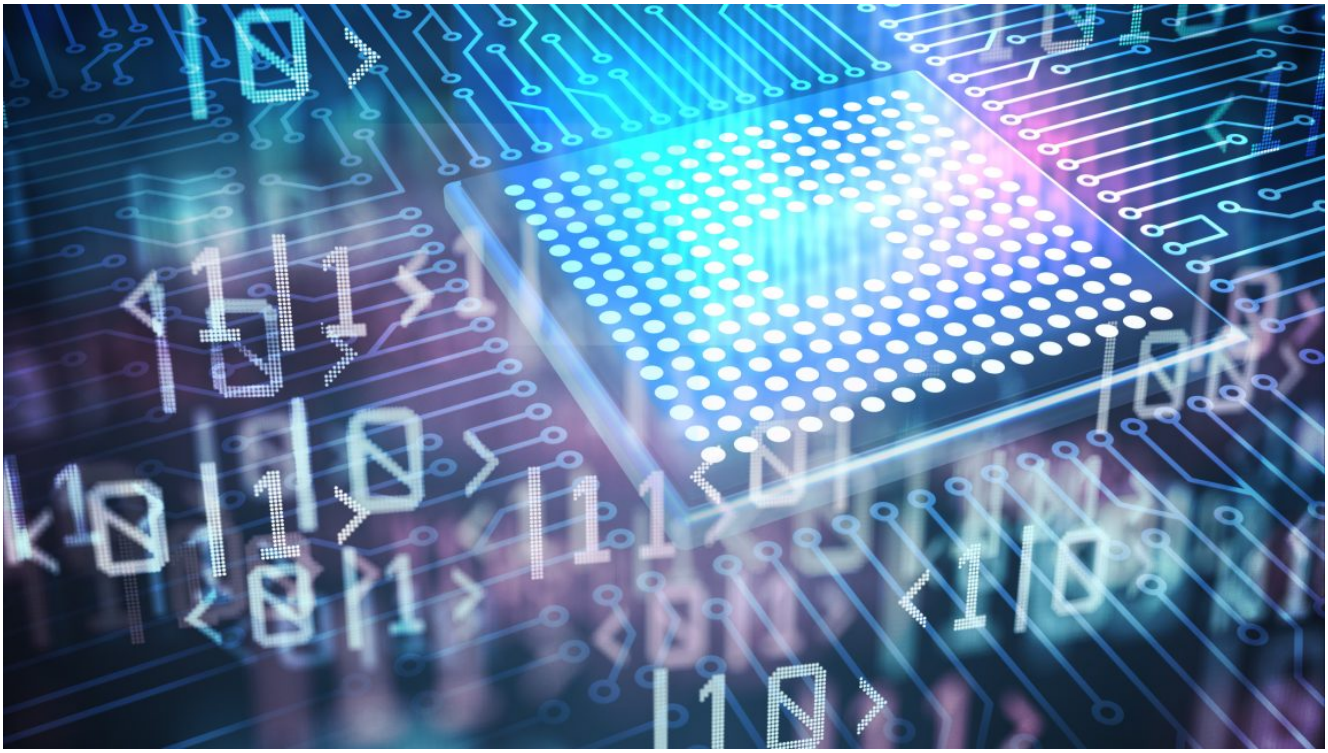
Recent advances push Big Tech closer to the Q-Day danger zone



Interestingly, Amazon is using SigV4, an impromptu algorithm it developed in-house to make authentication quantum-safe.

“AWS limits the transmission of these secrets to the moment of generation,” Campagna wrote. “Once initially distributed, it is never re-sent to the customer. While we made this decision to operate at the massive scale of AWS, we avoided the need to migrate [to] a public-key based authentication solution.”

For customers who need long-lived roots of trust, Amazon uses its AWS Private CA (certificate authority) with KMS, a key management service that complies with FIPS 204, a NIST certification for post-quantum readiness. Customer data at rest is encrypted and then stored using AES-256, a symmetric algorithm that quantum computers have no advantage over classical computing in breaking.

The most distant PQC readiness deadline is 2033 for Microsoft. Meta and Apple didn’t provide any date at all when asked earlier this week.

“Post-quantum cryptography (PQC) isn’t a flip-the-switch change,” Mark Russinovich, Azure CTO and deputy CISO and technical fellow at Microsoft, wrote in an email. “We have been at the forefront of PQC planning since 2014 as a founding member of the Open Quantum Safe project and a close collaborator with vendors, standards bodies, and government agencies.”

He added that Microsoft’s rollout is guided by three principles: “Prioritize standards—follow NIST, not proprietary crypto; avoid breaking global customers; and roll out in a platform-focused way, starting with Windows, Azure, and identity layers. This mirrors past transitions with SHA and TLS, but with greater urgency given quantum risk.” Note that Russinovich didn’t mention Microsoft’s migration off of MD5.

Meta, meanwhile, hasn’t publicly stated its deadline. On Thursday, the company published a post that mostly rehashed a previous one from two years ago. Neither set a deadline. Instead, Thursday’s post was aimed at advising the industry on key principles. It also introduced a taxonomy of “PQC maturity levels.” They are PQ hardened, PQ ready, PQ aware, and PQ unaware.

https://arstechnica.com/security/2026/04/while-some-big-tech-players-accelerate-pqc-readiness-others-stay-the-course/