Dr inż. Daniła Gorodecki, Instituto de Engenharia de Sistemas e Computadores - Investigação e Desenvolvimento (INESC-ID), University of Lisbon

Toward Boolean Functions in Post-Quantum Cryptography

This talk explores the role of Boolean functions in post-quantum cryptography, with a focus on their use in practical implementations. We focus on post-quantum cryptography and side-channel attacks regarding to KYBER and Dilithium algorithms. The presentation then examines the arithmetic operations underlying these schemes, emphasizing their Boolean structure, masking techniques, and transformations between arithmetic and Boolean domains. We discuss an approach to implementing arithmetic operations via multiple addition of low-bit-width products.