IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Building Quantum-Safe Systems: Post-Quantum Algorithms And Implementation Hurdles

Dr. Hiranand R. Khambayat

Assistant Professor
Department of Physics
A. V. College of Arts, K.M. College of Commerce, and E.S.A. College of Science

Vasai Rd. West, Dist. Palghar , Maharashtra

Abstract: The rise of quantum computing brings powerful capabilities but also poses risks to current cryptographic schemes like RSA and ECC, which depend upon problems that quantum procedures like Shor's and Grover's can solve. This creates an urgent need for new methods that can withstand both classical and quantum attacks.

Post-Quantum Cryptography (PQC) addresses this need by emerging secure algorithms for classical computers that can resist quantum threats. This paper reviews major families of PQC algorithms, including lattice-based, code-based, multivariate polynomial, hash- based, and isogeny-based. It analyses their security, performance, and implementation challenges.

It also looks at global standardization efforts, particularly by NIST, and emphasizes the importance of early adoption, adaptable cryptographic systems, and planned migration to ensure secure communication in the quantum era.

Index Terms - Post-Quantum Cryptography (PQC), Quantum Computing threats, Shor's Algorithm, Lattice-Based Cryptography, Quantum-Resistant Algorithms, Public Key Cryptography, Cryptographic Standardization, Digital Security, Quantum Security, NIST PQC project, Key Exchange, Multivariate Cryptography.

I. INTRODUCTION

Quantum computing is a paradigm change in computational power that holds the promise of great leaps forward in many areas such as material science, optimization, and cryptography. The same computer power that will help advance science poses a grave threat to today's communal key cryptography. Cryptosystems as if RSA, DSA, and ECC are based on the computational difficulty of linearly related problems integer factorization and the distinct logarithm both glitches, which can be resolved, efficiently with quantum algorithms most notably Shor's algorithm. Post-Quantum Cryptography (PQC) seeks to advance cryptographic systems can endure both classical and quantum attacks. These systems are designed to run on classical hardware while resisting cryptanalysis from quantum adversaries. This paper sightsees the landscape of PQC, concentrating on algorithmic families, standardization efforts, and the path to protected announcement in the post-quantum era.

1. Quantum Threats to Classical Cryptography

1.1 Shor's Algorithm

Shor's algorithm, invented in 1994, allows quantum computers to factor big integers and solve discrete logarithms in polynomial time. This does so directly against RSA, ECC, and other common public-key cryptosystems.

1.2 Grover's Algorithm

Grover's algorithm offers a quadratic speedup for brute-force search, affecting symmetric- key cryptography by reducing the effective key length by half. For example, AES-256 is still secure, but AES-128 would provide security for just 64 bits in a quantum world.

2. Post-Quantum Cryptographic Algorithm Families

2.1 Lattice-Based Cryptography

Lattice-based cryptography is based on the trouble of lattice difficulties like the Learning with errors (LWE) and Shortest Vector Problem (SVP) problems. These problems estimated to be secure against both classical and quantum attacks.

Advantages: Robust security proofs, efficient code, and versatility (e.g., signatures, encryption).

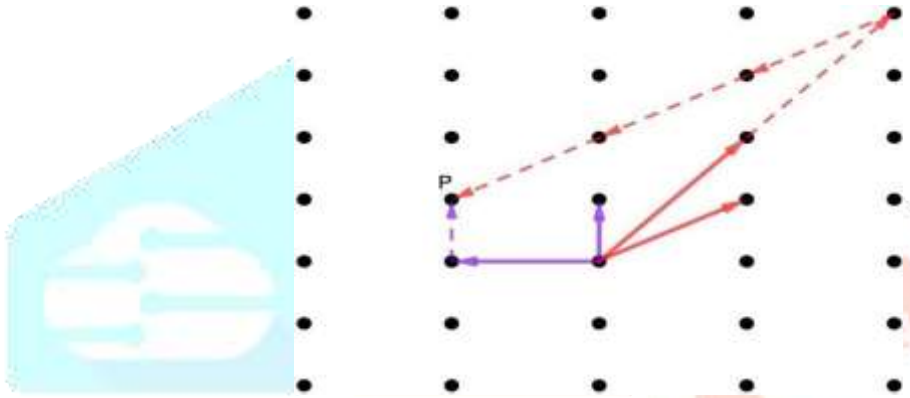


Fig. Lattice-Based Cryptography Examples: Kyber (key encapsulation), Dilithium (signatures), NTRU.

2.2 Code-Based Cryptography

It is originated based on the complexity of breaking rectilinear error-correcting codes, such as the McEliece cryptosystem, in particular.

Advantages: Long history of security. Disadvantages: Keys are quite long.

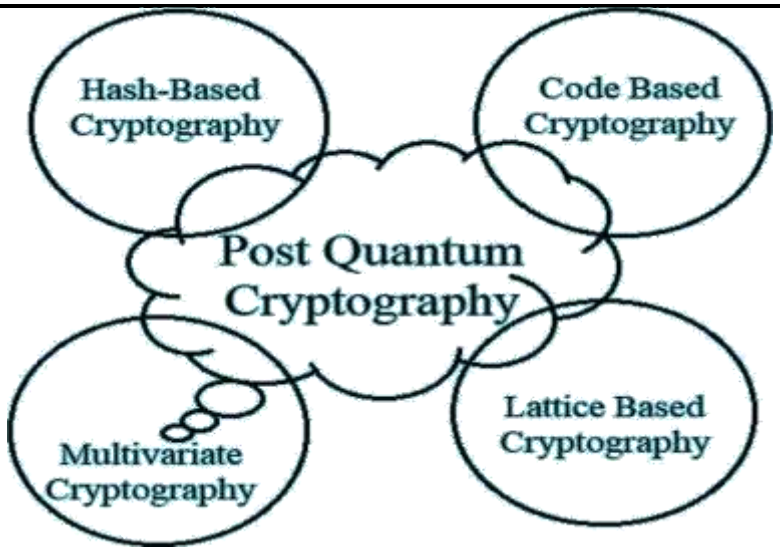
Implementations: Original McEliece (considered by NIST for adoption).

2.3 Multivariate Polynomial Cryptography

These schemes are created upon resolving systems of multivariate quadratic equations over finite fields, which has been proven NP-complete.

Advantages: Very fast signing.

Disadvantages: Some schemes have been attacked; signatures may be lengthy.



2.4 Hash-Based Cryptography

Cryptographic hash function-based alphanumeric autograph schemes alone.

Strengths: Low assumptions; very secure.

Challenges: Scallops and stateless designs are difficult to scale. Examples:

SPHINCS+, LMS, XMSS.

2.5 Isogeny-Based Cryptography

This comparatively new intimate employs the isomorphism problem of finding isogenies between super singular elliptic curves.

Strengths: Small keys.

Challenges**:** Performance and vulnerability to quantum attacks (e.g., SIKE was broken). Examples:

SIDH, SIKE (no longer in standardization due to cryptanalysis).

3. Standardization Efforts

The National Institute of Standards and Technology (NIST) initiated a public process in 2016 to standardize post-quantum cryptographic algorithms. After a few rounds of assessment, NIST chose the following algorithms for standardization (as of 2024):

Encryption Establishment:

Kyber (lattice-based), Classic McEliece (code-based)

Digital Signatures: Dilithium (lattice-based), SPHINCS+ (hash-based), Falcon (lattice- based)

NIST focused on performance, security, implementation practicability, and algorithm variety in its choice.

4. Implementation Challenges

4.1 Performance and Efficiency

Most PQC schemes consume more computational power or produce larger key/signature sizes than their traditional counterparts. Optimizations for embedded and resource- constrained environments continue to be challenging.

4.2 Integration and Compatibility

PQC integration into current infrastructure (e.g., TLS, VPNs, block chain) necessitates large protocol modifications, hybrid proposals, and backward compatibility.

4.3 Side-Channel Resistance

New algorithms are required to be hardened against timing, power analysis, and other side- channel attacks. Constant-time implementations are essential.

4.4 Migration Planning

Cryptographic migration is going to be challenging and needs to be strategic. Hybrid cryptography (classical + post-quantum) is usually advised during the transition phase.

5. Importance of Early Adoption

Active implementation of PQC is necessary because of the "harvest now, decrypt later" threat model, whereby attackers harvest encrypted information today to decrypt it in the future when quantum capabilities improve. Governments, businesses, and infrastructure providers should start planning for the transition by:

Taking inventory of existing cryptographic systems. Conducting testing

and evaluation of PQC implementations. Making hybrid deployment and

phased migration preparations.

Conclusion

The appearance of quantum computing threatens are foundation of secure digital communication in the form of contemporary cryptographic systems. Known algorithms RSA and ECC, that were thought to be strong, stand exposed in front of quantum algorithms Shor's and Grover's. This awaiting danger has encouraged the speedy evolution of Post-Quantum Cryptography (PQC) a discipline set to develop cryptographic schemes, which prevent both classical, and quantum attacks.

This paper has discussed the prominent families of PQC algorithms lattice-based, code- based, multivariate polynomial, hash-based, and isogeny-based each with its distinct security-efficiency-implementation complexity trade-offs. Although there are families like lattice-based cryptography that promise and perform very well, others continue to be overcome with issues that need to be solved before used at scale.

International standardization efforts, particularly by NIST, are at the forefront of testing and approving secure, quantum-resistant algorithms. Development of the effort speaks to the critical value of global cooperation and forward-thinking cryptographic transition.

As quantum computing progresses from theory to practical use, the imperative for early transition to PQC grows more critical. Companies need to start preparing now to upgrade infrastructure, implement hybrid models, and formulate migration plans in order to maintain long-term security. Post-quantum cryptography is not just a technical requirement but a strategic need to secure privacy, financial networks, national security, and world trust in digital infrastructure.

References:

1. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2021). (TCHES), 2021(1), 238–268.
2. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Günther, F. (2018). Hybrid key encapsulation mechanisms and authenticated key exchange. IACR Cryptology ePrint Archive, 2018(903)
3. Bavdekar, A., Yadav, D. K., Patil, S., & Sahu, A. K. (2022). Post-quantum cryptography: Techniques, challenges, and directions.
4. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange A new hope. In 25th USENIX Security Symposium (pp. 327–343).
5. Bernstein, D. J., et al. (2021). SPHINCS+ submission to NIST.
6. Hoffstein, J., Pipher, J., Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem.
7. Shor, Peter W. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”SIAM Journal on Computing, 1997.
8. Bernstein, Daniel J., Buchmann, Johannes, Dahmen, Erik (Eds.)“Post-Quantum Cryptography”Springer, 2009.
9. Regev, Oded.“On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”Journal of the ACM (JACM), 2009.

10. Alkim, Erdem et al.“CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM”IEEE European Symposium on Security and Privacy, 2018.
11. Ducas, Léo et al.“CRYSTALS-DILITHIUM: Digital Signatures from Module Lattices” PQCrypto 2017.
12. Marel Alvarado et al., "A Survey on Post-Quantum Cryptography State-of-the-Art and Challenges" (2023)
13. Seyed Mohammad Reza Hosseini & Hossein Pilaram, "A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances" (2024, Crypto-ePrint)
14. Arimondo Scrivano, “A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing” (arXiv, June 2025)
15. Ritik Bavdekar et al., “Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research” (2022)
16. Manish Kumar, “Post-Quantum Cryptography Algorithms Standardization and Performance Analysis” (2022)
17. Bindel, Nina et al.“Hybrid Key Exchange in TLS 1.3”Internet Engineering Task Force (IETF), 2021.
18. Albrecht, Martin R. et al.“On the Concrete Security of Module-LWE Encryption Schemes”ASIACRYPT2018.
19. National Institute of Standards and Technology. (2022). Post-Quantum Cryptography Standardization Project
20. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science(pp.124–134).IEEE
21. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461
22. Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone,
23. D(2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology.
24. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
25. Hülsing, A., Rijneveld, J., Schwabe, P., (2022). SPHINCS+: Submission to the NIST PQC Project.