UNIVERSITY OF NORTH CAROLINA
CHARLOTTE

Option 2: Post Quantum Cryptography

Ananya Sharma

ITIS 6240 Research Paper

Apr 20, 2025

Post-Quantum Cryptography: Securing the Future Beyond Quantum Threats

Introduction

In today's increasingly digital landscape, cryptography plays a critical role in securing communication channels and safeguarding everything from personal data to sensitive government and financial transactions. Widely used encryption algorithms such as RSA, ECC, and Diffie-Hellman derive their security from mathematical problems that are computationally intensive for traditional computers to solve.

However, the rise of quantum computing introduces a substantial threat to these classical cryptographic systems. Quantum algorithms—especially Shor's Algorithm—can efficiently solve the mathematical problems underpinning current public-key schemes, such as integer factorization and discrete logarithms. Though fully capable quantum computers have not yet been realized, their eventual emergence poses a serious risk to digital security.

Post-quantum cryptography (PQC) aims to address this concern by introducing cryptographic methods that remain secure against both classical and quantum-based attacks. Unlike quantum cryptography, which depends on specialized quantum technology, PQC is designed to function on classical computing systems. This paper reviews recent developments in PQC, explores its practical applications, and highlights the challenges of integrating quantum-resistant algorithms into existing digital frameworks.

The Quantum Threat to Classical Cryptography

Present-day public-key encryption schemes like RSA and ECC are based on problems that are difficult for classical machines to solve. RSA depends on the difficulty of factoring large primes, while ECC is built upon the complexity of the discrete logarithm problem. These problems provide the foundation for digital security.

Quantum computing introduces a paradigm shift through the use of qubits, which can represent multiple states simultaneously, enabling exponential processing power. Shor's Algorithm, introduced in the 1990s, can quickly solve factorization and discrete logarithm problems, which are infeasible for classical systems. If quantum computing advances sufficiently, these foundational cryptographic assumptions will no longer ensure data security.

Although quantum computing is still in its developmental phase, rapid progress is being made by organizations such as IBM, Google, and D-Wave. There is growing concern that encrypted data captured today could be stored and decrypted in the future when quantum hardware becomes capable. This potential vulnerability necessitates a transition to cryptographic systems that are secure against both classical and quantum attacks—especially for long-term data protection in sectors like defense, finance, and healthcare.

Understanding Post Quantum Cryptography

Post-quantum cryptography refers to a suite of cryptographic techniques engineered to remain secure in the presence of quantum computers. Unlike traditional systems that rely on problems such as factoring large integers or computing discrete logarithms, PQC is built on mathematical problems that are not efficiently solvable by known quantum algorithms. These methods aim to secure digital systems against both classical and quantum threats.

The five primary categories of PQC include

- **Lattice-based cryptography:** Built on hard problems like Learning With Errors (LWE), offering strong security and efficient implementations.

- **Code-based cryptography, such as** the McEliece cryptosystem, is known for its long-standing resistance to attacks but large key sizes.

- **Multivariate polynomial cryptography**: Relying on the difficulty of solving systems of nonlinear equations over finite fields.

- **Hash-based signature schemes:** Secure digital signatures derived solely from cryptographic hash functions, like SPHINCS+.

- **Isogeny-based cryptography**: Leveraging the mathematical complexity of finding isogenies between elliptic curves.

One major advantage of PQC over quantum key distribution (QKD) is its compatibility with existing computing infrastructure. While QKD requires specialized quantum channels and hardware, PQC algorithms can be integrated into current systems without significant hardware changes, making them more feasible for near-term deployment (Alagic et al., 2020).

A pivotal milestone in PQC development came when the National Institute of Standards and Technology (NIST) launched a global standardization initiative in 2016. After several years of

evaluation, NIST announced Kyber (a lattice-based key encapsulation mechanism) and Dilithium (a lattice-based digital signature scheme) as top candidates for standardization in 2022. Their selection underscores a growing consensus on the need for quantum-resilient algorithms and marks a critical point in global cybersecurity evolution.

The State of PQC: Challenges and Solutions

While post-quantum cryptography offers a promising defense against quantum-era threats, it brings technical and operational complexities that must be addressed for successful adoption. Algorithms such as Kyber and McEliece typically demand more memory and computational power than legacy cryptographic solutions. This can present difficulties in deploying PQC on devices with limited resources, like those found in IoT ecosystems and embedded platforms.

Migrating to PQC also requires overhauling existing cryptographic protocols, many of which are deeply embedded in current infrastructure. Careful integration is necessary to maintain system compatibility and performance. To ease this transition, hybrid encryption models are being explored. Companies like Google and Cloudflare have piloted hybrid Transport Layer Security (TLS) handshakes that pair elliptic-curve cryptography with quantum-resistant algorithms, ensuring forward compatibility while preserving interoperability.

Flexibility in cryptographic systems—known as *cryptographic agility*—is another critical factor. It enables systems to update or switch algorithms quickly in response to new threats or vulnerabilities. Designing for agility from the outset ensures long-term resilience as quantum capabilities evolve.

Finally, awareness and education must grow alongside technological advancements. Cybersecurity professionals must be well-informed and equipped to manage the transition to post-quantum systems. Coordinated efforts across academia, industry, and government sectors will be crucial to developing policies, conducting testing, and deploying secure, scalable, quantum-resistant solutions.

Applications of Post-Quantum Cryptography

As PQC evolves, it is finding increasing relevance across a broad range of industries. One of the most immediate applications is in securing internet protocols. Google and Cloudflare have already conducted experiments incorporating post-quantum algorithms into the TLS handshake,

creating hybrid systems that integrate classical and quantum-resistant methods without breaking existing infrastructure.

Government and defense agencies are particularly invested in PQC because of the long-term sensitivity of their data. National security requires that communications remain confidential not just today but well into the future. The U.S. government, through NIST, is leading the charge on PQC standardization, with similar efforts underway in Europe and Asia to ensure coordinated global preparedness.

The world of blockchain and cryptocurrency is another area being impacted. Cryptocurrencies like Bitcoin rely on public-key cryptography that could be compromised by quantum attacks. Researchers are actively exploring quantum-resistant alternatives, such as lattice-based and hash-based digital signatures, to secure blockchain technologies and ensure the future of decentralized financial systems.

Conclusion

As we move closer to the era of quantum computing, the urgency of securing digital systems against quantum threats grows ever more apparent. While the transition from classical to post-quantum cryptography presents significant challenges, the progress made so far is promising. The development of quantum-resistant algorithms, such as those based on lattice problems, code-based cryptography, and hash functions, has provided a strong foundation for the future of secure communications. However, the computational complexity of these algorithms, the need for backward compatibility with existing systems, and the demand for cryptographic agility all represent hurdles that must be carefully navigated.

The efforts by global organizations, especially NIST, to standardize post-quantum algorithms have provided much-needed direction in the development of these algorithms. As the field continues to evolve, the collaboration between researchers, industry professionals, and governments will play a critical role in ensuring a smooth transition to a post-quantum world. The ability to integrate hybrid systems, optimize algorithms for resource-constrained environments, and maintain flexibility in cryptographic choices will be key to overcoming the challenges ahead.

In addition to these technical and infrastructural challenges, educating the broader cybersecurity community and raising awareness about quantum threats will be crucial. As organizations begin to understand the full scope of quantum risks, they will be better equipped to adopt post-quantum solutions proactively. The transition to quantum-safe systems will not be instantaneous, but with sustained effort and global cooperation, we can ensure that the systems we rely on today remain secure in a quantum-powered future.

References

1. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*(7671), 188–194. https://doi.org/10.1038/nature23461

2. Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., ... & Yaga, D. (2020). *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST. https://doi.org/10.6028/NIST.IR.8309

3. Bindel, N., Buchmann, J., Krausz, R., & Struck, P. (2020). Post-quantum cryptography: Current state and quantum mitigation. *Journal of Cybersecurity*, 6(1). https://doi.org/10.1093/cybsec/tyaa012

4. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NIST IR 8105). https://doi.org/10.6028/NIST.IR.8105

5. Cisco. (2023). Preparing for Post-Quantum Cryptography. Cisco Blogs. https://blogs.cisco.com

6. Jao, D., & De Feo, L. (2020). Isogeny-based cryptography: An overview. In T. Takagi (Ed.), *Post-Quantum Cryptography* (pp. 179–196). Springer. https://doi.org/10.1007/978-3-030-25510-7_8

7. Langley, A., Turner, S., & Wood, C. A. (2022). Hybrid key exchange in TLS. *IETF Internet-Draft*. https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

8. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

9. National Institute of Standards and Technology (NIST). (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process (NIST SP 800-208)*. https://doi.org/10.6028/NIST.SP.800-208

10. White House. (2022). *Quantum Computing Cybersecurity Preparedness Act*. https://www.whitehouse.gov