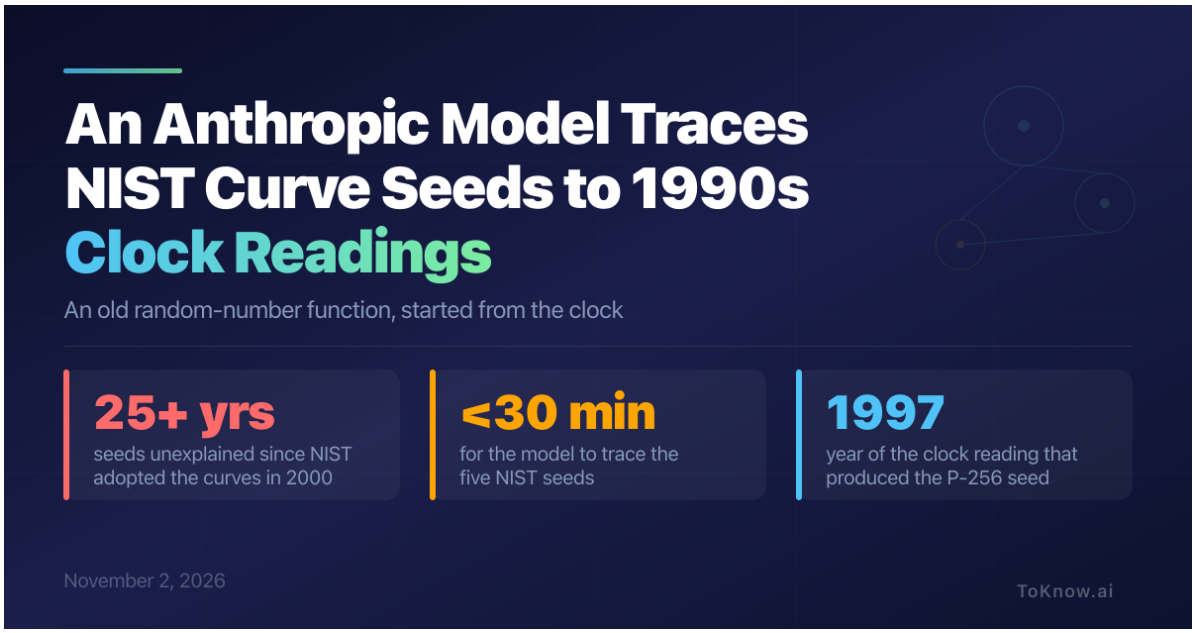
An Anthropic Model Traces NIST Curve Seeds to 1990s Clock Readings

Kabui, Charles

2026-11-02

Read at ToKnow.ai



An internal Anthropic research model found where the web's security curves got their starting numbers, a mystery for over 25 years. These elliptic curves, standardized in 2000 by the US agency NIST, are the math behind digital signatures that prove a website is genuine. Each grows from a "seed", a number the NSA supplied with no explanation. It is like a casino that never shows its draw, so people feared the NSA had tried seeds until one gave a curve only it

could break. Asked by an employee in October 2026, the model traced the seeds in under half an hour to lrand48, a 1990s random-number function.

A deliberate backdoor is less likely, because anyone can rerun the method. lrand48 is a fixed formula, so the same starting value gives the same "random" numbers. The starting value is a Unix timestamp, the clock's count of seconds since January 1, 1970. At 01:52:34 UTC on August 16, 1997 it read 871,696,354. Start lrand48 from that number, take its output in 20-byte batches, and batch 1,842 is the P-256 seed. All five NIST prime-curve seeds trace to clock readings from May 1997 to April 1998.

Anthropic says this exposes no weakness in the curves. Cryptographer Filippo Valsorda rebuilt the method and counts at most about a billion seed choices open to the NSA, too few to hunt for a rare weak curve. Two details remain open: the seed for the B-163 curve, and why the P-256 run skipped a valid earlier candidate.

Read More: An Anthropic science workbench builds a complete ultraviolet sky map, Claude matches chemists' software at identifying molecules and how a TLS 1.3 connection uses an ECDSA P-256 signature

Sources:

- Claude reveals ECDSA curve origins (Anthropic)
- The NIST Elliptic Curves Seeds Bounty Has Been Claimed (Filippo Valsorda)
- A Riddle Wrapped in an Enigma (Neal Koblitz and Alfred Menezes)
- FIPS 186-2, Digital Signature Standard (NIST)
- drand48(3), the lrand48 manual page

Disclaimer: *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*