From: AIKATA <aikata@iitbhilai.ac.in> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] KaLi: A Crystal for Post-Quantum Security using Kyber and Dilithium
Date: Wednesday, November 02, 2022 01:47:14 PM ET

Dear PQC Community,

We introduce KaLi, a compact unified cryptoprocessor for performing both lattice-based digital signature and key encapsulation operations using CRYSTALS-Dilithium and CRYSTALS-Kyber solely in hardware. The architecture has a compact area due to synergies in Dilithium and Kyber.

Kyber's modulus (12-bit prime) is half the size of Dilithium's modulus (a 23-bit prime modulus). A unified yet flexible polynomial arithmetic unit is designed that can process Kyber operations 2x as fast as Dilithium operations using the wide datapath. Several additional optimizations are performed at the scheduling, architecture, and circuit levels. In the 28nm ASIC technology, KaLi occupies 0.263 mm2 and achieves a clock frequency of 2GHz.

For more information, see the paper "KaLi: A Crystal for Post-Quantum Security using Kyber and Dilithium" which has been accepted for publication in IEEE TCAS-1. It is currently available at: https://eprint.iacr.org/2022/1086

Regards
Aikata

--