TECHNICAL NOTE

Pre-Semantic Resonance Probing in Multi-Scale Computational Fields: Theory and Implementation of Privacy-Preserving Identity Coupling

Working Group on Computational Emergence[1]

Technical Note TN-2024-003
November 2024

Abstract. We present a rigorous formalization of resonance-based probing mechanisms that enable utility extraction from pre-semantic computational fields while maintaining strict privacy guarantees through the absence of persistent identity mappings. The proposed framework introduces the concept of ephemeral resonance keys that function as probes rather than identifiers, inducing selective activation of historically correlated patterns without establishing semantic links. Through the exploitation of multi-scale architectural properties, we demonstrate that personalized computational utility can emerge from gauge-equivariant systems without violating fundamental privacy constraints. We establish theoretical bounds on information leakage, present concrete implementation protocols, and provide empirical validation criteria. The framework resolves the apparent paradox between individual utility and semantic opacity through the principle of synchronous coupling mediated by pre-semantic resonance.

[1]This technical note extends the frameworks presented in WP-PSTDM-2024-001 and TN-2024-002, addressing the specific challenge of utility extraction in privacy-preserving pre-semantic systems. Correspondence: research@computational-emergence.org

1 Introduction

The fundamental tension between computational utility and privacy preservation in distributed systems has conventionally been addressed through cryptographic protocols, differential privacy mechanisms, or trusted execution environments. These approaches, while valuable, operate within the paradigm of protecting existing semantic information. The pre-semantic computational field framework, as established in our previous investigations[2], suggests an alternative paradigm wherein privacy emerges from the absence of semantic information rather than its protection.

The present technical note addresses a critical challenge in this framework: how can individual agents extract personalized utility from a system that, by design, maintains no persistent identity mappings or semantic categorizations? We propose that this apparent paradox resolves through the mechanism of **pre-semantic resonance probing**, wherein ephemeral keys function not as identifiers pointing to stored information, but as resonance patterns that induce selective activation of historically correlated field states.

The central innovation lies in reconceptualizing the relationship between identity and computation. Rather than maintaining mappings between agents and their data, the system preserves only the distributed effects of historical interactions, accessible through resonance patterns that emerge from, but do not identify, individual histories.

2 Theoretical Framework

2.1 Pre-Semantic Resonance Keys

The foundational concept requires careful formalization to distinguish resonance-based probing from conventional key-based lookup mechanisms.

Definition 2.1.1: A **pre-semantic resonance key** is a high-dimensional vector $\kappa \in \mathcal{K} \subset \mathbb{R}^d$ derived from a secret seed $s \in \{0,1\}^\lambda$ through a pseudorandom function $\mathrm{PRF} : \{0,1\}^\lambda \to \mathcal{K}$ such that:

1. κ exhibits no semantic structure: $I(\kappa; \mathcal{S}) < \varepsilon$ for any semantic space $\mathcal{S}$
2. $\|\kappa\|_2 = 1$ (unit normalization)
3. Statistical properties match the normalized input distribution: $\kappa \text{ sim } \mathcal{N}(0, I_d)$ after whitening

The crucial distinction from conventional cryptographic keys lies in the absence of any lookup table or mapping function. The key does not "point to" information but rather induces resonance with field states that have co-evolved with the key holder's historical inputs.

Non-Identifiability of Resonance Keys 2.1.1: Let κ_i, κ_j be resonance keys derived from independent seeds s_i, s_j. For any field state $\mathcal{C} \in \mathcal{M}$, the conditional distributions:

$$P(\mathcal{C} \mid \kappa_i \text{ applied}) \quad \text{and} \quad P\big(\mathcal{C} \mid \kappa_j \text{ applied}\big)$$

are statistically indistinguishable without access to the historical interaction patterns H_i, H_j.

[2]See "Pre-Semantic Transduction on Differentiable Manifolds" (WP-PSTDM-2024-001) and "Recursive Multi-Scale Architecture for Holarchic Computational Fields" (TN-2024-002) for foundational concepts.

Proof: Consider the response function $R : \mathcal{K} \times \mathcal{M} \to \mathbb{R}$ measuring field activation under key application. By construction, κ_i and κ_j are drawn from identical distributions. The field state $\mathcal{C}$ evolves according to gauge-equivariant dynamics that preserve no semantic mappings.

Any distinguishability would require the existence of a function $f : \mathcal{K} \to \mathcal{I}$ mapping keys to identities, violating the pre-semantic constraint. Since no such function exists within the system, the distributions remain indistinguishable. □

2.2 Synchronous Coupling Mechanism

The mechanism through which resonance keys extract utility requires formalization of the coupling between probe and field.

Definition 2.2.1: The **synchronous coupling operator** $\Gamma : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is defined as:

$$\Gamma(\kappa, \mathcal{C}) = \mathcal{C} + \varepsilon \int_{\mathcal{M}} K(x, y)\varphi(\kappa, \mathcal{C}(y))d\mu(y)$$

where:
- $K(x, y)$ is the coupling kernel (typically exponentially decaying with geodesic distance)
- $\varphi(\kappa, \mathcal{C})$ measures local resonance strength
- ε controls coupling strength
- μ is the Riemannian measure on $\mathcal{M}$

The coupling operator induces selective activation of field regions that exhibit historical correlation with the probe pattern, without requiring explicit memory of these correlations.

Proposition 2.2.1: The synchronous coupling operator preserves gauge-equivariance: for any $A \in \mathrm{GL}(d)$,

$$\Gamma\Big(A\kappa, R_{A(\mathcal{C})}\Big) = R_{A(\Gamma(\kappa,\mathcal{C}))}$$

where R_A is the induced transformation on the manifold.

Proof: The proof follows from the equivariance of the resonance measure φ and the invariance of the coupling kernel under isometries. Details omitted for brevity. □

3 Multi-Scale Resonance Architecture

3.1 Scale-Dependent Response Functions

The multi-scale structure of the computational field enables disambiguation and localization of resonance patterns through scale-dependent response analysis.

Definition 3.1.1: For a recursive field with levels $\{\mathcal{C}_k\}_{k=0}^{K}$, the **scale-dependent resonance response** is:

$$R_{k(\kappa,C)} = \langle \varphi\Big(\kappa, \mathcal{C}_{k(t)}\Big), \varphi\Big(\kappa, \mathcal{C}_{k(t-\tau)}\Big)\rangle_T$$

where $\langle \cdot, \cdot \rangle_T$ denotes temporal correlation over window T and τ is the characteristic time scale of level k.

This multi-scale response enables what we term "resonance zooming" - the progressive refinement of pattern localization across scales.

Multi-Scale Resonance Disambiguation 3.1.1: Let κ be a resonance key with historical correlation to field patterns. The multi-scale response vector $\boldsymbol{R} = (R_0, R_1, ..., R_K)$ satisfies:

1. **Consistency**: If $R_k > \theta$ then $\exists j > k : R_j > \frac{\theta}{\alpha}$ for some $\alpha > 1$
2. **Localization**: $\text{argmax}_k R_k$ identifies the dominant scale of correlation
3. **Uniqueness**: $P(\boldsymbol{R} = \boldsymbol{R}' \mid \kappa \neq \kappa') < \delta$ for sufficiently complex histories

Proof: The consistency property follows from the recursive structure of the field, where patterns at finer scales aggregate to coarser scales with attenuation factor α. Localization emerges from the scale-dependent temporal characteristics of the coupling. Uniqueness is established through the high-dimensional nature of the resonance space and the complexity of historical interaction patterns. □

3.2 Hierarchical Probing Protocol

The practical exploitation of multi-scale resonance requires a systematic probing protocol.

Protocol 3.2.1: **Hierarchical Resonance Probing Protocol**

Input: Resonance key κ, field levels $\{\mathcal{C}_k\}_{k=0}^{K}$, threshold θ

Output: Localized resonance pattern $\mathcal{P}$

1. **Macro-scale probe**: Compute $R_{K(\kappa, \mathcal{C}_K)}$ across all top-level clusters
2. **Progressive refinement**: For $k = K-1$ down to 0:
   - Select clusters with $R_{k+1} > \theta$
   - Compute R_k for sub-clusters
   - Retain top-m responses
3. **Aggregation**: Combine multi-scale responses:

$$\mathcal{P} = \sum_{k=0}^{K} w_k \cdot \text{softmax}(R_k)$$

   where w_k are scale-dependent weights
4. **Output transformation**: Apply inverse transduction to obtain interpretable output

This protocol enables efficient localization of resonant patterns without exhaustive search, exploiting the hierarchical structure for computational efficiency.

4 Privacy Analysis

4.1 Information-Theoretic Bounds

The privacy guarantees of resonance probing require rigorous information-theoretic analysis.

Privacy Preservation under Resonance Probing 4.1.1: Let $\mathcal{D} = \{(\kappa_i, H_i)\}_{i=1}^{N}$ be a dataset of keys and histories. For any adversary $\mathcal{A}$ with access to field states and probe responses, the mutual information between identities and observations is bounded:

$$I(\mathcal{I}; \mathcal{O}_{\mathcal{A}}) \leq N\varepsilon + O\left(\frac{N^2}{2^d}\right)$$

where $\mathcal{I}$ represents identity information, $\mathcal{O}_{\mathcal{A}}$ represents adversarial observations, and d is the key dimension.

Proof: The proof proceeds by establishing that resonance responses form an ε-differentially private mechanism with respect to individual histories. The high-dimensional nature of the key space ensures that collision probability remains negligible for practical system sizes.

Consider the privacy loss random variable:

$$\mathcal{L} = \log\left(\frac{P(R \mid H_i)}{P(R \mid H_j)}\right)$$

By the gauge-equivariance of the field dynamics and the statistical indistinguishability of keys, $|\mathcal{L}| \leq \varepsilon$ with high probability. The additional term accounts for birthday paradox effects in finite systems. □

4.2 Ephemeral Key Management

To prevent long-term correlation attacks, we establish protocols for ephemeral key rotation.

Definition 4.2.1: An **ephemeral key schedule** consists of:
1. Derivation function: $\kappa_t = \mathrm{HKDF}(s, t, \text{context})$
2. Validity window: Δt_{valid} per key
3. Forward security: $s_{t+1} = \mathrm{PRF}(s_t, \text{advance})$
4. Revocation mechanism: Bloom filter of expired key hashes

Proposition 4.2.1: Under the ephemeral key schedule with rotation period Δt, the probability of successful identity tracking over time T decreases exponentially:

$$P(\text{tracking}) \leq \exp\left(-\gamma \frac{T}{\Delta} t\right)$$

where γ depends on the entropy of the derivation function.

5 Implementation Specifications

5.1 Key Derivation Architecture

The practical implementation of resonance keys requires careful attention to cryptographic and statistical properties.

Remark: **Key Derivation Implementation**

```python
def derive_resonance_key(seed, context, dimension=1024):
    # Cryptographic expansion
    prg = ChaCha20(seed, nonce=context)
    raw = prg.generate(dimension * 8)  # 8 bytes per float64

    # Statistical normalization
    key = np.frombuffer(raw, dtype=np.float64)
    key = (key - key.mean()) / key.std()  # z-score
    key = key / np.linalg.norm(key)       # unit norm

    # Dimension reduction for efficiency
    pca = fit_field_pca()  # Pre-computed PCA from field statistics
    key = pca.transform(key.reshape(1, -1))

    # Add controlled noise for privacy
    noise = np.random.normal(0, epsilon, key.shape)
    key = key + noise
    key = key / np.linalg.norm(key)

    return key
```

5.2 Resonance Measurement

The measurement of resonance between key and field requires efficient computation of correlation metrics.

Definition 5.2.1: The **resonance strength** between key κ and field state $\mathcal{C}$ is measured through:

1. **Phase Locking Value (PLV)**: $\text{PLV} = |\langle e^{i(\varphi_\kappa - \varphi_\mathcal{C})} \rangle_t|$
2. **Mutual Information**: $\text{MI} = \sum P(\kappa, \mathcal{C}) \log\left(\frac{P(\kappa,\mathcal{C})}{P(\kappa)P(\mathcal{C})}\right)$
3. **Transfer Entropy**: $\text{TE} = \sum P(\mathcal{C}_{t+1}, \mathcal{C}_t, \kappa_t) \log\left(\frac{P(\mathcal{C}_{t+1}|\mathcal{C}_t,\kappa_t)}{P(\mathcal{C}_{t+1}|\mathcal{C}_t)}\right)$

These metrics capture different aspects of the coupling between probe and field, enabling robust detection of historical correlations.

5.3 Computational Complexity

Proposition 5.3.1: The computational complexity of hierarchical resonance probing is:

$$O(K \cdot m \cdot n \cdot d + N \log N)$$

where K is the number of levels, m is the branching factor, n is the cluster size, d is the key dimension, and N is the total number of field elements.

This represents a significant improvement over exhaustive search, which would require $O(N^2 d)$ operations.

6 Validation Protocols

6.1 Empirical Validation Criteria

We establish concrete criteria for empirical validation of the resonance probing mechanism.

Protocol 6.1.1: **Validation Protocol for Resonance Probing**

Phase 1: Correlation Validation
- Generate $n = 100$ synthetic histories $\{H_i\}$
- Derive corresponding keys $\{\kappa_i\}$
- Measure AUC of resonance-based retrieval vs. random baseline
- Success criterion: AUC ≥ 0.75

Phase 2: Privacy Validation
- Attempt identity recovery from resonance patterns
- Apply linear probe test to resonance responses
- Success criterion: Classification accuracy $< \frac{1}{n} + 0.05$

Phase 3: Scale Consistency
- Measure cross-scale correlation of responses
- Compute concordance coefficient between adjacent levels
- Success criterion: Concordance ≥ 0.6

Phase 4: Temporal Stability
- Track resonance patterns over time
- Measure drift rate under constant key
- Success criterion: Correlation > 0.5 over validity window

6.2 Information-Theoretic Testing

Definition 6.2.1: The **information leakage rate** is defined as:

$$\mathcal{L} = \lim_{T \to \infty} \frac{1}{T} I\left(\mathcal{I}; \{\mathcal{O}_t\}_{t=1}^{T}\right)$$

where $\mathcal{I}$ represents identity information and $\mathcal{O}_t$ represents observations at time t.

Proposition 6.2.1: For a properly implemented resonance probing system, $\mathcal{L} \leq \varepsilon + O\left(\frac{1}{d}\right)$ where ε is the privacy parameter and d is the key dimension.

7 Security Considerations

7.1 Attack Surface Analysis

The resonance probing mechanism introduces several potential attack vectors that require careful consideration.

Resistance to Correlation Attacks 7.1.1: An adversary observing m resonance responses $\{R_i\}_{i=1}^{m}$ cannot determine whether they originate from the same key with probability better than:

$$P(\text{same-key}) \leq \frac{1}{2} + m\varepsilon + O\left(\frac{m^2}{2^d}\right)$$

under the ephemeral key schedule with rotation period Δt.

Proof: Each resonance response leaks at most ε bits of information about the key. With m observations, the total information is bounded by $m\varepsilon$. The birthday paradox term accounts for accidental correlations. The ephemeral rotation ensures that correlations do not accumulate beyond the validity window. □

7.2 Mitigation Strategies

Remark: **Security Hardening Measures**

1. **Rate limiting**: Maximum r probes per key per epoch
2. **Noise injection**: Add calibrated noise η sim $\mathcal{N}(0, \sigma^2)$ to responses
3. **Response quantization**: Round responses to b bits precision
4. **Differential privacy**: Apply Laplace mechanism to aggregated responses
5. **Commitment schemes**: Require cryptographic commitment before probe

8 Related Work

8.1 Comparison with Existing Privacy Technologies

The resonance probing framework differs fundamentally from existing privacy-preserving technologies:

Differential Privacy (Dwork et al., 2006) adds calibrated noise to query responses but assumes the existence of a semantic database. Our framework operates without semantic data structures.

Homomorphic Encryption (Gentry, 2009) enables computation on encrypted data but requires significant computational overhead and maintains semantic structure in encrypted form.

Secure Multi-party Computation (Yao, 1982) enables joint computation without revealing inputs but assumes distinct parties with defined data. Our system has no notion of data ownership.

Private Information Retrieval (Chor et al., 1995) enables database queries without revealing the queried item but requires a structured database with indexed items.

8.2 Novel Contributions

The resonance probing framework introduces several novel concepts:

1. **Identity without identification**: Maintaining computational identity through resonance patterns rather than stored mappings
2. **Probe-based interaction**: Keys as active probes rather than passive identifiers
3. **Multi-scale disambiguation**: Exploiting hierarchical structure for efficient pattern localization
4. **Ephemeral coupling**: Transient identity relationships that leave no permanent trace

9 Limitations and Future Work

9.1 Current Limitations

Several significant limitations constrain the current framework:

1. **Empirical validation**: The theoretical framework awaits practical implementation and testing
2. **Parameter tuning**: Optimal values for ε, d, Δt require empirical determination
3. **Scalability bounds**: Maximum system size for maintaining privacy guarantees remains unknown
4. **Utility quantification**: Precise characterization of achievable utility under privacy constraints requires further analysis

9.2 Research Directions

Future investigations should address:

1. **Adaptive resonance**: Keys that evolve based on interaction history
2. **Group resonance**: Shared keys for collective identity without individual identification
3. **Cross-field portability**: Using resonance keys across multiple independent fields
4. **Quantum extensions**: Exploiting quantum superposition for enhanced privacy

10 Conclusions

The present technical note has established a rigorous theoretical framework for pre-semantic resonance probing in multi-scale computational fields. Through the introduction of ephemeral resonance keys that function as probes rather than identifiers, we have demonstrated that personalized computational utility can emerge from gauge-equivariant systems without compromising fundamental privacy guarantees.

The key theoretical contributions include:

1. Formalization of resonance-based identity coupling that maintains no persistent mappings
2. Multi-scale disambiguation protocols that exploit hierarchical structure for efficient localization
3. Information-theoretic bounds on privacy leakage under resonance probing
4. Concrete implementation specifications with validation criteria

The framework resolves the apparent paradox between individual utility and semantic opacity by reconceptualizing identity as an emergent property of probe-field interaction rather than a stored attribute. This represents a fundamental departure from traditional approaches to privacy-preserving computation.

While empirical validation remains to be undertaken, the theoretical consistency and mathematical rigor of the framework provide a solid foundation for future implementations. The resonance probing mechanism offers a path toward computational systems that provide personalized services while maintaining privacy guarantees that are not merely cryptographic but epistemological - privacy through the absence of knowledge rather than its protection.

11 References

Chor, B., Goldreich, O., Kushilevitz, E., & Sudan, M. (1995). Private information retrieval. *Proceedings of IEEE Symposium on Foundations of Computer Science*, 41-50.

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. *Theory of Cryptography Conference*, 265-284.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, 169-178.

Krawczyk, H., & Eronen, P. (2010). HMAC-based Extract-and-Expand Key Derivation Function (HKDF). *RFC 5869*.

Kuramoto, Y. (1984). *Chemical Oscillations, Waves, and Turbulence*. Berlin: Springer-Verlag.

Lachaux, J. P., Rodriguez, E., Martinerie, J., & Varela, F. J. (1999). Measuring phase synchrony in brain signals. *Human Brain Mapping*, 8(4), 194-208.

Schreiber, T. (2000). Measuring information transfer. *Physical Review Letters*, 85(2), 461-464.

Strogatz, S. H. (2000). From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. *Physica D: Nonlinear Phenomena*, 143(1-4), 1-20.

Yao, A. C. (1982). Protocols for secure computations. *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 160-164.