1. Problem Statement

Let $E(\mathrm{F}_p)$ be an elliptic curve defined over a finite field with base point G of large prime order n.
The **Elliptic Curve Discrete Logarithm Problem (ECDLP)** is defined as follows:

> Given a public point
>
> $$Q = d \cdot G \in E(\mathrm{F}_p),$$
>
> determine the unknown private scalar
>
> $$d \in \{1, \dots, n-1\}.$$

Classical approaches treat d as an element of an unstructured cyclic group and rely on generic algorithms (Pollard's rho, baby-step giant-step), whose complexity is $O(\sqrt{n})$.

The research presented here **rejects the assumption that scalar multiplication is information-theoretically opaque** and instead studies the *structural traces* induced by the binary expansion of d.

---

2. Core Observation

Scalar multiplication is not an abstract black box.
It is implemented as a **deterministic sequence of doubling and conditional addition operations** derived from the binary representation of d:

$$d = \sum_{i=0}^{\ell-1} b_i 2^i, \quad b_i \in \{0, 1\}.$$

Thus, computing $Q = dG$ implicitly defines:

- an ordered sequence of curve doublings,
- a sparse subset of indices at which additions occur,
- and a cumulative geometric trajectory on $E(\mathrm{F}_p)$.

This trajectory is **not random**.
It encodes a *topological signature* uniquely determined by d.

---

3. Topological Model of the Private Key

3.1 Double-Point Chain

Define the sequence:

$$P_i = 2^i G, \quad i = 0, 1, \dots, \ell - 1.$$

This sequence is fixed for a given curve and generator and is independent of d.

3.2 Addition Index Set

Define the **addition index set**:

$$A(d) = \{\, i \mid b_i = 1 \,\}.$$

Then:

$$Q = \sum_{i \in A(d)} P_i.$$

The private key is therefore equivalent to the **subset structure** $A(d) \subset \{0, \ldots, \ell - 1\}$.

---

4. Topological Invariants

The research introduces a family of **discrete topological invariants** derived from the geometry of partial sums:

$$S_k = \sum_{i \in A(d),\, i \le k} P_i.$$

From the interaction of S_k with the fixed double-point chain $\{P_i\}$, one can define invariants of the form:

$$(a, b, c, d),$$

where these parameters encode:

- relative ordering of additions,
- distances between activated indices,
- boundary constraints imposed by curve order,
- and admissible regions of the scalar trajectory.

These invariants partition the key space into **equivalence classes (topologies)**.

---

5. Combinatorial Structure of the Key Space

Let ℓ be the bit-length of the curve order.
The number of *theoretically possible* binary keys is 2^ℓ.

However, the number of **distinct topologies** induced by admissible quadruples (a, b, c, d) satisfies:

$$T(\ell) \ll 2^\ell,$$

and grows polynomially with respect to ℓ under analytically derived constraints.

This yields a **massive dimensionality reduction**:

$$\text{Key space} \longrightarrow \text{Topology space.}$$

6. Deterministic Key Reconstruction

A crucial result of the research is:

> **If the addition index set $A(d)$ is known, the private key d is uniquely and trivially reconstructed.**

Formally:

$$d = \sum_{i \in A(d)} 2^i.$$

Thus, the ECDLP is reduced to the problem:

> **Recover the hidden addition index set from topological constraints.**

This is a **structured inference problem**, not an unstructured discrete logarithm.

7. Perspective on "Prediction" vs. Brute Force

The research explicitly distinguishes itself from brute-force or exhaustive search:

- No enumeration of $d \in [1, n)$
- No random walk in the group
- No collision-based heuristics

Instead, the problem is reframed as:

- reconstruction of a sparse binary signal,
- constrained by deterministic geometric rules,
- embedded in a low-dimensional topological space.

This justifies the use of **predictive and analytical frameworks** rather than classical cryptanalytic enumeration.

8. Theoretical Significance

The topological approach establishes that:

1. Scalar multiplication leaks **structural information** by construction.
2. The private key induces a **deterministic geometric signature**.

3. ECDLP can be reframed as a **structured inverse problem**.
4. The hardness of ECDLP is not purely algebraic but **algorithm- and representation-dependent**.

This does **not** claim an immediate break of standard curves.
It demonstrates that the prevailing security model is **incomplete** with respect to structural leakage.

9. Conclusion

The ECDLP-Research project proposes a fundamentally different viewpoint:

- The private key is not an abstract scalar.
- It is a **topological object** defined by its interaction with the doubling structure of the curve.
- Recovering the key becomes a matter of **topology reconstruction**, not brute force.

This perspective opens a new research direction at the intersection of:

- elliptic curve arithmetic,
- combinatorial topology,
- and structured inverse problems.

The value of the research lies not in immediate cryptanalytic impact, but in exposing **previously ignored structural degrees of freedom** in elliptic-curve cryptography.