MOBILALLY WHITE PAPER SERIES · No. 2

Obscurity's Half-Life

Google concealed a cryptographic breakthrough. AI agent swarms reproduced it in eight hours — and beat it in three days. What that means for how we secure anything.

The event

In March 2026, researchers at Google Quantum AI and their collaborators announced a significant optimization of Shor's algorithm against 256-bit elliptic-curve cryptography — the mathematics securing most internet traffic and most cryptocurrency. Their construction required roughly 1,200–1,450 logical qubits, encodable in fewer than half a million physical qubits, completing the attack in under half an hour of runtime. It was the second time in two years that the estimated quantum resources for breaking deployed cryptography had fallen by roughly a factor of twenty — and both reductions came from better algorithms, not better hardware.

Then the researchers did something unprecedented: after consultation with the U.S. government, they published the result behind a *zero-knowledge proof* — a cryptographic technique that let outsiders verify the attack worked without learning how to perform it. For the first time, a major cryptanalytic advance was deliberately released as a verified secret.

Seventy-two hours

The secret did not survive the week. A small Seattle research startup, Eigen Labs, built software to test candidate quantum circuits against Google's public verifier, then pointed swarms of AI agents — coordinated with human quantum scientists through an open crowdsourcing platform — at the problem. Within eight hours, the open effort matched Google's concealed result. Within roughly seventy-two hours, it surpassed it. By the end of June, the open network's best circuit was 47.5 percent more efficient than the one Google had tried to keep hidden. An academic researcher in France, working independently and citing only public literature, matched the result in the same window.

The researchers involved drew the honest conclusion. Google's own scientist wrote afterward that concealment was not the right strategy going forward. Academics were blunter: in a competitive research environment saturated with capable AI tooling, no result stays ahead of the community for long.

> ***"In the AI era, secrecy has a half-life measured in hours. The only defenses left standing are mathematics and physics."***

What this actually teaches

It is tempting to read this story as being about quantum computing timelines — and it is; standards officials said on the record that these results should accelerate migration plans, and U.S. policy now requires high-value federal systems to complete the post-quantum transition by the end of 2030. But the deeper lesson is architectural, and it applies to every security program, quantum or not:

- **Obscurity is no longer a control.** Any defense whose effectiveness depends on an adversary not knowing how it works now has a measurable expiry — and the measurement just came in at hours, not

years. Hidden mechanisms, proprietary protocols, secret configurations, and undisclosed vulnerabilities all decay on the same curve.

- **AI industrializes cryptanalysis and reverse engineering.** The attackers' side of the ledger just gained the ability to coordinate thousands of tireless optimizers against a single target. Whatever asymmetry defenders enjoyed from complexity is gone.
- **Verifiability beat secrecy — even for the secret-keeper.** The one part of Google's release that worked exactly as designed was the mathematics: the zero-knowledge proof let the world verify the claim without trusting anyone. The concealment failed; the cryptography held.

What still holds

Strip away everything with a half-life and two foundations remain. The first is **mathematics**: cryptographic algorithms whose security rests on published, worldwide-attacked hard problems — which today means the standardized post-quantum suite, deployed with the agility to replace any member of it that falls. The second is **physics**: security properties enforced by hardware boundaries — keys generated from physical entropy and held in silicon that no software, however clever and however assisted, can reach across. A secret key inside a hardware boundary is not obscurity; it is not a hidden *mechanism* but a protected *object*, and its protection does not depend on the adversary's ignorance of the design.

This is also the honest completion of the Zero Trust doctrine. Zero Trust won the argument a decade ago: verify everything, trust nothing. But verification has to bottom out somewhere — some claim must be true not because software asserts it but because physics enforces it. In an era when AI can manufacture perfect forgeries of nearly any digital claim, the last ground truth is a claim the hardware refuses to forge.

The takeaway for builders and operators

- Audit your architecture for obscurity dependencies — anything whose failure mode is "the adversary figured out how it works." Assume that date is near.
- Migrate to standardized post-quantum cryptography on the federal clock, and require cryptographic agility so the next algorithmic surprise is a configuration change, not a fleet replacement.
- Anchor identity and key custody in hardware. Mathematics protects data in flight; physics protects the keys at rest. A security program standing on both has nothing left that decays in seventy-two hours.

About MobilALLY

MobilALLY LLC is a service-disabled veteran-owned small business building hardware-rooted, post-quantum cryptographic modules for edge, mobility, and defense platforms. Our design doctrine is the one this story vindicates: security that requires no belief — standardized mathematics, physically isolated key custody, hardware entropy, and a root of trust that can be updated as the standards evolve. Learn more at www.mobilally.io.

Sources

IEEE Spectrum, "Independent Labs Crack Google's Secret Cryptography Work," July 7, 2026.

Google Research blog, "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly," 2026.

Gidney et al., quantum resource estimates for RSA-2048 (2025) and 256-bit ECC (2026), arXiv.
Executive Order, “Securing the Nation Against Advanced Cryptographic Attacks,” June 22, 2026.
NIST FIPS 203/204/205 (2024); NIST CSWP 39, Considerations for Achieving Cryptographic Agility (2025).