IV. International Conference on Mathematics and its Applications in Science and Engineering

[ICMASE 2023]

Title: Applicabilityof AI to Cryptographic Algorithms

Abstract: Recently, the National Institute of Standards and Technology set CRYSTALS--Kyber as post-quantum public key encryption/key encapsulation mechanism standard, and CRYSTALS--Dilithium as post--quantum digital signature standard. These post quantum cryptosystems are also recommended for national security systems. As a result, it is important to identify and analyze the weaknesses and potential information leakage points, so that they can be resolved. In this talk, the newest side channel attacks based on artificial intelligence models against Kyber and Dilithium are presented, focusing on the specific function attacked.