Contribution ID: **20** Type: **Poster**

Post-Quantum Cryptography: Benchmarking ML-KEM Against RSA

Thursday 24 April 2025 10:45 (30 minutes)

The rise of quantum computing presents a significant threat to classical cryptographic systems, particularly those relying on hard mathematical problems such as integer factorization and discrete logarithms. This paper explores the impact of quantum computing on traditional cryptographic algorithms and the necessity of transitioning to quantum-resistant cryptography. We provide an overview of post-quantum cryptographic (PQC) algorithms newly standardized by the National Institute of Standards and Technology (NIST) in the Federal Information Processing Standards (FIPS) 203, 204, and 205, which define quantum-secure key encapsulation and digital signature schemes. We examine existing implementations of these algorithms and evaluate the performance of ML-KEM against its classical alternative – RSA. Our findings highlight the feasibility of deploying PQC in real-world systems by demonstrating that at high security levels, ML-KEM can achieve significantly faster operation speeds than RSA, proving its ability to provide both strong security and practical efficiency.

Authors: PACEK, Dominika (Warsaw University of Technology); ŁABĘCKA, Nina (Warsaw University of Technology)

Presenter: ŁABĘCKA, Nina (Warsaw University of Technology)

Session Classification: Session B (Poster)