TECHNICAL WHITEPAPER

Post-Quantum Cryptography: Preparing for the Next Security Frontier

December 2024

SSA

Contents

1. Introduction

"What happens when today’s strongest encryption becomes tomorrow’s broken lock?"

Public-key cryptography has facilitated digital trust for decades. Protocols such as RSA and elliptic-curve cryptography (ECC) secure financial transactions, protect classified communications, and authenticate nearly every interaction on the internet. Their security rests on the computational intractability of mathematical problems, large-integer factoring and discrete logarithms, hard for standard computers to calculate.

Quantum computing changes that assumption. By exploiting quantum mechanical principles, quantum computers could, in theory, perform calculations that would take classical computers millennia. While large-scale, fault-tolerant quantum computers remain years away, their eventual arrival creates a unique challenge: encrypted data harvested today may be decrypted in the future once quantum capabilities mature.

Post-quantum cryptography (PQC) is a set of primitives that are quantum as well as classical attack-resistant. From 2025, the need for deployment of PQC has grown manifold. The United States National Institute of Standards and Technology (NIST) finished its first standardization by issuing draft standards for the first batch of quantum-resistant algorithms in 2024. Governments, organizations, and cloud providers are now facing the problem of how to incorporate PQC into their existing infrastructure.

This paper provides a deep dive into PQC: what it is, why it matters, and how organizations can begin transitioning.

2. Why Current Encryption Is at Risk

2.1 Public-Key Methods Today

- RSA: Security depends on the difficulty of factoring large integers.
- Elliptic-Curve Cryptography (ECC): Relies on the hardness of the elliptic-curve discrete logarithm problem.
- Diffie–Hellman Key Exchange: Based on discrete logarithms in finite fields.

These algorithms underpin protocols like TLS (for secure web traffic), VPNs, digital certificates, and blockchain consensus mechanisms.

2.2 Shor's Algorithm

Mathematician Peter Shor introduced a quantum algorithm for integer factoring and discrete logarithms in polynomial time in 1994. On a sufficiently powerful quantum computer, RSA-2048 encryption could be broken in hours, rendering decades of digital infrastructure obsolete.

2.3 Timeline Considerations

Experts debate when a cryptographically relevant quantum computer (CRQC) will exist. Predictions stretch from the early 2030s to over 2040. The "harvest now, decrypt later" threat gives urgency an argument. Adversaries could store encrypted data today and decrypt it once quantum capabilities are realized, effectively making PQC not just a future requirement but an immediate concern.

3. Post-Quantum Cryptography Explained

3.1 Definition

PQC refers to cryptographic algorithms designed to remain secure against both conventional and quantum adversaries. Unlike quantum key distribution (QKD), PQC does not rely on specialized hardware or quantum networks. It is implemented in software, making it far more scalable for global adoption.

3.2 Leading Algorithm Families

- Lattice-Based Cryptography
    - Hard problems: Learning with Errors (LWE), Ring-LWE, and Module-LWE.
    - Candidates: CRYSTALS-Kyber (key encapsulation), CRYSTALS-Dilithium (digital signatures).
- Code-Based Cryptography
    - Hard problems: Decoding random linear codes.
    - Candidate: Classic McEliece (key encapsulation).
- Multivariate Quadratic Equations

    - Hard problems: Solving systems of nonlinear equations.
    - Candidate: Rainbow (digital signatures, although recently withdrawn after cryptanalysis).
- Hash-Based Signatures
    - Security based on collision resistance of cryptographic hash functions.
    - Example: SPHINCS+ (stateless hash-based signatures).

3.3 NIST Standardization Process

- 2016: NIST launched a multi-year process for the selection of PQC algorithms.
- 2022: Four overall algorithms selected: Kyber (encryption), Dilithium (signatures), Falcon (signatures), SPHINCS+ (hash-based signatures).
- 2024: Draft standards published for public comment.
- 2025: Enterprises will begin pilot deployments, with final standards expected in 2026.

4. Industry Impact & Use Cases

4.1 Finance

Banks and payment processors rely on cryptography for securing online transactions, mobile wallets, and interbank transfers. Post-quantum upgrades are essential to prevent long-term data exposure, particularly for records with regulatory retention periods of 7–10 years.

4.2 Healthcare

Electronic health records contain highly sensitive data that would not be compromised for decades. PQC adoption is critical to guard against retrospective breaches and compliance failures under HIPAA and GDPR.

4.3 Defense & Government

Classified communications require protection for 20–30 years or longer. The U.S. Department of Defense has already directed agencies to prepare migration strategies in line with NIST recommendations.

TLS handshakes, VPN tunnels, and digital certificates must be re-engineered to support hybrid or PQC-only cryptographic suites. Cloud hyperscalers (AWS, Azure, Google Cloud) are piloting PQC-enabled services to support enterprise transitions.

5. Migration Challenges

5.1 Scale

Global PKI ecosystems include billions of endpoints, from web browsers and IoT devices to satellites and critical infrastructure. Replacing or upgrading these systems requires unprecedented coordination.

5.2 Interoperability

Hybrid cryptography, combining PQC with classical algorithms, is a recommended transitional strategy. However, designing efficient hybrid protocols introduces new engineering complexities.

5.3 Performance

Some PQC algorithms have larger key sizes and slower computation compared to RSA or ECC. For example, Classic McEliece offers robust security but uses public keys exceeding 200 KB, complicating deployment in constrained environments.

5.4 "Harvest Now, Decrypt Later"

Adversaries may already be stockpiling encrypted communications. The longer organizations delay migration, the greater the risk that today’s data will be exposed once quantum capabilities mature.

6. Actionable Steps Organizations Can Take Today

1. Cryptographic Inventory

- Map all cryptographic assets in use, including TLS certificates, VPN endpoints, and internal key management systems.

2. PQC Testing
   - Begin pilot programs with PQC libraries (e.g., Open Quantum Safe project, BoringSSL with PQC extensions).
3. Hybrid Deployments
   - Implement dual algorithms (RSA/ECC + PQC) for gradual rollout and compatibility testing.
   - Follow NIST Roadmap
4. Align with NIST Roadmap
   - Monitor NIST publications and vendor guidance. Avoid adopting proprietary “quantum-safe” solutions not aligned with standards.
5. Risk Prioritization
   - Focus first on high-value, long-lifespan data (e.g., financial records, medical archives, classified government communications).

7. The Road Ahead

The timeline for quantum readiness remains uncertain, but the direction is clear: all public-key cryptography in use today must eventually be replaced. Organizations that delay will face greater technical debt and higher costs once migration becomes mandatory.

Research Directions

- Further reductions in key sizes and signature lengths.
- Hardware acceleration for PQC in CPUs, GPUs, and dedicated cryptographic chips.
- Hybrid directions bringing PQC and symmetric cryptography research together.

Expected Milestones

- 2026: Final NIST PQC standards published.
- 2030: Early majority adoption in finance, government, and healthcare.
- 2040: Broad PQC deployment across most digital systems.

8. Conclusion

The shift to post-quantum cryptography represents one of the largest security migrations in history. Unlike past cryptographic transitions, such as moving from DES to AES, this shift is driven not by immediate vulnerabilities but by the certainty that existing algorithms will fail against future adversaries.

Organizations that begin preparing today will be positioned to maintain trust, compliance, and resilience in a quantum-capable world. Those that delay may find themselves scrambling once the lock on their data has already been broken.

9. References

1. National Institute of Standards and Technology (NIST). (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*. NIST Cybersecurity White Paper. Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2021/04/20/getting-ready-for-post-quantum-cryptography/final
2. National Institute of Standards and Technology (NIST). (n.d.). *Post-Quantum Cryptography (PQC) Project*.Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography
3. Chhetri, G., Alzahrani, B., & Baz, A. (2025). *Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey*. arXiv preprint arXiv:2510.10436. Retrieved from https://arxiv.org/html/2510.10436v1
4. Commey, D., Mensah, D., & Boateng, E. (2024). *Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics*. arXiv preprint arXiv:2505.02239. Retrieved from https://arxiv.org/abs/2505.02239
5. Ahmed, N., Zhang, L., & Gangopadhyay, A. (2024). *A Survey of Post-Quantum Cryptography Support in Cryptographic Libraries*. arXiv preprint arXiv:2508.16078. Retrieved from https://arxiv.org/abs/2508.16078
6. Cintas Canto, A., Bindel, N., & Schneider, T. (2023). *Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum*

Security. arXiv preprint arXiv:2305.13544. Retrieved from https://arxiv.org/abs/2305.13544

7. National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), & NIST. (2023). *Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now*. Press Release. Retrieved from https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/
8. National Cyber Security Centre (NCSC). (2023). *Next Steps in Preparing for Post-Quantum Cryptography*.Whitepaper. Retrieved from https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
9. World Economic Forum. (2024, October). *Why the New NIST Standards Mean Quantum Cryptography May Just Have Come of Age*. Retrieved from https://www.weforum.org/stories/2024/10/quantum-cryptography-nist-standards/
10. Le, T. D., Do, P. H., Dinh, T. D., & Pham, V. D. (2024). *Are Enterprises Ready for Quantum-Safe Cybersecurity?*arXiv preprint arXiv:2509.01731. Retrieved from https://arxiv.org/abs/2509.01731
11. Wikipedia. (n.d.). *Kyber (Post-Quantum Cryptography)*. Retrieved from https://en.wikipedia.org/wiki/Kyber

Release Information

Content Version: December 2024

Trademarks and Patents

SSA Institute Inc. SAS Campus Drive, Cary, North Carolina 27513

SSA® and all other SSA Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are registered trademarks or trademarks of their respective companies.

To contact your local SAS office, please visit: ssa.com/offices