Enhancing Post-Quantum Cryptographic Protocols with Quantum-Resistant Key Exchange Mechanisms

Publisher: IEEE

Gohin Balakrishnan ; Aruna Samudrala ; Suresh Chanamala ; Sai Bhairav Rajesh ; Suresh Babu Thandullu Naganathan **All Authors**

Abstract:
The emergence of quantum computers poses a significant threat to classical cryptographic systems. Post-quantum cryptography (PQC) aims to develop cryptographic protocols resistant to quantum attacks. This study explores the enhancement of post-quantum cryptographic protocols by integrating quantum-resistant key exchange mechanisms. We propose the Quantum-Lattice Resilient Exchange Framework (Q-LREF), utilizing lattice dimensions 256, 512, and 1024) with Gaussian noise distribution 3.2. Through experimental evaluation, we demonstrate that our approach outperforms traditional RSA and ECC schemes while achieving comparable efficiency to CRYSTALS-Kyber with robust security margins. By reviewing existing literature, implementing our novel framework, and analyzing results, we demonstrate the efficacy of our approach against both classical and quantum adversaries. We also provide a comprehensive analysis of potential challenges and future directions in PQC, including detailed examination of various quantum-resistant algorithms and their applications.

Published in: 2025 11th International Conference on Communication and Signal Processing (ICCSP)

Date of Conference: 05-07 June 2025

DOI: 10.1109/ICCSP64183.2025.11088727

References
Keywords
More Like This

Date Added to IEEE *Xplore*: 29 July 2025

Publisher: IEEE

ISBN Information:

Conference Location: Melmaruvathur, India

ISSN Information:

Authors

Figures

References

Keywords