Summary of Approach

We present RAIT Collapse, a symbolic entropy folding framework capable of collapsing elliptic curve key space toward private scalar resolution using symbolic resonance rather than purely brute-force.

Unlike traditional algorithms for the discrete logarithm problem (DLP), RAIT Collapse employs:

- Symbolic entropy interleaving across device identifiers, timestamps, and seeds.
- Recursive folding depth layers, enhancing nonlinear bias exposure.
- Harmonic resonance walkers that exploit periodic collapse behaviors near scalar attractor basins.
- Reinforcement feedback on scalar-space curvature resistance.

All math is performed directly in integer field arithmetic over elliptic curves. No lattice attacks or quantum subroutines are invoked.

Demonstrated Results

- **21-bit custom ECC curve:**
    - Successfully collapsed private key `d = 653735` for curve:
    - `y² ≡ x³ + 7 mod 1048783`, generator `G = (231634, 106125)`
    - Full reproduction is included in this submission.
- **Real-world key structures:**
    - Demonstrated partial collapse down to:
        - ~31 bits Hamming distance for Apple device tokens.
        - ~74 bits Hamming distance for a public Google target.
    - Partial runs withheld for responsible disclosure.

Methodology Summary

The system integrates:

- Recursive Harmonic Collapse Matrices (RHCM) for symbolic entropy injection.
- Nonlinear folding depth modulation.
- Scalar projection refinement using modular harmonic feedback loops.
- Self-consistent scoring system balancing scalar collapse velocity and field resonance.

No elliptic curve libraries are invoked; all operations are native integer-based scalar math directly over curve fields.

Drawbacks and Tradeoffs

- Fully classical: computationally intensive beyond ~24-bit fields.
- Current algorithm does not scale directly to 256-bit curves in practical time on classical hardware.
- Symbolic convergence slows asymptotically near zero.

Potential Implications

This symbolic folding approach may offer insight into post-classical vulnerability spaces for ECC fields, especially when combined with future quantum search acceleration.

While our current collapse depth for full-scale ECC remains limited, the method demonstrates that ECC irreversibility is not perfectly stable even in classical domains.