# **Quantum-Safe Cryptography in Software Engineering**

**Introduction:** Modern public-key cryptography faces a looming threat from quantum computers. Algorithms like RSA and ECC, which secure today’s digital communications, could be **broken by Shor’s algorithm on a sufficiently powerful quantum computer** ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Shor%E2%80%99s%20algorithm%20breaks%20all%20widely,between%20them%20are%20quite%20different)) This means an adversary with a future quantum computer might decrypt sensitive data that was encrypted under current methods. Experts warn that attackers may already be **harvesting encrypted data now to decrypt later** (“store-now, decrypt-later”) once quantum capabilities arrive ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=More%20urgently%2C%20though%2C%20an%20attacker,is%20at%20risk)) ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=%E2%80%9CWhat%E2%80%99s%20the%20data%20that%20you%E2%80%99d,%E2%80%9D)) In anticipation of this, the field of *quantum-safe* or *post-quantum cryptography (PQC)* has developed new algorithms believed secure against quantum attacks. The U.S. National Institute of Standards and Technology (NIST) has led a multi-year effort to standardize these new algorithms ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=In%202016%2C%20NIST%20recognized%20the,the%20%2023%20%20Federal)) This report examines key aspects of quantum-safe cryptography in software engineering, including the NIST-selected post-quantum algorithms, strategies for migrating existing systems, performance considerations, library and protocol support, ongoing research/standardization efforts, and real-world case studies of PQC adoption.

## **1. Post-Quantum Algorithms**

**NIST-Recommended Algorithms:** After a six-year public competition, NIST announced in 2022 the first group of quantum-resistant algorithms to be standardized ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=The%20first%20four%20algorithms%20NIST,resist%20a%20quantum%20computer%27s%20assault)) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=replacement%20for%20two%20types%20of,Processing%20Standards%20%28FIPS)) For **public-key encryption and key exchange**, NIST selected **CRYSTALS-Kyber**, a lattice-based Key Encapsulation Mechanism (KEM). Kyber’s design offers strong security from the hardness of the lattice *Learning-With-Errors (LWE)* problem and features **small encryption keys and fast operation** ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=the%20CRYSTALS,as%20its%20speed%20of%20operation)) Reviewers noted that Kyber achieves a good balance of performance and key size – for example, its keys and ciphertexts are on the order of a kilobyte, much smaller than some other PQC candidates, making it practical for network use ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=the%20CRYSTALS,as%20its%20speed%20of%20operation)) In fact, **Kyber is very fast—considerably faster than the popular X25519 elliptic-curve key exchange**—with the trade-off of slightly larger messages (about an extra 1.5 KB in a TLS handshake) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) This efficiency and moderate size made Kyber the primary choice for post-quantum key agreement.

For **digital signatures**, NIST selected three algorithms: **CRYSTALS-Dilithium**, **FALCON**, and **SPHINCS+** ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections)) Dilithium and FALCON are both lattice-based signature schemes, while SPHINCS+ uses a hash-based (Merkle tree) approach. **CRYSTALS-Dilithium** is recommended as the primary general-purpose signature algorithm due to its **high efficiency** in signing and verification ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections)) Its keys and signatures, based on module lattices, are relatively compact (e.g. a Dilithium signature is a few kilobytes) and it has fast performance, making it suitable for many applications. **FALCON** is another lattice scheme which produces **smaller signatures than Dilithium** (hundreds of bytes) at the cost of a more complex implementation; NIST suggests FALCON for use-cases that demand very small signature sizes (such as certain certificates) ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections)) The third, **SPHINCS+**, is a stateless hash-based signature scheme. SPHINCS+ has much larger signatures (tens of kilobytes) and slower signing times compared to the lattice schemes, **trading efficiency for a completely different security basis** ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=algorithms%20CRYSTALS,three%20of%20NIST%E2%80%99s%20other%20selections)) NIST included SPHINCS+ mainly as a *conservative backup*, since its security relies only on hash functions. Having diversity in math approaches is considered wise in case a breakthrough occurs against lattice-based assumptions ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=high%20efficiency%20of%20the%20first,three%20of%20NIST%E2%80%99s%20other%20selections))

All **four NIST PQC algorithms (Kyber, Dilithium, FALCON, SPHINCS+) are designed to withstand quantum attacks**, unlike RSA or ECC. Their security comes from problems believed to be hard for both classical *and* quantum computers ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=messages%20are%20inaccessible%20to%20unwelcome,third%20parties)) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=called%20%20learning%20with%20errors,help%20of%20a%20quantum%20computer)) For example, Kyber and Dilithium rely on lattice problems (like LWE) for which no efficient quantum algorithm is known ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Although%20NIST%20chose%20CRYSTALS,with%20help%20of%20a%20quantum)) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=called%20%20learning%20with%20errors,help%20of%20a%20quantum%20computer)) SPHINCS+ relies on hash preimage resistance, which is only mildly affected by Grover’s algorithm (Grover’s can at most halve the security of hash-based schemes, manageable by choosing larger hashes). This contrasts with traditional public-key cryptography: **RSA’s factoring problem and ECC’s discrete logarithm problem are both solvable by Shor’s algorithm**, meaning a quantum computer could break them in polynomial time ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=computers,has%20been%20underway%20for%20decades)) In summary, the NIST PQC algorithms are built on mathematical foundations (lattices and hash functions) that are believed to resist all known quantum attacks ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=The%20first%20four%20algorithms%20NIST,resist%20a%20quantum%20computer%27s%20assault)) ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=high%20efficiency%20of%20the%20first,three%20of%20NIST%E2%80%99s%20other%20selections)) They have also undergone extensive public cryptanalysis during the NIST competition, giving confidence in their resilience.

**Comparison to Traditional Cryptography:** Post-quantum algorithms generally require larger key and ciphertext sizes than legacy algorithms, but offer security against quantum adversaries. For example, Kyber adds about 1500 bytes of overhead to a key exchange compared to the widely used X25519 elliptic curve ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) Dilithium signatures are on the order of 2–3 KB (kilobytes), whereas an RSA-2048 signature is 256 bytes, yet Dilithium is much faster to generate and verify than RSA. These increases in size are the price of quantum safety. Fortunately, in many cases the sizes are still practical – Kyber’s **“comparatively small encryption keys”** are specifically highlighted as an advantage that “two parties can exchange easily” in network protocols ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=the%20CRYSTALS,as%20its%20speed%20of%20operation)) Performance-wise, many PQC schemes are quite competitive with or even faster than classical algorithms. A meta-analysis of NIST’s finalists found that **lattice-based schemes like Dilithium excel in performance**, offering low latency and efficient operation even on constrained devices () () In tests, Dilithium stood out as one of the **most efficient options for low-latency applications**, demonstrating that quantum safety can be achieved without sacrificing speed () Overall, the NIST-selected algorithms aim to replace RSA/ECC by providing similar functionality (key exchange, signatures) with acceptable performance and significantly improved security margins in the quantum era.

NIST is finalizing standards for these algorithms (to be published as FIPS standards). In fact, by 2024 NIST **released draft standards for Kyber (as “ML-KEM”), Dilithium (“ML-DSA”), and SPHINCS+ (“SLH-DSA”)** and deemed them ready for use ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=NIST%20has%20finalized%20the%20three,infrastructure%20for%20the%20quantum%20era)) ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=NIST%20earlier%20today%20released%20three,could%20serve%20as%20backup%20standards)) These will form the core of cryptographic suites going forward. It’s worth noting that NIST is also evaluating additional candidates in a fourth round (such as a code-based encryption scheme like Classic McEliece) to further diversify the quantum-safe toolbox ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=Four%20additional%20algorithms%20are%20under,the%20event%20one%20proves%20vulnerable)) But **Kyber and Dilithium, in particular, are expected to be the workhorses** of post-quantum encryption and signing for most software engineering needs, much as RSA and ECC have been for the past decades ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections))

## **2. Migration Strategies**

Transitioning existing cryptographic infrastructure (PKI, TLS/SSL, digital signatures, etc.) to quantum-safe algorithms is a complex endeavor. Organizations cannot simply “flip a switch” without risking service disruptions, because these new algorithms must interoperate with vast legacy systems and standards. Instead, careful **migration strategies** and *crypto-agility* are required.

**Planning and Crypto-Agility:** A first best-practice step is for organizations to **discover and inventory all uses of cryptography** in their systems ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page)) NIST and cybersecurity agencies recommend that companies *identify every application, system, and protocol* that relies on public-key cryptography, since **those will need replacement or upgrading before quantum attacks become a reality** ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page)) Many large organizations have begun this process. For example, a U.S. White House memo in 2022 directed federal agencies to inventory their vulnerable cryptographic systems within months ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=The%20White%20House%20in%202022,so%20they%20can%20be%20replaced)) Knowing where RSA, ECC, or other quantum-vulnerable algorithms are used (in certificates, TLS configurations, code bases, embedded devices, etc.) is crucial to formulate a migration plan.

Once the inventory is in place, organizations should embrace **crypto-agility** – designing systems to be flexible and updatable in terms of cryptographic algorithms. IBM, for instance, has advised enterprises to approach quantum safety as a **“people, process, and technology” transformation**, emphasizing the need to *increase cryptographic maturity* and be ready to “update, change, monitor, and retire cryptography” as needed ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=The%20journey%20toward%20quantum,platforms%2C%20systems%20and%20applications%20to)) In practice, this means building support for new algorithms alongside old ones, using modular cryptographic libraries, and avoiding hard-coded assumptions about key sizes or algorithm types. A crypto-agile system can more readily swap in a post-quantum algorithm (or switch again if a chosen algorithm is later found flawed) with minimal disruption. Organizational leaders are establishing **“quantum-safe transition” programs** to coordinate these efforts ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=IBM%20has%20engaged%20with%20many,powered%20risks)) This often involves training personnel, allocating budget for upgrades, and raising awareness at the executive level that a crypto migration is a strategic imperative, not just an IT task ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=IBM%20has%20engaged%20with%20many,powered%20risks))

**Hybrid Deployment Approaches:** One key migration strategy emerging from both NIST guidance and industry practice is *hybrid cryptography*. Rather than replacing existing algorithms overnight, **new quantum-safe algorithms are deployed in tandem with traditional algorithms** during a transition period ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Now%20that%20NIST%20has%20standardized,in%20conjunction%20with%20existing%20techniques)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=In%20this%20experiment%20we%20used,will%20have%20little%20performance%20impact)) For example, in TLS handshakes, one can perform **dual key agreement**: the client and server generate a shared secret using a classical algorithm (like ECDH with X25519) *and* a shared secret using a PQC algorithm (like Kyber), and then combine them. This was exactly the approach used in Google’s Chrome experiments (CECPQ1, CECPQ2) where a hybrid of X25519 and a lattice-based KEM were used to negotiate TLS keys ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=Similarly%20to%20its%20predecessor%20CECPQ1,52%20supersingular%20isogeny%20key)) ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=a%20plugin%20for%20the%20TLS,2)) The benefit of a hybrid is defense in depth: even if the new post-quantum scheme later turned out to be weak, the classical scheme would still provide security (and vice versa). NIST currently **advises deploying PQC alongside existing well-vetted crypto** rather than as a wholesale replacement in the immediate term ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Now%20that%20NIST%20has%20standardized,in%20conjunction%20with%20existing%20techniques)) to maintain safety until the new standards are battle-tested. In practice, many real-world implementations follow this advice. For instance, OpenSSH 9.0 by default uses a *hybrid key exchange* combining *NTRU Prime (a PQC algorithm) with X25519*, so that the resulting SSH session key is secure unless both the lattice scheme and ECDH are broken ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Of%20course%2C%20TLS%20is%20not,quantum%20SSH%20keys)) Similarly, certificates or digital signatures can be dual-signed: one signature with ECDSA and one with Dilithium, for example, to ease migration for verifiers. This approach ensures **backward compatibility** (old clients can ignore the new algorithm and still work with the old, and vice versa) and buys time to field-harden PQC.

**Maintaining Services During Migration:** Organizations are wary of disrupting running systems like websites, VPNs, or software update channels. Thus, migrations are often phased gradually. A typical strategy might be: enable quantum-safe ciphersuites on servers **in addition to** existing ciphersuites, rather than replacing them immediately. This way, clients that understand the new algorithms can use them, and others will gracefully fall back to the old ones. For example, Cloudflare and Google’s joint experiment added new hybrid ciphers to TLS and only clients that knew about them (a special build of Chrome) would negotiate them ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=secret%20key,should%20HRSS%20be%20found%20insecure)) ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=The%20algorithm%20was%20to%20be,users%20accessing%20websites%20hosted%20by)) This kind of gradual rollout can be done in a controlled manner (perhaps start with internal or beta users, then expand) to monitor for issues.

**Challenges and Real-World Hurdles:** Despite careful planning, there are challenges to migrating mission-critical systems to PQC:

* *Compatibility:* Some software or hardware cannot handle the larger key sizes or message lengths of PQC algorithms, which can cause failures if not addressed. An example encountered during trials was that certain TLS implementations would **crash or error out when presented with the larger handshake messages** containing post-quantum keys ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=So%20can%20we%20switch%20to,Stay%20tuned)) These implementations had assumptions (like buffer sizes or message formats) tuned for legacy algorithms. The solution is often to patch or update those systems, but it requires effort. Part of migration planning is identifying such incompatible components early. Anne Neuberger (U.S. Deputy National Security Advisor) noted that agencies have been *“identifying systems that can’t support post-quantum cryptography so they can be replaced”* in advance ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=The%20White%20House%20in%202022,so%20they%20can%20be%20replaced)) Replacing or upgrading legacy hardware (e.g. an older VPN appliance or smart card) may be necessary if it cannot be made compliant – a process that can be **time and resource intensive** ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=sensitive%20IT%20systems%20%20that,so%20they%20can%20be%20replaced)) reinforcing the need to start migrations early.
* *Standards and Protocol Integration:* Every protocol (TLS, SSH, IPsec, etc.) and every PKI element (X.509 certificates, signatures in code signing, etc.) needs standard formats for the new algorithms. These standards are in progress (the IETF, for example, is specifying how to use Kyber in TLS and how to encode Dilithium signatures in certificates). Until standards solidify, implementers face a moving target. NIST cautions not to **“bake [the new algorithms] into systems yet”** until final standardization is done ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=While%20the%20standard%20is%20in,before%20the%20standard%20is%20finalized)) – hence many organizations test in labs or pilot programs first. That said, preparation (inventory, vendor engagement, prototyping) should proceed. NIST’s National Cybersecurity Center of Excellence (NCCoE) has even set up a project to provide guidance on migrating to PQC, helping organizations with templates and best practices for this journey ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page))
* *Performance and UX:* Users expect secure services to remain fast and responsive. If a new cryptographic method significantly slows down transactions or bloats network traffic, there’s risk of resistance. We discuss performance in detail in the next section, but generally migration plans should include **performance benchmarking** and possibly infrastructure upgrades (e.g., using TLS 1.3 which has fewer round trips, or enabling TLS record compression if appropriate) to offset any added latency from larger PQC keys. So far, experiments show that careful choices of algorithms (Kyber, Dilithium) have minimal impact on typical user-facing performance ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement))
* *Crypto-Agility Processes:* Beyond technology, organizations must institute processes to maintain agility. This includes **monitoring the cryptographic landscape** (e.g., stay aware of new NIST guidance or any vulnerabilities found in PQC algorithms) and having an **update plan**. As IBM’s guidance outlines, being able to *“update cryptography when it is broken and retire cryptography when out of date”* is a core requirement going forward ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=ability%20for%20platforms%2C%20systems%20and,applications%20to)) Many organizations are establishing policies that mandate periodic review of cryptographic algorithms (something that wasn’t routine when RSA/ECC were assumed to last forever). This cultural shift is part of becoming quantum-ready.

In summary, migration to quantum-safe cryptography is a gradual, multi-year process that organizations are beginning now. **Best practices** include inventorying cryptographic assets ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page)) adopting crypto-agile architectures ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=The%20journey%20toward%20quantum,platforms%2C%20systems%20and%20applications%20to)) using hybrid solutions during the transition ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Now%20that%20NIST%20has%20standardized,in%20conjunction%20with%20existing%20techniques)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=In%20this%20experiment%20we%20used,will%20have%20little%20performance%20impact)) and closely following standards development. With these strategies, critical systems can be upgraded **without “breaking” the Internet or enterprise applications**, ensuring continuity of secure operations throughout the quantum transition.

## **3. Performance Overheads**

Introducing post-quantum algorithms into software systems inevitably raises questions about **performance and resource overhead**. Key metrics include key generation time, encryption/decryption (or sign/verify) speed, and memory usage (for keys, signatures, and intermediate computation). Early concerns were that PQC schemes might be too slow or too memory-heavy compared to RSA/ECC, but extensive research and testing have shown that many PQC algorithms are quite efficient on modern hardware.

**Key Generation:** For lattice-based schemes like Kyber and Dilithium, key generation involves sampling random polynomials and is **extremely fast** – on the order of microseconds to milliseconds on typical CPUs. In fact, these schemes have *simpler and faster key generation* than RSA (which requires large prime generation). For example, Dilithium’s key generation was designed to be lightweight, making it feasible even on smart cards or mobile devices () One analysis noted that **Dilithium’s modest key sizes and efficient operations suit resource-constrained environments**, striking a good balance between security and speed () Code-based schemes (like Classic McEliece) have an opposite profile: key generation is slow and public keys are huge (on the order of a megabyte), which is partly why NIST has held those as alternates rather than primaries. In our focus algorithms, keygen is not a bottleneck. For signatures, SPHINCS+ has the most expensive keygen (because it builds many hash trees), but even that is manageable if done infrequently.

**Encryption/Decryption (Encapsulation/Decapsulation):** Post-quantum **encryption operations can be very fast**. Lattice KEMs like Kyber require just matrix multiplications and additions in a finite field, operations which are easily optimized. As a result, **Kyber’s encapsulation/decapsulation throughput is high**, outperforming classical Diffie-Hellman in many benchmarks ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) Cloudflare reported that **Kyber is “much faster than X25519”** for key agreement on their test platforms ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) In a side-by-side comparison at NIST security Level 1, Kyber processed key exchanges significantly faster than RSA-3072 and even outpaced X25519, while using more bandwidth ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) The main cost is that the **ciphertext size is larger** (on the order of ~1.5 KB for Kyber-768 vs 32 bytes for an X25519 public key) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) This increases network traffic slightly, but **does not tend to bottleneck CPU performance**. Even on constrained devices (like a Raspberry Pi), studies have shown post-quantum KEMs can perform key exchanges in a few milliseconds ([Constrained Device Performance Benchmarking with the ... - MDPI](https://www.mdpi.com/2410-387X/8/2/21#:~:text=MDPI%20www,a%20Raspberry%20Pi%204%20device)) Decryption (decapsulation) for these schemes is also efficient, typically a bit more than encryption but still very fast due to similar algebraic operations.

For **digital signatures**, performance varies by algorithm family. Dilithium again is **highly efficient in signing and verifying**, capable of handling thousands of signatures per second on a laptop CPU. Its design avoids heavy operations and leverages lattice structures that are amenable to optimization (even supporting vector instructions, etc.). **FALCON** is extremely fast at verification (due to small signature size and structure) and reasonably fast at signing, though it requires careful implementation (floating-point sampling). **SPHINCS+**, being hash-based, is noticeably slower: generating one SPHINCS+ signature can take tens of milliseconds or more (because it computes many hashes). This is acceptable for some use cases (like code signing where you sign rarely) but not for high-frequency signing. Thus, SPHINCS+ is not intended for performance-critical contexts; it’s chosen for its robustness. In summary, **lattice-based signatures (Dilithium, Falcon) offer performance on par with or better than RSA/ECDSA**, while hash-based signatures trade speed for security diversity ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections))

**Memory and Size Overheads:** The most salient overhead of PQC is in **key and signature sizes**. Lattice schemes have public keys and signatures in the kilobyte range, and ciphertexts of similar size. For instance, Kyber-768 (approx AES-192 security) has a public key ~1,184 bytes and ciphertext ~1,088 bytes ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) Dilithium at security level 2 has public key ~1.3KB and signature ~2.7KB. In contrast, RSA-2048 public key is 256 bytes and signature 256 bytes. These larger sizes can impact network bandwidth (especially in handshake-heavy protocols or certificate chains) and memory if many keys are stored. However, these sizes are still quite manageable for modern systems. A TLS handshake that includes a Kyber KEM and a Dilithium certificate will have on the order of a few kilobytes of extra data – which on today’s networks is negligible for most applications. That said, **careful engineering is needed for constrained environments** (microcontrollers, IoT devices with very tight memory). Researchers have noted that among the PQC finalists, **Dilithium’s relatively small key and its efficiency make it suitable for mobile and IoT devices**, whereas schemes like SPHINCS+ with huge signatures would be impractical there () In scenarios like embedded systems, one might choose a variant with slightly larger computation but smaller keys (e.g., FALCON for signatures if code size and RAM allow its more complex math).

One notable outlier was the isogeny-based encryption scheme SIKE, which had *tiny* keys (only a few hundred bytes) but was **“computationally very expensive”** in practice ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=We%20have%20some%20indirect%20data,This%20is%20what%20we%20found)) In experiments, SIKE’s encryption could be orders of magnitude slower than lattice schemes ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=We%20have%20some%20indirect%20data,This%20is%20what%20we%20found)) This illustrates the trade-off spectrum: SIKE minimized bandwidth but at a great cost in CPU cycles. (SIKE was later broken by a classical attack, so it’s no longer in consideration, but it provided a useful data point on performance extremes.) Most of the remaining PQC algorithms occupy a middle ground of **moderate size increase with equal or better speed** compared to classical algorithms. For example, NTRU-based KEMs and Kyber have **“very similar performance”** and all are quite fast, as cryptographers noted any of those lattice KEMs would have been a fine choice from a performance standpoint ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=match%20at%20L300%20Just%20like,chose%20to%20implement%20NTRU%20Prime))

**Benchmark Results:** In aggregate, studies and benchmarks (including NIST’s official performance reports) have concluded that the chosen post-quantum algorithms are **computationally feasible for widespread deployment** () () A meta-analysis of NIST finalists showed **“substantial resistance against quantum attacks”** can be achieved with these algorithms **while still balancing security and efficiency** () For example, it found that **CRYSTALS-Kyber processes data with higher throughput (lower cycle counts) than earlier lattice schemes like NTRU**, indicating its more optimized design () It also highlighted that **CRYSTALS-Dilithium offered the best efficiency among signature schemes**, making it ideal for low-latency needs () On the other hand, **SPHINCS+ emphasized security at the cost of efficiency** () – an intentional choice for a fallback algorithm.

In real-world tests, the impact of PQC on **TLS handshake performance** has been encouragingly low. In a 2019 Google/Cloudflare experiment, a TLS 1.3 handshake using a hybrid X25519+NTRU (post-quantum) key exchange was only **a few milliseconds slower** on average than a traditional handshake ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) The added network bytes did not meaningfully delay the handshake, and the CPU overhead was minimal (since the bottleneck remained network latency in most cases). The **difference in performance was very small** – so much so that engineers expect that *“switching to a hybrid of Kyber and X25519 will have little performance impact”* on TLS ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) This demonstrates that, at least for web traffic and similar applications, PQC can be introduced without users noticing a slowdown.

**Computational Feasibility:** Summing up, **post-quantum algorithms introduce moderate overhead in size but are efficient in computation**. Modern CPUs (and even many microcontrollers) can handle the math of lattices and hashes easily, often leveraging existing instruction sets. Memory and network usage will increase slightly, but for most platforms the increases (kilobytes, not megabytes) are acceptable. Where performance *is* constrained (say, battery-powered IoT devices that wake up just to do a handshake), careful algorithm selection (maybe a smaller parameter set or a stateful hash-based signature like XMSS if appropriate) can mitigate issues. Many implementations also provide different security levels – e.g., “Dilithium2, Dilithium3, Dilithium5” – allowing engineers to trade off security margin vs. performance as needed, similar to choosing RSA-2048 vs RSA-4096.

In conclusion, **the performance overhead of PQC, while not zero, is well within practical limits** for most software engineering purposes. Engineers will need to account for larger key material (impacting bandwidth and storage) and ensure their systems can handle slightly bigger cryptographic objects. But the speed of cryptographic operations themselves remains high – in many cases even higher than the classical algorithms they replace ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) This gives confidence that we can deploy quantum-safe cryptography broadly without unacceptable performance penalties.

## **4. Library Support and Integration Efforts**

Adoption of quantum-safe cryptography is being facilitated by major cryptographic libraries and protocols, which are rapidly adding support for the new algorithms. This section looks at how libraries like OpenSSL, BoringSSL, and others are integrating PQC, as well as compatibility considerations and timelines for industry adoption.

**OpenSSL and Open Quantum Safe (OQS):** OpenSSL – one of the most widely used crypto libraries for TLS/SSL – has been preparing for PQC through the Open Quantum Safe project. The **Open Quantum Safe (OQS) project**, a Linux Foundation initiative, provides an open-source liboqs C library implementing many PQC algorithms, and it has integrated these into forks of OpenSSL and BoringSSL ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=The%20Open%20Quantum%20Safe%20project%2C,of%20TLS%20ciphers%20should%20consider)) There is an **OQS-fork of OpenSSL 1.1.1 and an OQS provider module for OpenSSL 3.x**, which make the NIST PQC algorithms available in the OpenSSL API ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=produced%20an%20implementation%20of%20ML,well%20in%20advance%20of%20any)) This means developers can experiment with PQC ciphersuites in OpenSSL-based applications even before official OpenSSL releases include them. The OpenSSL team is expected to incorporate the final NIST algorithms in an upcoming release once the standards are fully finalized (likely soon, given NIST’s 2024 publication). In general, **developers who stay up-to-date with OpenSSL will get PQC support largely by upgrading the library**, as the heavy lifting of implementing Kyber, Dilithium, etc., is being handled within OpenSSL’s provider/engine framework ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=produced%20an%20implementation%20of%20ML,well%20in%20advance%20of%20any)) It’s recommended that any custom or explicit cipher configurations be updated to allow the new algorithms when available ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=also%20integrated%20liboqs,later%20attacks%20in%20the%20future))

**BoringSSL and NSS:** BoringSSL (Google’s fork of OpenSSL used in Chrome/Android) and NSS (Mozilla’s crypto library) have also been experimenting with PQC. Google’s BoringSSL, in particular, included the code for the CECPQ2 hybrid key agreement (X25519 + HRSS) during its Chrome experiments ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=Similarly%20to%20its%20predecessor%20CECPQ1,52%20supersingular%20isogeny%20key)) As part of that, **BoringSSL integrated the NTRU-HRSS KEM as an option**. Google has continued to track NIST’s progress, and we can expect BoringSSL to integrate Kyber (which is very similar to HRSS in performance) in the near future for broader deployment. In fact, many libraries had a head start: Cloudflare noted in mid-2022 that *“in the coming months, many libraries and protocols will add preliminary support”* for Kyber and others, and that Cloudflare was working to **contribute upstream support to popular open-source libraries** for these algorithms ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=In%20the%20coming%20months%2C%20many,source%20libraries)) This collaborative push means that by the time standards are official, the ecosystem of TLS libraries (OpenSSL, BoringSSL, wolfSSL, mbedTLS, etc.) should all have PQC capability.

Indeed, other TLS libraries like **wolfSSL have been early adopters** – wolfSSL announced support for various post-quantum ciphers (via OQS integration) and markets itself to IoT developers who need PQC. According to an LWN report, **wolfSSL and BoringSSL have already integrated liboqs** to provide prototype post-quantum algorithms in TLS ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=produced%20an%20implementation%20of%20ML,well%20in%20advance%20of%20any)) The same report mentions that as of 2024, these algorithms are not yet on by default, but can be enabled by developers or for testing modes ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=also%20integrated%20liboqs,later%20attacks%20in%20the%20future)) Another example is **OpenSSH**: as noted earlier, OpenSSH 9.0 added support for the **NTRU Prime** algorithm for key exchange, making it one of the first widely used protocols to go quantum-safe by default (via a hybrid) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Of%20course%2C%20TLS%20is%20not,quantum%20SSH%20keys)) OpenSSH’s team chose NTRU Prime (which NIST did not ultimately pick) to not delay their quantum-safe offerings; however, they are likely to incorporate Kyber as well in the future as it becomes standardized ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Of%20course%2C%20TLS%20is%20not,quantum%20SSH%20keys))

**TLS and Certificate Standards:** The Internet Engineering Task Force (IETF) has been active in standardizing PQC for protocols. There are drafts for adding Kyber to TLS 1.3 handshakes, and for defining signature scheme identifiers for Dilithium, Falcon, etc., in X.509 certificates. This standardization work is crucial so that, for instance, a web browser and a server can agree on a Kyber-based ciphersuite and so that certificate authorities can begin issuing quantum-safe certificates. Cloudflare, which operates a large TLS infrastructure, mentioned it is **working within the IETF to add Kyber to TLS** and generally help make PQC available to the Internet ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=In%20the%20coming%20months%2C%20many,source%20libraries)) Many companies (Cloudflare, Google, AWS, Mozilla, Microsoft) are participating in these IETF efforts. The timeline for official RFCs might trail NIST’s publication by a little, but experimental numbers have been assigned and test implementations are already using them. The **first quantum-safe TLS handshake spec** is expected to be standardized soon after NIST’s algorithms are finalized, enabling mainstream browsers and servers to begin default support perhaps in the next couple of years.

**Compatibility and Adoption Concerns:** One concern with introducing PQC into existing protocols is older software versions that don’t recognize the new algorithms. For example, a legacy TLS client that hasn’t been updated might simply reject a server’s list of ciphers if it includes unknown ones, causing a connection failure. To mitigate this, most deployments use the hybrid approach or wait to enable PQC until clients have been updated. During Cloudflare’s tests, they found some non-compliant TLS implementations *crashed* when seeing large PQC key shares ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=So%20can%20we%20switch%20to,Stay%20tuned)) – clearly a serious compatibility bug in those implementations. Such issues have prompted developers to issue patches; it highlights that **extensive testing is needed** across different clients and devices. Some IoT devices or old systems might never get updates, so there is a possibility that not everyone can move to PQC at the same time. In critical infrastructure, one strategy is to place quantum-safe gateways or proxies in front of legacy devices – effectively offloading the cryptography to a device that can handle PQC, while the older device continues using classical crypto within a protected network.

Another area of compatibility is **certificate chains**. Certificate Authorities (CAs) will need to begin issuing quantum-safe certificates. Those certificates might be larger (due to PQ signatures). There is a limit on certificate size that some TLS clients impose; to address this, experts have proposed using combinations of signatures to keep certificate size reasonable. One suggestion (from Cloudflare research) was that using **Dilithium for end-entity certificate signatures and Falcon for intermediate CA signatures** could keep the whole chain under about 9KB, which most clients can handle ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=concluded%20that%20early%20adoption%20of,offline%29%20signatures)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=likely%20be%20more%20successful%20if,offline%29%20signatures)) Work like this is ongoing to ensure a smooth transition of the Web PKI. Some CAs have already experimented with issuing test Dilithium or Falcon-signed certs. As library support comes, we’ll likely see browsers begin trusting hybrid certificate chains (e.g., a certificate that has two signatures – one classical, one PQC).

**Adoption Timelines:** We can anticipate the following rough timeline: Now that NIST’s standards are set (late 2024), library support is rapidly maturing (OpenSSL, etc., adding official support). In **2025-2026, major software products** (operating systems, browsers, server software) will include these updated libraries. For example, a future update to Android or iOS could add support for Kyber in its TLS stack, allowing mobile apps to use it. Cloud providers and VPN appliances will likely offer “quantum-safe mode” options around the same timeframe. By the late 2020s, quantum-safe algorithms should be a standard part of cryptographic APIs everywhere. Developers are encouraged even now to **start experimenting** with PQC in their systems – for instance, by using OpenSSL’s OQS fork or libraries like IBM’s libcircl for Go that already implement Kyber and Dilithium ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=,today)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=ready%20to%20migrate)) Such experimentation is low-risk at this stage and helps uncover any integration issues early (such as unforeseen memory bugs or performance hiccups).

It’s important to note that **adopting PQC is proactive, not reactive**. As one industry article put it, NIST’s standards are published *“well in advance of any reasonable threat from quantum computers”*, so there isn’t an emergency rush ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=also%20integrated%20liboqs,later%20attacks%20in%20the%20future)) This lead time is by design: it gives the community time to **implement, test, and optimize** the new crypto. The benefit of early adoption, even before quantum computers exist, is to reduce the window of vulnerability from store-now-decrypt-later attacks ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=also%20integrated%20liboqs,later%20attacks%20in%20the%20future)) So while PQC adoption isn’t urgent in the sense of “must happen this month,” it is highly advisable to integrate in the next few years. Many library maintainers have acknowledged this and thus treat PQC support as a top priority in their roadmaps.

In conclusion, **library and protocol support for quantum-safe cryptography is well underway**. Open-source projects, backed by industry and academic collaborations, have paved the path for integration. Compatibility issues are recognized and being addressed through careful standardization and hybrid approaches. We are likely on track such that, by the time quantum computers pose a genuine threat, the software ecosystem will have quantum-resistant options widely deployed and tested.

## **5. Standardization and Industry Research Outlook**

**NIST’s Standardization Process:** NIST’s post-quantum cryptography standardization project has been a cornerstone of research and development in this field. Launched in 2016, it invited cryptographers worldwide to submit candidate algorithms and underwent **three main rounds of evaluation** ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=In%202016%2C%20NIST%20recognized%20the,the%20%2023%20%20Federal)) Dozens of algorithms were gradually narrowed down through cryptanalysis and performance assessments. In July 2022, NIST **announced the winners**: CRYSTALS-Kyber for key establishment, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=replacement%20for%20two%20types%20of,Processing%20Standards%20%28FIPS)) This announcement marked the end of the competition phase and the beginning of drafting official standards. NIST has since published draft standards (with some minor tweaks and renaming, e.g. Dilithium is being standardized under the name **“Module Lattice DSA (ML-DSA)”** ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=NIST%20has%20finalized%20the%20three,infrastructure%20for%20the%20quantum%20era)) . After a period of public comment, NIST is expected to finalize these standards (FIPS 203, etc.) by 2024. In fact, in **August 2024 NIST released three finalized PQC standards** (for Kyber/ML-KEM and two signature schemes) – the **first set of quantum-resistant cryptographic standards ready for general use** ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=NIST%20earlier%20today%20released%20three,could%20serve%20as%20backup%20standards)) Officials stated there is *“no need to wait for future standards”* to begin implementation ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=effort%20eight%20years%20ago,could%20serve%20as%20backup%20standards)) underscoring that these algorithms are mature enough to deploy now.

However, NIST is not stopping with those four algorithms. **Round 4 of the process is ongoing** to consider additional algorithms for standardization ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=Four%20additional%20algorithms%20are%20under,the%20event%20one%20proves%20vulnerable)) This includes candidates like Classic McEliece (code-based encryption), and possibly others from earlier rounds (NTRU Prime, HQC, etc.) to ensure alternative hardness assumptions beyond lattices and hashes. NIST plans to announce a second batch of algorithms (the “finalists” of Round 4) in the coming years ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=Four%20additional%20algorithms%20are%20under,the%20event%20one%20proves%20vulnerable)) This staggered approach provides a *“robust variety of defense tools”*, so that if a breakthrough (mathematical or cryptanalytic) affects one family (say, lattices), there are other standards to fall back on ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=Four%20additional%20algorithms%20are%20under,the%20event%20one%20proves%20vulnerable)) The standardization process also includes publishing reference implementations and test vectors on NIST’s site ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page)) which helps industry adoption.

NIST is also actively producing guidance on how to **transition to these new standards**. For example, NIST’s NCCoE has published draft Special Publications on migration (SP 1800-38 series) ([[PDF] pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf#:~:text=%5BPDF%5D%20pqc,Quantum%20Cryptography%20in%20TLS.%201320)) and is working with industries (like banking, energy) in cooperative research to pilot PQC integration. Keeping track of NIST’s bulletins and project updates is a key part of any organization’s quantum-safe roadmap. The agency’s messaging is clear: *start preparing now*. As early as 2021, NIST urged planning for the “transition toward quantum-safe cryptography” ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=Since%20as%20early%20as%202021%2C,and%20begin%20the%20process%20of)) and they continue to engage with stakeholders through workshops and documents.

**Industry Pilots and Tech Company Initiatives:** Even before NIST announced the winners, major tech companies began testing post-quantum schemes in real-world scenarios:

* **Google:** Google has been at the forefront, conducting public experiments by integrating PQC into Chrome and internet traffic. In 2016, Google’s Chrome tested “CECPQ1” (a combination of a newhope lattice-based KEM with ECDH) with a subset of users. In 2019, Google partnered with Cloudflare for the **CECPQ2 experiment**, deploying a hybrid X25519 + NTRU-HRSS key exchange between Chrome Canary and Cloudflare’s servers ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=Similarly%20to%20its%20predecessor%20CECPQ1,52%20supersingular%20isogeny%20key)) ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=The%20algorithm%20was%20to%20be,users%20accessing%20websites%20hosted%20by)) These experiments collected performance data at scale, confirming that post-quantum handshakes can be done with minimal latency penalty ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) Building on this, Google has already **enabled post-quantum cryptography in its internal communications protocols** for added security ([Securing tomorrow today: Why Google now protects its internal ...](https://www.agilekaizen.com/library/programming-excellence/programming-best-practices/why-google-now-uses-post-quantum-cryptography-for-internal-comms#:~:text=,Here%27s%20why)) By late 2022, Google announced it now protects internal traffic (e.g., data center links) using PQC, not waiting until the last minute ([Securing tomorrow today: Why Google now protects its internal ...](https://www.agilekaizen.com/library/programming-excellence/programming-best-practices/why-google-now-uses-post-quantum-cryptography-for-internal-comms#:~:text=,Here%27s%20why)) This not only secures Google’s own infrastructure against future threats but also serves as a massive real-world testbed for the technology. Google has also contributed to open source; for instance, BoringSSL’s integration of PQC and the release of performance data help the community. We can expect Google to enable PQC by default in consumer products (Chrome, Android) once standards are finalized and widely implemented – likely in the next year or two.
* **Cloudflare:** As a major CDN and security provider, Cloudflare has invested heavily in PQC R&D. It participated in the Chrome experiments, implemented many candidate algorithms in its own libraries (e.g., CIRCL for Go) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=ready%20to%20migrate)) and has written extensive research blogs examining the practicality of post-quantum TLS ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=So%20can%20we%20switch%20to,Stay%20tuned)) Cloudflare has been working on integrating Kyber into TLS through the IETF and even offered a test service where developers could try quantum-safe TLS connections to Cloudflare’s servers. Their work often feeds back into standards and open-source; for example, Cloudflare’s engineers have been improving implementations (making them faster, more secure against side-channels, etc.) and contributing those improvements to projects like Open Quantum Safe. This kind of industry involvement shortens the timeline from academic algorithm to production-ready solution.
* **IBM:** IBM has taken a broad approach: contributing to standards, preparing its product lines, and engaging customers. IBM Research was deeply involved in developing some candidate algorithms (IBM researchers co-authored algorithms like Falcon and CRYSTALS-Dilithium). IBM is also a founding member of the **PQC coalition** under the Linux Foundation, collaborating with other companies to drive adoption ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=The%20Open%20Quantum%20Safe%20project%2C,of%20TLS%20ciphers%20should%20consider)) On the product side, IBM announced that its **IBM z16 mainframe (2022) is “quantum-safe”**, having implemented lattice-based cryptography in its core hardware and firmware ([IBM Unveils IBM z16, Quantum-Safe System for Real-Time AI](https://www.hpcwire.com/off-the-wire/ibm-unveils-ibm-z16-quantum-safe-system-for-real-time-ai/#:~:text=IBM%20Unveils%20IBM%20z16%2C%20Quantum,approach%20for%20constructing%20security)) In practice, IBM **migrated the firmware signing keys on IBM Z systems to Dilithium** during the development of z15 and z16, ensuring that even the updates to those systems are protected against future quantum attacks ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=Our%20own%20systems%20were%20the,submitted%20to%20the%20NIST%20competition)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=This%20is%20crucial%2C%20given%20the,signature)) IBM has also released services like “IBM Quantum Safe Roadmap” for clients and integrated quantum-safe algorithms into offerings like Cloud services and IBM Key Protect. Furthermore, IBM has been advising financial institutions and others on how to do risk assessments and plan their transitions – for example, through the IBM Institute for Business Value report *“The quantum clock is ticking”*. Over the past 18 months (as of 2024), IBM observed many large organizations treating **quantum-safe transformation as a strategic imperative** and starting initiatives accordingly ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=IBM%20has%20engaged%20with%20many,powered%20risks)) This indicates a shift from pure research to execution in industry.
* **Microsoft:** Microsoft has a dedicated “Quantum Safe” program as well. They contributed a candidate (called Picnic, a signature scheme, which though not selected, advanced research on symmetric-based signatures). Microsoft’s research and Azure teams have explored PQC integration, for example by creating a PQCrypto-VPN prototype that combined OpenVPN with post-quantum algorithms ([Post-quantum Cryptography VPN - Microsoft Research](https://www.microsoft.com/en-us/research/project/post-quantum-crypto-vpn/#:~:text=Post,test%20these%20algorithms%20with%20VPNs)) Microsoft is also updating its developer tools; an interesting example is Microsoft’s work on identifying cryptographic code that needs upgrading (they even used CodeQL queries to find hard-coded algorithm usages in code repositories ([Addressing post-quantum cryptography with CodeQL](https://github.blog/security/vulnerability-research/addressing-post-quantum-cryptography-with-codeql/#:~:text=Addressing%20post,quantum)) . Additionally, Microsoft is part of standards efforts and has been preparing guidance for customers on quantum-safe planning through its cloud and enterprise channels ([Quantum-safe overview](https://quantum.microsoft.com/en-us/vision/quantum-cryptography-overview#:~:text=Quantum,safe%20future))
* **Others:** Many other organizations are running pilots. For instance, **AWS (Amazon Web Services)** has experimented with post-quantum TLS in some of its services and is involved in the standards process. Telecommunications companies like **Verizon** ran trials for quantum-safe VPNs in 2021 ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=,PQC)) ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but)) and **AT&T** and others have similar efforts via industry groups (ATIS in telecom released a roadmap for quantum-safe security in communications). The automotive industry, through standards bodies like ETSI, has looked at post-quantum schemes for vehicle-to-x communication security (since cars may be on the road for decades, their security needs to last). Even organizations like **NATO** have reportedly tested hybrid PQ VPN technology in secure communications between member states ([Cyber security through quantum-safe crypto - TNO](https://www.tno.nl/en/digital/digital-innovations/trusted-ict/cyber-security-post-quantum-crypto/#:~:text=way%20we%20keep%20confidential%20information,safe%20for%20a%20long%20time))

These pilot projects by tech leaders serve a dual purpose: they validate the readiness of PQC in real environments, and they signal to the market that it’s time to get on board. The collective findings from these pilots have been positive, generally showing that **PQC can be deployed without breaking existing systems or incurring high costs**. They also identify the rough edges to smooth out (like software bugs with large keys, user-agent incompatibilities, etc., which are being addressed as noted).

**Risk Assessment for Critical Infrastructure:** A significant part of the research methodology around quantum-safe cryptography is assessing *when* quantum attacks might become a viable threat and which systems are most at risk. Experts regularly produce reports on the “quantum threat timeline.” One such report, by the Global Risk Institute, gathers opinions from quantum computing experts to estimate the odds of a quantum computer of a given power by certain dates. The consensus in recent years has been that **by the mid-2030s there is a significant likelihood of a cryptographically relevant quantum computer** capable of breaking RSA/ECC ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=and%20Marco%20Piani%2C%20which%20gives,relevant%20quantum%20computer%20will%20exist) ) In quantitative terms, one survey concluded that *“around mid-2030s it will be more likely than not”* that such a quantum computer exists ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=and%20Marco%20Piani%2C%20which%20gives,relevant%20quantum%20computer%20will%20exist) ) This does not mean it couldn’t happen earlier (there’s uncertainty—some optimistic forecasts say maybe 2030, some pessimistic say not until 2040+), but planning with 2035 in mind is prudent. Government agencies have taken this to heart: the U.S. federal government set a **mandate for agencies to adopt quantum-resistant cryptography by 2035** ([Federal Agencies Should Adopt Quantum-Proof Encryption by 2035 ...](https://www.vitallaw.com/news/federal-agencies-should-adopt-quantum-proof-encryption-by-2035-nist-says/cspd0176304aa8cd64419f82b92a4647a8e0bd#:~:text=Federal%20Agencies%20Should%20Adopt%20Quantum,broken%20by%20quantum%20computing%20technology)) This 2035 deadline was chosen to align with the expected timeline of quantum threat emergence, giving roughly a 10-year window to transition starting now (2025).

Risk assessment also involves identifying data that must remain secure *for the long term*. For example, intelligence or military secrets, or critical personal data (health records, biometric info), might need confidentiality for 20-30+ years. Those are high-priority to migrate to quantum-safe encryption *sooner*, because even if a quantum computer is a decade away, data intercepted today could still be sensitive when that computer arrives. As Anne Neuberger pointed out, they consider “what data would we care about if an adversary could decrypt it in ~9–10 years” and focus on that for near-term quantum-safe protections ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=%E2%80%9CWhat%E2%80%99s%20the%20data%20that%20you%E2%80%99d,%E2%80%9D)) Banks and financial systems also consider the integrity of ledgers and transactions – even a single break could be catastrophic, so they want plenty of safety margin. The **cost of transitioning** is another factor in risk: the U.S. OMB estimated it will cost around **$7.1 billion between 2025 and 2035** for federal agencies to fully transition to PQC (excluding some classified systems) ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=In%20a%20report%20released%20last,by%20DoD%20and%20intelligence%20agencies)) This figure underscores that it’s a significant but manageable investment spread over a decade. It includes replacing hardware that can’t be upgraded, updating software, testing, and certification processes.

**Expected Timeline of Threat and Response:** In summary, most experts expect that we have roughly **10-15 years from now (2025)** before quantum computers can routinely break current cryptography. NIST’s timeline and the U.S. government’s mandates align with that: finalize standards by 2024/25, begin widespread implementation by 2025-2030, and aim to have most of the critical systems quantum-safe by 2030-2035. This way, even if a major quantum breakthrough occurs in 2030, the damage can be limited. The situation is often compared to a ticking clock – we are in a race to upgrade our cryptography before the quantum computer arrives. Fortunately, the research and standardization were started early enough that the *solutions are ready ahead of time*. The onus is now on industry and government to implement them in time.

It’s worth mentioning that **quantum-safe cryptography is not the only approach** to addressing the quantum threat. There’s also quantum key distribution (QKD), a physics-based method to share encryption keys with security from quantum mechanics. Some critical infrastructure projects (like the JPMorgan Chase pilot in Singapore ([IDQ enables 100Gbps IPSec VPN demo at JPMorgan Chase](https://www.idquantique.com/idq-enables-successful-100gbps-ipsec-vpn-demo-at-jpmorgan-chase/#:~:text=IDQ%20enables%20successful%20100Gbps%20IPSec,VPN%20demo%20at%20JPMorgan%20Chase)) ([IDQ enables 100Gbps IPSec VPN demo at JPMorgan Chase](https://www.idquantique.com/idq-enables-successful-100gbps-ipsec-vpn-demo-at-jpmorgan-chase/#:~:text=This%20demonstration%20is%20part%20of,quantum%20cryptography%20and%20QKD)) are exploring *combining* QKD with PQC in a “defense in depth” approach ([IDQ enables 100Gbps IPSec VPN demo at JPMorgan Chase](https://www.idquantique.com/idq-enables-successful-100gbps-ipsec-vpn-demo-at-jpmorgan-chase/#:~:text=This%20demonstration%20is%20part%20of,quantum%20cryptography%20and%20QKD)) However, QKD requires new hardware (quantum fiber links, etc.) and is limited in range and use-case. For broad software engineering purposes, **post-quantum algorithms (which run on classical computers and networks) are the primary focus**, and the only practical option to secure most systems (internet, software, IoT, etc.) against quantum threats. Thus, risk assessments overwhelmingly assume that deploying PQC is the necessary step to mitigate the quantum risk for the vast majority of digital communications.

The research community continues to monitor progress in quantum computing closely. Any advancements (for example, a lab achieving a new qubit milestone or a new algorithm that reduces the resources needed for cryptanalysis) are immediately factored into threat models. As of now, building a quantum computer to break 2048-bit RSA is estimated to require millions of physical qubits and error-corrected operations – something **not expected to be feasible until at least the 2030s**, barring an unforeseen revolution in quantum tech ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=that%20they%20do,park%20figures) ) ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=Their%20estimation%20is%20that%20RSA,a%20factor%20of%201000%20gates) ) IBM’s quantum hardware roadmap, for instance, projects that by 2033 they might support on the order of $10^9$ quantum gate operations in a computation, whereas breaking RSA-2048 might need $10^{12}$ or more – about **1000× beyond** that projected 2033 capability ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=that%20they%20do,park%20figures) ) ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=Their%20estimation%20is%20that%20RSA,a%20factor%20of%201000%20gates) ) This gap suggests we have a bit of time, but also that progress is being made steadily. The cautious stance (which NIST and others advocate) is not to be complacent. By moving to quantum-safe crypto well in advance, even if a breakthrough comes earlier, our infrastructure stays secure.

## **6. Case Studies and Real-World Implementations**

To illustrate the transition to quantum-safe cryptography, this section highlights **real-world examples of organizations implementing PQC**, the challenges they encountered, and the outcomes of these efforts.

* **Google & Cloudflare – Post-Quantum TLS Experiment:** *Case:* In 2019, Google and Cloudflare conducted a large-scale experiment (CECPQ2) to test post-quantum key exchange in TLS 1.3. They deployed a hybrid key agreement (classical X25519 ECDH combined with the quantum-safe **NTRU-HRSS** algorithm) in Chrome Canary browsers and Cloudflare’s edge servers ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=Similarly%20to%20its%20predecessor%20CECPQ1,52%20supersingular%20isogeny%20key)) ([CECPQ2 - Wikipedia](https://en.wikipedia.org/wiki/CECPQ2#:~:text=a%20plugin%20for%20the%20TLS,2)) *Challenges:* The main concerns were performance and compatibility. Would the larger key exchange data slow down page loads? Would any network devices or clients choke on the new cipher? *Outcome:* The results were very encouraging. **TLS handshakes with the hybrid PQC algorithm showed only a tiny increase in handshake time** – on the order of one or two milliseconds added to a typical 100ms TLS handshake ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) Cloudflare published that even with the post-quantum KEM in use, the difference in performance was *“very small”*, and they expect that switching to a Kyber+X25519 hybrid in the future will similarly have **little to no performance impact** ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) They did discover that a few older TLS implementations had issues (some would misbehave due to the larger KeyShare message) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=So%20can%20we%20switch%20to,Stay%20tuned)) but these were bugs that could be fixed. No fundamental barriers were found. This experiment demonstrated **feasibility at scale** – thousands of users browsed with quantum-safe crypto without even noticing. It gave browser vendors and internet companies confidence that they can proceed to integrate PQC. Google has since iterated on these experiments (CECPQ2-b tried SIKE as an alternative, which proved slower), and Cloudflare reported they have been able to successfully enable post-quantum cipher suites on their network for testing. **Key takeaway:** Quantum-safe TLS is practically achievable now; performance and user experience can remain virtually unchanged ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) The experiment also validated the hybrid approach, as the sessions combined classical and PQC security – an approach now informing TLS 1.3 design for PQC.
* **IBM – Quantum-Safe Mainframe (IBM z15/z16):** *Case:* IBM, known for its mainframe systems used in banking and government, undertook an internal project to “quantum-proof” its IBM Z series. Around 2018–2019, IBM researchers began testing PQC algorithms on actual hardware security modules (HSMs) in the mainframe. They focused on the then-leading candidates from NIST. Notably, they **migrated the root of trust in IBM’s hardware security module to use a Dilithium digital signature** ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=Our%20own%20systems%20were%20the,submitted%20to%20the%20NIST%20competition)) In an IBM z15 system (released 2019), they successfully replaced the HSM’s firmware signing key – originally an RSA or ECC key – with a **CRYSTALS-Dilithium key** and used Dilithium to sign HSM firmware updates ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=Our%20own%20systems%20were%20the,submitted%20to%20the%20NIST%20competition)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=This%20is%20crucial%2C%20given%20the,signature)) *Challenges:* Mainframes have stringent performance and security requirements. The HSMs are resource-limited environments, so IBM had to ensure Dilithium’s larger keys wouldn’t overwhelm storage, and that latency for signature verification was acceptable ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=for%20IBM%20zSystems,to%20their%20higher%20computational%20demand)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=key%20sizes%20were%20never%20as,to%20their%20higher%20computational%20demand)) They also had to ensure *implementation maturity*: PQC schemes were new, so IBM used a hybrid approach here too – the HSM’s certificate was implemented as a **hybrid signature (classical + Dilithium)** to guard against any unforeseen weaknesses ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=of%20a%20cryptosystem)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=So%20combining%20an%20implementation,channel)) *Outcome:* The trials were a **success**, and IBM found that lattice-based algorithms “excelled in performance and key size” for their use case ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=HSM%20for%20the%20IBM%20z15,paper1%20submitted%20to%20the%20NIST)) By early adoption and testing, IBM ensured that by the time the next-gen system (IBM z16, 2022) launched, it was **fully quantum-safe for key cryptographic functions**. IBM z16 was advertised as *“the industry’s first quantum-safe system”*, underpinned by lattice-based cryptography ([IBM Unveils IBM z16, Quantum-Safe System for Real-Time AI](https://www.hpcwire.com/off-the-wire/ibm-unveils-ibm-z16-quantum-safe-system-for-real-time-ai/#:~:text=IBM%20Unveils%20IBM%20z16%2C%20Quantum,approach%20for%20constructing%20security)) This means that critical operations like boot process integrity, firmware updates, and certain TLS/IPSec functions on the mainframe can use PQC out-of-the-box. **Key takeaway:** A complex, real-world system like a banking mainframe can be transitioned to quantum-safe cryptography without performance degradation, even improving security posture. IBM’s case also highlights the importance of starting early – they began experiments in 2018, long before standards, which allowed them to contribute to NIST’s analysis and be ready to deliver quantum-safe features by 2022. Their use of **hybrid certificates** in the HSM illustrates a smart strategy to mitigate risk during the transition ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=of%20a%20cryptosystem)) Now, major banks running on z16 have quantum-resistant security for their core systems, one of the first tangible deployments of PQC in critical infrastructure.
* **Verizon – Quantum-Safe VPN Trial:** *Case:* In August 2021, Verizon (a global telecom provider) publicly announced it had **successfully tested a quantum-safe VPN** tunnel in a trial between two 5G network sites ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=,PQC)) ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but)) They replaced the standard Diffie-Hellman key exchange in IPsec VPN with a post-quantum key exchange (the specific algorithm isn’t named, but likely one of the NIST Round-3 candidates, possibly a lattice KEM). The trial linked a lab in London with one in the U.S., simulating a real-world enterprise VPN over an international link ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but)) *Challenges:* The main challenge was to demonstrate that the VPN could establish and run normally using PQC, and that the performance (throughput, latency) would remain high – especially since this was a **100 Gbps high-speed link** environment. Additionally, they wanted to ensure the software integration of PQC into the IPsec stack worked properly with all other network components. *Outcome:* Verizon reported the trial as a success: the quantum-safe VPN established encryption keys using PQC and maintained the secure link without issues ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=,PQC)) ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but)) This proved that “early adoption of PQC” is feasible on existing network infrastructure ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but)) Verizon likened the threat to “stealing a bank safe today and holding onto it until someone can pick the lock” ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=BASKING%20RIDGE%2C%20N,session%20key%20exchange%20security%20mechanisms)) – and showed that using PQC in VPNs is a way to future-proof that safe so it *can’t* be opened later. Following this, Verizon and others in the telecom sector have been working on quantum-safe cryptography for 5G and upcoming 6G security standards. **Key takeaway:** The Verizon case demonstrates a pragmatic approach to secure communications lines that carry sensitive data (corporate or government). Even at very high data rates, PQC algorithms (particularly KEMs like Kyber/NTRU) can operate without slowing down the link, and can be deployed as software updates to existing VPN devices. This is crucial for industries like telecommunications, where upgrading millions of devices must be done seamlessly. Verizon’s public stance also helps raise awareness in enterprise customers that they should be demanding quantum-safe options from vendors in the near future.
* **HSBC – Quantum-Secure Blockchain Project:** *Case:* HSBC, a global bank, in 2024 collaborated with Quantinuum (a quantum technology firm) to **implement quantum-safe cryptography in a distributed ledger platform** ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=HSBC%20has%20worked%20with%20Quantinuum,and%20does%20not%20impact%20performance)) The project involved a tokenization platform for physical gold (the “HSBC Gold Token”), where transactions are recorded on a blockchain. HSBC needed to ensure that the movement of these tokens between ledgers and networks would remain secure in the face of future quantum threats ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=HSBC%20has%20worked%20with%20Quantinuum,and%20does%20not%20impact%20performance)) They trialed a **post-quantum VPN tunnel** to connect different ledger systems, using PQC to encrypt the data traffic of the tokenization system ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=HSBC%20has%20worked%20with%20Quantinuum,and%20does%20not%20impact%20performance)) ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=According%20to%20HSBC%2C%20the%20work,architecting%20the%20DLT)) *Challenges:* One challenge was **performance on a distributed ledger** – blockchains and DLTs already have throughput and latency considerations, so adding heavier encryption could impact transaction speeds. HSBC’s goal was to show they could layer quantum-safe encryption “*without the need for re-architecting the DLT*” and *“without impacting performance.”* ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=financial%20networks%20requires%20encryption%20that,and%20does%20not%20impact%20performance)) *Outcome:* The trial was deemed successful. HSBC announced it as “the first application of quantum-secure technology for distributing tokenised assets” and emphasized that it did **not degrade performance** while enhancing security ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=HSBC%20has%20worked%20with%20Quantinuum,and%20does%20not%20impact%20performance)) ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=According%20to%20HSBC%2C%20the%20work,architecting%20the%20DLT)) They demonstrated that their quantum-safe approach could interoperate: e.g., converting their proprietary gold tokens to a standard Ethereum token format and transferring over a quantum-safe link, proving interoperability and security simultaneously ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=According%20to%20HSBC%2C%20the%20work,architecting%20the%20DLT)) A whitepaper was published detailing the solution and calling quantum-safe migration “crucial to ensure continued resilience of financial systems against emerging threats” ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=In%20a%20whitepaper%20looking%20at,current%20and%20emerging%20cryptographic%20threats)) **Key takeaway:** The finance sector is actively testing PQC in complex environments like blockchain and showing that it can be done in a **cost-effective, non-disruptive way** ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=According%20to%20HSBC%2C%20the%20work,architecting%20the%20DLT)) This case also underlines the forward-thinking stance – even though blockchain systems use strong cryptography, HSBC is looking ahead to upgrade them preemptively. It’s a real-world validation that PQC can integrate with modern fintech systems (like digital asset platforms) now, rather than as an afterthought.
* **National Security Agency (NSA) & US Government:** *Case:* Although details are often classified, it’s publicly known that the U.S. NSA announced plans for transitioning to “**Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)**”, which will be a set of quantum-resistant algorithms for securing classified and defense systems. The government’s broader efforts (via CISA, NIST, etc.) include pilot programs at agencies to implement PQC in various applications (secure email, VPNs, etc.). *Challenge:* The U.S. government operates many legacy systems and custom protocols, so migrating them is a mammoth task. *Outcome:* As an example, in 2023, the U.S. Army’s IT agency conducted tests using quantum-safe TLS on their internal networks to ensure that software like web servers and email gateways could support it. Additionally, NATO’s cybersecurity groups have run trials of **quantum-safe communications among allies** using hybrid approaches (one vendor, Post-Quantum, revealed their tech was in a NATO trial for secure communications) ([Cyber security through quantum-safe crypto - TNO](https://www.tno.nl/en/digital/digital-innovations/trusted-ict/cyber-security-post-quantum-crypto/#:~:text=way%20we%20keep%20confidential%20information,safe%20for%20a%20long%20time)) While specifics are scarce, the **overall outcome is a clear commitment to switch all high-security communications to PQC within the next decade**, with concrete milestones like the 2035 deadline and interim requirements (e.g., by 2025 agencies must submit transition plans, by 2027 begin implementing on high-value assets, etc.). This governance and policy aspect is a key example for other governments and large organizations worldwide.

These case studies collectively show that **quantum-safe cryptography is moving out of the lab and into real deployments**. The challenges faced – whether technical (performance, integration) or logistical (interoperability, standards, inventory of systems) – are being systematically addressed, and the results so far are positive:

* Performance impact has been minimal in network and enterprise scenarios (Google/Cloudflare, Verizon, HSBC cases).
* Compatibility issues can be managed via hybrids and updates (OpenSSH, Chrome experiments).
* Critical infrastructure (IBM mainframe, government networks) can be upgraded in a phased way, maintaining security throughout.
* Early adopters are gaining valuable experience that is feeding into best practices for everyone else.

**Conclusion:** Quantum-safe cryptography represents a pivotal evolution in secure software engineering. With the specter of quantum computers that could unravel current encryption, the tech community has proactively developed new algorithms that can resist these future attacks. We have identified the leading **post-quantum algorithms** – like Kyber and Dilithium – and seen that they offer strong security grounded in hard mathematical problems outside the reach of quantum algorithms ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=called%20%20learning%20with%20errors,help%20of%20a%20quantum%20computer)) Transitioning to these algorithms is a complex but manageable process: organizations must use **strategic migration plans** that include crypto-agility, hybrid deployments, and thorough testing to avoid disruption ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Now%20that%20NIST%20has%20standardized,in%20conjunction%20with%20existing%20techniques)) ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page)) Performance evaluations reassure us that the new schemes are efficient and practical for use at scale, incurring some overhead in size but often improving speed ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) ()

Crucially, **the ecosystem is gearing up** – major cryptographic libraries, protocols, and tech companies are deeply involved in integrating and standardizing PQC, aiming for a smooth adoption curve over the coming years ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=produced%20an%20implementation%20of%20ML,well%20in%20advance%20of%20any)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=In%20the%20coming%20months%2C%20many,source%20libraries)) Research and pilot programs by industry leaders (IBM’s quantum-safe systems, Google’s TLS experiments, financial and telecom trials) are validating the technology in real-world conditions and refining the playbook for others ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=HSM%20for%20the%20IBM%20z15,paper1%20submitted%20to%20the%20NIST)) Risk assessments emphasize that while a quantum adversary is likely years away, the **time to act is now**: a safe cryptographic transition may take a decade, and we want to be finished *before* the threat is at the door ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=and%20Marco%20Piani%2C%20which%20gives,relevant%20quantum%20computer%20will%20exist) ) ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=In%20a%20report%20released%20last,by%20DoD%20and%20intelligence%20agencies))

In summary, quantum-safe cryptography is entering a deployment phase. **Software engineers and security professionals should start engaging with these new algorithms**, whether by experimenting in non-production systems or insisting on vendor support in upcoming products. The cases highlighted show that even large-scale and critical systems have begun the journey and achieved encouraging outcomes. As standards finalize and tools become readily available, the path is clear for all organizations to follow. By embracing quantum-safe methods with careful planning and robust engineering, we can **ensure that our digital infrastructure remains secure against the next generation of computing threats** – preserving privacy and trust well into the quantum era.

**Sources:**

1. NIST News – *“NIST Announces First Four Quantum-Resistant Cryptographic Algorithms”*, Jul 5, 2022 ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=the%20CRYSTALS,as%20its%20speed%20of%20operation)) ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=For%20digital%20signatures%2C%20often%20used,three%20of%20NIST%E2%80%99s%20other%20selections))
2. NIST Report – Status of PQC Standardization (Round 3 results) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=replacement%20for%20two%20types%20of,Processing%20Standards%20%28FIPS)) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=called%20%20learning%20with%20errors,help%20of%20a%20quantum%20computer))
3. Cloudflare Blog – *“NIST’s pleasant post-quantum surprise”*, Jul 2022 (analysis of Kyber, performance, and TLS integration) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Kyber%20is%20a%20balanced%20post,Is%20this%20problematic)) ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=Handshake%20times%20for%20TLS%20with,with%20a%20X25519%20key%20agreement))
4. IBM Security Intelligence – *“What NIST’s post-quantum cryptography standards mean for data security”*, Oct 2024 ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=The%20journey%20toward%20quantum,platforms%2C%20systems%20and%20applications%20to)) ([What NIST's post-quantum cryptography standards mean for data security](https://securityintelligence.com/posts/nist-post-quantum-cryptography-standards-data-security/#:~:text=NIST%20has%20finalized%20the%20three,infrastructure%20for%20the%20quantum%20era))
5. Federal News Network – *“White House to require post-quantum encryption plans from agencies”*, Aug 2024 ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=In%20a%20report%20released%20last,by%20DoD%20and%20intelligence%20agencies)) ([White House to require post-quantum encryption plans from agencies](https://federalnewsnetwork.com/cybersecurity/2024/08/white-house-to-require-post-quantum-encryption-plans-from-agencies/#:~:text=The%20White%20House%20in%202022,so%20they%20can%20be%20replaced))
6. ISC2 Community – *“When will a quantum computer break RSA?”* (引用 Global Risk Institute’s Quantum Threat Report), Aug 2024 ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=and%20Marco%20Piani%2C%20which%20gives,relevant%20quantum%20computer%20will%20exist) ) ( [When will a quantum computer break RSA? - ISC2 Community](https://community.isc2.org/t5/Tech-Talk/When-will-a-quantum-computer-break-RSA/td-p/73406#:~:text=that%20they%20do,park%20figures) )
7. OpenSSL/OQS Project – LWN.net, *“NIST finalizes post-quantum encryption standards”*, Aug 2024 ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=produced%20an%20implementation%20of%20ML,well%20in%20advance%20of%20any)) ([NIST finalizes post-quantum encryption standards [LWN.net]](https://lwn.net/Articles/973231/#:~:text=Of%20course%2C%20TLS%20is%20not,quantum%20SSH%20keys))
8. NIST NCCoE Migration Draft (SP 1800-38) – Guidance on adopting post-quantum crypto ([NIST Announces First Four Quantum-Resistant Cryptographic Algorithms | NIST](https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms#:~:text=To%20prepare%2C%20users%20can%20inventory,Center%20of%20Excellence%20project%20page))
9. IBM Research Blog – *“How we quantum-proofed IBM z16”*, Apr 2022 (details on Dilithium in HSM) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=HSM%20for%20the%20IBM%20z15,paper1%20submitted%20to%20the%20NIST)) ([How we quantum-proofed IBM z16 - IBM Research](https://research.ibm.com/blog/z16-quantum-safe-migration#:~:text=of%20a%20cryptosystem))
10. ComputerWeekly – *“HSBC tests post-quantum VPN tunnel for digital ledgers”*, Sep 2024 ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=HSBC%20has%20worked%20with%20Quantinuum,and%20does%20not%20impact%20performance)) ([HSBC tests post-quantum VPN tunnel for digital ledgers | Computer Weekly](https://www.computerweekly.com/news/366611375/HSBC-tests-post-quantum-VPN-tunnel-for-digital-ledgers#:~:text=According%20to%20HSBC%2C%20the%20work,architecting%20the%20DLT))
11. Verizon News – *“Verizon explores how Quantum Safe VPNs could protect data”*, Aug 2021 ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=,PQC)) ([Verizon explores how Quantum Safe VPNs could protect today’s data from tomorrow’s hackers | News Release | Verizon](https://www.verizon.com/about/news/verizon-quantum-safe-vpns-data#:~:text=In%20a%20recent%20trial%2C%20Verizon,be%20fast%20and%20trustworthy%2C%20but))
12. Google Cloud Blog – *“Why Google now uses post-quantum cryptography for internal comms”*, Nov 2022 ([Securing tomorrow today: Why Google now protects its internal ...](https://www.agilekaizen.com/library/programming-excellence/programming-best-practices/why-google-now-uses-post-quantum-cryptography-for-internal-comms#:~:text=,Here%27s%20why))
13. Cloudflare Blog – *“Towards Post-Quantum Cryptography in TLS”*, Jun 2019 ([NIST’s pleasant post-quantum surprise](https://blog.cloudflare.com/nist-post-quantum-surprise/#:~:text=We%20have%20some%20indirect%20data,This%20is%20what%20we%20found)) ([Towards Post-Quantum Cryptography in TLS](https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/#:~:text=With%20Google%2C%20we%20are%20proposing,With))