xploiting Montgomery Reduction in Kyber Through Side-Channel Analysis

Kevin Andrae Delgado Vargas

Centro de Investigación en Computación, Instituto Politécnico Nacional, Mexico

Kyber, a standardized post-quantum cryptographic key encapsulation mechanism (KEM), relies on modular arithmetic operations, including Montgomery reduction, to achieve efficient computation. However, the mathematical properties of Montgomery reduction may introduce side-channel leakage that adversaries may exploit. In this presentation, we discuss the vulnerability of Kyber's Montgomery reduction to side-channel attacks, focusing on power and electromagnetic analysis. We demonstrate that leakage patterns can be leveraged to extract sensitive information by isolating and analyzing the reduction process. Our findings highlight the need for stronger countermeasures in PQC implementations, especially in constrained embedded environments.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T08