Securing the Global Digital Future: The Rise of Post-Quantum Cryptography

Sunny Shang ’27

Much like the creation of the atomic bomb, which redefined military power in the 20th century, the advancement of quantum computing threatens to redefine digital supremacy in modern day society. That is the promise and danger of quantum computing. Quantum computers, machines that use the fundamental properties of quantum mechanics like superposition and entanglement, can process large amounts of data, solving complex mathematical problems that would take ordinary computers thousands of years to complete. Superposition permits a quantum bit to represent both 0 and 1 digits simultaneously, while entanglement allows for the linking of quantum bits over distance. Although this advancement in computational ability holds enormous potential for some fields, it also poses a catastrophic threat to cybersecurity, as quantum computing is able to decrypt even the most complicated encryptions. Algorithms like RSA, which relies on the difficulty of factoring large primes, and Elliptic Curve Cryptography (ECC), which protect nearly all digital communications today based on the hardness of the elliptic curve logarithm problem, rely on problems that are hard for classical computers but easy for quantum computers to solve. This danger has prompted researchers to develop post-quantum cryptography (PQC)—a new generation of encryption systems designed to withstand quantum attacks and protect global digital security (NIST, 2025).

While current systems have remained secure due to their reliance on specific “trapdoor” problems, RSA and ECC are vulnerable because reversing their core operations, such as factoring large numbers or finding discrete logarithms, is only difficult for classical computers, which would take an impractical amount of time. However, these problems are exactly what

quantum computers are good at solving. Using Shor's algorithm, a quantum computer can dismantle this security in a fraction of the time.

Post-quantum cryptography fundamentally reimagines cryptographic security, replacing the vulnerable mathematical foundations of current cryptosystems with new problems believed to resist quantum attacks. Current cryptosystems rely primarily on two models: symmetric cryptography (e.g. AES), which remains secure against quantum computing but requires key exchange, and asymmetric cryptography (e.g. RSA and Elliptic Curve Cryptography), which enables key exchange and digital signatures—a cryptographic code that uses a private key to authenticate a message's sender and verify its integrity, ensuring it wasn't altered—across the internet. These PQC algorithms are generally categorized into several distinct families, each based on different computational assumptions and offering unique security-performance trade-offs.

One of the most promising approaches is lattice-based cryptography, deriving its security from the computational difficulty of problems in high-dimensional geometric lattices: mathematical structures consisting of regularly spaced points in multiple dimensions. The difficulty of challenges like finding the shortest vector in a complex lattice or solving learning-with-errors problems–tasks that remain computationally difficult even for quantum algorithms–increase the security of these systems (Regev, 2009). This mathematical foundation enables efficient encryption and digital signatures, providing guaranteed strong security.

Another major approach is code-based cryptography, which builds on the difficulty of decoding random linear codes, which are error-correcting codes defined by a random generator matrix. The McEliece cryptosystem, developed in 1978, exemplifies this method. It has withstood decades of cryptanalysis—the study of analyzing information systems to find

weaknesses—establishing itself as one of the most thoroughly tested and reliable options in the PQC field (Bernstein, 2023). These systems conceal information using error-correcting codes in such a way that one must be able to identify and correct deliberately added errors, a task that is virtually impossible without knowing the specific code structure.

Hash-based signatures provide a third approach, offering digital authentication based solely on the security of cryptographic hash functions that convert input data into a fixed-size string of characters. Modern implementations create signature protocols where the security is tied directly to the difficulty of finding two different inputs that produce the same hash output, a property known as collision resistance. These fundamental security properties have been extensively analyzed and verified through decades of real-world use and academic scrutiny.

The urgency behind adopting post-quantum cryptography is driven by a serious threat known as "harvest now, decrypt later" (NIST, 2024). This strategy involves opponents intercepting and storing encrypted data—such as confidential communications, financial records, or government secrets—who plan to decrypt it in the future once powerful quantum computers become a reality (Alagic et al., 2022). This risk means that sensitive information protected by today's encryption is already vulnerable and at risk, making the shift to PQC an urgent priority.

The integration of PQC will be overarching, affecting nearly all digital systems. Fundamentally, it must be embedded into core internet protocols like Transport Layer Security (TLS), which secures web traffic, email, and VPNs. PQC is also essential for creating quantum-resistant digital signatures to verify software updates. Ultimately, PQC is necessary for critical infrastructure, such as financial networks and power grids, to guarantee protection against upcoming quantum threats.

After years of global research and testing, several post-quantum cryptographic algorithms have emerged as standard industry solutions. The most popular among these is the CRYSTALS suite, which includes two key algorithms: Kyber for establishing secure connections and Dilithium for creating digital signatures. These lattice-based algorithms have become the primary candidates due to their strong, reliable security and practical performance characteristics. Kyber allows efficient secure key exchange, while Dilithium provides fast signature generation and verification, making both suitable for widespread deployment across various applications.

Additional algorithms also provide specialized abilities to complement the CRYSTALS suite. FALCON offers significantly smaller digital signatures than Dilithium, making it ideal for systems with limited bandwidth or storage capacity. On the other hand, SPINCS+ serves as an important backup option, using a completely different mathematical approach based on hash functions rather than lattices. Thus, this diversity ensures that if vulnerabilities are discovered in one type of algorithm, alternative secure options are still available (NIST, 2024)

However, despite this progress, several significant challenges remain in using post-quantum cryptography. The most immediate concern includes performance trade-offs, as the new algorithms typically require larger key sizes, longer signatures, and more computational power compared to current standards. These increased demands may strain systems with limited resources, particularly high-volume network applications where efficiency is essential (Moody, 2022).

Another major obstacle is the lack of cryptographic agility in existing digital infrastructure. Many current systems were not designed to easily swap out cryptographic algorithms, making the transition to PQC complex and costly. Developing this flexibility will require a considerable amount of re-engineering software systems and protocols to allow

smoother cryptographic updates in the future (Griffin, 2023). Additionally, while the selected algorithms have undergone extensive review, they lack the decades of analysis that has established confidence in the current standards such as RSA and ECC.

Thus, the development and standardization of post-quantum cryptography marks a critical step in preparing for the quantum computing era. The advancement of powerful quantum computers, while potentially years away, requires action today to protect the long-term confidentiality of our data. The leading PQC algorithms, based on robust mathematical problems from lattice, codes, and hash-functions, provide a possible path to securing our digital future. While challenges in performance and implementation remain, the transition to these new algorithms is essential for protecting the security, privacy, and trust that form the foundation of our modern digital society.

References

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NIST IR 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413

Bernstein, D. J. (2023). A quick code-based cryptography glossary. The Code-Based Cryptography Wiki. https://cb.crypto/wiki/A_Quick_Code-Based_Cryptography_Glossary

Griffin, P. (2023, May 15). The challenge of crypto-agility in a post-quantum world. Security Week. https://www.securityweek.com/challenge-crypto-agility-post-quantum-world/

IBM Research. (2024). What is quantum computing? IBM. https://www.ibm.com/topics/quantum-computing

Moody, D. (2022). The NIST PQC standardization process. National Institute of Standards and Technology. https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

National Institute of Standards and Technology. (2024). PQC: Selected algorithms. U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, *56*(6), 1–40. https://doi.org/10.1145/1568318.1568324

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring.

Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700