Navigating the Legal Safety Net of NIST's Post-Quantum Cryptography Patent Licenses

James Gatto and Fred Qiu

The global migration to post-quantum cryptography (PQC) is no longer a theoretical exercise. It is actively underway. Following the National Institute of Standards and Technology's (NIST) release of its finalized FIPS standards for quantum-resistant algorithms, including the Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM) and the Module-Lattice-Based Digital Signature Standard (ML-DSA), commercial entities are engaging in a massive infrastructure overhaul.

Yet, for general counsel and IP attorneys, cybersecurity and technical feasibility are only part of the challenge. When transitioning vital digital infrastructure to a new cryptographic standard, intellectual property can become a significant roadblock. Certain PQC algorithms—most notably CRYSTALS-Kyber, now standardized as ML-KEM—have been the subject of third-party patent claims. To remove that obstacle to widespread adoption, NIST secured two broad, royalty-free patent licensing agreements for the benefit of implementers. But these licenses have important limitations. Understanding their boundaries, mechanics, and legal protections is crucial for any organization mapping out its post-quantum migration strategy.

The IP Bottleneck in Standardized Cryptography

Historically, implementing new cryptographic standards has been a legal minefield. If a standardized algorithm relies on technology covered by third-party patents, implementers risk facing patent-license demands or infringement lawsuits.

During the multi-year PQC selection process, concerns arose when public commenters asserted that implementations of certain candidate algorithms—most notably CRYSTALS-Kyber[1] (now standardized as **ML-KEM**)—could implicate privately owned patent portfolios.

NIST understood the practical reality: even the most secure algorithm would fail as a standard if commercial developers were too concerned about patent enforcement to deploy it. To clear the legal runway, NIST did more than select and publish a technical standard: it acted as a master negotiator, securing two royalty-free patent licenses for the benefit of ML-KEM implementers.

Anatomy of the NIST PQC Patent Licenses

NIST successfully secured two broad, royalty-free licensing agreements covering patents alleged to be essential to implementations of CRYSTALS-Kyber. [2] The two agreements address:

---

[1] CRYSTALS-Kyber is a key encapsulation mechanism (KEM) designed for secure key establishment, particularly in the context of post-quantum cryptography. It is based on the presumed hardness of the learning-with-errors (LWE) problem over module lattices. CRYSTALS-Kyber aims to provide security against both classical and quantum attacks.

[2] See here for NIST's license summary and excerpts.

1. **The U.S. Portfolio:** An agreement covering patents privately held by Algo Consulting, Inc.

2. **The French Portfolio:** An agreement covering a patent portfolio controlled by the French National Center for Scientific Research (CNRS) and the University of Limoges.

Key Terms and Legal Protections

Together, the agreements create several layers of protection for implementers and their end users:

- **Automatic Protection for "Implementers":** The agreements are structured so that any "Implementer"—defined broadly as any entity, person, company, organization, foundation, or business, whether private, public, or governmental, that implements the algorithm for commercial or non-commercial purposes—receives the benefits of the patent license.

- **Enforcement in Abeyance:** The licensors have legally agreed, on a royalty-free basis, to place into abeyance any right of enforcement against implementers and their end-users.
- **Fully Paid-Up and Irrevocable:** The license grants are fully paid-up and irrevocable and are made on behalf of the licensors and their successors and assigns, ensuring that the protections survive a corporate restructuring or subsequent transfer of the licensed patents.
- **Release of Past Claims:** The agreements also release infringement claims arising before their effective dates.

The "Field of Use" Limitation: These protections are strictly limited to implementations of current and future CRYSTALS-Kyber-based PQC standards published by NIST.[3] If a developer's implementation falls outside those covered standards, the developer leaves the "Field of Use" safety zone and may face potential patent claims.

Why This Matters for Corporate Counsel and C-Suites

1. Open Source Certainty

Many enterprise-grade software solutions rely heavily on open-source libraries, such as OpenSSL and BoringSSL, to handle encryption. Standard open-source licenses are notoriously ambiguous regarding explicit patent grants from third parties. The NIST agreements help close that gap by providing independent protection under the licensed patent portfolios for in-scope implementations of ML-KEM, regardless of the underlying software license.

2. De-Risking the Supply Chain

When auditing an organization's cybersecurity supply chain, customers often seek assurances and sometimes indemnification against patent infringement. The NIST agreements reduce the patent risk associated with in-scope ML-KEM implementations, simplifying vendor diligence and procurement and lowering software deployment costs.

3. Compliance and Deprecation Deadlines

The federal government is already setting aggressive PQC migration deadlines. Executive Order 14412 directs the FAR Council to propose rules requiring covered federal contractors to comply with applicable PQC-related FIPS by December 31, 2030. This moves the deadline up from the previously proposed 2035 timeline. With the identified patent issues resolved for in-scope ML-KEM implementations, "IP risk" becomes a far less persuasive justification for delaying PQC migration.

---

[3] The French portfolio agreement defines the "Field of Use" more broadly to include any standards based on NIST-selected PQC algorithms.

4. A Safe Harbor, Not a Blanket Clearance

The NIST agreements neutralize the risks associated with the licensed patent portfolios, but they are not a blanket freedom-to-operate for every ML-KEM product. Other potentially relevant patents may still require consideration, particularly where an implementation departs from the standardized algorithm or incorporates additional proprietary technology.

The Road Ahead: Ongoing Vigilance Required

While NIST has secured a major legal coup for ML-KEM implementation, the job is not completely finished. The agreements do not extend to ML-DSA or other PQC algorithms, and NIST is developing additional standards based on Falcon (FN-DSA) and HQC to provide alternative signature and key-establishment options.

As these additional standards emerge, legal teams must continue to monitor public IP disclosures and licensing commitments. NIST has not published comparable negotiated patent licenses for Falcon or HQC, and each new standard must be evaluated on its own IP record. This adds one more layer to the complexity of PQC migration.

Conclusion

The patent issues with PQC encryption are just one of many patent and other IP-related quantum issues. For quantum developers, patenting quantum technology presents its own nuances. Patent filings are increasing at a double-digit rate, and a growing number of quantum patent applications have reached the appeal stage, providing valuable insight into how patent law applies to quantum technologies. For practical guidance, see *Patenting the Quantum Future – Practical Tips Based on PTAB Decisions*. And patents are just one piece of the quantum IP puzzle. For more of an overview of quantum IP issues, see *Quantum Computing and Intellectual Property Law in the United States: Emerging Challenges and Strategic Considerations*.

Contacts

James Gatto

Partner | AI, Robotics and Quantum Team Co-Leader

+1.202.747.1945

jgatto@sheppard.com

Bio

Fred Qiu

Partner

+1.650.815.2652

fqiu@sheppard.com

Bio