Hardware Implementations of Post-Quantum Cryptography Digital Signature Schemes

Luke Beckwith, Robert Wallace, and Kris Gaj
George Mason University, U.S.A.

In August 2024, the first two general-purpose Post-Quantum Cryptography (PQC) digital signature schemes were standardized by the U.S. National Institute of Standards and Technology (NIST). These schemes are referred to as ML-DSA (based on the NIST standardization-process candidate called CRYSTALS-Dilithium) and SLH-DSA (based on SPHINCS+). An additional standard, FN-DSA, based on the candidate called FALCON, is currently under development. In June 2023, NIST launched Round 1 of a new onramp process for digital signatures aimed at identifying strong candidates for additional PQC signature standards, with the preference given to non-lattice-based schemes and schemes with certain unique features, such as very short signatures. This process is currently in Round 2, with 14 candidates representing six different families (code-based, isogeny-based, lattice-based, MPC-in-the-head, multivariate, and symmetric-based) remaining in the competition.

In this talk, we will investigate the current state of standardization in the area of PQC signature schemes. We will analyze and compare the best-known hardware implementations of emerging PQC standards ML-DSA and SLH-DSA. We will contrast them with the recently developed hardware implementations of selected Round 2 onramp signature schemes, such as LESS, MAYO, UOV, and SDiTH. All investigated signature schemes will be compared from the point of view of the public key and signature sizes, execution times in software and hardware, and the relative cost of their hardware implementations.

We will discuss the major operations of these schemes and the challenges of implementing these operations efficiently in hardware. We will also investigate the suitability of each of the investigated schemes for particular application scenarios. We will conclude the presentation by describing the next steps of the standardization process and open problems related to the efficient and secure implementation of future standards.