High-Speed Hardware Implementations of Post-Quantum Cryptography Digital Signature Schemes

Luke Beckwith, Robert Wallace, Duc T. Nguyen, Kamyar Mohajerani, and Kris Gaj
George Mason University, U.S.A.

Post-Quantum Cryptography (PQC) refers to a new class of cryptographic algorithms that are resistant to all known attacks using classical and quantum computers but, at the same time, can be implemented by themselves using traditional computing platforms, such as microprocessors, microcontrollers, and Field Programmable Gate Arrays (FPGAs). These algorithms support two major applications - secure key exchange and digital signature - and fall into five major families: code-based, isogeny-based, lattice-based, multivariate, and symmetric-based.

In 2016, the U.S. National Institute of Standards and Technology (NIST) initiated a comprehensive process aimed at selecting the best candidates and developing standards based on them. The initial submissions included over 20 digital signature schemes. This number was reduced to 9 in Round 2 (Jan. 2019-July 2020) and 6 in Round 3 (July 2020-July 2022). In February 2022, one of the finalists, belonging to the family of multivariate cryptosystems, Rainbow, was effectively broken. It took a weekend on a laptop to recover a private key for one of the proposed parameter sets that was expected to make the scheme as secure as AES-128. Eventually, in July 2022, NIST announced the selection of two lattice-based schemes: CRYSTALS-Dilithium and FALCON, and one symmetric/hash-based scheme, SPHINCS+, for near-term standardization. All remaining candidates were judged to be unsuitable for standardization, and none was qualified for Round 4. Instead, NIST announced a call for new, preferably non-lattice-based signature schemes with the deadline on June 1, 2023. Known candidates include a recently developed code-based signature scheme called LESS.

In this talk, we will briefly describe our high-speed hardware implementations of three of these schemes: CRYSTALS-Dilithium, FALCON, and LESS. We will first characterize these schemes in terms of their signature and public key sizes. We will then evaluate them in terms of their latency, throughput, and resource utilization in Xilinx Artix-7 FPGAs. We will demonstrate that all our implementations are resistant to timing attacks. We will discuss the major operations of these schemes and the challenges of implementing these operations efficiently in hardware. For CRYSTALS-Dilithium, these challenges amount to the complexity of polynomial multiplication and sampling, including the efficient implementation of polynomial multiplication using the best-known algorithm called Number Theoretic Transform. For FALCON, the need to implement floating-point operations and Fast Fourier Transform. For LESS, an efficient conversion of a large matrix over a prime field to its unique representation called the Reduced Row Echelon Form (RREF). All our designs will also be compared with the best available hardware implementations of SPHINCS+ and CRYSTALS-Dilithium, developed by other groups.

We will discuss 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.