POST-QUANTUM CRYPTOGRAPHY: ALGORITHMS AND CHALLENGES IN THE QUANTUM PHYSICS ERA

Dr. Hiranand R. Khambayat
A. V. College of Arts, K.M. College of Commerce, and E.S.A. College of Science Vasai Rd. West, Dist. Palghar , Maharashtra 401202.
Email-id: hiranand.khambayat@avc.ac.in

Abstract :

As quantum physics moves into practical computing, traditional cryptographic systems face serious threats from quantum algorithms like Shor's and Grover's. These can break widely used encryption methods, including RSA and ECC. This shift has led to the rise of Post-Quantum Cryptography (PQC), a new class of cryptographic algorithms meant to withstand the computing power of quantum computers. This paper examines PQC within the context of quantum physics, showing how concepts like quantum superposition and entanglement challenge old security beliefs. It looks at important PQC algorithms, such as lattice-based, code-based, multivariate polynomial, and hash-based cryptography, while focusing on their design principles and resistance to quantum attacks. The paper also addresses the practical challenges of implementing PQC, including performance issues, integration with current systems, and standardization efforts led by organizations like NIST. By connecting quantum physics with cryptographic design, this study highlights the need for proactive development and use of quantum-secure solutions to ensure long-term data protection in the quantum age. [1-5]

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

Introduction :

The start-up of quantum computing is a fundamental change in computing capability. It has the potential to accelerate capabilities in fields such as material science, optimization, pharmaceutical discovery, and artificial intelligence. That shift poses a very serious threat to the fundamental security controls of the digital world. Traditional cryptographic systems, especially public-key algorithms like RSA, Diffie-Hellman, and elliptic curve cryptography (ECC), depend on the difficulty of mathematical problems such as integer factorization and discrete logarithms. Solving these problems with classical computers is extremely hard and takes a long time. This is what keeps modern communication systems secure.[6-8]

Peter Shor demonstrated that a sufficiently powerful quantum computer could speedily solve these problems by means of what is called Shor's algorithm. This breakthrough implies that when large-scale quantum computers are developed, popular public-key cryptosystems might be broken when they become available, rendering current practices regarding data confidentiality, digital signatures, and key exchanges insecure.

Furthermore, Grover's algorithm provides a quicker method for carrying out brute-force searches. These encryption techniques enhance their key strength.

To counter this new threat, Post-Quantum Cryptography (PQC) created. PQC focused on developing cryptographic tools and techniques that remain secure against both quantum and classical threats. It designed to function on classical computers with protection against quantum attacks. In contrast to quantum key distribution (QKD), which is based on quantum mechanics and needs special hardware, PQC is primarily software-oriented and compatible with existing systems.[9-13]

Looking at the pressing requirement for standardization, the National Institute of Standards and Technology (NIST) initiated an international competition in 2016 to evaluate and standardize post-quantum cryptographic algorithms. The multi-year process has resulted in the identification of several finalists to standardize in 2024, including CRYSTALS-Kyber to encrypt and encapsulate keys, and CRYSTALS-Dilithium and SPHINCS+ for digital signatures.

This study seeks to discuss post-quantum cryptographic algorithms and the numerous challenges involved in embracing them. It begins by discussing the quantum threat model and vulnerabilities of existing cryptographic systems. It then discusses the various categories of PQC schemes with emphasis on their mathematical underpinnings, performance characteristics, and security premises. Lastly, the research discusses the practical and theoretical challenges of adopting PQC, the present state of standardization, and prospective studies to safeguard the digital world once quantum computing becomes pervasive. [14-15]

Quantum Computing and Cryptographic Threats :

Quantum computers operate based on principles of quantum physics such as superposition and entanglement, which enable them to perform computations in ways that classical computers cannot. It improve the solving certain problems. Shor's Algorithm: Efficiently factors large integers, breaking RSA and ECC. Grover's Algorithm: Speeds up brute-force attacks, affecting symmetric cryptography. These developments mean that current cryptographic systems, especially those used in secure communications, digital signatures, and key exchange, will eventually become insecure.[16-18]

Post-Quantum Cryptographic Algorithms :

Post-Quantum Cryptographic Algorithms are cryptographic protocols that are specifically developed to be secure against quantum computers.

Quantum computers may decrypt many conventional encryption algorithms like RSA, DSA, and ECC with algorithms like Shor's algorithm and Grover's algorithm. Thus, post-quantum algorithms seek to secure Encrypted messages, Digital signatures, secure communications.

Even in a world in which quantum computers are potent and prevalent. PQC algorithms based on mathematical problems, which are assumed quantum attack-resistant. It include-

Lattice-Based Cryptography :

Lattice-Based Cryptography is a new form of post-quantum cryptography that employs the sophisticated geometric shapes known as lattices to construct encryption and digital signature schemes.

It is one of the most promising and widely recommended methods for keeping data safe from quantum computer attacks and encompasses schemes such as Kyber (for encryption) and Dilithium (for digital signatures),both of which are under standardization by NIST. [19-22]

Code-Based Cryptography :

Code-Based Cryptography is one of the forms of post-quantum cryptography which applies error-correcting codes for generating secure digital signatures and encryption. It was one of the first forms of public-key cryptography (proposed in 1978!) and remains one of the most promising contenders for being able to withstand attack by quantum computers.[23]

Multivariate Polynomial Cryptography :

It is founded on solving multivariate quadratic systems of equations. Multivariate Polynomial Cryptography is a post-quantum cryptography that employs mathematical equations with several variables and polynomials to make digital communication secure. It is made to be secure even against future quantum computers, which are predicted to compromise a large number of conventional cryptography systems (such as RSA or ECC).[24-26]

Hash-Based Cryptography :

Hash-Based Cryptography is a form of post-quantum cryptography that employs cryptographic hash functions(such as SHA-256) to create secure digital signatures. It is among the oldest and best-understood types of quantum-resistant cryptography, and is regarded as being very secure even against quantum computers.

Challenges in Implementation :

Adoption of post-quantum cryptography poses some practical challenges:[27-30] Overhead in Performance: Several PQC algorithms have bigger key sizes or slower processing than classical equivalents.

Post-Quantum Cryptographic Algorithms :

Post-Quantum Cryptographic Algorithms are cryptographic protocols that are specifically developed to be secure against quantum computers. Quantum computers may decrypt many conventional encryption algorithms like RSA, DSA, and ECC with algorithms like Shor's algorithm and Grover's algorithm.

Thus, post-quantum algorithms seek to secure Encrypted messages, Digital signatures, secure communication Even in a world in which quantum computers are potent and prevalent.

PQC algorithms based on mathematical problems, which are assumed quantum attack-resistant. It include-

Lattice-Based Cryptography :

Lattice-Based Cryptography is a new form of post-quantum cryptography that employs the sophisticated geometric shapes known as lattices to construct encryption and digital signature schemes.

It is one of the most promising and widely recommended methods for keeping data safe from quantum computer attacks and encompasses schemes such as Kyber (for encryption) and Dilithium (for digital signatures), both of which are under standardization by NIST.[19-22]

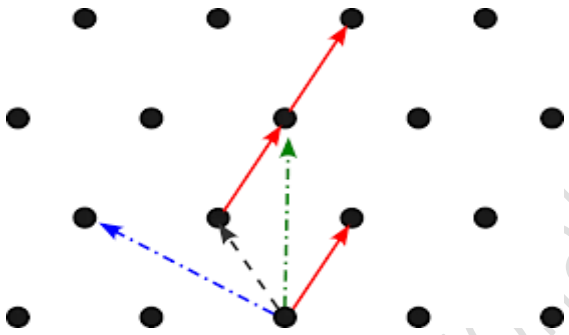

Fig. Lattice-Based Cryptography

Code-Based Cryptography :

Code-Based Cryptography is one of the forms of post-quantum cryptography, which applies error-correcting codes for generating secure digital signatures and encryption.

It was one of the first forms of public-key cryptography (proposed in 1978!) and remains one of the most promising contenders for being able to withstand attack by quantum computers.[23]

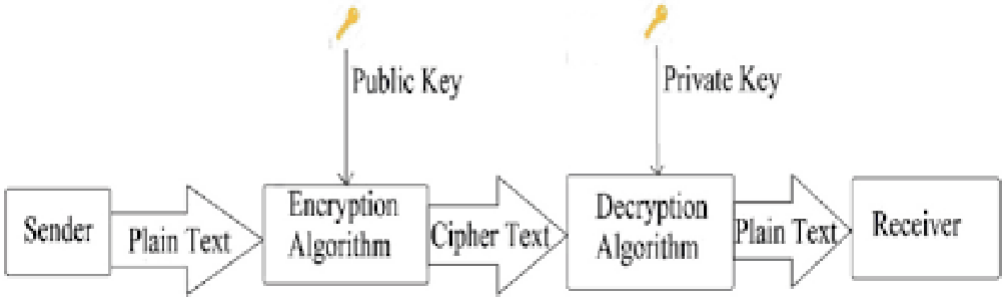

Fig. Code-Based Cryptography

Multivariate Polynomial Cryptography :

It is founded on solving multivariate quadratic systems of equations. Multivariate Polynomial Cryptography is a post-quantum cryptography that employs mathematical equations with several variables and polynomials to make digital communication secure.

It is made to be secure even against future quantum computers, which are predicted to compromise a large number of conventional cryptography systems (such as RSA or ECC).[24-26]

Hash-Based Cryptography :

Hash-Based Cryptography is a form of post-quantum cryptography that employs cryptographic hash functions (such as SHA-256) to create secure digital signatures.

I t is among the oldest and best-understood types of quantum-resistant cryptography, and is regarded as being very secure even against quantum computers.

Challenges in Implementation :

Adoption of post-quantum cryptography poses some practical challenges:[27-30]

Overhead in Performance:

Several PQC algorithms have bigger key sizes or slower processing than classical equivalents.

System Integration:

Replacing existing cryptographic primitives in protocols and infrastructures (e.g., TLS, VPNs, IoT).

Security Assurance:

Ongoing examination is needed to certify quantum resistance of these new algorithms.

Standardization and Adoption:

NIST's standardization effort on PQC is a crucial milestone toward large-scale deployment. The Role of Quantum Physics in PQC Development

Quantum physics must be understood in creating cryptographic systems that can withstand quantum attacks. Fundamental physical principles are:

No-Cloning Theorem:

Constrains certain forms of quantum attacks.

Quantum Parallelism:

Accounts for the exponential speedup of algorithms such as Shor's.

Entanglement and Measurement:

Influence the dynamics of quantum systems in cryptographic contexts.Through making

cryptographic, design consistent with the facts of quantum mechanics, our hope to future-proof digital security.

Conclusion :

The advent of quantum computers threatens existing cryptographic infrastructures, particularly public-key algorithms such as RSA and ECC. Post-Quantum Cryptography (PQC) provides a software-only solution based on algorithms that are secure against classical and quantum attacks alike. These algorithms are built upon hard mathematical problems such as lattices, codes, or multivariate equations.

This study analyzed the most prevalent PQC algorithms, highlighting their advances, weaknesses, and development in standardization. Indeed, NIST's efforts have seen the finalization of Kyber, Dilithium, and SPHINCS+ as post-quantum security standards. Nevertheless, real-world limitations such as high key sizes, performance in constrained devices, and side-channel attack resistance remain primary concerns.

Although PQC offers a promising way out, its adoption will require robust strategies, adaptability of cryptography, and global collaboration. It is essential to get ready today in order to guarantee safe communication in a world with widespread quantum technology.

References :

- Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
- Hülsing, A., Rijneveld, J., Schwabe, P., (2022). SPHINCS+: Submission to the NIST PQC Project.
- Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2021). (TCHES), 2021(1), 238–268.
- 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)
- Bavdekar, A., Yadav, D. K., Patil, S., & Sahu, A. K. (2022). Post-quantum cryptography: Techniques, challenges, and directions.
- Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange A new hope. In 25th USENIX Security Symposium (pp. 327–343).
- Bernstein, D. J., et al. (2021). SPHINCS+ submission to NIST.
- Hoffstein, J., Pipher, J., Silverman, J.H. (1998). NTRU: A ring-based public key cryptosystem.
- Shor, Peter W**.** “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”SIAM Journal on Computing, 1997.
- Bernstein, Daniel J., Buchmann, Johannes, Dahmen, Erik (Eds.)**“**Post-Quantum Cryptography”Springer, 2009.
- Regev, Oded.“On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”Journal of the ACM (JACM), 2009.
- Alkim, Erdem et al**.**“CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based

KEM"IEEE European Symposium on Security and Privacy, 2018.

- Ducas, Léo et al.**"**CRYSTALS-DILITHIUM: Digital Signatures from Module Lattices" PQCrypto 2017.
- Marel Alvarado et al., "A Survey on Post-Quantum Cryptography State-of-the-Art and Challenges" (2023)
- Seyed Mohammad Reza Hosseini & Hossein Pilaram, "A Comprehensive Review of Post-Quantum Cryptography: Challenges and Advances" (2024, Crypto-ePrint)
- Arimondo Scrivano, "A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing" (arXiv, June 2025)
- Ritik Bavdekar et al., "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research" (2022)
- National Institute of Standards and Technology. (2022). Post-Quantum Cryptography Standardization Project
- 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
- Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461
- Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R., & Smith-Tone,
- D(2016). Report on post-quantum cryptography (NISTIR 8105). National Institute of Standards and Technology.
- Manish Kumar, "Post-Quantum Cryptography Algorithms Standardization and Performance Analysis" (2022)
- Bindel, Nina et al**.**"Hybrid Key Exchange in TLS 1.3"Internet Engineering Task Force (IETF), 2021.
- Albrecht, Martin R. et al.**"**On the Concrete Security of Module-LWE Encryption Schemes"ASIACRYPT2018