IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 9, April 2025
Impact Factor: 7.67

A Comprehensive Study of Crystal Kyber

Kulsum Abdullah Sayed, Nabila Anwar Jamal Qureshi, Mishkat Moinuddin Khan, Shifa Farooqui
Computer Engineering
M. H. Saboo Siddik College of Engineering, Byculla, Mumbai, India
kulsum.222267.co@mhssce.ac.in, nabila.222265.co@mhssce.ac.in
Indiamishkat.222264.co@mhssce.ac.in, shifa.211217.co@mhssce.ac.in

Abstract: *Quantum computing threatens classical cryptographic systems, prompting the need for quantum-resistant algorithms. This paper introduces Crystal Kyber, a lattice-based Key Encapsulation Mechanism (KEM) standardized by the National Institute of Standards and Technology (NIST) as a post-quantum cryptographic solution. KEMs enable secure key exchange over insecure channels, facilitating encryption and authentication. Crystal Kyber is based on the Module Learning with Errors (MLWE) problem, a hard mathematical problem resistant to both classical and quantum attacks. The mechanism securely encapsulates a shared secret key, ensuring that only the intended recipient can decapsulate it. Crystal Kyber offers three parameter sets—Kyber512, Kyber768, and Kyber1024—balancing security and performance for various applications, from constrained environments to high-security domains. This paper examines Crystal Kyber's key generation, encapsulation, and decapsulation processes, highlighting its computational efficiency, scalability, and quantum resistance. It positions Crystal Kyber as a crucial component of future-proof cryptographic standards for securing communication in the quantum era..*

Keywords: Advanced Encryption Standard, Federal Information Processing Standard, Key-Encapsulation Mechanism, Learning with Errors, MLWE-Module Learning with Errors, NIST- National Institute of Standards and Technology, NISTIR-NIST Interagency or Internal Report, NTT-Number-Theoretic Transform, PKE-Public-KeyEncryption, PQC-Post-Quantum Cryptography, PRF-Pseudorandom Function, RBG-RandomBit Generator, SHA-Secure Hash Algorithm