Analytical Review of the Proposed Topological Approach to Private-Key Inversion
(Research context: ECDLP-Research project; test curve: a reduced-size artificial Weierstrass curve defined by `TEST_PARAMS` in the local implementation, not secp256k1)

---

1. Scope and Context

The proposed methodology introduces **topological classifications of private-key trajectories** as a structural layer on top of the elliptic-curve group law. The empirical component is based on synthetic key generation using a **non-secp256k1 test curve** defined in the repository (the curve corresponding to `TEST_PARAMS` in `secp256k1.py`). This prevents misleading interpretations: **all observed distributions, topologies and condition frequencies do not describe secp256k1**, but only the behaviour of the much smaller test curve used for experimentation.

The pipeline for dataset generation and topological extraction is defined in `generate_data.py` , and the resulting condition distributions are in the accompanying statistics files .

This review focuses strictly on the mathematical viability, conceptual coherence, and theoretical risks of the topological approach.

---

2. Mathematical Core of the Proposed Approach

2.1. Topological Encoding of Key Trajectories

The method associates each private key k with a **topology**—a structured representation derived from:

1. the iterative doubling sequence 2^iP,
2. the behaviour of points under modular reduction patterns,
3. the relative placement of a key's public point within a combinatorial partition of the curve group.

In the implementation, each topology is encoded as a vector of segment descriptors of the form

$$(a, b, c, d, e, f, flag)$$

and only those with `flag = 1` are retained for dataset inclusion.

This effectively maps the discrete logarithm problem onto a **classification problem over a discrete topological invariant**. Mathematically, this resembles:

- stratification of $E(\mathbb{F}_p) \cong \mathbb{Z}_n$ by combinatorial partitions,
- extraction of **local geometric signatures** of multiplication-by-k trajectories,
- an attempt to compress the search space by identifying structural "neighbourhoods" of keys.

2.2. Statistical Concentration of Topologies

Empirical results show extreme frequency concentration in a small subset of conditions. For instance, in the large dataset, the top few conditions reach frequencies on the order of **one million** occurrences each .

This implies:

- the combinatorial partition used is **highly non-uniform**,
- the map $k \mapsto \mathrm{topology}(k)$ has **heavy collisions**,
- topologies cluster large key intervals into the same structural signature.

From a mathematical viewpoint, this is expected: any coarse partition of a cyclic group Z_n produces large equivalence classes unless tied to deep algebraic invariants (e.g., isogeny classes, Frobenius angles). Here, the partition seems to depend mainly on arithmetic patterns, not intrinsic geometry.

3. Potential Theoretical Promise

3.1. Reformulating ECDLP Through Local Structures

The main conceptual motivation is:
Instead of attempting global inversion of the map $k \mapsto kP$, one may attempt **local reconstruction inside each topology**, reducing the inversion problem to 2000–3000 subproblems.

Mathematically, this corresponds to:

- decomposing Z_n into equivalence classes under a topology map

  $$\tau : \mathrm{Z}_n \rightarrow \mathrm{T}$$

  where $|\mathrm{T}| \ll n$.
- hoping for a **bi-directional mapping**

  $$(\tau(k), P, Q = kP) \mapsto k,$$

  using structural constraints specific to each topology.

If one topology exhibited an **injective or near-injective relation** between observable trajectory data and the key, this would be significant. Conceptually, this resembles extracting *non-generic structure*, contradicting the assumptions of the **Generic Group Model**.

3.2. Compatibility with Machine-Learning Frameworks

Because topologies generate extremely large, densely sampled clusters, there is potential for ML-based pattern recognition:

- supervised approximations of k conditioned on topology and public point,
- autoencoders or diffusion models for trajectory reconstruction,
- contrastive learning for identifying discriminative substructures within topologies.

The presence of large homogeneous clusters is mathematically advantageous for training, though not necessarily advantageous for solving ECDLP.

4. Fundamental Mathematical Risks

4.1. Risk 1: Topological Classes Are Too Coarse

The frequency data show that each topology contains **hundreds of thousands** of keys. Unless the substructure inside a topology is extremely rigid, no deterministic inversion is possible:

$$\text{If } |\tau^{-1}(t)| \approx 10^6, \text{ then inversion requires narrowing within that set.}$$

This contradicts the expectation that ECDLP on a generic curve has no exploitable local structure.

4.2. Risk 2: The Partition May Not Capture True Geometry

The topology extraction in the implementation is derived from combinatorial patterns involving doubling points and discrete arithmetic irregularities. These are unlikely to correspond to:

- the endomorphism ring of the curve,
- the Galois representation of torsion points,
- isogeny invariants,
- Frobenius eigenvalues or Sato–Tate distribution.

Thus the constructed topologies might reflect **artefacts of the test curve size**, not real geometric invariants.

4.3. Risk 3: Violations of the Generic Group Model Require Non-Generic Information

The generic group model implies:

- any algorithm that uses only the group law behaves no better than Pollard's rho,
- structural partitions must arise from non-generic properties (e.g. special coordinates, field properties, endomorphisms).

The current topologies seem to depend on:

- coordinate-specific logic,
- data structures tied to this particular implementation.

Such dependencies *cannot* transfer to cryptographically strong curves like secp256k1.

4.4. Risk 4: Scaling From Test Curve to secp256k1 Is Non-Trivial

The test curve in `TEST_PARAMS` has vastly smaller order. Phenomena such as:

- short cycles,
- uneven modular distributions,
- statistical clustering of derivatives,

are common in small finite groups but vanish in groups of size $\approx 2^{256}$.

Without proof that the topology map preserves meaningful structure asymptotically, extrapolation is mathematically unjustified.

5. Requirements for the Approach to Become Mathematically Viable

To transform the approach from heuristic exploration to a credible attack model, several mathematical milestones are necessary:

5.1. A Formal Definition of the Topology Map

A rigorous algebraic definition:

$$\tau : E(\mathrm{F}_p) \to \mathrm{T} \,,$$

including:

- its dependence on arithmetic operations,
- its invariance under isomorphisms of elliptic curves,
- whether it is stable under scalar multiplication by small primes.

5.2. Complexity Bounds and Entropy Reduction

To claim an advantage over Pollard’s rho, one must show:

- entropy of keys conditioned on topology is significantly reduced,
- or, more strongly, that

$$H(k \mid \tau(k), kP) \ll 256.$$

Empirical distributions must be complemented with **information-theoretic analysis**, not just frequency tables.

5.3. Connection to Algebraic Geometry

If trajectory topologies reflect genuine curve invariants, they should relate to:

- height functions on elliptic curves,
- equidistribution of scalar multiples,
- arithmetic of short Weierstrass models,
- interaction with Sato–Tate distributions.

Without such connections, topology classes have no theoretical predictive power for inversion.

---

6. Overall Assessment

Strengths

- Provides a structured framework to investigate hidden patterns beyond the generic model.
- Offers a clean decomposition into subproblems that could, in principle, be studied independently.
- Creates extensive empirical data useful for ML-driven hypothesis discovery.
- Encourages exploration of non-standard invariants of scalar trajectories.

Weaknesses and Critical Risks

- Strong statistical clustering indicates **loss of information**, not gain.
- Lacks formal justification that topologies reveal any invertible structure.
- Observed patterns arise from a test curve of modest size, not from secp256k1-scale groups.
- No demonstrated reduction in entropy or improved inversion complexity.
- At present, no mechanism contradicts the Generic Group Model assumptions.

Final Scientific Verdict

The approach is mathematically creative and opens an unconventional line of inquiry: investigating whether scalar trajectories exhibit structural, topologically classifiable features. However, as currently formulated, the method lacks theoretical evidence that these features correlate with any reduction of ECDLP hardness.

Any claim of future feasibility must show **non-generic structure** tied to real algebraic or geometric invariants. Without such justification, the approach remains exploratory and should be treated as an empirical hypothesis-generation tool rather than a cryptanalytic method.