Googles roadmap for the post-quantum transition

We often talk about quantum computing in the context of physics or future hardware capabilities. However, for software engineers and infrastructure architects, the “quantum era” is primarily a migration project. It involves a fundamental swap of the mathematical primitives that underpin internet security, moving from classical algorithms to Post-Quantum Cryptography (PQC).

Google’s recent publication outlines their internal roadmap for this transition, offering a valuable case study for the rest of the industry. The focus here is not on the "if" or "when" of quantum hardware, but on the concrete engineering steps required to modernize our cryptographic stack today.

Standardizing the math

The most significant shift is that PQC is no longer an abstract research topic; it has standardized implementations. The National Institute of Standards and Technology (NIST) has finalized the primary algorithms: **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism) for general encryption and **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm) for digital signatures.

Google is actively integrating these standards into Chrome and its internal infrastructure. This moves PQC from the realm of academic papers into production libraries, meaning developers can—and should—start treating these new algorithms as the default targets for long-term system design.

The inventory challenge

Perhaps the most practical insight from Google’s roadmap is that the biggest hurdle isn't mathematical—it's organizational. Before you can upgrade your encryption, you have to find it. Many systems rely on "shadow cryptography": keys and algorithms hardcoded into legacy appliances, older codebases, or third-party dependencies.

The transition to PQC forces organizations to solve the **cryptographic discovery** problem. It requires building automated tooling to scan binaries, network traffic, and configurations to create a comprehensive inventory of where and how encryption is being used. You cannot upgrade what you cannot see.

Building for agility

Ultimately, this transition highlights the importance of **crypto-agility**. In the past, encryption protocols were often baked deeply into application logic, making them difficult to replace. The modern approach treats cryptography as a modular component.

By abstracting cryptographic implementations, systems can switch between algorithms (classical, PQC, or hybrid) via configuration rather than requiring code rewrites. Google’s approach suggests that this agility is not just a preparation for quantum computing, but a best practice for healthy, maintainable software architecture in general.

Contributor: Alessandro Linzi