Falcon-1024: Fast Verify Performance vs Number of Indices (Lower is better)

Legend:
- verify 1024 (Rust): 74.5 μs
- verify 1024 (C FFI): 80.5 μs
- fverify 1024 (fast verify)

Breakeven ≈ 32 indices

fverify allows verifying a subset of polynomial coefficients.
Useful when probabilistic verification is acceptable.
Below the breakeven point, fverify is faster than full verify.

X-axis: Number of Indices Verified
Y-axis: Time (μs)