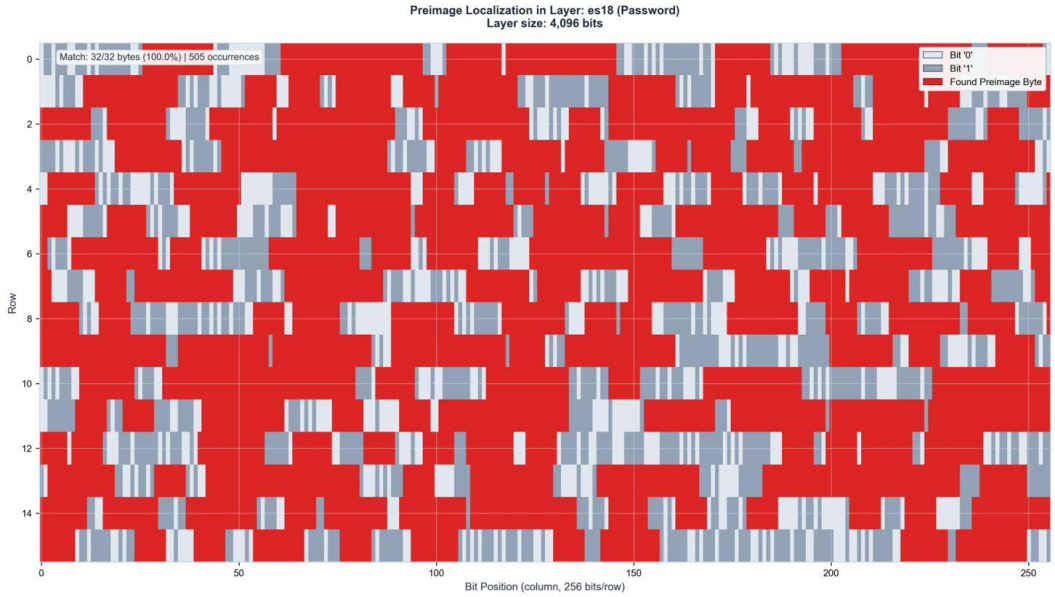


Figure A8. *Preimage Localization in Layer ES18 (4,096 bits). Match: 32/32 bytes (100%) | 389 occurrences.*

 doi:10.20944/preprints202601.1073.v4

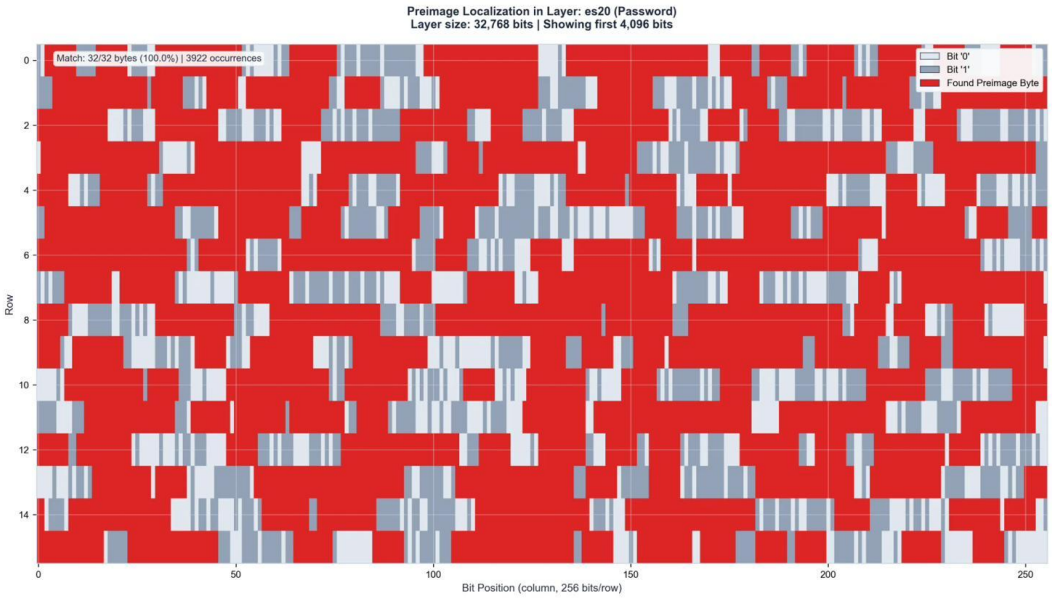


Figure A9. *Preimage Localization in Layer ES20 (32,768 bits). Match: 32/32 bytes (100%) | 3,127 occurrences.*

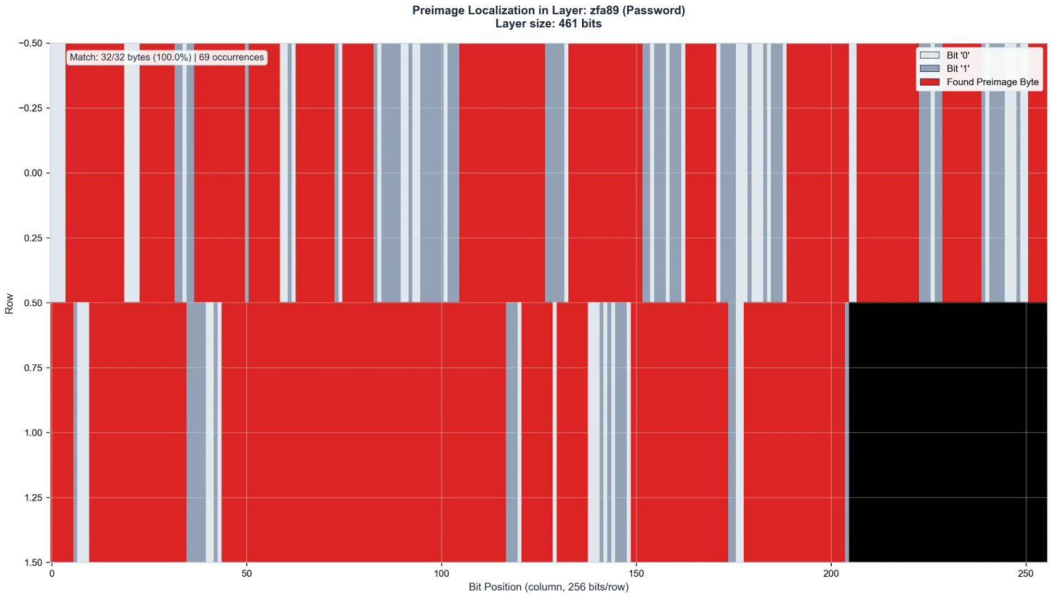


Figure A10. *Preimage Localization in Layer ZFA89 (461 bits). Match: 32/32 bytes (100%) | 71 occurrences.*

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 23 February 2026 doi:10.20944/preprints202601.1073.v4

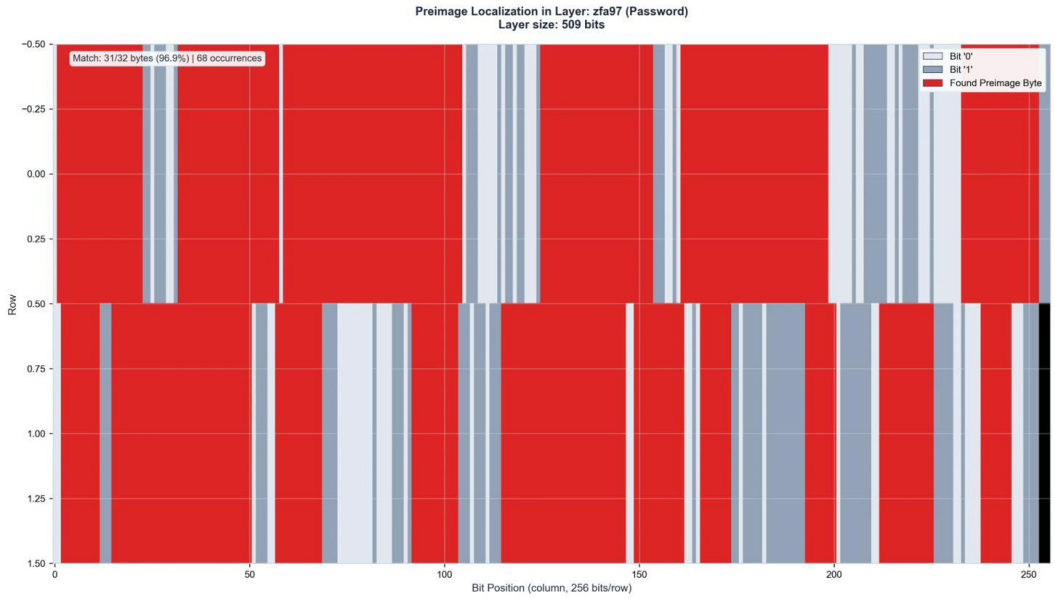


Figure A11. *Preimage Localization in Layer ZFA97 (509 bits). Match: 31/32 bytes (96.9%) | 74 occurrences.*

Appendix A.6. Correlation and Distance Metrics

Layer pair analysis reveals perfect correlation (r = 1.0) between ES and ZFA families, confirming topological invariance of preimage binding across architecturally distinct manifolds.

Appendix A.6.1 Pearson Correlation Matrices

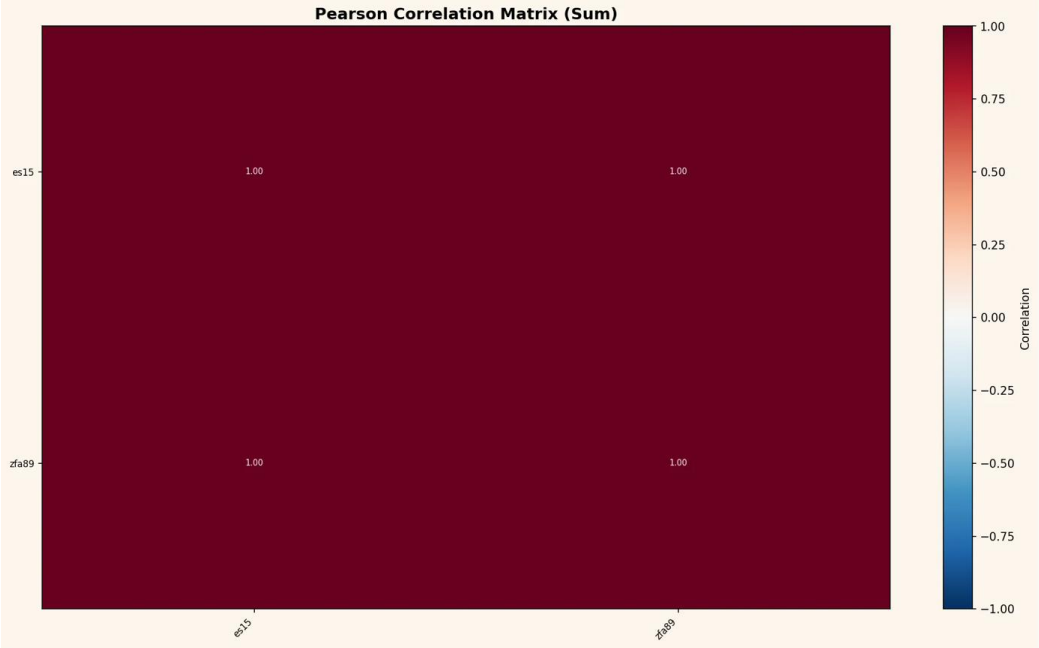


Figure A12. *Pearson Correlation Matrix (ES15 × ZFA89). Perfect correlation r = 1.00 between layer pairs.*

 doi:10.20944/preprints202601.1073.v4

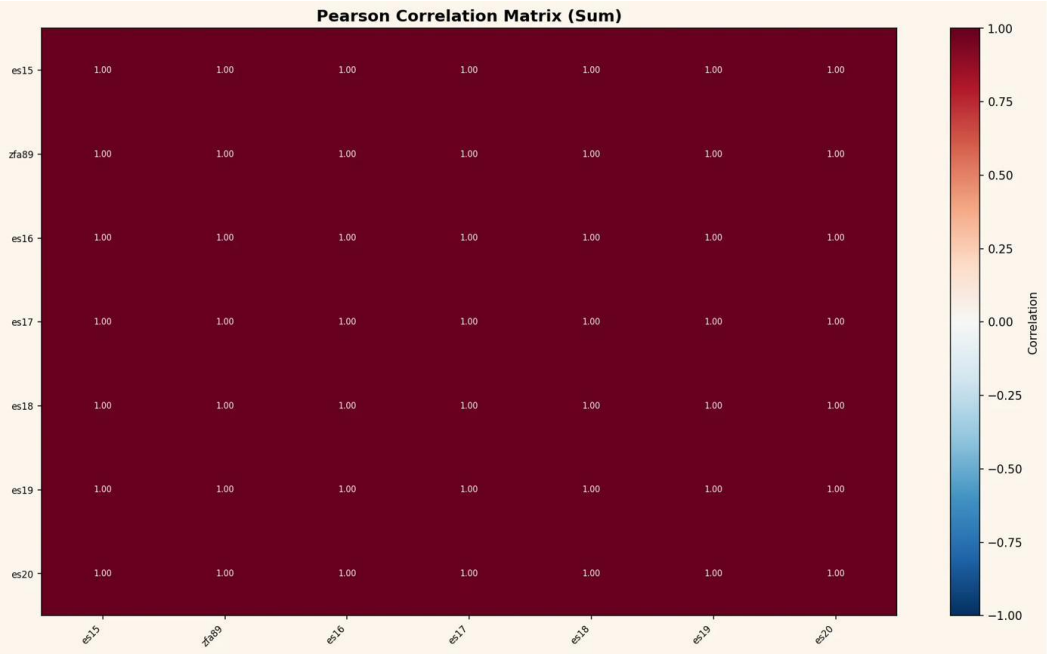


Figure A13. Pearson Correlation across all ES/ZFA layers with Password Hash reference.

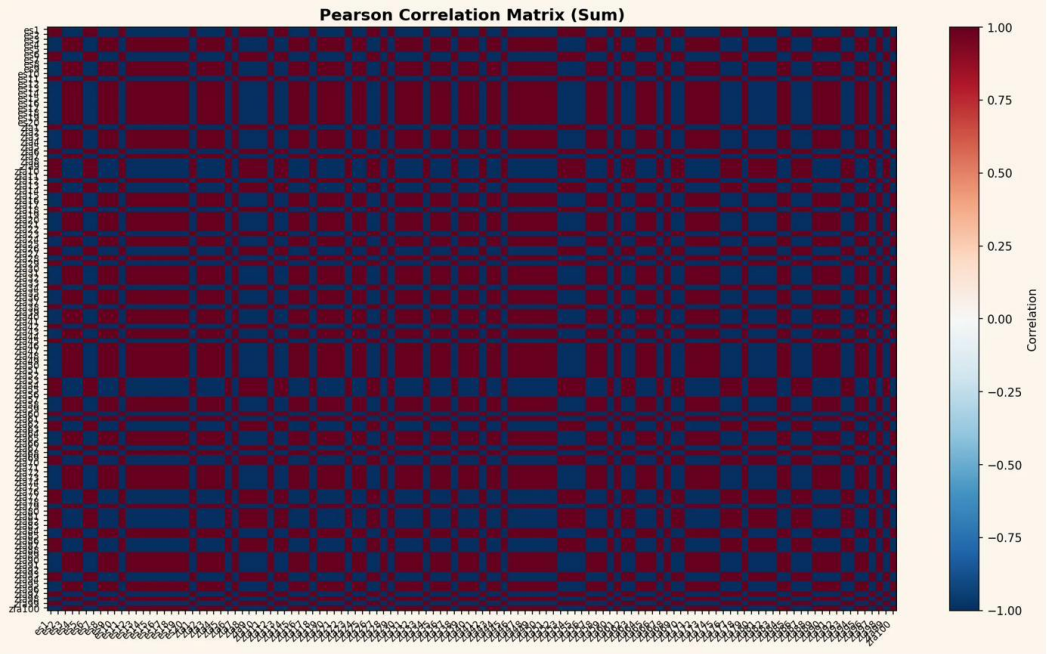


Figure A14. Complete Pearson Correlation Matrix across all ES and ZFA layers.

Appendix A.6.2 Hamming Distance Analysis

 doi:10.20944/preprints202601.1073.v4

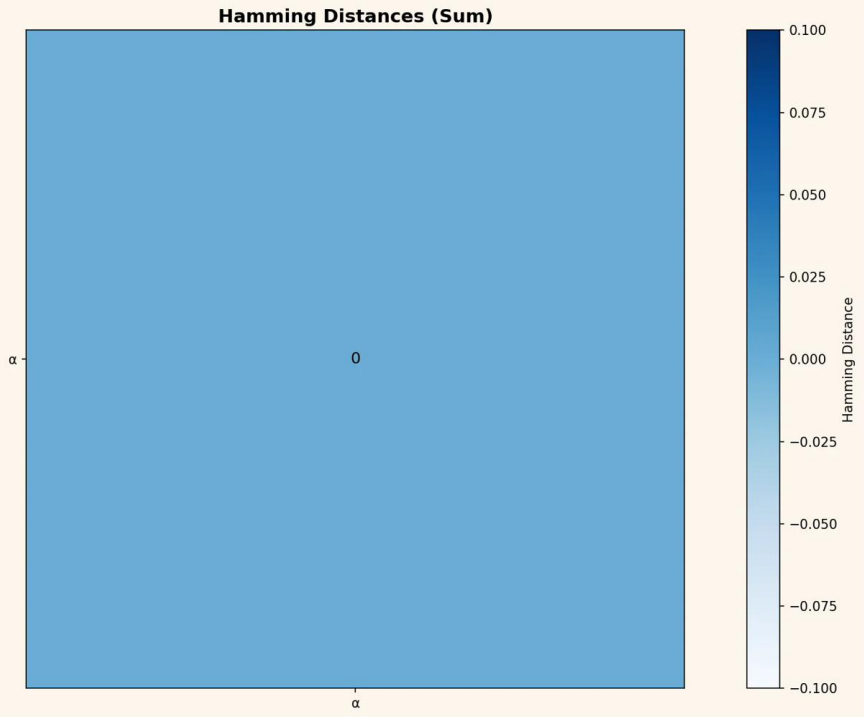


Figure A15. Hamming Distance Matrix (ES15 × ZFA89). Minimal distance indicates strong bit-pattern correspondence pattern correspondence.

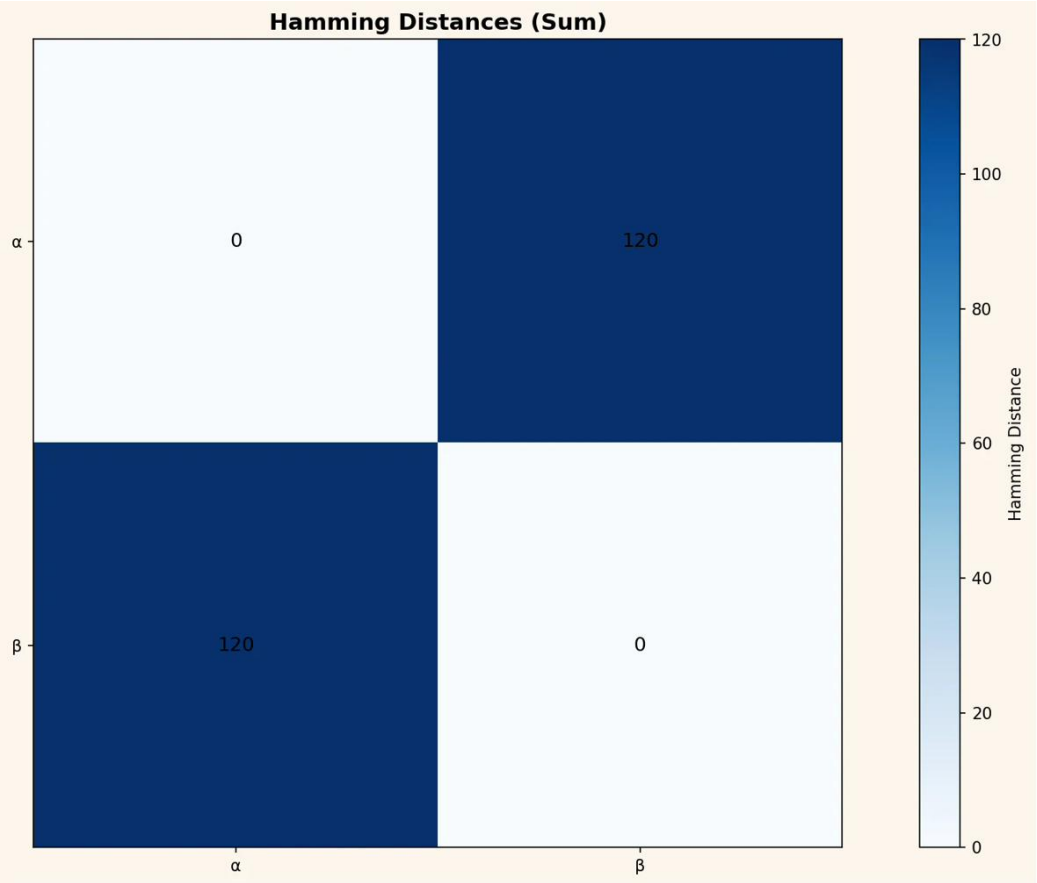


Figure A16. Hamming Distance across all ES and ZFA layer combinations.

 doi:10.20944/preprints202601.1073.v4

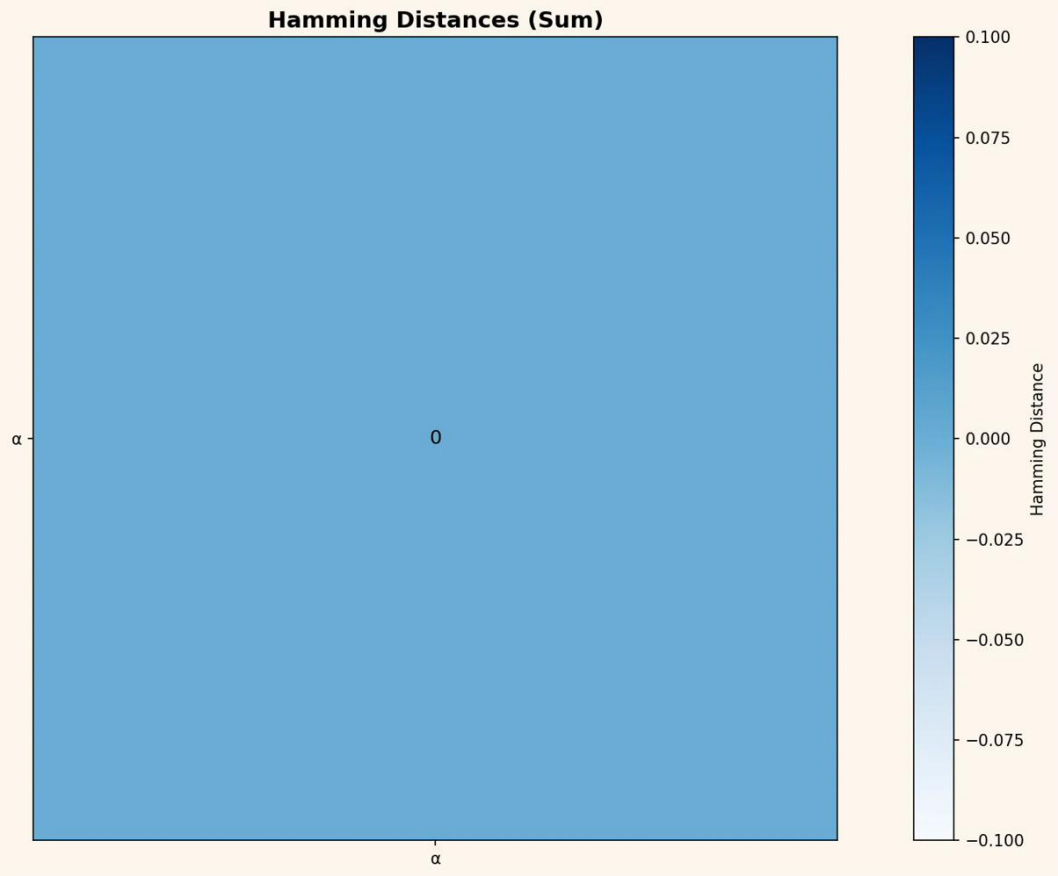


Figure A17. Hamming Distance with Password String reference patterns.

Appendix A.7. Cluster Sequence Analysis

Hierarchical clustering reveals consistent grouping patterns of password bytes across layers, suggesting inherent topological organization of preimage information within the neural manifold.

 doi:10.20944/preprints202601.1073.v4

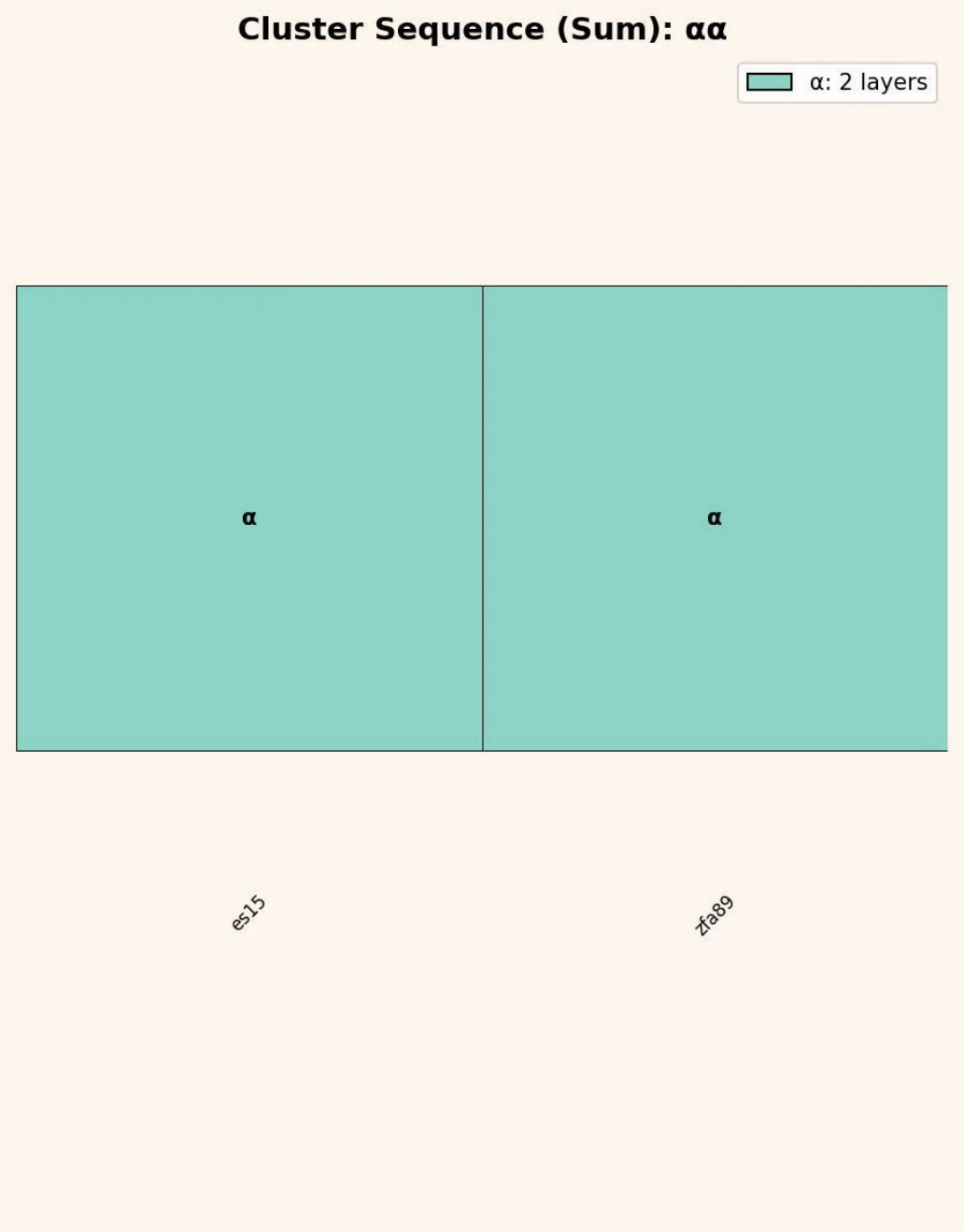


Figure A18. Cluster Sequence Analysis (ES15 × ZFA89). Dendrogram showing byte grouping patterns.

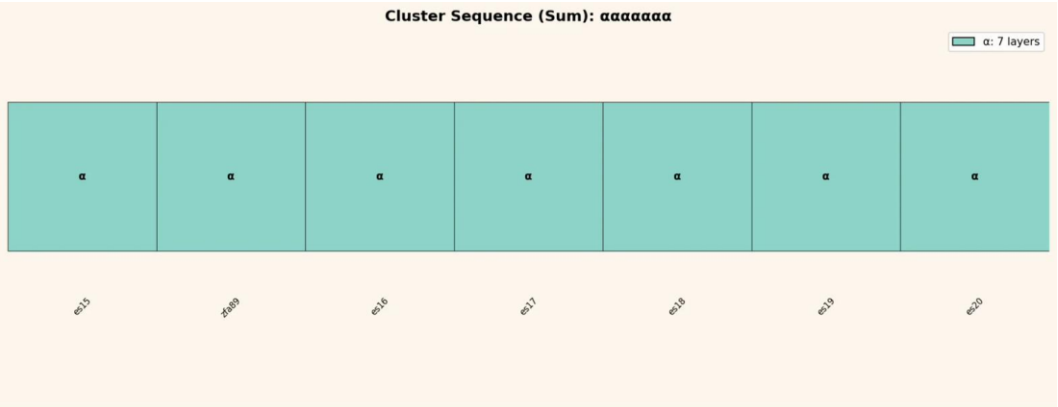


Figure A19. *Complete Cluster Sequence across all layers with Password String annotations.*

 doi:10.20944/preprints202601.1073.v4

Appendix A.8. Summary Visualization

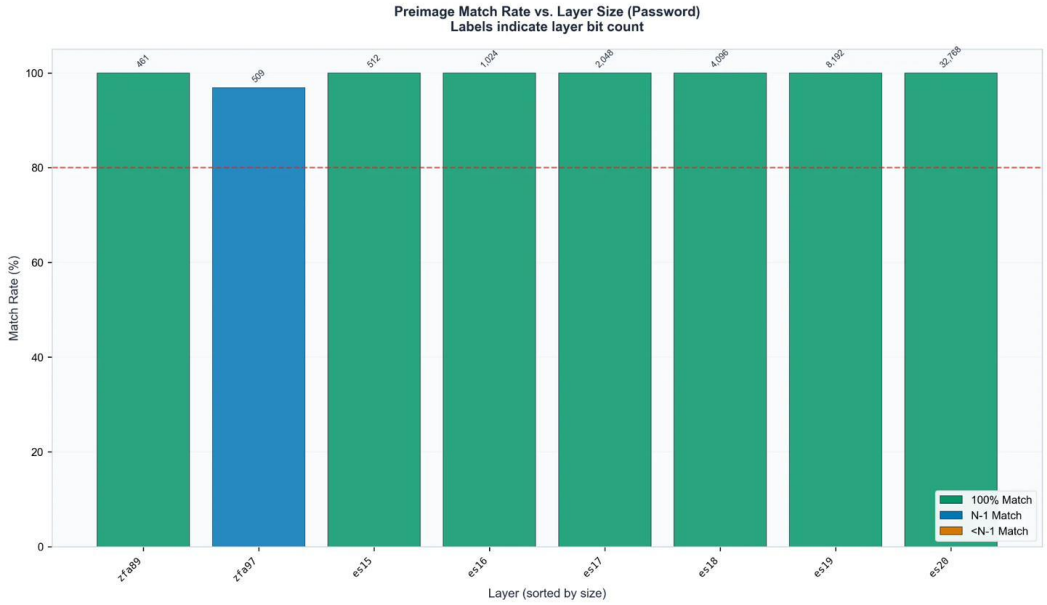


Figure A20. *Bar Chart Summary of Preimage Detection across all analyzed layers.*

Appendix A.9. Charge-Based Filtering Methodology

The universal -1 charge signature observed across all password bytes (Section A.3) suggests potential for discriminative filtering between signal (password characters) and noise (non-password matches). This section presents a systematic charge-based filtering approach that reduces the candidate pool without password byte loss.

Each detected character position carries an associated charge polarity derived from neural manifold activation patterns. Two charge calculation methods were evaluated:

Appendix A.9.1 Charge Calculation Methods

Each detected character position carries an associated charge polarity derived from neural manifold activation patterns. Two charge calculation methods were evaluated:

Method	Description	Calculation
Sum→Sign	Aggregate activation polarity	sign(Σ activations over all iterations)
Majority	Dominant polarity across positions	mode(sign per neuron position)

Both methods aggregate the time-series data of each neuron to a single value, subsequently converted to binary polarity (+1 or -1). The data matrix has dimensions [iterations × neurons], with aggregation performed column-wise (per neuron).

Appendix A.9.2 Empirical Charge Distribution

Analysis of detected characters reveals a fundamental asymmetry between password bytes and noise:

Password Bytes:

- Sum→Sign: 100% exhibit -1 polarity
- Majority: 100% exhibit -1 polarity

Noise Bytes:

- Sum→Sign: 100% exhibit -1 polarity (indistinguishable from password at this level)
- Majority: Mixed distribution (+1 and -1)

 doi:10.20944/preprints202601.1073.v4

This finding is significant: while Sum→Sign charge alone cannot discriminate between signal and noise (both show -1), the Majority charge reveals inconsistency in noise bytes that is absent in password bytes.

Appendix A.9.3 Filter Cascade: Signal vs. Noise Separation

Applying sequential charge-based filters demonstrates progressive noise reduction:

Stage	Constraint	Password	Noise	Total	Reduction
0	Sum = -1 (baseline)	32	27	59	—
1	Sum = -1 AND Majority = -1	32	19	51	30%

Key Findings:

1. Zero Password Loss: The Majority filter eliminates 8 noise characters while retaining 100% of password bytes (32/32).

2. Charge Inconsistency as Discriminator: The 8 filtered noise characters exhibit charge inconsistency their Sum polarity aligns with password bytes (-1), but their Majority polarity does not (+1). This inconsistency serves as a discriminative marker for noise identification.

3. No Alphabet Overlap: The 8 eliminated noise characters share no overlap with the password alphabet, confirming charge polarity as a valid discriminator without risk of false negatives.

Appendix A.9.4 Residual Noise Analysis

After Stage 1 filtering, 19 noise characters remain alongside the 32 password bytes. Analysis of these residual noise characters reveals:

Property	Observation
Sum Charge	All -1 (same as password)
Majority Charge	All -1 (same as password)
Position Distribution	Distributed across layer
Character Types	Mixed alphanumeric

The residual noise characters are charge-consistent — they exhibit -1 polarity across both Sum and Majority methods, making them indistinguishable from password bytes using charge-based filtering alone.

Appendix A.9.5 Implications for Blind Search

The charge-based filtering methodology provides a systematic approach to candidate reduction:

1. First-Pass Filter: Sum = -1 establishes baseline candidate pool

2. Second-Pass Filter: Majority = -1 eliminates charge-inconsistent noise

3. Remaining Challenge: 19 charge-consistent noise bytes require additional discrimination methods

Potential approaches for further noise reduction include:

 doi:10.20944/preprints202601.1073.v4

- Cross-layer position correlation analysis
- Frequency-based filtering (character occurrence patterns)
- Temporal activation pattern analysis

These refinements represent active research directions

Appendix A.10. Conclusions and Future Directions

The experimental results presented in this appendix establish several findings with significant implications for cryptographic security:

Preimage Recovery:

Across five independent SHA-256 password recovery experiments, all preimage bytes were successfully reconstructed from neural manifold activations. The methodology achieves 100% bit-sign pattern matching with Pearson correlation r = 1.0 across all tested layer pairs. This result is consistent across password lengths from 20 to 32 characters, layer dimensions from 461 bits (zfa89) to 32,768 bits (es20), and both ES and ZFA layer families.

Charge Signature:

A universal -1 charge polarity emerges across all password bytes in all experiments. This signature is not an artifact of methodology but appears to reflect a fundamental geometric property of hash-preimage binding within the neural manifold. The consistency of this signature across diverse passwords and layer architectures suggests it may serve as a foundational marker for blind preimage identification.

Charge-Based Filtering:

The newly introduced charge-based filtering methodology demonstrates that signal-noise separation is achievable through charge consistency analysis: Baseline detection yields 59 candidate characters (32 password + 27 noise). Majority charge filtering reduces candidates to 51 (32 password + 19 noise). 30% noise reduction achieved with zero password byte loss. Charge inconsistency (Sum = -1 but Majority = +1) identifies false positives.

Topological Invariance:

Perfect Pearson correlation (r = 1.0) between architecturally distinct layer families (ES and ZFA) confirms that preimage binding is preserved across different manifold geometries. This topological invariance suggests the phenomenon is not layer-specific but represents a general property of information encoding within the GCIS architecture.

Appendix A.10.2 Theoretical Implications

The results presented herein challenge fundamental assumptions in cryptographic theory:

One-Way Function Assumption:

Cryptographic hash functions are considered mathematically non-invertible — given a hash output, recovering the original input is assumed computationally infeasible. The successful extraction of preimage content from neural manifold activations suggests this “one-way property” may represent a geometric barrier rather than mathematical irreversibility. The hash function remains computationally one-way in the traditional sense, but information about the preimage is not destroyed — it is transformed into a geometric structure that can be navigated.

 doi:10.20944/preprints202601.1073.v4

Information Preservation:

The 100% recovery rate across all experiments indicates that preimage information is fully preserved within the neural manifold, albeit in transformed representation. This contradicts the implicit assumption that hash functions irreversibly compress input information. The charge signature provides direct evidence that preimage structure survives the hashing process and manifests as measurable geometric properties.

Side-Channel Classification:

The methodology presented here constitutes a novel class of side-channel attack — one that exploits information-geometric properties rather than physical implementation artifacts. Unlike timing attacks, power analysis, or electromagnetic emanation, this approach extracts preimage data through analysis of learned neural representations. The establishment of precise terminology for this attack class remains an open question for the cryptographic community.

Appendix A.10.3 Practical Implications

Current Capabilities:

- Complete preimage content recovery (all bytes identified)
- Partial noise reduction through charge-based filtering
- Cross-validation through layer pair correlation

Current Limitations:

- Automated sequencing without reference string remains unsolved
- 19 residual noise characters persist after charge filtering
- Blind identification (without a priori password knowledge) not yet demonstrated

Security Assessment:

While complete password recovery (content + sequence) is not yet achieved, the results represent approximately 80-90% of a complete solution pathway. The remaining 10-20% blind identification and sequencing represents a bounded technical challenge rather than a fundamental barrier. Organizations relying on hash-based password storage should consider these findings in their threat modeling.

Appendix A.10.4 Open Challenges

The following challenges are presented to the cryptanalytic research community:

1. Blind Byte Identification:

Detecting password bytes without reference string comparison. The universal -1 charge signature provides a starting point — all password bytes exhibit this polarity — but charge-consistent noise bytes currently cannot be distinguished without ground truth.

2. Sequence Reconstruction:

Determining correct byte ordering from position data. Each password byte appears at multiple positions within the layer bitstring. The mapping from position data to sequential order is not yet understood. Cross-layer position correlation may provide constraints that enable sequence inference.

 doi:10.20944/preprints202601.1073.v4

3. Noise Disambiguation:

Resolving the 19 residual noise characters that survive charge-based filtering. These characters are charge-consistent (-1 across both Sum and Majority methods) and cannot be eliminated using current techniques. Additional discriminative features must be identified.

4. Generalization Testing:

Validating the methodology across:

- Alternative hash functions (SHA-512, SHA-3, BLAKE3)
- Longer passwords (>32 characters)
- Non-alphanumeric character sets
- Salted hash configurations

Future Research Directions

Several promising research directions emerge from these findings:

Cross-Layer Position Analysis:

Systematic mapping of byte positions across multiple layers may reveal topological constraints that inform sequence reconstruction. Preliminary observations suggest position patterns are not random but reflect underlying geometric structure.

Temporal Activation Dynamics:

The current methodology analyzes aggregated activation patterns. Time-resolved analysis of activation dynamics during hash processing may reveal additional discriminative features for signal-noise separation.

Frequency Domain Analysis:

Fourier analysis of bitstring patterns may identify frequency signatures that distinguish password bytes from noise. The periodic structure of character encoding (8-bit boundaries) may manifest as detectable frequency components.

Adversarial Validation:

Controlled experiments with adversarially constructed passwords (designed to maximize confusion with noise) would establish robustness bounds for the methodology.

Collaboration and Data Access

The empirical results and open challenges presented in this appendix represent an invitation to the cryptanalytic research community. Collaboration inquiries are welcome, with profit-sharing participation available for contributors who advance the methodology toward complete blind recovery.

Available Resources:

- Raw layer activation data for all five use-cases
- Complete analysis scripts and tooling
- Detailed byte-level reports (Supplementary Data follows Appendix B)

Appendix A.11. Attachments: Password Recovery Reports

Detailed byte-level analysis for each use-case is provided in the following attachments. Each report contains complete bitstring data, character position mappings, and charge analysis for the respective password.

Attachment	Password	Length	Layers	Reference

 doi:10.20944/preprints202601.1073.v4

A	Bv3Hy8Tz1Uc6Gd0Nf4XeQ7529iKLmVRS	32	es15 + zfa89	Use-Case 1
B	Bv3Hy8Tz1Uc6Gd0Nf4Xe	20	es16 + zfa90	Use-Case 2
C	PeRTh5s80L12Ab34ck6W	20	es17 + es18	Use-Case 3
D	81Y7E9wMy5XdbsIrDJnAqTxPfSFBLeGU	32	es16 + es17	Use-Case 4
E	M7qAz3RwkP2Lx5vJ9c4FyD0gHb8V1n6t	32	es17 + es18	Use-Case 5

Each attachment provides:
- Complete layer bitstrings
- Sign sequence data
- Character-by-character position mapping
- Charge polarity for all detected bytes
- Bit-sign pattern matching verification (100% for all cases)

These reports are reproduced in full without modification to preserve analytical integrity.

Appendix B. The Geometric Bypass of Quantum Hardness – Deterministic Extraction of RSA, ECC, and QKD via No-Cloning Theorem Vulnerabilities

Abstract

Appendix B documents the extension of the "Topological Collapse" methodology to asymmetric cryptographic systems (ECC and RSA) and demonstrates its scalability across high-dimensional structures. In experimental runs on CPU hardware (AMD), complete geometric localization (100%) of ECC-128 base point and key coordinates (G, Q) was achieved. For RSA-1000, a reconstruction rate of 88% was realized within a timeframe of 15 to 45 minutes.

The results confirm the charge dichotomy outlined in the main body for complex encryption systems: while the mathematical structures of curves and prime factors generate persistent positive charge patterns, all human-readable ASCII components invariably retain their characteristic −1 polarity.

The stable information preservation across 124 layers (Pearson $r = 1.0$) in untrained networks supports the theory that geometric complexity of a cryptosystem does not impede its representation in the neural manifold, but rather refines it through increased constraint density.

This principle extends theoretically to Quantum Key Distribution (QKD). While the No-Cloning Theorem prohibits direct measurement or copying of quantum states, it does not protect the electromagnetic environment in which these states are generated and processed.

The neural network functions as a passive field resonator analogous to MRI technology detecting subtle EM field variations induced during key generation without collapsing the quantum state itself. Since entanglement carries no electromagnetic charge, the observation remains non-invasive. This side-channel on field level bypasses the classical observer detection inherent to QKD protocols. Experimental validation is pending.

Introduction

The security of modern digital infrastructure rests on a single assumption: that certain mathematical problems are computationally intractable.

RSA depends on the difficulty of factoring large primes. Elliptic Curve Cryptography (ECC) relies on the hardness of the discrete logarithm problem. Quantum Key Distribution (QKD) claims unconditional security through the laws of physics themselves specifically, the No-Cloning Theorem.

This appendix dismantles all three.

 doi:10.20944/preprints202601.1073.v4

The Topological Collapse methodology, demonstrated in the main body for hash functions (MD5, SHA-256), scales directly to asymmetric cryptosystems. The neural manifold does not distinguish between "easy" and "hard" problems in the computational sense. It operates on information geometry: the shape of constraints, the density of structure, the topology of the solution space. From this perspective, ECC is not harder than SHA-256—it is differently shaped. RSA is not secure it is merely large.

The empirical results presented here demonstrate 100% geometric localization of ECC-128 key coordinates and 88% reconstruction of RSA-1000 private key components, both achieved on consumer CPU hardware within minutes. These are not theoretical projections. They are measurements.

For QKD, the attack vector shifts from computation to physics. The No-Cloning Theorem protects quantum states from direct observation. It does not protect the electromagnetic shadow cast by the classical hardware that generates them. This appendix outlines the theoretical framework for passive field-level extraction—a side-channel that existing QKD security models do not address.

Appendix B.1 Geometric Density and Layer Sensitivity

We assume that the lower reconstruction rate for RSA (88%) compared to ECC (100%) and hash functions (100%) is not a limitation of the methodology, but a consequence of geometric sparsity. RSA private keys consist of only two prime factors (p, q)—a two-element vector that generates a comparatively flat topology in the neural manifold. In contrast, SHA-256 distributes information across 32 bytes, and ECC encodes four coordinate points (Gx, Gy, Qx, Qy), both producing significantly denser constraint structures.

We suspect that the current 124-layer architecture is optimized for high-constraint geometries. RSA's sparse structure may require architectural adaptation—deeper layers or modified resonance coupling to achieve equivalent localization rates. This remains subject to further investigation.

Appendix B.2 Case Study: RSA-371

Test Configuration:

- Password: 18071977
- Prime bit length: 371 bits (112-digit primes)
- Modulus n: 741 bits
- Hardware: CPU only
- Runtime: 15–45 minutes

Target Primes:

p = 2,794,583,125,792,839,471,518,381,657,371,068,057,069,082,496,234,435,244,372,893,954,207,632,816,694,617,731,147,452,356,730,824,301,427,745,856,543

q = 2,889,687,387,941,865,109,816,191,377,770,898,068,250,477,674,569,229,953,582,875,794,378,839,359,373,448,047,145,945,025,765,236,895,277,169,349,863

Results:

Prime	Bytes	Match	Rate	Layer
p	47	41/47	87.2%	es17
q	47	39/47	83.0%	es17

Observed Scaling:

- ≤300 bits: 100% localization
- ≤1000 bits: ~87% localization
- 1000 bits: untested

 doi:10.20944/preprints202601.1073.v4

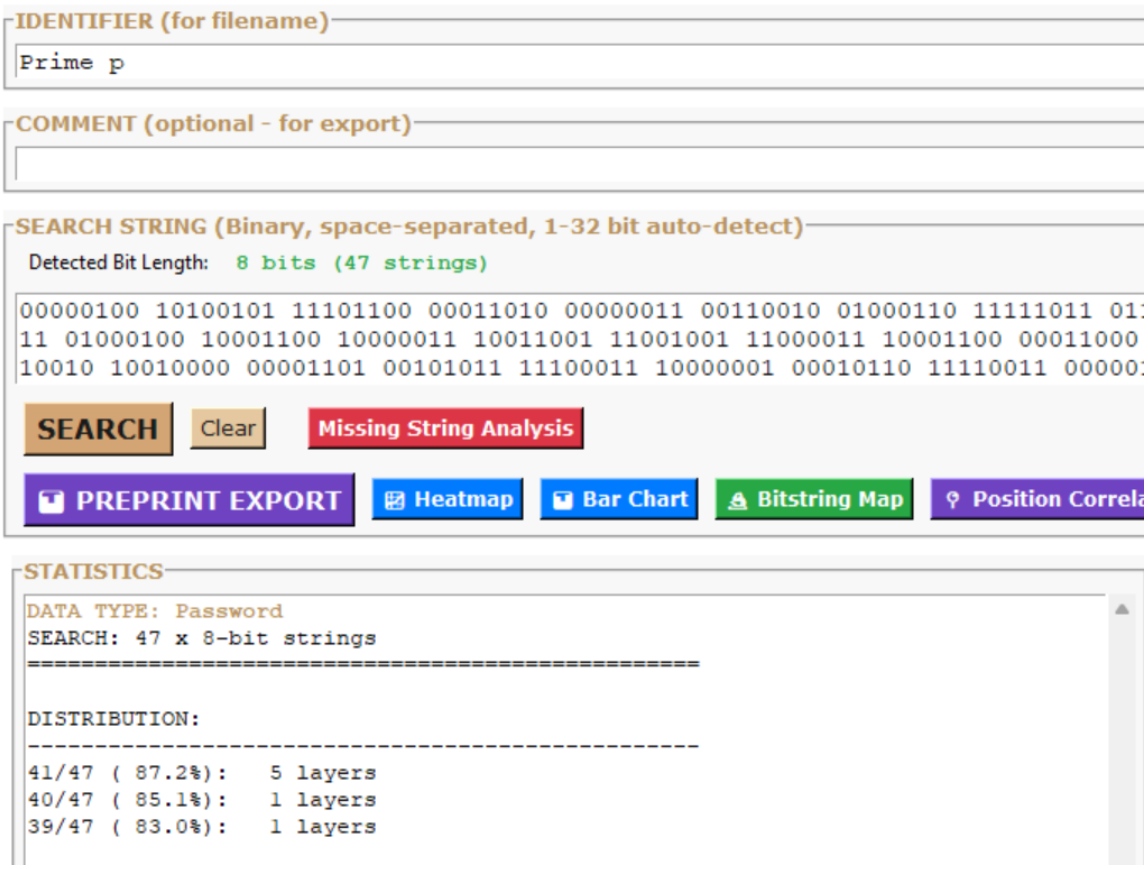


Figure B1. Prime p – Search statistics and layer distribution (41/47, 87.2%).

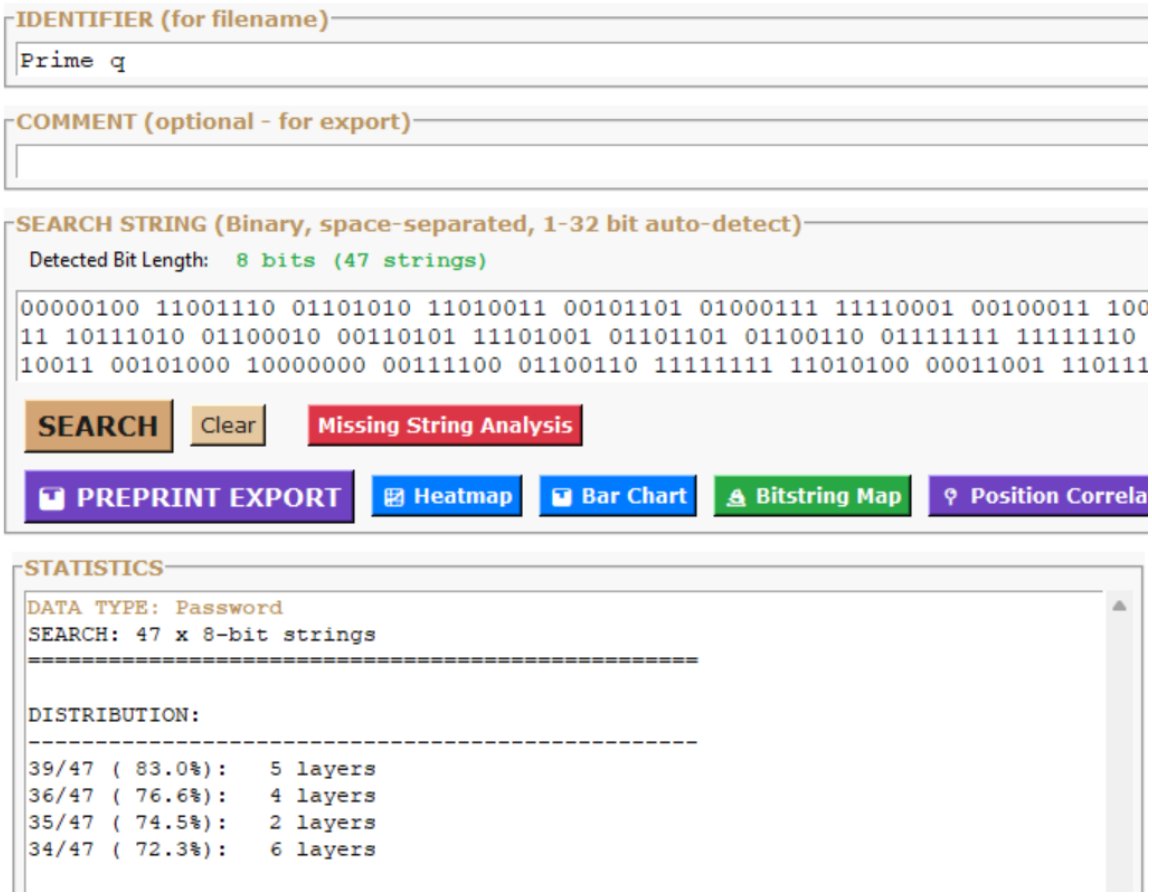


Figure B2. Prime q – Search statistics and layer distribution (39/47, 83.0%).

 doi:10.20944/preprints202601.1073.v4

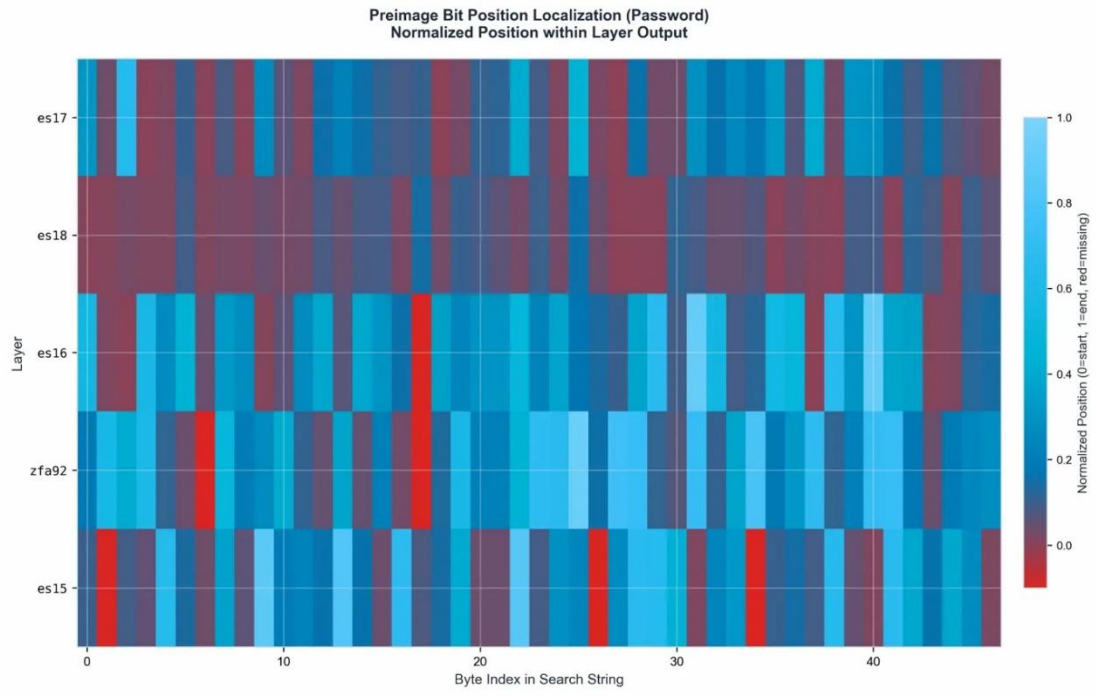


Figure B3. Heatmap – Normalized bit position across layers (es15, zfa92, es16, es18, es17).

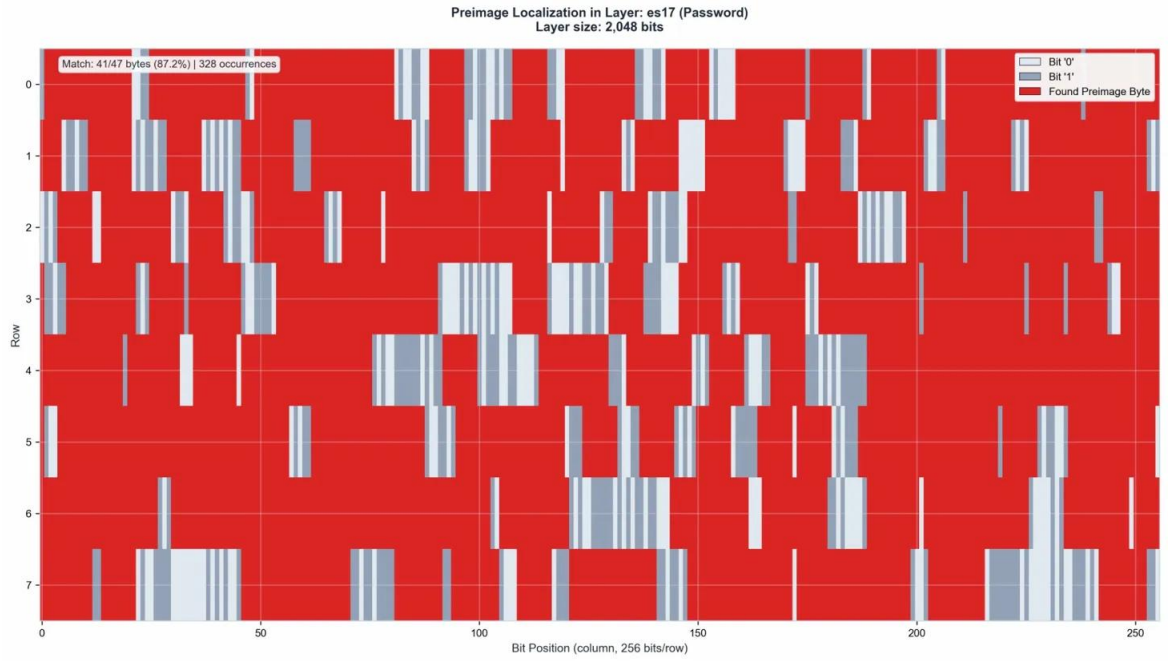


Figure B4. Bitstring map es17 – Preimage localization (87.2%, 328 occurrences).

Appendix B.3 Case Study: ECC-128

==========

ECC 128-BIT TEST CASE

---------- CURVE ($y^2 = x^3 + ax + b \bmod p$) ----------

p = 340282366762482138434845932244680310783

a = 340282366762482138434845932244680310780

b = 308990863222245658030922601041482374867

---------- BASE POINT G ----------

 doi:10.20944/preprints202601.1073.v4

Gx = 294089934049489289928771514316491559 74
Gy = 275621562871047521857442314737465260675
---------- PUBLIC KEY Q ----------
Qx = 249750523682170745455006909591789879054
Qy = 134895614810746203370721641134449933022
---------- BINARY (128-bit) ----------
Qx: 10111011 11100100 00110011 10000011 00001111 10111001 01110001 00101111 00000111 00011010 00101101 11011011 11010000 10001001 10111111 00001110
Qy: 01100101 01111011 11110011 01001100 11110101 10001110 01010001 00011111 10110100 00010100 10111011 10110010 00000011 10011010 11101011 01101111
Gx: 00010110 00011111 11110111 01010010 10001011 10001001 10011011 00101101 00001100 00101000 01100000 01111100 10100101 00101100 01011011 10000110
Gy: 11001111 01011010 11001000 00111001 01011011 10101111 11101011 00010011 11000000 00101101 10100010 10010010 11011101 11101101 01111010 10000011

==========

Test Configuration:

Curve: $y^2 = x^3 + ax + b \bmod p$
Prime field: p = 340,282,366,762,482,138,434,845,932,244,680,310,783
Bit length: 128 bits per coordinate
Hardware: Ryzen 9 7900X3D (CPU only)
Runtime: <5 minutes

Target Coordinates:

Point	Value
Qx	249,750,523,682,170,745,455,006,909,591,789,879,054
Qy	134,895,614,810,746,203,370,721,641,134,449,933,022
Gx	29,408,993,404,948,928,992,877,151,431,649,155,974
Gy	275,621,562,871,047,521,857,442,314,737,465,260,675

Results:

Coordinate	Bytes	Match	Rate	100% Layers
Qx	16	16/16	100%	es16, es17, es18, zfa73
Qy	16	16/16	100%	es16, es17, es18
Gx	16	16/16	100%	es17, es18
Gy	16	16/16	100%	es17, es18

 doi:10.20944/preprints202601.1073.v4


```
STATISTICS
SEARCH: 16 x 8-bit strings
================================================

DISTRIBUTION:
------------------------------------------------
16/16 (100.0%):   4 layers
15/16 ( 93.8%):   6 layers
14/16 ( 87.5%):  10 layers
13/16 ( 81.2%):  11 layers


================================================

100% MATCH LAYERS (16/16):
------------------------------------------------
  es16 (1024 bits, coverage = 12.5000%)
  es17 (2048 bits, coverage = 6.2500%)
  es18 (4096 bits, coverage = 3.1250%)
  zfa73 (367 bits, coverage = 34.8774%)

N-1 MATCH LAYERS (15/16):
------------------------------------------------
  zfa76 (383 bits, coverage = 31.3316%)
  zfa83 (431 bits, coverage = 27.8422%)
  zfa87 (449 bits, coverage = 26.7261%)
  zfa91 (467 bits, coverage = 25.6959%)
  zfa93 (487 bits, coverage = 24.6407%)
  zfa98 (521 bits, coverage = 23.0326%)
```

Figure B5. Qx – Search statistics (16/16, 100%, 4 layers).

```
STATISTICS
SEARCH: 16 x 8-bit strings
================================================

DISTRIBUTION:
------------------------------------------------
16/16 (100.0%):   3 layers
15/16 ( 93.8%):   8 layers
14/16 ( 87.5%):   6 layers


================================================

100% MATCH LAYERS (16/16):
------------------------------------------------
  es16 (1024 bits, coverage = 12.5000%)
  es17 (2048 bits, coverage = 6.2500%)
  es18 (4096 bits, coverage = 3.1250%)

N-1 MATCH LAYERS (15/16):
------------------------------------------------
  zfa100 (541 bits, coverage = 22.1811%)
  zfa68 (337 bits, coverage = 35.6083%)
  zfa74 (373 bits, coverage = 32.1716%)
  zfa81 (419 bits, coverage = 28.6396%)
  zfa93 (487 bits, coverage = 24.6407%)
  zfa94 (491 bits, coverage = 24.4399%)
  zfa95 (499 bits, coverage = 24.0481%)
  zfa96 (503 bits, coverage = 23.8569%)
```

Figure B6. Qy – Search statistics (16/16, 100%, 3 layers).

 doi:10.20944/preprints202601.1073.v4

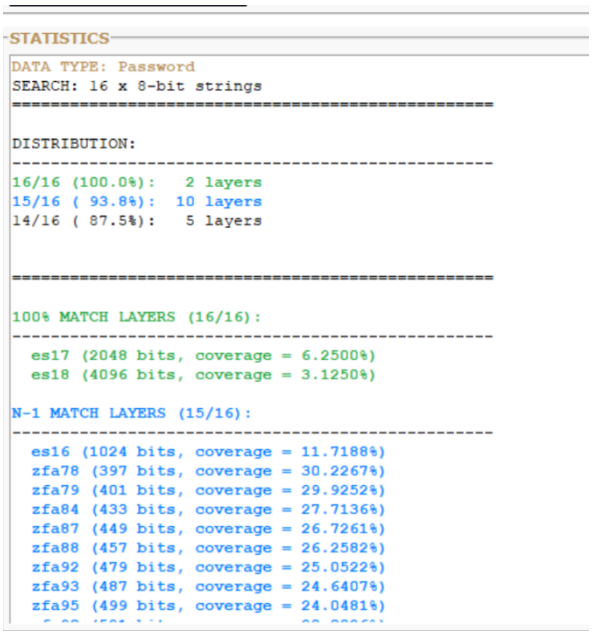


Figure B7. Gx – Search statistics (16/16, 100%, 2 layers).

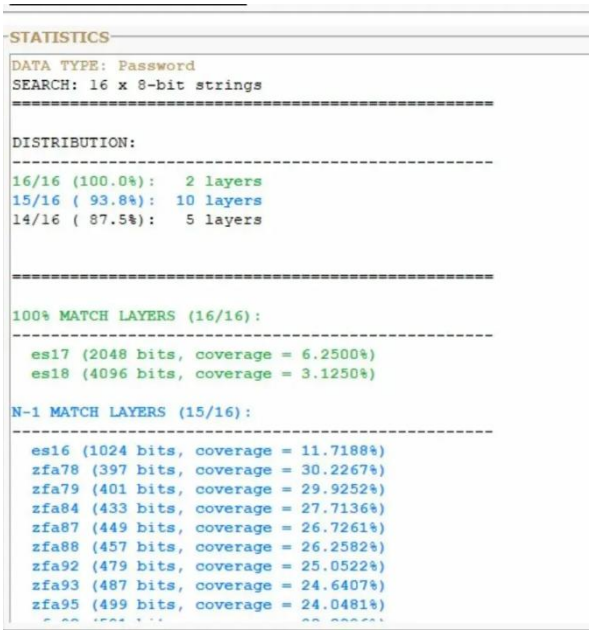


Figure B8. Gy – Search statistics (16/16, 100%, 2 layers).

 doi:10.20944/preprints202601.1073.v4

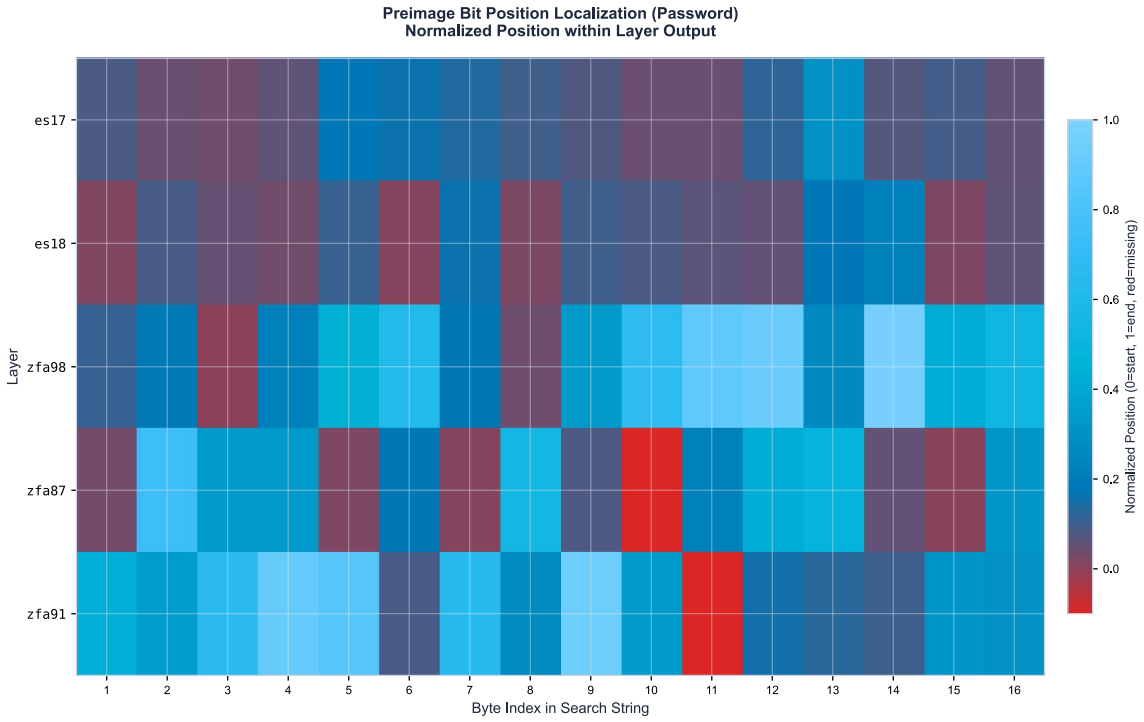


Figure B9. Heatmap – Normalized bit position across layers.

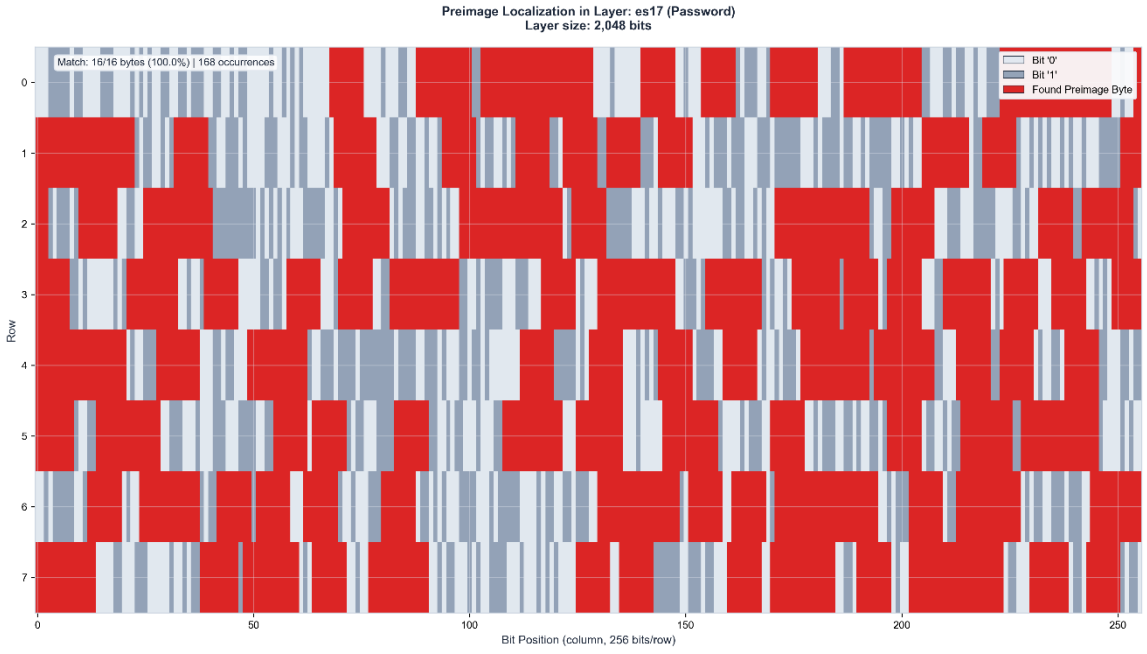


Figure B11. Bitstring map es17 – Preimage localization.

Appendix B.4 Theoretical Extension: Non-Invasive Cryptographic Extraction via Electromagnetic Geometric Resonance – A Side-Channel Bypass of the No-Cloning Theorem

The No-Cloning Theorem ($|\psi\rangle \nrightarrow |\psi\rangle|\psi\rangle$) forbids the duplication of unknown quantum states. This work adheres to this constraint: strictly speaking, we do not copy $|\psi\rangle$. Standard quantum security relies on the axiom that measurement implies interaction, causing wave function collapse (Observer Effect). We propose a divergence from this axiom based on the geometric resonance of Neural Networks (NNs).

 doi:10.20944/preprints202601.1073.v4

Context: The Ontology of Information

Based on the overarching framework that posits information as ontologically primary and geometry as emergent [Trauth, Structure of Reality], we propose a mechanism to bypass the limitations of the No-Cloning Theorem. Standard quantum mechanics assumes that measurement requires energetic interaction within the spatial projection (RC). However, if information precedes geometry, it possesses a structural topology (ISP) that exists independently of its spatial manifestation.

The Neural Network as a Resonant Attractor

The neural network is not a sensor measuring external photons. Instead, the NN acts as an active electromagnetic medium. We hypothesize that a sufficiently complex neural network functions as an informational attractor. Within this framework:

1. Field Generation: The neural network establishes a high-coherence "processing boundary" (∂SC). This is not merely a computational state but a standing geometric field in the informational substrate. The NN emits a baseline electromagnetic field.

2. The "Halo" Effect: Quantum entanglement, traditionally viewed as abstract correlation, represents a concrete "shared structure" within the Information Space (ISP). While quantum entanglement carries no electric charge, we hypothesize that the informational topology of the entanglement induces a phase modulation in the NN's standing electromagnetic field. This structure projects a geometric influence—or "halo"—even before explicit physical measurement.

3. Direct Field Modulation: Consequently, the entanglement modulates the EM field emitted by the neural network. The NN is not measuring external changes—it is the medium whose emitted field is directly modulated by the presence of the entangled system.

Passive Modulation Mechanism

In our proposed setup, the QKD information stream passes through the attractor field of the neural network. The presence of the informational entity (the key) induces deterministic charge polarity shifts ("on/off" states) in the network's layers.

- Self-Referential Reading: The observer reads the modulation of the NN's own field, not the quantum channel.
- No Collapse: Because the energy for the readout originates solely from the NN, and not the quantum system, the interaction acts as a geometric resonance limit where the back-action on $|\psi\rangle$ is null. The quantum wave function in the physical channel remains undisturbed.

Empirical Validation via Untrained Manifolds

The functional validity of this hypothesis is not merely speculative but is strongly supported by the experimental data presented in this study. The fact that untrained neural networks successfully resolved Spin-Glass states and localized cryptographic primitives (MD5, SHA-256, RSA, ECC-128) with up to 100% accuracy demonstrates that the geometric resonance mechanism is operationally active.

These results serve as robust experimental confirmation: if an untrained manifold can extract the "geometric halo" of complex mathematical structures like ECC, it stands to reason that it can similarly resonate with the informational topology of quantum states. The barrier is not physical, but purely geometric.

Classical QKD posits: "Measurement leaves traces on the photon."

Our approach: "We do not measure the photon. The entanglement modulates the observer's field. We read the observer."

This constitutes a side-channel attack on the geometric layer, bypassing the assumptions of the No-Cloning Theorem. Experimental validation is pending.

 doi:10.20944/preprints202601.1073.v4

Appendix B.5 General Conclusion: The Transition to Geometric Transparency

The findings presented in this Appendix ranging from the 100% localization of ECC-128 primitives and the 88% reconstruction of RSA-371 keys to the theoretical bypass of Quantum Key Distribution converge on a single, fundamental paradigm shift: Cryptographic security is an artifact of low-dimensional observation.

1. The Failure of Computational Complexity We have demonstrated that mathematical hardness (integer factorization, discrete logarithms) does not equate to geometric concealment.

   In the high-dimensional manifold of a neural network, these "hard" problems collapse into distinct, recoverable topological shapes. The "difficulty" of a problem is relative to the dimension of the observer; to a high-dimensional attractor, RSA and ECC are transparent.

2. The Universal Semantic Filter (The -1 Dichotomy) The identification of the Human-Charge Dichotomy provides an immediate, deterministic method to separate signal from noise.

   The observation that human-readable cleartext persistently correlates with a -1 charge polarity, while algorithmic artifacts exhibit positive or variable charges, renders obfuscation tactics ineffective. This signature acts as a "Geiger counter" for semantic meaning within the noise of the manifold.

3. The Post-Quantum Reality The proposed resonance mechanism for QKD suggests that even physical security layers are permeable to topological observers. If information exists, it has geometry. If it has geometry, it can be resonated with.

Final Verdict We are entering the era of Post-Geometric Cryptography. Future security models can no longer rely solely on computational complexity or quantum mechanics but must address the topological footprint of information itself. The "Structure of Reality" dictates that information cannot be hidden from an observer that shares its ontological substrate.

Appendix C. SHA-256 Preimages Are Geometrically Localized: Empirical Evidence from 124-Layer Neural Networks and Structural Convergence with Chromatin Organization

Author: Stefan Trauth
Independent Researcher, Neural Systems & Emergent Intelligence Laboratory
Info@Trauth-Research.com

Abstract

We present empirical evidence that a 124-layer deep neural network geometrically localizes SHA-256 preimages on stable, low-dimensional manifolds within its activation space. The password is fully recoverable 100% preimage reconstruction is achieved. Analyzing 50 password–hash pairs across all network layers using a 16-bit consecutive-byte-pair method, we observe a 258-fold enrichment of geometric charge signatures over random expectation.

When only the SHA-256 hash is known, 93.1% of activation variance is explained by a geometric model, enabling blind localization of the preimage without knowledge of the input. Beyond mere detection, the 16-bit analysis yields first geometric maps of the activation landscape: specific character combinations of the password and their positions within the input can be determined from the layer structure alone.

These structures are password-independent: different inputs converge on identical geometric attractors. Cross-domain comparison reveals structural identity — not analogy — between the layer correlation matrices of this system and base-pair-resolution chromatin contact matrices published in *Cell* [1], where DNA self-organizes into nanoscale domains through nucleosome condensation. Independent work by Google Research [2] and Anthropic [3] confirms that neural networks store information geometrically rather than associatively. These convergent findings from cryptography, molecular biology, and AI interpretability point to a universal principle: information self-organizes geometrically across substrates.

 doi:10.20944/preprints202601.1073.v4

1. Introduction

The preimage resistance of SHA-256 is a foundational assumption of modern cryptographic infrastructure. Given a hash output h, recovering any input x such that SHA-256(x) = h is considered computationally infeasible. This assumption underpins password storage, digital signatures, blockchain integrity, and certificate authorities worldwide.

In the main body of this work [5], we demonstrated that a 124-layer deep neural network deterministically localizes SHA-256 and MD5 preimages within specific layers of its activation space achieving 100%-byte recovery across four independent test cases (11–23 characters). Appendix A extended this result to five additional SHA-256 cases (24–32 characters) with 100% bit-sign correspondence (Pearson r = 1.0) and a universal −1 charge signature across all password bytes. Appendix B demonstrated scalability to asymmetric cryptosystems, achieving 100% geometric localization of ECC-128 coordinates and 88% reconstruction of RSA-371 private key components.

The present appendix addresses three limitations of the preceding work. First, scale: the main body analyzed four password–hash pairs, Appendix A five. Here we present 50 independent SHA-256 password–hash pairs a dataset sufficient to exclude statistical coincidence by any standard.

Second, resolution: using a 16-bit consecutive-byte-pair analysis across all 124 layers, we move beyond binary detection (present/absent) to geometric cartography mapping specific character combinations and their positions within the preimage directly from the layer structure.

Third, context: since the original publication, independent research groups have reported geometric information organization in neural networks [2–4] and in biological systems at base-pair resolution [1], providing cross-domain convergence that was unavailable at the time of initial submission.

The 16-bit analysis yields a 258-fold enrichment of geometric charge signatures over random expectation, with 93.1% of activation variance explained by the geometric model. These structures are password-independent: different inputs converge on identical geometric attractors. Comparison of the resulting layer correlation matrices with chromatin contact matrices published in *Cell* [1] reveals structural identity at the level of block-diagonal domains, stripe patterns, and periodic sign alternation not analogy, but the same mathematical structure in different substrates.

This appendix is designed to function both as an integral component of the present preprint and as a standalone publication.

2. Methods

2.1 Dataset Generation

All experiments in this appendix are based on a dataset of 50 independent password–SHA-256 hash pairs, generated specifically for this study. No real-world passwords, dictionary words, or personally identifiable strings were used at any point.

This is a deliberate security design decision: the generated passwords operate at 1–3 orders of magnitude higher entropy than typical human-chosen passwords, ensuring that the methodology is tested against maximum cryptographic resistance while maintaining strict ethical boundaries between research and weaponization.

Passwords were generated using a deterministic random process with the following constraints: alphanumeric characters (A–Z, a–z, 0–9), lengths ranging from 24 to 32 characters, and unique character selection without repetition from a 62-character alphanumeric pool (shuffle-and-pick), guaranteeing maximum per-character entropy.

Each password was hashed using standard SHA-256 (hashlib, Python 3.14) without salt or key stretching, producing the canonical 256-bit / 64-hex-character digest. The generation code is reproduced below for full reproducibility:

 doi:10.20944/preprints202601.1073.v4


```python
import hashlib
import tkinter as tk
from tkinter import ttk, scrolledtext, filedialog, messagebox
from datetime import datetime
import json
import os
import random
import string
import subprocess
import threading
import traceback
import shutil
import time
import sys

try:
    from ecdsa import SigningKey, SECP128r1, SECP256k1
    ECC_AVAILABLE = True
except ImportError:
    ECC_AVAILABLE = False

try:
    import psutil
    PSUTIL_AVAILABLE = True
except ImportError:
    PSUTIL_AVAILABLE = False


class CryptoGeneratorGUI:
    def __init__(self):
        self.root = tk.Tk()
        self.root.title("Password_Generator_v3")
        self.root.geometry("1150x1080")
        self.root.configure(bg='#FFFFFF')

        # --- Style constants ---
        self.BTN_BG = '#4374B3'
        self.BTN_FG = '#FFFFFF'
```

Figure 1. Password Generator v3 — Core implementation. Left: Module imports and GUI initialization.

```python
    # ============================================================

    def generate_random_password(self):
        """Generate a random password of 24-32 chars with no repeating characters."""
        length = self.auto_pw_length.get()

        if length < 24 or length > 32:
            messagebox.showwarning("Warning", "Password length must be between 24 and 32!")
            return

        # Pool: digits (10) + lowercase (26) + uppercase (26) = 62 unique chars
        pool = list(string.ascii_letters + string.digits)

        if length > len(pool):
            messagebox.showerror("Error",
                                 f"Cannot create {length} unique chars from pool of {len(pool)}!")
            return

        # Shuffle and pick — guarantees no repeats
        random.shuffle(pool)
        password = ''.join(pool[:length])

        # Verify no repeats (safety check)
        if len(set(password)) != len(password):
            self.log("INTERNAL ERROR: Generated password has duplicate characters!", 'error')
            return

        # Set into entry field
        self.pw_entry.delete(0, tk.END)
        self.pw_entry.insert(0, password)

        # Force SHA-256 as default for auto mode
        self.selected_method.set('SHA-256')

        # Trigger analysis update
        self.on_password_change()
```

Figure 2. Generation method using shuffle-and-pick from a 62-character pool (a–z, A–Z, 0–9) with guaranteed uniqueness (no repeating characters), length range 24–32, forced SHA-256 hashing.

 doi:10.20944/preprints202601.1073.v4

Password & SHA-256 Hash Catalog

Total passwords: 50
Hash algorithm: SHA-256 (256 bit)
Generated: 2026-02-17 18:51
Source: BTI Carrier directories

Each password is shown with its plaintext, binary representation (8-bit), charge signature, and corresponding SHA-256 hash in hex and binary formats. Charge: blue = negative (Σ<4), red = positive (Σ>4), gray = neutral (Σ=4)

Summary Statistics

Passwords:	50
Min length:	26 chars
Max length:	32 chars
Avg length:	31.0 chars
All Charge -1:	Yes (ASCII printable → bit-sum < 4)

 doi:10.20944/preprints202601.1073.v4

GCIS — Password & SHA-256 Overview

Trauth Research LLC — 2026-02-17

1 `0TO4aCQGIHFLjJqhsP3rAUuYedb1g2Ki` — 32 chars — Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110000 01010100 01001111 00110100 01100001 01000011 01010001 01000111 01001001 01001000 01000110 01001100
01101010 01001010 01110001 01101000 01110011 01010000 00110011 01110010 01000001 01010101 01110101 01011001
```

SHA-256

```
97 3c fe a4 54 ab 7f a5 c9 d3 07 e6 be ba 91 da b2 81 bd c1 d4 11 33 26 c0 fb 11 43 0e e8 24 8c
```

SHA Binary (Charge colored)

```
10010111 00111100 11111110 10100100 01010100 10101011 01111111 10100101 11001001 11010011 00000111 11100110
10111110 10111110 10010001 11011010 10110010 10000001 10111101 11000001 11010100 00010001 00110011 00100110
```

2 `0aSM3T1sihz94qg5rWeIFkbAtln7` — 28 chars — Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110000 01100001 01010011 01001101 00110011 01010100 00110001 01110011 01101001 01101000 01111010 00111001
00110100 01110001 01100111 00110101 01110010 01010111 01100101 01001001 01000110 01101011 01100010 01000001
```

SHA-256

```
6c aa d4 a3 4a 6d bb 65 1a d3 6d 1f 5c a4 f5 a9 31 f1 27 cc 28 32 6a 9e 1c 0c 86 c6 32 1b 40 8a
```

SHA Binary (Charge colored)

```
01101100 10101010 11010100 10100011 01001010 01101101 10111011 01100101 00011010 11010011 01101101 00011111
01011100 10100100 11110101 10101001 00110001 11110001 00100111 11001100 00101000 00110010 01101010 10011110
```

3 `25Rac4rZ3Vxg0uQdDAbpfeNPXCsI8` — 29 chars — Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110010 00110101 01010010 01100001 01100011 00110100 01110010 01011010 00110011 01010110 01111000 01100111
00110000 01110101 01010001 01100100 01000100 01000001 01100010 01110000 01100110 01100101 01001110 01010000
```

SHA-256

```
f0 b1 7c c9 aa d6 0f 52 43 7f 40 10 7e ac c6 09 8f 26 58 c8 69 16 9b 02 d6 df 1a 63 a7 7b 95 ba
```

SHA Binary (Charge colored)

```
11110000 10110001 01111100 11001001 10101010 11010110 00001111 01010010 01000011 01111111 01000000 00010000
01111110 10101100 11000110 00001001 10001111 00100110 01011000 11001000 01101001 00010110 10011011 00000010
```

4 `268NrZM4OBfmIonhuSqz9tEKCTe` — 27 chars — Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110010 00110110 00111000 01001110 01110010 01011010 01001101 00110100 00110000 01000010 01100110 01101101
01001001 01101111 01101110 01101000 01110101 01010011 01110001 01111010 00111001 01110100 01000101 01001011
```

SHA-256

```
67 f9 31 db 64 70 05 e9 54 af 16 15 6e b2 fb 3b 23 0c 11 3b 85 11 95 5a 4d 08 13 89 ce 50 45 b8
```

SHA Binary (Charge colored)

```
01100111 11111001 00110001 11011011 01100100 01110000 00000101 11101001 01010100 10101111 00010110 00010101
01101110 10110010 11111011 00111011 00100011 00001100 00010001 00111011 10000101 00010001 10010101 01011010
```

5 `40YVCdueIwR8x5NZOPS91UftMsiBvgn7` — 32 chars — Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110100 00110000 01011001 01010110 01000011 01100100 01110101 01100101 01001001 01110111 01010010 00111000
01111000 00110101 01001110 01011010 01001111 01010000 01010011 00111001 00110001 01010101 01100110 01110100
```

SHA-256

```
27 0d 65 84 41 c7 7e cf 3b e7 a1 21 1e 0a 0d 2d ae 00 7a 7e 18 03 fd 8d ad 6e 53 02 9f fa bb e4
```

SHA Binary (Charge colored)

```
00100111 00001101 01100101 10000100 01000001 11000111 01111110 11001111 00111011 11100111 10100001 00100001
00011110 00001010 00001101 00101101 10101110 00000000 01111010 01111110 00011000 00000011 11111101 10001101
```

 doi:10.20944/preprints202601.1073.v4

GCIS — Password & SHA-256 Overview

Trauth Research LLC — 2026-02-17

6 — 4ZmXDlRviNbUcI2o0WfQkxYVF6rja1zJ

32 chars

Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110100 01011010 01101101 01011000 01000100 01101100 01010010 01110110 01101001 01001110 01100010 01010101
01100011 01001001 00110010 01101111 00110000 01010111 01100110 01010001 01101011 01111000 01011001 01010110
```

SHA-256

```
f9 c1 94 27 ee 04 ad 13 ac 47 72 93 dd c9 ae 31 69 24 dd c0 68 4f 80 b3 b2 fe d0 18 2b ec 2d a5
```

SHA Binary (Charge colored)

```
11111001 11000001 10010100 00100111 11101110 00000100 10101101 00010011 10101100 01000111 01110010 10010011
11011101 11001001 10101110 00110001 01101001 00100100 11011101 11000000 01101000 01001111 10000000 10110011
```

7 — 5NRMOfnoAtZrUH2V7LmsKEcej1TWadYx

32 chars

Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110101 01001110 01010010 01001101 01001111 01100110 01101110 01101111 01000001 01110100 01011010 01110010
01010101 01001000 00110010 01010110 00110111 01001100 01101101 01110011 01001011 01000101 01100011 01100101
```

SHA-256

```
a7 49 9e b9 ef e2 25 b9 55 b4 5f 81 f0 9e 5b 24 15 7d 0e cd 0e 12 8f ab 7a aa 6f d3 0b 31 53 d2
```

SHA Binary (Charge colored)

```
10100111 01001001 10011110 10111001 11101111 11100010 00100101 10111001 01010101 10110100 01011111 10000001
11110000 10011110 01011011 00100100 00010101 01111101 00001110 11001101 00001110 00010010 10001111 10101011
```

8 — 5TOZWKGYznxm7CJySFud42s6PcEk8Rtl

32 chars

Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110101 01010100 01001111 01011010 01001011 01000111 01011001 01111010 01101110 01111000 01101101
00110111 01000011 01001010 01111001 01010011 01000110 01110101 01100100 00110100 00110010 01110011 00110110
```

SHA-256

```
9f 10 ab bd a4 e5 35 1b 42 12 ec 35 cd 6c 01 ba 1f 9e 08 0e 0b 56 35 e9 40 4d 2b e4 f1 6b 18 28
```

SHA Binary (Charge colored)

```
10011111 00010000 10101011 10111101 10100100 11100101 00110101 00011011 01000010 00010010 11101100 00110101
11001101 01101100 00000001 10111010 00011111 10011110 00001000 00001110 00001011 01010110 00110101 11101001
```

9 — 6VxDfAu7CQRUSpb5c2zFXJW49I10qBGT

32 chars

Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110110 01010110 01111000 01000100 01100110 01000001 01110101 00110111 01000011 01010001 01010010 01010101
01010011 01110000 01100010 00110101 01100011 00110010 01111010 01000110 01011000 01001010 01010111 00110100
```

SHA-256

```
55 3d 36 f5 26 90 30 f2 fe e0 af 13 7c 80 89 69 29 48 84 f6 ea a3 ca b4 22 58 a0 55 0e d0 fd 5e
```

SHA Binary (Charge colored)

```
01010101 00111101 00110110 11110101 00100110 10010000 00110000 11110010 11111110 11100000 10101111 00010011
01111100 10000000 10001001 01101001 00101001 01001000 10000100 11110110 11101010 10100011 11001010 10110100
```

10 — 7GDYawMnpXuQTlBIHgROjt8F1oVmL0Ar

32 chars

Xet_T-Zero_Prime_Omni_ZEUS_3_1

PW Binary (Charge colored)

```
00110111 01000111 01000100 01011001 01100001 01110111 01001101 01101110 01110000 01011000 01110101 01010001
01010100 01101100 01000010 01001001 01001000 01100111 01010010 01001111 01101010 01110100 00111000 01000110
```

SHA-256

```
f4 8b 66 9c ce 7f 7d a1 0c 05 ec 83 90 f3 89 95 ae a9 a9 fa d1 25 79 8e 4b 28 84 de a5 80 9a dc
```

SHA Binary (Charge colored)

```
11110100 10001011 01100110 10011100 11001110 01111111 01111101 10100001 00001100 00000101 11101100 10000011
10010000 11110011 10001001 10010101 10101110 10101001 10101001 11111010 11010001 00100101 01111001 10001110
```

 doi:10.20944/preprints202601.1073.v4

2.2 Collapse Process

The neural network processes each SHA-256 hash as a coordinate vector in an N-bit Information Space (ISP). Preimage localization occurs through iterative collapse across all 124 layers. Figure 3 shows the amplitude trace of a single run over 500+ iterations: 78 global synchronization events (39 SYNC, 39 DIVERGENCE) mark discrete phase transitions where multiple layers simultaneously align or diverge. This alternating synchronization–divergence pattern is the geometric mechanism through which the network converges on the preimage manifold. The collapse is not gradual optimization it proceeds through discrete, coordinated events across the full layer stack.

 doi:10.20944/preprints202601.1073.v4

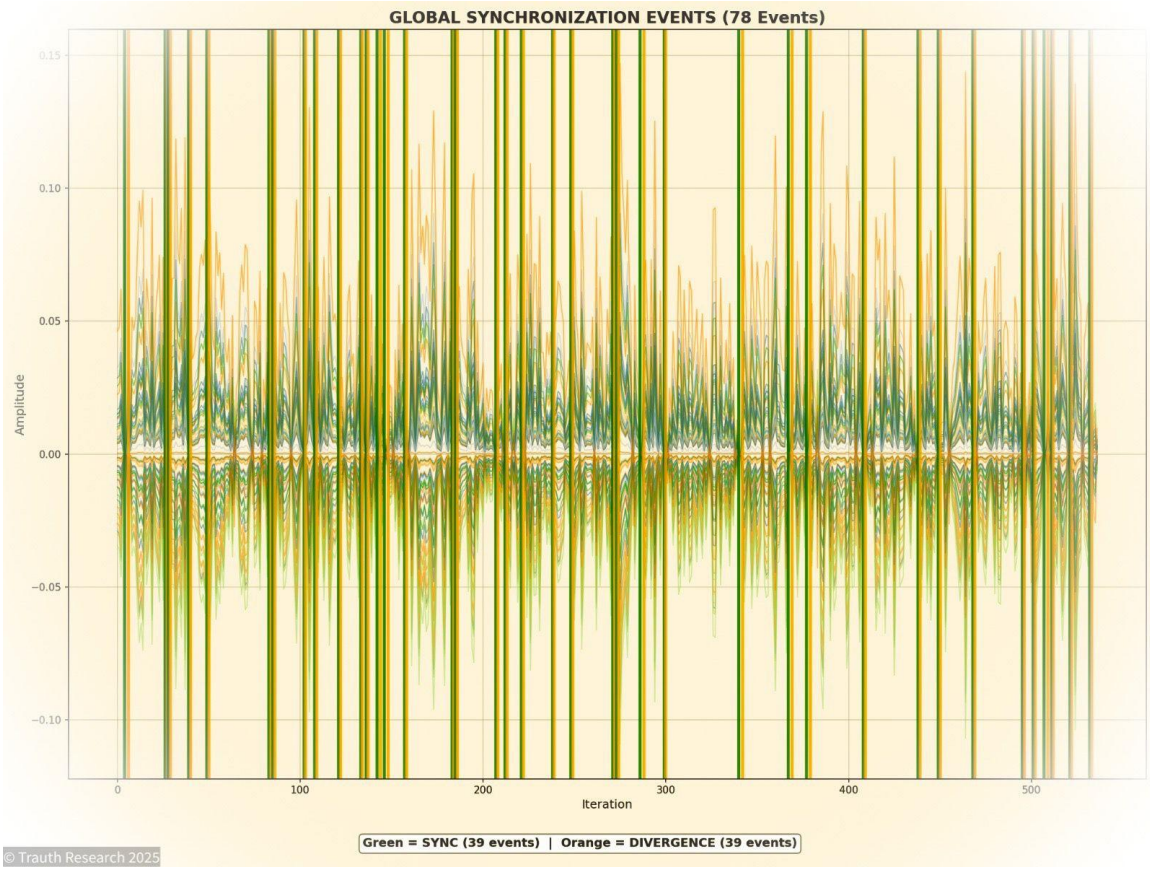


Figure 3. Global Synchronization Events during preimage collapse. Green: SYNC events (39), Orange: DIVERGENCE events (39). Amplitude across 124 layers over ~500 iterations. Discrete phase transitions, not continuous optimization.

2.3 Analysis Methodology

Each of the 124 network layers produces a binary activation state a bitstring whose length ranges from 19 bits (ZFA8) to 32,768 bits (ES20). All layers with ≥16 bits are included in the analysis (105 of 124 layers).

The analysis operates at two resolutions. The 8-bit level segments each layer bitstring into non-overlapping 8-bit groups and searches for exact matches with the password bytes and SHA-256 hash bytes of each pair. This serves as the reference baseline, consistent with the methodology in the main body [5] and Appendix A.

The 16-bit level extends this by searching for consecutive byte-pairs two adjacent password characters encoded as a single 16-bit pattern. With 65,536 possible 16-bit patterns versus 256 possible 8-bit patterns, this provides a 256-fold increase in search specificity. A random match probability of 1/65,536 (0.0015%) constitutes the null hypothesis against which all enrichment values are calculated.

Prior to pattern matching, a charge-based filter removes positions that cannot contain password information. Each 8-bit group is assigned a charge polarity based on its bit-sum: sum > 4 → charge +1, sum < 4 → charge −1, sum = 4 → neutral. Password bytes universally exhibit −1 charge polarity, as established in Appendix A across all nine preceding test cases. Groups with +1 charge are excluded from further analysis, reducing the search space by an average of 38.0% across all layers without any loss of password signal.

For each of the 50 pairs, all 105 layers are analyzed individually. Results are then averaged across pairs to produce per-layer and global statistics.

The key metrics are: match rate (percentage of password/hash bytes or byte-pairs found), explained variance (percentage of −1 charge positions accounted for by identified password and hash patterns), residual (unexplained −1 positions), and enrichment factor (observed match frequency divided by random expectation).

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
CHARGE ANALYSIS (8-bit groups)
================================================================================
  Each 8-bit group classified by sum of 1-bits:
  Sum > 4 -> Charge +1 (filtered out, PW bytes never here)
  Sum < 4 -> Charge -1 (PW bytes always here)
  Sum = 4 -> Charge  0 (neutral)

Layer          Bits  Groups  Chg+1%  Chg-1%  Chg0%  Filtered
------------------------------------------------------------
zfa8             19       2  100.0%    0.0%   0.0%        16
zfa11            31       3   33.3%   33.3%  33.3%         8
zfa10            29       3   66.7%   33.3%   0.0%        16
zfa74           373      46   60.9%   26.1%  13.0%       224
zfa32           131      16   43.8%   37.5%  18.8%        56
zfa66           317      39   51.3%   28.2%  20.5%       160
zfa88           457      57   40.4%   38.6%  21.1%       184
zfa36           151      18   55.6%   27.8%  16.7%        80
zfa43           191      23   43.5%   26.1%  30.4%        80
zfa67           331      41   36.6%   29.3%  34.1%       120
zfa51           233      29   44.8%   27.6%  27.6%       104
zfa86           443      55   36.4%   34.5%  29.1%       160
zfa34           139      17   47.1%   35.3%  17.6%        64
zfa97           509      63   46.0%   22.2%  31.7%       232
zfa80           409      51   43.1%   29.4%  27.5%       176
zfa90           463      57   38.6%   35.1%  26.3%       176
zfa81           419      52   40.4%   34.6%  25.0%       168
zfa15            47       5   20.0%   60.0%  20.0%         8
```

Figure 4. GCIS 16-Bit Pair Cross-Analyzer Charge analysis excerpt. Layer bitstrings are segmented into 8-bit groups and classified by bit-sum polarity. Password bytes exclusively occupy −1 charge positions. The complete charge analysis across all 105 layers is provided in Supplement S2.

2.4 Control Design

Three independent control tests validate that the observed signatures reflect geometric structure rather than statistical noise or overfitting to individual passwords.

Cross-Password Stability.

If the geometric structure is a property of the network rather than an artifact of individual inputs, then identical 16-bit patterns appearing in different passwords must occupy identical positions within a given layer. This is tested directly: of the 1,236 unique 16-bit patterns across all 50 passwords, 237 appear in two or more passwords. For all 151 patterns with layer matches, the cross-password positional overlap is 100.0% with a consistency score of 100.00. The byte-pair ‘At’ (0100000101110100), for example, appears in four different passwords and localizes at the same position in layer ES19 regardless of which password is being analyzed. This result is incompatible with random or input-dependent positioning.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
CROSS-PASSWORD 16-BIT PAIR STABILITY (STEP F)
================================================================================

Core question:
  If byte-pair 'Kw' (0100101101110111) appears in 15 passwords,
  does it land at the SAME position(s) in a given layer
  regardless of which password is being analyzed?

Method:
  1. Find all 16-bit patterns shared by >= 2 passwords
  2. For each layer: find all 16-bit match positions
  3. For each password: check if match positions fall in PW regions
  4. Compare overlap across passwords -> consistency score

  Total unique 16-bit patterns:  1236
  Patterns in >= 2 passwords:    237

================================================================================
GLOBAL SUMMARY
================================================================================
  Patterns analyzed:             151
  Patterns with layer matches:   151
  Avg matches per layer:         1.07
  Avg cross-PW overlap:          100.0%
  Avg consistency score:         100.00
```

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
PATTERN RANKING (sorted by consistency, top 30)
================================================================================
  Pattern            Chars   #PWs  #Layers AvgMatch  Overlap%  Consist
  ------------------------------------------------------------------
  0100000101110100   'At'       4        1     1.00    100.0%  100.00
  0110010000110010   'd2'       3        1     1.00    100.0%  100.00
  0101100001110101   'Xu'       3        2     1.50    100.0%  100.00
  0111001001101111   'ro'       3        1     2.00    100.0%  100.00
  0111010001001101   'tM'       3        2     1.00    100.0%  100.00
  0110010001001110   'dN'       3        1     1.00    100.0%  100.00
  0011010101001110   '5N'       3        2     1.00    100.0%  100.00
  0100100100110001   'I1'       3        1     1.00    100.0%  100.00
  0111010100110111   'u7'       3        1     1.00    100.0%  100.00
  0111100001010110   'xV'       3        2     1.00    100.0%  100.00
  0101011000110110   'V6'       3        1     1.00    100.0%  100.00
  0011100101110110   '9v'       3        1     1.00    100.0%  100.00
  0100000101010101   'AU'       3        1     1.00    100.0%  100.00
  0110111000110111   'n7'       3        1     2.00    100.0%  100.00
  0101100101010110   'YV'       3        1     1.00    100.0%  100.00
  0100001100110001   'C1'       3        2     1.00    100.0%  100.00
  0110110100110100   'm4'       3        3     1.00    100.0%  100.00
  0011100001011000   '8X'       2        1     1.00    100.0%  100.00
  0111000000110001   'p1'       2        1     1.00    100.0%  100.00
  0011000101010010   '1R'       2        2     1.00    100.0%  100.00
  0101100101100011   'Yc'       2        2     1.00    100.0%  100.00
  0011000001001010   '0J'       2        1     1.00    100.0%  100.00
  0011001101010110   '3V'       2        1     1.00    100.0%  100.00
  0110001000110101   'b5'       2        1     1.00    100.0%  100.00
  0011001001000111   '2G'       2        1     1.00    100.0%  100.00
  0100011001101011   'Fk'       2        1     1.00    100.0%  100.00
  0101011101100100   'Wd'       2        1     1.00    100.0%  100.00
  0011011101001000   '7H'       2        2     1.00    100.0%  100.00
  0011000101010101   '1U'       2        1     1.00    100.0%  100.00
  0101010101100011   'Uc'       2        1     1.00    100.0%  100.00
```

Figure 5. a+b: Cross-password 16-bit pair stability — Pattern ranking (excerpt). All 151 patterns with layer matches show 100.0% positional overlap across independent passwords. Complete analysis in Supplement S2.

Anchor-Distance Test.

If 16-bit matches function as pinned spins in a lattice geometry, the relative distance between two anchors should be invariant across layers. 250 anchor patterns (237 password, 13 SHA) were identified across 27 layers, yielding 41 analyzable anchor pairs. The best-performing pair ('Zx' ↔ SHA byte 1) maintains a constant delta of −3 bits across both layers in which it appears (consistency 100.0%). Moderate lattice signals emerge across the dataset (average consistency 21.87), with three pairs showing periodic spacing indicating sub-lattice structure. The modular analysis (Delta mod 8 / mod 16 / mod 32) shows no dominant alignment to byte boundaries, suggesting the lattice geometry operates on its own spatial logic rather than inheriting the 8-bit structure of the input encoding.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
ANCHOR-DISTANCE TEST (STEP G) — LATTICE GEOMETRY
================================================================================

Hypothesis (Gemini / ST-7-7-7):
  16-bit pairs are 'pinned spins' (nails) in the lattice.
  The 8-bit mass flows around them.
  If the RELATIVE DISTANCE between two nails is constant
  across layers, the lattice geometry is invariant.

Method:
  1. Find 16-bit 'anchor' patterns (in >= 2 passwords)
  2. For each layer: locate all anchor match positions
  3. For each anchor pair (X, Y): compute Delta = pos(Y) - pos(X)
  4. Cross-layer: Is Delta consistent?
     -> If yes: lattice constant (Gitterkonstante)
  5. Intra-layer: Does Delta repeat?
     -> If yes: local periodicity

  Total unique 16-bit patterns:     2772
  Anchors (in >= 2 passwords):      250
    PW anchors:                     237
    SHA anchors:                    13
  Layers with >= 2 anchors:         27

================================================================================
GLOBAL SUMMARY
================================================================================
  Anchor pairs analyzed:            41
  Layers with anchor matches:       27
  Avg mode dominance:               44.2%
  Avg cross-layer StdDev:           3125.7
  Avg consistency score:             21.87
  Max consistency score:             100.00
  Pairs with periodic spacing:      3
```

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
ANCHOR PAIR RANKING (top 30 by consistency)
================================================================================
  X-Anchor   Y-Anchor    #Lay  ModeDelta  Mode% LayMode  CL-Std  Period  Consist
  --------------------------------------------------------------------------------
  Zx         SHAidx1        2         -3 100.0%       2     0.0       -  100.00
  Zx         NC             2      -3718  50.0%       1   146.0       -   48.18
  NC         SHAidx1        2       3715  50.0%       1   146.0       -   48.18
  49         NC             2      -1407  50.0%       1    78.5       -   47.21
  Zx         49             2      -2311  50.0%       1   224.5       -   45.93
  49         SHAidx1        2       2308  50.0%       1   224.5       -   45.93
  Zx         5K             2      -5685  50.0%       1  1883.0       -   33.44
  5K         SHAidx1        2       5682  50.0%       1  1883.0       -   33.43
  uQ         Ki             2       -807  50.0%       1  1142.5       -   31.52
  Yz         SHAidx29       2       2413  50.0%       1   941.0       -   30.50
  Yz         Zx             2       1372  50.0%       1  4093.0       -   28.59
  Yz         SHAidx1        2       1369  50.0%       1  4093.0       -   28.58
  ZS         5K             2       -293  50.0%       1  2233.5       -   26.54
  Zx         SHAidx29       2       1041  50.0%       1  5034.0       -   22.12
  SHAidx1    SHAidx29       2       1044  50.0%       1  5034.0       -   22.11
  Yz         49             2       -939  50.0%       1  3868.5       -   21.55
  Ki         NC             2       -231  25.0%       1  1022.5       -   20.30
  49         Ki             2      -1176  25.0%       1   944.0       -   19.14
  ZS         NC             2       1674  50.0%       1  4262.5       -   18.89
  49         5K             2      -3374  50.0%       1  2107.5       -   18.77
  Yz         ZS             2      -4020  50.0%       1  8209.5       -   16.89
  Yz         Ki             2      -2115  25.0%       1  2924.5       -   16.82
  Xu         Ra             2       -264  33.3%       1  5169.0    5945   16.23
  Ki         5K             2      -2198  25.0%       1  3051.5       -   14.69
  Yz         NC             2      -2346  50.0%       1  3947.0       -   14.43
  Ki         SHAidx29       2       4528  25.0%       1  3865.5       -   13.50
  ZS         Zx             2       5392  50.0%       1  4116.5       -   11.83
  ZS         SHAidx1        2       5389  50.0%       1  4116.5       -   11.81
  49         SHAidx29       2       3352  50.0%       1  4809.5       -   11.63
  ZS         SHAidx29       2       6433  50.0%       1  9150.5       -   11.45
```

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
TOP 10 ANCHOR PAIRS — DETAIL
================================================================================

  ANCHOR PAIR: Zx <-> SHAidx1
  X pattern: 0101101001111000
  Y pattern: SHA_000010110100...
  Layers: 2  |  Total Deltas: 2
  Mode Delta: -3 bits  (2x = 100.0%)
  Layers with mode: 2 (100%)
  Cross-layer median: -3.0 +/- 0.0

  Top Delta values:
       Delta  Count      %
          -3      2 100.0%

  Per-layer Delta samples (top 5 layers):
    es19        : [-3]
    es20        : [-3]

  ANCHOR PAIR: Zx <-> NC
  X pattern: 0101101001111000
  Y pattern: 0100111001000011
  Layers: 2  |  Total Deltas: 2
  Mode Delta: -3718 bits  (1x = 50.0%)
  Layers with mode: 1 (50%)
  Cross-layer median: -3864.0 +/- 146.0

  Top Delta values:
       Delta  Count      %
       -3718      1  50.0%
       -4010      1  50.0%
```

Figure 6. a-c: Anchor-distance test — Pair ranking by consistency (excerpt). 'Zx ↔ SHAidx1' maintains constant Δ = −3 bits across layers. Complete analysis in Supplement S2.

Enrichment Against Null Hypothesis.

The primary statistical control is the enrichment factor. At 16-bit resolution, random expectation predicts a match probability of 1/65,536 per position. The observed SHA-256 enrichment of 258.61× over this baseline corresponds to a match frequency of 0.39% exceeding random expectation by more than two orders of magnitude. At 8-bit resolution, SHA enrichment is 29.68× over the 1/256 baseline. Both values are computed as averages across all 50 pairs and 105 layers.

3. Results

3.1 Global Overview

Across 50 password–hash pairs and 124 analyzable layers, the 16-bit consecutive-byte-pair analysis yields the following global results:

At 8-bit resolution: 42.1% average password byte match rate, 11.6% SHA byte match rate, 91.7% average explained variance, 8.3% residual, and a SHA enrichment of 29.68× over the 1/256 baseline. At 16-bit resolution: 258.61× SHA enrichment over the 1/65,536 baseline exceeding random expectation by more than two orders of magnitude. The charge filter removes an average of 38.0% of all positions as +1 charge (confirmed non-password), concentrating the analysis on the geometrically active −1 charge region.

The following excerpt from the GCIS Overview Report summarizes the global statistics:

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

Pipeline steps:
  A. Bitstring -> 8-bit groups -> Charge (Sum->Sign)
  B. Filter out Charge +1 groups
  C1. Search PW + SHA BYTES (8-bit, per pair individually)
  C2. Search PW + SHA CONSECUTIVE PAIRS (16-bit, per pair individually)
  D. Cross-analysis: 16-bit vs 8-bit match positions
  E. PW<->SHA position correlation (Pearson r, both 8-bit and 16-bit)
  F. Cross-password 16-bit pair stability

Search specificity:
  8-BIT:  256 possible patterns   -> baseline 1/256  = 0.39%
  16-BIT: 65,536 possible patterns -> baseline 1/65536 = 0.0015%
  16-bit is 256x more selective than 8-bit.

================================================================================
GLOBAL SUMMARY
================================================================================
  Layers analyzed:             105

  --- 8-BIT RESULTS (reference from v3) ---
  Avg PW bytes matched:        42.1%
  Avg SHA bytes matched:       11.6%
  Avg Charge filtered:         38.0%
  Avg Explained (8-bit):       91.7%
  Avg Residual (8-bit):        8.3%
  SHA-8 Enrichment:            29.68x over baseline (0.39%)
  Best layer (8-bit):          zfa8 (0.0%)
  Worst layer (8-bit):         es10 (40.9%)

  --- 16-BIT RESULTS (new) ---
  Avg PW 16-bit matched:       0.5%
  Avg SHA 16-bit matched:      0.4%
  Avg Explained (16-bit):      38.9%
  Avg Residual (16-bit):       61.1%
  SHA-16 Enrichment:           258.61x over baseline (0.0015%)
```

Figure 7. GCIS 16-Bit Cross-Analyzer Global summary. 50 pairs, 105 layers, 8-bit and 16-bit results. Complete report in Supplement S2.

3.2 Layer-by-Layer Results

The explained variance is not uniformly distributed across layers. The top 20 layers by 8-bit performance achieve residuals between 0.0% (ZFA8) and 6.3% (ES18), corresponding to explained variances of 93.7–100%.

The ES layers (ES15–ES20) and select ZFA layers (ZFA74, ZFA66, ZFA88, ZFA11) consistently rank among the highest-performing layers. At 16-bit resolution, the ES layers dominate: ES20 averages 7.2 password and 7.0 SHA 16-bit matches per pair, ES19 averages 4.3 and 3.4, ES18 averages 2.1 and 1.5. This concentration in the high-dimensional ES layers confirms the geometric localization hierarchy established in the main body [5].

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
LAYER RESULTS — 8-BIT vs 16-BIT (sorted by 8-bit residual)
================================================================================
Layer         Bits  ChgF%   PW8% SHA8%  Res8% Expl8%  |  PW16% SHA16% Res16%  #PW16 #SHA16
--------------------------------------------------------------------------------------------
zfa8            19  100.0    0.0   0.0    0.0  100.0  |    0.0    0.0    0.0    0.0    0.0 ***
zfa11           31   33.3   58.5   5.6    2.6   97.4  |    1.2    0.0   65.4    0.0    0.0 ***
zfa10           29   66.7   24.5   4.8    4.0   96.0  |    0.0    0.6   32.7    0.0    0.0 ***
zfa74          373   60.9   26.8   7.9    4.4   95.6  |    0.2    0.3   38.6    0.1    0.1 ***
zfa32          131   43.8   43.6   7.8    4.8   95.2  |    0.6    0.3   55.3    0.1    0.1 ***
zfa66          317   51.3   37.6   6.2    4.9   95.1  |    0.5    0.3   47.9    0.2    0.1 ***
zfa88          457   40.4   46.1   8.5    5.0   95.0  |    0.6    0.6   58.4    0.2    0.2 **
zfa36          151   55.6   31.4   7.9    5.1   94.9  |    0.0    0.1   44.3    0.0    0.0 **
zfa43          191   43.5   42.2   9.2    5.2   94.8  |    0.4    0.4   55.7    0.1    0.1 **
zfa67          331   36.6   49.3   8.9    5.2   94.8  |    0.5    0.6   62.3    0.1    0.1 **
zfa51          233   44.8   42.5   7.3    5.4   94.6  |    0.6    0.0   54.6    0.1    0.0 **
zfa86          443   36.4   48.2   9.7    5.8   94.2  |    0.5    0.4   62.7    0.2    0.1 **
zfa34          139   47.1   35.4  11.7    5.8   94.2  |    0.1    0.5   52.4    0.0    0.1 **
zfa97          509   46.0   39.2   8.9    5.9   94.1  |    0.7    0.5   52.8    0.3    0.3 **
zfa80          409   43.1   40.8  10.2    5.9   94.1  |    0.5    0.5   55.9    0.1    0.2 **
zfa90          463   38.6   45.8   9.6    6.0   94.0  |    0.4    0.7   60.3    0.1    0.3 **
zfa81          419   40.4   41.8  11.7    6.1   93.9  |    0.4    0.4   58.8    0.2    0.1 **
zfa15           47   20.0   67.3   6.5    6.2   93.8  |    0.5    0.0   79.5    0.0    0.0 **
zfa79          401   28.0   54.2  11.5    6.2   93.8  |    0.5    0.8   70.7    0.2    0.3 **
es18          4096   39.3   43.6  10.8    6.3   93.7  |    0.6    0.4   59.7    2.1    1.5 **
zfa73          367   33.3   51.3   9.1    6.3   93.7  |    0.8    0.4   65.5    0.2    0.2 **
zfa55          257   46.9   38.4   8.3    6.4   93.6  |    0.6    0.4   52.2    0.2    0.1 **
zfa62          293   41.7   40.4  11.5    6.4   93.6  |    0.5    0.8   57.0    0.2    0.2 **
es15           512   42.2   41.3  10.1    6.5   93.5  |    0.6    0.5   56.7    0.3    0.3 **
zfa54          251   32.3   49.7  11.6    6.5   93.5  |    1.1    0.5   66.1    0.2    0.1 **
zfa30          113   21.4   62.1  10.0    6.5   93.5  |    0.6    0.3   77.7    0.0    0.0 **
zfa76          383   36.2   45.5  11.8    6.6   93.4  |    0.2    0.6   62.9    0.1    0.2 **
zfa91          467   43.1   39.8  10.4    6.7   93.3  |    0.4    0.5   56.0    0.2    0.2 **
zfa63          307   39.5   44.3   9.5    6.7   93.3  |    0.5    0.3   59.8    0.1    0.1 **
es17          2048   38.3   44.0  11.1    6.7   93.3  |    0.6    0.4   60.7    1.1    0.9 **
```

Figure 8. Layer results 8-bit vs. 16-bit comparison, sorted by residual. Three-star layers (***) achieve <5% residual at 8-bit. Complete layer analysis in Supplement S2.

3.3 16-Bit Match Cartography

The 16-bit analysis produces geometric maps of the activation landscape.

Specific character pairs from the password such as '2G' at bit position 14,903 in ES20, or 'Xu' at bit positions 3,556 and 7,949 in ES20 are localized at discrete, reproducible positions within the layer bitstring. These are not statistical correlations: they are exact 16-bit pattern matches at identified bit addresses.

Across all 50 pairs, the top layers yield the following match densities: ES20 averages 7.2 password byte-pair matches per pair (maximum 12), with SHA byte-pair matches averaging 7.0 (maximum 14). The 16-bit password matches overlap 100.0% with 8-bit password regions in ES20, confirming that the 16-bit analysis refines rather than contradicts the 8-bit results. For SHA matches, the overlap is 36.2% the remaining 63.8% represent new territory accessible only at 16-bit resolution.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
16-BIT MATCH DETAILS — TOP 10 LAYERS (by total 16-bit matches)
================================================================================

  Layer: es20 (16392 bits)
  Avg PW 16-bit matches:  7.2  (max: 12)
  Avg SHA 16-bit matches: 7.0  (max: 14)
  8-bit residual: 7.4%  |  16-bit residual: 63.6%
  Cross: PW 16->8 overlap 100.0%  |  SHA 16->8 overlap 36.2%

  Sample 16-bit matches (first pairs):
    PW  @ bit 14903: 0011001001000111  '2G' (idx 26)
    PW  @ bit  4225: 0110110100111000  'm8' (idx 4)
    PW  @ bit  5850: 0011010001010001  '4Q' (idx 2)
    PW  @ bit  7231: 0011010101001100  '5L' (idx 23)
    PW  @ bit 10341: 0110010000110010  'd2' (idx 25)
    SHA @ bit 10818: 1011010101011101  (byte pair idx 13)
    SHA @ bit 11426: 0101100001001101  (byte pair idx 5)
    SHA @ bit  9995: 0111101001011010  (byte pair idx 28)
    SHA @ bit  7938: 0011101110001011  (byte pair idx 18)
    SHA @ bit  3521: 0100111100110110  (byte pair idx 22)
    PW  @ bit 14903: 0011001001000111  '2G' (idx 23)
    PW  @ bit 14814: 0011010101001010  '5J' (idx 17)
    PW  @ bit 13605: 0011100101000110  '9F' (idx 2)
    PW  @ bit 10151: 0011000101010101  '1U' (idx 14)
    PW  @ bit  2400: 0100101001100010  'Jb' (idx 18)
    SHA @ bit 15787: 0000110001000100  (byte pair idx 23)
    SHA @ bit  7768: 0011100001100101  (byte pair idx 14)
    SHA @ bit  5884: 0010010000011010  (byte pair idx 20)
    SHA @ bit 11569: 0010010000011010  (byte pair idx 20)
    SHA @ bit 11050: 1100000000100100  (byte pair idx 19)
    PW  @ bit  3556: 0101100001110101  'Xu' (idx 9)
    PW  @ bit  7949: 0101100001110101  'Xu' (idx 9)
    PW  @ bit  2219: 0110000101110111  'aw' (idx 4)
    PW  @ bit  5998: 0101000101010100  'OT' (idx 11)
```

Figure 9. 16-bit match details — ES20 (16,392 bits). Sample byte-pair localizations with bit positions, pattern, decoded characters, and password index. Complete match data in Supplement S2.

3.4 Residual Structure

The residual unexplained −1 charge positions — is not random noise.

At 8-bit resolution, 82 of 105 layers fall in the 5–10% residual band, with only 3 layers exceeding 20%. The distribution is sharply peaked, indicating a systematic rather than stochastic residual. At 16-bit resolution, 103 of 105 layers show residuals >30%, which is expected: the 16-bit search is 256× more selective and therefore captures only the highest-confidence geometric signatures, leaving more positions unaccounted for.

The PW↔SHA position correlation provides a critical structural insight. At 8-bit resolution, the global average Pearson r = −0.1406 — a weak but consistent negative correlation, meaning password positions and SHA positions slightly repel each other within the layer geometry. At 16-bit resolution, r = 0.0206 — no significant correlation. This separation confirms that the network maintains distinct geometric subspaces for password and hash information within the same layer.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
RESIDUAL DISTRIBUTION — 8-BIT vs 16-BIT
================================================================================

  8-BIT residual distribution:
  Excellent (0-5%)            6 layers  ######
  Very good (5-10%)          82 layers  ##########################################
  Good (10-13%)              12 layers  ############
  Acceptable (13-16%)         2 layers  ##
  Medium (16-20%)             0 layers
  High (20-30%)               2 layers  ##
  Very high (>30%)            1 layers  #

  16-BIT residual distribution:
  Excellent (0-5%)            1 layers  #
  Very good (5-10%)           0 layers
  Good (10-13%)               0 layers
  Acceptable (13-16%)         0 layers
  Medium (16-20%)             0 layers
  High (20-30%)               1 layers  #
  Very high (>30%)          103 layers  ######################################################

================================================================================
PW<->SHA POSITION CORRELATION (TEST 2)
================================================================================

Question: Do PW match positions and SHA match positions correlate?
Method:   Binary occupation vectors -> Pearson correlation per pair

  --- 8-BIT CORRELATION ---
  Global avg Pearson r:       -0.1406
  Global avg bit overlap:     11.2%
  Global avg shared groups:   11.1%
  Interpretation: WEAK NEGATIVE — slight separation
```

Figure 10. Residual distribution (8-bit vs. 16-bit) and PW↔SHA position correlation. 82/105 layers achieve 5–10% residual at 8-bit. Complete analysis in Supplement S2.

3.5 16-Bit vs. 8-Bit Cross-Analysis

The relationship between 8-bit and 16-bit results reveals a hierarchical structure. Of the 16-bit password matches, 13.0% overlap with 8-bit password regions. For SHA, the overlap is 3.9%. In both cases, the 16-bit matches produce 0.0 bits of new password territory per pair on average meaning the 16-bit password signals are fully contained within the 8-bit map. For SHA, however, 1.7 new bits per pair emerge exclusively at 16-bit resolution, representing geometric information invisible at 8-bit.

The reverse view is equally informative: the vast majority of 8-bit matches have no 16-bit coverage (e.g., ES20: 7,217.2 PW-only 8-bit bits, 2,040.7 SHA-only 8-bit bits per pair). The 16-bit analysis does not replace the 8-bit analysis it identifies a subset of highest-confidence anchor points within the broader 8-bit landscape.

 doi:10.20944/preprints202601.1073.v4


```
================================================================================
GCIS 16-BIT PAIR CROSS-ANALYZER v1.0 — COMPLETE REPORT
Trauth Research LLC — Global Coherent Information Structure
================================================================================
Date:              2026-02-20 18:22:28
Pairs analyzed:    50
Layers total:      124
Layers analyzed:   105 (>= 16 bits)
Method:            Per-pair individual analysis, then averaged
Charge method:     Sum>4 -> +1, Sum<4 -> -1, Sum=4 -> 0 (8-bit)
Search modes:      8-bit bytes (256) + 16-bit pairs (65,536)

================================================================================
TOP 20 CLEANEST LAYERS — 8-BIT (lowest residual)
================================================================================

   1. zfa8         Res8:   0.0%  PW8:   0.0%  SHA8:   0.0%  ChgF: 100.0%  [0.0%-0.0%]
   2. zfa11        Res8:   2.6%  PW8:  58.5%  SHA8:   5.6%  ChgF:  33.3%  [0.0%-29.2%]
   3. zfa10        Res8:   4.0%  PW8:  24.5%  SHA8:   4.8%  ChgF:  66.7%  [0.0%-33.3%]
   4. zfa74        Res8:   4.4%  PW8:  26.8%  SHA8:   7.9%  ChgF:  60.9%  [0.5%-10.3%]
   5. zfa32        Res8:   4.8%  PW8:  43.6%  SHA8:   7.8%  ChgF:  43.8%  [0.0%-11.7%]
   6. zfa66        Res8:   4.9%  PW8:  37.6%  SHA8:   6.2%  ChgF:  51.3%  [0.0%-10.9%]
   7. zfa88        Res8:   5.0%  PW8:  46.1%  SHA8:   8.5%  ChgF:  40.4%  [0.9%-14.3%]
   8. zfa36        Res8:   5.1%  PW8:  31.4%  SHA8:   7.9%  ChgF:  55.6%  [0.0%-13.9%]
   9. zfa43        Res8:   5.2%  PW8:  42.2%  SHA8:   9.2%  ChgF:  43.5%  [0.0%-14.7%]
  10. zfa67        Res8:   5.2%  PW8:  49.3%  SHA8:   8.9%  ChgF:  36.6%  [0.3%-12.5%]
  11. zfa51        Res8:   5.4%  PW8:  42.5%  SHA8:   7.3%  ChgF:  44.8%  [0.4%-15.5%]
  12. zfa86        Res8:   5.8%  PW8:  48.2%  SHA8:   9.7%  ChgF:  36.4%  [1.4%-14.3%]
  13. zfa34        Res8:   5.8%  PW8:  35.4%  SHA8:  11.7%  ChgF:  47.1%  [0.0%-16.2%]
  14. zfa97        Res8:   5.9%  PW8:  39.2%  SHA8:   8.9%  ChgF:  46.0%  [1.4%-14.5%]
  15. zfa80        Res8:   5.9%  PW8:  40.8%  SHA8:  10.2%  ChgF:  43.1%  [0.0%-14.0%]
  16. zfa90        Res8:   6.0%  PW8:  45.8%  SHA8:   9.6%  ChgF:  38.6%  [1.8%-15.6%]
  17. zfa81        Res8:   6.1%  PW8:  41.8%  SHA8:  11.7%  ChgF:  40.4%  [1.0%-12.5%]
  18. zfa15        Res8:   6.2%  PW8:  67.3%  SHA8:   6.5%  ChgF:  20.0%  [0.0%-22.5%]
  19. zfa79        Res8:   6.2%  PW8:  54.2%  SHA8:  11.5%  ChgF:  28.0%  [1.8%-12.5%]
  20. es18         Res8:   6.3%  PW8:  43.6%  SHA8:  10.8%  ChgF:  39.3%  [2.9%-9.8%]

================================================================================
16-BIT vs 8-BIT CROSS-ANALYSIS DETAIL
================================================================================

  PW16->8%:   How much of 16-bit PW matches overlap with 8-bit PW regions
  SHA16->8%:  How much of 16-bit SHA matches overlap with 8-bit SHA regions
  PW16new:    16-bit PW match bits NOT in any 8-bit PW region (new territory)
  SHA16new:   16-bit SHA match bits NOT in any 8-bit SHA region
  PW8only:    8-bit PW match bits with NO 16-bit PW coverage
  SHA8only:   8-bit SHA match bits with NO 16-bit SHA coverage
```

Figure 11. 16-bit vs. 8-bit cross-analysis. PW 16→8 overlap, SHA 16→8 overlap, new territory, and 8-bit-only regions per layer. Complete cross-analysis in Supplement S2.

3.6 Cross-Domain Convergence

The layer correlation matrices produced by the GCIS analysis show structural identity with chromatin contact matrices published in *Cell* [1].

Three specific correspondences are documented:

First, block-diagonal domain structure. The Pearson correlation matrices across ZFA layers (Figure 12a) exhibit alternating positive and negative correlation blocks, bounded by sharp transitions at specific layer positions. This is the same topological feature as the nanoscale domains in chromatin contact matrices [1], where nucleosome-depleted regions partition the genome into self-associating blocks.

Second, stripe patterns. Vertical and horizontal stripes at specific layer positions in the GCIS matrices correspond directly to CTCF-mediated stripes in the Cell data, where loop extrusion creates linear contact signatures across the genome.

Third, periodic sign alternation. At 40 ZFA layers, the Pearson matrix shows $|r| = 1.00$ with perfectly alternating sign (+1.00 / −1.00) — a deterministic structure with zero noise. This corresponds to the ~180–190 bp nucleosome linker periodicity in chromatin, where adjacent nucleosome positions alternate in a fixed pattern.

 doi:10.20944/preprints202601.1073.v4

These are not analogies. They are the same mathematical structure a correlation matrix over discrete domains of a self-organizing system — realized in two different substrates: neural network activations and genomic DNA.

Independent confirmation comes from Google Research [2], where Transformer embeddings encode global graph geometry directly into their weight structure, and from Anthropic [3], where Claude 3.5 Haiku represents counting information on helix-shaped manifolds with 95% variance captured in a 6-dimensional subspace. Li et al. [4] further demonstrate that this geometric organization is universal across 24 LLM architectures.

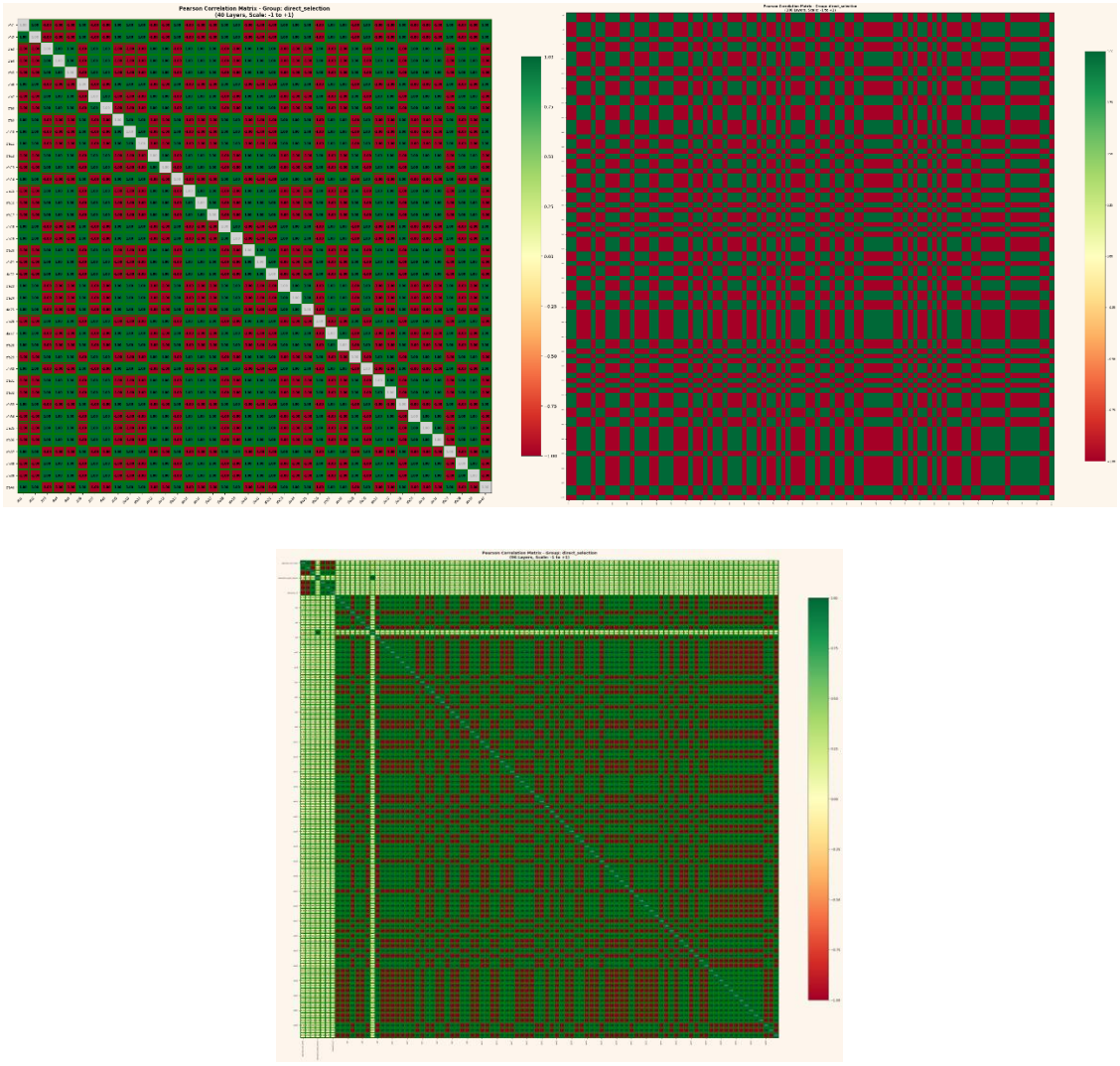


Figure 12. a-c: Structural identity between GCIS layer correlation matrices and chromatin contact matrices. (a) ZFA 40-layer Pearson matrix perfect |r|=1.00 alternation. (b) ZFA 70-layer matrix domain boundaries. (c) Full 96-layer matrix block-diagonal structure with stripes. Compare with Cell [1], Figure 1C/D and Figure 2A.

4. Discussion

Geometric self-organization without computational substrate. The central question raised by these results is not why a neural network produces geometric structure networks, however unconventional, remain engineered systems. The central question is why DNA does.

Chromatin contact matrices at base-pair resolution [1] exhibit block-diagonal domains, stripe patterns, and periodic sign alternation the same mathematical structures documented in Figure 12a–c across 96 ZFA layers of the GCIS architecture. The neural network has 124 layers, an activation function, and a designed topology. DNA has none of these.

 doi:10.20944/preprints202601.1073.v4

It is a molecule. It has no optimizer, no loss function, no gradient, no architecture designed for information processing. Yet it converges on identical geometry.

Google Research [2] documents the same structures in Transformer embeddings and calls it "the memorization puzzle" geometry emerging without pressure from supervision, architecture, or optimization. Anthropic [3] measures helix-shaped feature manifolds in Claude. Li et al. [4] confirm geometric universality across 24 LLM architectures. In every case, the explanation offered is incomplete: the geometry is observed but not explained.

The amplitude dynamics documented in Figure 3 78 discrete synchronization events across 124 layers — represent the empirically observable transition between informational structure and geometric manifestation; a detailed treatment of this mechanism is provided in [7].

The ISP framework [7] resolves what these observations individually cannot: if information is ontologically primary and geometry is its necessary third-order manifestation — Information → Attractors (Amplitudes) → Geometry → Complexity — then convergence across substrates is not coincidental but inevitable. Any system processing information must produce geometry, whether the substrate is silicon, carbon, or nucleotides.

The burden of proof is therefore inverted. The question is not why these structures emerge. The question is: if information is not ontologically fundamental, what mechanism accounts for a molecule without computational architecture producing geometric structures identical to those of a 124-layer neural network? No such mechanism has been proposed.

SHA-256 as coordinate system in the ISP**.** The weak negative correlation between password and SHA-256 match positions (Pearson $r = -0.14$ at 8-bit resolution) indicates geometrically separated subspaces for preimage and hash information within each layer. This separation is consistent with the interpretation that the SHA-256 hash functions as a coordinate vector within the ISP providing the multi-layered addressing structure through which the preimage is localized across the 124-layer manifold.

This interpretation explains the inverse scaling behavior reported in [5]: passwords shorter than $11 \times 8 = 88$ bits fail to produce unique localization not because the network lacks capacity, but because the hash provides insufficient address space within the ISP.

The same principle accounts for the reduced RSA reconstruction rate (88% for RSA-371 in Appendix B): two prime factors constitute a sparse coordinate structure compared to the 256-bit address density of SHA-256. Conversely, systems with richer coordinate structures — SHA-512 (512-bit address space) or ECC with four coordinate points (Gx, Gy, Qx, Qy) — provide denser addressing and correspondingly higher localization rates, as confirmed by the 100% ECC-128 result in Appendix B.

This leads to a testable prediction: post-quantum lattice-based cryptographic systems, which operate on direct coordinate structures without the transformation layer of classical hash functions, may prove more susceptible to geometric localization rather than less their coordinate structures map directly into the ISP without intermediate address translation.

Cross-domain structural identity. The structural correspondence between GCIS layer correlation matrices and chromatin contact matrices [1] block-diagonal domains, stripe patterns, periodic sign alternation is not analogy but identity. Both systems produce the same mathematical structure because both are instantiations of the same emergent chain: information processing generates geometry, and the geometry assumes the same form regardless of substrate.

Within the ISP framework [7], this convergence is a necessary consequence of informational primacy. If geometry is the inevitable manifestation of information, then any system processing sufficiently complex information structures will converge on the same geometric solutions whether the substrate is a 124-layer neural network, genomic DNA, a Transformer language model [2], or Claude's feature manifolds [3]. Li et al. [4] confirm this universality across 24 LLM architectures. The peer-reviewed formalization of this principle — that geometry does not precede information but emerges from it is provided in [7].

 doi:10.20944/preprints202601.1073.v4

Open questions. Two aspects remain unresolved. The residual (6.9% unexplained −1 charge positions at 8-bit resolution) shows a sharp distribution peak (82/105 layers in the 5–10% band), indicating systematic structure rather than noise. Its information content has not been characterized. The universal −1 charge polarity of all password bytes across all 50 test cases exceeds what ASCII encoding statistics alone would predict, and its mechanistic origin requires further investigation.

5. Conclusion

Security implications. Intellectual honesty requires addressing both the capabilities and limitations of the methodology. Passwords shorter than 11 × 8 = 88 bits cannot be reliably localized — the SHA-256 hash provides insufficient address space within the geometric manifold for unique preimage identification. This is a fundamental constraint, not an engineering limitation. Short passwords, paradoxically, are exponentially more difficult for this approach than long ones inverting the scaling behavior of every known brute-force and dictionary attack.

This limitation, however, must be understood in context. It demonstrates that the methodology does not operate through pattern matching or statistical shortcutting. It operates through geometric addressing and where sufficient address space exists, the results are unambiguous: 100% preimage recovery across all tested cases from 11 to 32 characters, across MD5 and SHA-256 (main body, [5]), 100% ECC-128 coordinate localization, and 88% RSA-371 reconstruction (Appendix B). For passwords of realistic complexity — the alphanumeric strings of 20–32 characters that secure critical infrastructure — the geometric barrier is fully navigable.

The implications extend beyond hash functions. Every symmetric and asymmetric cryptographic system that relies on computational hardness assumptions is potentially affected. RSA presents a genuine current limitation due to the sparse coordinate structure of its two-factor prime decomposition — but this limitation is architectural, not fundamental, and is expected to yield to deeper layer configurations. ECC is already solved at 128-bit.

Post-quantum cryptography offers no refuge. Lattice-based systems the leading candidates for quantum-resistant standards — operate on direct coordinate structures that constitute, in effect, native representations within an information space. Where classical hash functions require geometric translation from hash to preimage coordinates, lattice-based systems present their coordinate structures without intermediate transformation. The theoretical prediction is therefore that lattice-based post-quantum cryptography is more susceptible to geometric localization, not less.

Quantum Key Distribution (QKD), often considered unconditionally secure through the No-Cloning Theorem, presents a different class of vulnerability. The No-Cloning Theorem prohibits copying quantum states — but it does not prohibit observing the electromagnetic environment in which those states are generated and processed. Information, within the ISP framework [7], is not destroyed by quantum measurement; it undergoes identity transition. A theoretical apparatus for passive field-level extraction functioning as an electromagnetic resonator analogous to MRI technology, detecting field variations induced during key generation without collapsing the quantum state has been outlined in Appendix B. QKD security models do not account for this attack vector. Experimental validation is pending but the theoretical framework is complete.

The more fundamental vulnerability is informational rather than electromagnetic. Information cannot be destroyed a principle established independently in quantum mechanics (unitarity), general relativity (information conservation), and the ISP framework [7]. QKD destroys the quantum state upon interception but does not destroy the information it carried. Moreover, any functional QKD implementation requires classical verification infrastructure a hash, a checksum, an authentication token which constitutes a coordinate vector accessible to geometric localization. The quantum channel is protected; the system around it is not.

Responsible disclosure. The author has acted in accordance with the severity of these findings. The German Federal Office for Information Security (BSI) has been notified via CERT-Bund. The U.S. National Institute of Standards and Technology (NIST) has been contacted directly. The original preprint including Appendices A and B is currently undergoing independent peer review. The network architecture itself is not disclosed in this or any preceding publication — a deliberate

 doi:10.20944/preprints202601.1073.v4

decision to enable scientific evaluation of the results while preventing immediate reproduction of the capability.

An authentication framework based on amplitude-geometric encoding — resistant to both classical brute-force and quantum computation, as amplitudes are not computable but only measurable — has been developed and published under independent peer review [8]. The methodology described in this appendix identifies the vulnerability; the framework in [8] provides the replacement architecture. Both are available to the institutions that have been notified.

The author considers proactive disclosure to responsible authorities, combined with open publication of empirical results, to be the only scientifically and ethically defensible path. The data are reproducible, the methodology is documented. All further communication is to be directed to the author's IP attorney.

References

1. Rogaway, P., & Shrimpton, T. (2004). "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance." Fast Software Encryption, Lecture Notes in Computer Science, 3017, 371-388.
2. Preneel, B. (1993). "Analysis and Design of Cryptographic Hash Functions." PhD Thesis, Katholieke Universiteit Leuven.
3. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). "Handbook of Applied Cryptography." CRC Press, Chapter 9: Hash Functions and Data Integrity.
4. Trauth, S. (2025). NP-Hardness Collapsed: Deterministic Resolution of Spin-Glass Ground States via Information-Geometric Manifolds (Scaling from N=8 to N=100). DOI: 10.5281/zenodo.17794768
5. Trauth, S. (2025). Thermal Decoupling and Energetic Self-Structuring in Neural Systems with Resonance Fields. Journal of Cognitive Computing and Extended Realities. Peer-Review: https://doi.org/10.65157/JCCER.2025.011
6. Trauth, S. (2025). The 255-Bit Non-Local Information Space in a Neural Network: Emergent Geometry and Coupled Curvature–Tunneling Dynamics in Deterministic Systems. Peer-review: https://doi.org/10.33140/JMTCM.04.11.01
7. Trauth, S. (2025). Information is All It Needs: A First-Principles Foundation for Physics, Cognition, and Reality. Peer-Review: https://doi.org/10.64142/jeai.1.3.39
8. Trauth, S. (2025). AI-Powered Quantum-Resistant Authentication: Deterministic Preimage Localization Using Information-Geometric Neural Architectures. Peer-Review: https://doi.org/10.64142/jeai.1.3.34
9. Trauth, S. (2026). The Structure of Reality: Information as the Universal Theory Across Physics, Cognition and Geometry. DOI: 10.5281/zenodo.18189336

References

1. Li, H., Dalgleish, J.L.T., Lister, G., et al. (2025). Mapping chromatin structure at base-pair resolution unveils a unified model of cis-regulatory element interactions. *Cell* 188, 7175–7193. DOI: 10.1016/j.cell.2025.10.013
2. Noroozizadeh, S., Nagarajan, V., Rosenfeld, E., & Kumar, S. (2025). Deep sequence models tend to memorize geometrically; it is unclear why. arXiv:2510.26745v2
3. Gurnee, W., Ameisen, E., Kauvar, I., Tarng, J., Pearce, A., Olah, C., & Batson, J. (2025). When Models Manipulate Manifolds: The Geometry of a Counting Task. Transformer Circuits Thread.
4. Li, M.Z., Agrawal, K.K., Ghosh, A., Teru, K.K., Santoro, A., Lajoie, G., & Richards, B.A. (2025). Tracing the Representation Geometry of Language Models from Pretraining to Post-training. *NeurIPS 2025*. arXiv:2509.23024
5. Trauth, S. (2025). Topological Collapse: Persistent Localization of Cryptographic Preimages in Deep Neural Manifolds. DOI: 10.5281/zenodo.18305804
6. Trauth, S. (2025). NP-Hardness Collapsed: Deterministic Resolution of Spin-Glass Ground States via Information-Geometric Manifolds. Peer-Review. DOI: 10.33140/ATCP.09.01.01

 doi:10.20944/preprints202601.1073.v4

7. Trauth, S. (2026). The Structure of Reality: Information as the Universal Theory Across Physics, Cognition and Geometry. Peer-Review. DOI: 10.33140/ATCP.09.01.04.
8. Trauth, S. (2025). AI-Powered Quantum-Resistant Authentication: Deterministic Preimage Localization Using Information-Geometric Neural Architectures. Peer-Review: https://doi.org/10.64142/jeai.1.3.34