NEXT GEN HYBRID CRYPTOGRAPHY

ABSTRACT

With the advent of quantum computing, traditional cryptographic algorithms, particularly RSA and ECC, face vulnerabilities due to Shor's algorithm, which can efficiently break their security foundations. Post-Quantum Cryptography (PQC) is emerging as a solution, leveraging lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptographic schemes to resist quantum attacks. However, transitioning entirely to PQC is challenging due to performance trade-offs, implementation complexities, and uncertain security guarantees against future quantum advancements.

This project explores the integration of PQC with hybrid cryptographic models that combine classical and quantum-resistant approaches to achieve enhanced security and performance. Hybrid cryptography enables a gradual transition to quantum-safe encryption while maintaining compatibility with existing infrastructure. The proposed hybrid framework utilizes symmetric encryption for data confidentiality, classical asymmetric cryptography for efficiency, and PQC-based key exchange mechanisms for long-term security. Additionally, it analyzes potential vulnerabilities, computational overhead, and real-world applicability in secure communication protocols.

By integrating PQC with traditional cryptographic methods, this hybrid approach provides a resilient and scalable solution, ensuring robust security in both pre-quantum and post-quantum computing environments.

K RANGANATH BHARADWAJ
1602-22-733-035
T CHARAN VIVEKANANDA
1602-22-733-008

Project Guide :

Ms. T.Jalaja
Assistant Professer
Dept. of CSE