Are short proofs hard to find?

Andrew V. Sutherland
Massachusetts Institute of Technology

ICEAGE October 28, 2026

Joint work with Alexa McLain, part of the DARPA expMath program.

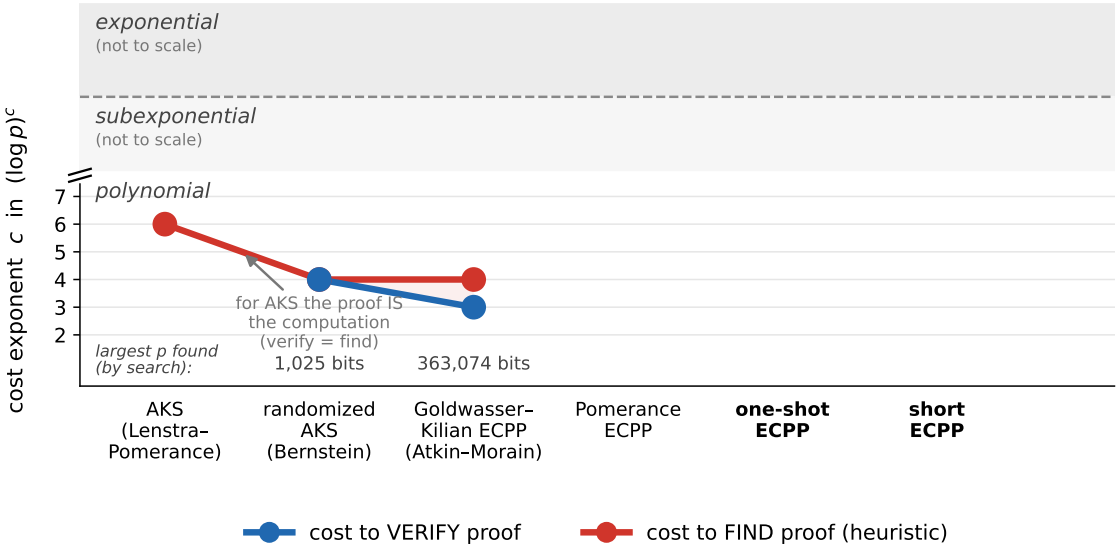
All the computations discussed in this talks were implemented using LLM-based coding agents;
Claude Opus 5.5 wrote the first draft of these slides.

Someone hands you an alleged prime

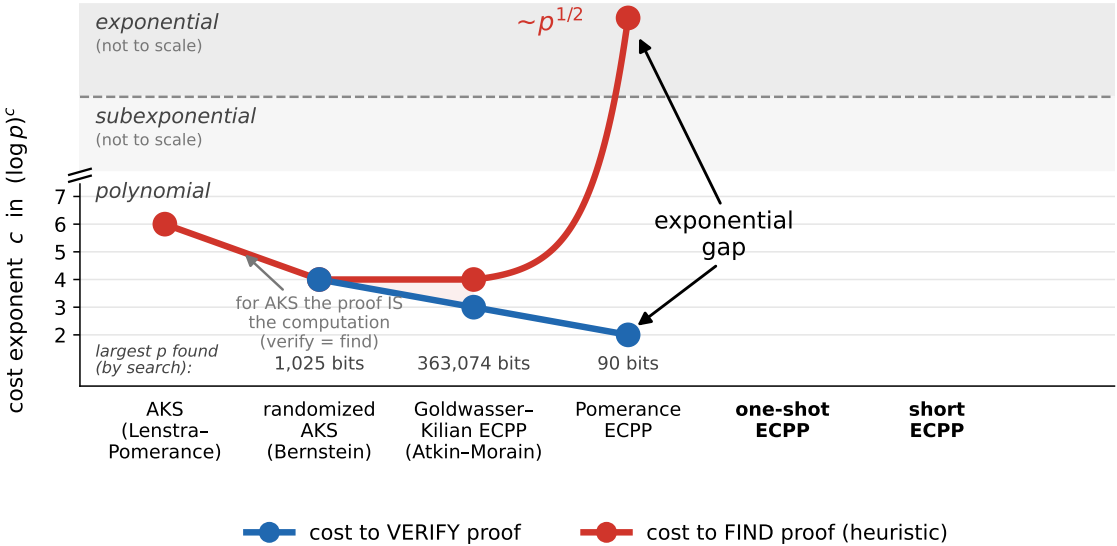
- Field primes of standard curves (P-256, Curve25519, secp256k1, BLS12-381), parameters chosen by someone else (possibly an adversary).
- Probabilistic tests prove nothing; adversarially chosen composites have fooled real libraries. OpenSSL 3 requires ≥ 64 Miller–Rabin rounds (≥ 128 above 2048 bits).
- A primality certificate for p: data whose validity is checked by an efficient *deterministic* algorithm and implies, *unconditionally*, that p is prime.
- Two costs, as for any proof system:
  - FIND the certificate: once, by anyone (or anything); heuristic algorithms are fine;
  - VERIFY it: by everyone, every time; rigorously.

How cheap can verification be, and what does finding then cost?

Find vs. verify



Find vs. verify



The lemma behind every elliptic curve primality certificate

Lemma (Goldwasser–Kilian 1986, Pomerance 1987)

Let $p > 3$ be odd and $L(p) = q + 1 + \lfloor 2\sqrt{q} \rfloor$ with $q = \lfloor \sqrt{p} \rfloor$. If x_0 is the x-coordinate of a point of order *exactly* $m > L(p)$ on $By^2 = x^3 + Ax^2 + x$ modulo every prime $\ell \mid p$, then p is prime. These hypotheses can be satisifed for prime $p > 3$ (using $m = 2^k$).

Proof. If not, a prime $\ell \le \sqrt{p}$ divides p, and $m \le \#E(\mathbb{F}_\ell) \le \ell + 1 + 2\sqrt{\ell} \le L(p) < m$, contradicting the Hasse bound. For existence, $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ contains a multiple of 2^k with $k = \lceil \log_2 L(p) \rceil$, now use the CM method + isogeny volcanoes. □

The verifier runs the Montgomery x-only ladder (as in X25519) modulo p:

- $[m](x_0 : 1) = (X : 0)$ with $\gcd(X, p) = 1$;
- $[m/q](x_0 : 1) = (X : Z)$ with $\gcd(Z, p) = 1$ for each prime $q \mid m$.

No need to check that x_0 is on E: it is on E or its twist, and the ladder serves both.

The verifier must know and verify the prime factorization of m.

Pomerance triples (p, A, x_0): 2.5 Miller–Rabin rounds

$k := \lceil \log_2 L(p) \rceil$. Double $(x_0 : 1)$ k times mod p, check $\gcd(Z_{k-1}, p) = 1$ and $Z_k \equiv 0$.

- Verify: $5k \approx \frac{5}{2} \log_2 p$ multiplications mod p, about 2.5 Miller–Rabin rounds.
- Find: $\#E$ must be one of the 2–4 multiples of 2^k in the Hasse interval, so $\widetilde{\Theta}(\sqrt{p})$ curves. Neither point counting nor CM helps. Best test: one ladder projects P into the 2-Sylow subgroup, then double with early abort.

DANGER3 challenge (BIRS, April 2026); every entry a human + AI collaboration:

p	candidates	resources
$10^{19} + 51$	3.7×10^9	400 s, multithreaded C (Apr 2026)
$10^{24} + 7$	1.8×10^{10}	6 h, laptop (Jun 2026)
$10^{26} + 67$	1.4×10^{11}	45 min, one RTX 6000 GPU (Jun 2026)
$10^{27} + 103$	5.6×10^{12}	52 min, 16 RTX 5090 GPUs (Aug 2026)

One-shot ECPP: relax 2^k to "smooth"

Certificate $(p, A, x_0, m, q_1, \ldots, q_k)$ with $n = \lceil \log_2 p \rceil$: m is n^4-smooth, $L < m < rL$ (r the least prime of m), and $q_1 < \cdots < q_k$ are the primes of m in (n^2, n^4).

- Verify: trial-divide m by the primes below n^2 (remainder trees); what is left must be exactly the q_i. No primality tests needed: a composite in (n^2, n^4) has no divisors $> n^2$. $O(n^2(\log n)^2)$ bit operations.

- Find: need the n^4-smooth part of $\#E$ to exceed $L \approx \sqrt{p}$. By Dickman, this happens with probability

$$\rho(u/2)^{1+o(1)} = p^{-1/8+o(1)}, \qquad u = \frac{\ln p}{\ln n^4},$$

so $p^{1/8+o(1)}$ with random curves (SEA) and $p^{1/4+o(1)}$ with the CM method. Both $o(1)$ are negative, especially the second (CM beats SEA for a long time).

Your favorite primes, certified

Curve25519: $p = 2^{255} - 19$, $n = 255$, $(n^2, n^4) = (65025,\ 4.2 \times 10^9)$

```
A  = 437239380964693581744653678253266551762067077077329106579272222259745941308
x0 = 213115656186445074078169027384953638449830067523086529248868815733501378176 62
m  = 149 * 727 * 679409 * 770503 * 12519979 * 15032243 * 58136053
```
(129 bits)

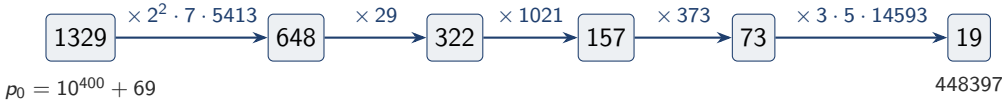
Verification time is under 200 microseconds.

prime	how
Curve25519, P-256, secp256k1	CM search, 4–11 s on 16 cores
BLS12-381	CM search, 18 s on 256 cores
P-384	$p \equiv 3 \bmod 4$, so $y^2 = x^3 + x$ has $p + 1$ points; $p + 1$ has a 197-bit n^4-smooth part
P-521	$p + 1 = 2^{521}$, so $y^2 = x^3 + x$ gives a Pomerance triple with $m = 2^{261}$
$10^{120} + 79$ (generic, 399 bits)	CM search, minutes on 256 cores

Short ECPP: add recursion

Certificate $(p_0;\ A_0, x_0, o_0;\ \ldots;\ A_k, x_k, o_k)$; $n = \lceil \log_2 p_0 \rceil$ fixed, $B = \lceil n^2 / \log_2 n \rceil$.

- $o_i = m_i \cdot p_{i+1}$: m_i is B-smooth with $\log_2 \mathrm{rad}(m_i) \le \lceil n / \log_2 n \rceil$; p_{i+1} is B-rough with $B^2 < p_{i+1} < \sqrt{p_i}$.
- $L(p_i) < o_i < r_i L(p_i)$; point of order exactly o_i modulo every prime $\ell \mid p_i$.
- Primality of p_{i+1} is the next level's job. Stop at $p_{k+1} < B^2$: B-rough and below B^2 means 1 or prime.



Bits at least halve: $O(\log n)$ levels, $\lesssim 5n$ bits (6,328 here); ≈ 10 Miller-Rabin rounds.
Verify: $O(n^2 \log n)$ Find: subexponential.

Why finding is subexponential

One level: find $E/\mathbb{F}_p$ with $\#E = S \cdot q$, q prime $\approx\sqrt{p}$ (the next level).
The prover has to *see* q: the rest of $\#E$ must peel off by ECM within a budget y.

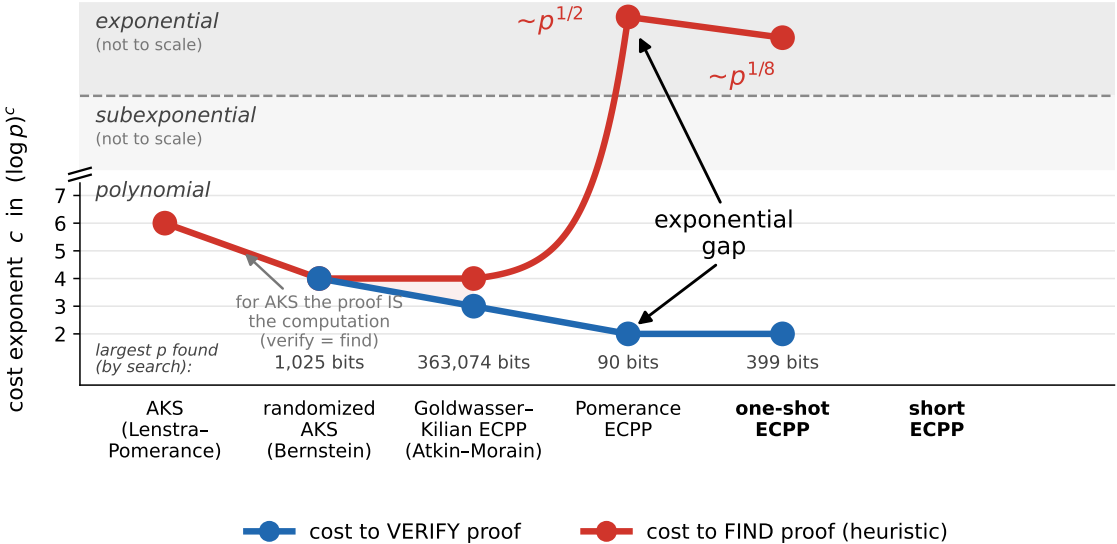
- candidates needed: $1/\rho(u)$, $u = \ln\sqrt{p}\,/\ln y$ (Dickman)
- cost per candidate: $L_y(1/2, \sqrt{2})$ (ECM)
- balance with $\ln y = \gamma(\ln p)^{2/3}(\ln\ln p)^{1/3}$; the total is $L_p(1/3,\ \frac{1}{6\gamma} + 2\sqrt{\gamma/3})$, minimized at $\gamma = 12^{-1/3}$:

$$L_p(1/3,\ (3/2)^{1/3} \approx 1.14),$$

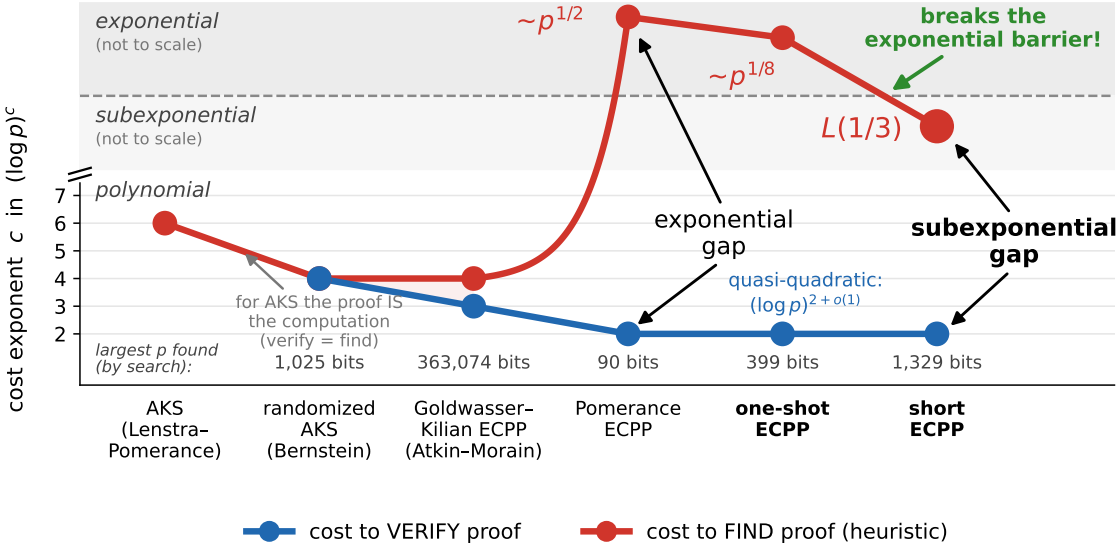
cheaper than factoring p by the number field sieve, $L_p(1/3, (64/9)^{1/3} \approx 1.92)$, which is also what a Pratt certificate costs.

- The same constant for both supplies of orders: random curves + SEA, or CM. The CM discriminant scan costs $L_p(1/3, 0.76)$ and never dominates.
- Each level down shrinks the exponent by $2^{-1/3}$, so the top level dominates.

Are short proofs hard to find?



Are short proofs hard to find?



Open problems

1. Beat $\widetilde{\Theta}(\sqrt{p})$ for Pomerance triples, or explain why CM, isogenies, torsion families and sieving cannot: "$2^k \mid \#E$" has no multiplicative structure to sieve on.

2. One-shot via CM: close $p^{1/4}$ vs. $p^{1/8}$. This needs an output-sensitive enumeration of $4p = t^2 + |D|v^2$ *and* a root of H_D mod p in $h(D)^{1+o(1)}$ time.

3. The find/verify trade-off. Is there a certificate with (even heuristic) polynomial-time finding and $n^{2+o(1)}$ verification?
   - AKS–Bernstein: $(\log p)^{2+o(1)}$ to find, $(\log p)^{4+o(1)}$ to verify.
   - Short ECPP: $(\log p)^{2+o(1)}$ to verify, $L(1/3)$ to find.

4. Rigor: prove that a positive proportion of curves $E/\mathbb{F}_p$ have a y-smooth part of $\#E$ exceeding $\sqrt{p}$. Every finding bound here is heuristic.

5. Is $\frac{5}{2}\log_2 p$ multiplications optimal for general p?

Thank you

- Challenges (definitions, reference verifiers, leaderboards):
  - `github.com/AndrewVSutherland/DANGER3`
  - `github.com/AndrewVSutherland/OneShotPrimalityProofs`
  - `github.com/AndrewVSutherland/ShortPrimalityProofs`
- Certificates welcome.