Notice and Invitation

Oral Defense of Master's Thesis

The Volgenau School of Engineering, George Mason University

Ahmed Ferozpuri

Bachelor of Science, George Mason University

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

Wednesday, December 6, 2017, 10:30am

Engineering Building, Room 2901

All are invited to attend.

Committee

Dr. Kris Gaj, Thesis Director

Dr. Jens-Peter Kaps

Dr. Avesta Sasan

Abstract

Multivariate cryptosystems belong to the five most promising families of post-quantum cryptography (PQC) schemes. Among them, the Unbalanced Oil and Vinegar (UOV) and the Rainbow signature schemes have been extensively studied since 1999 and 2005, respectively. The main advantage of UOV is high confidence in its security; the disadvantages include large key and signature sizes. Rainbow is a multi-layer version of UOV that offers better performance, smaller keys, and smaller signatures. In this thesis, we present and compare hardware implementations of both schemes in high-performance Field Programmable Gate Arrays (FPGAs). The optimization is for the minimum signature generation and verification time. The generation of keys is assumed to be done in software. Compared to the previous state-of-the-art high-speed implementation, the proposed design for Rainbow is more than twice as fast, and introduces two architectural innovations: a novel pivot calculation circuit and a memory based microprogrammed architecture. Additionally, in order to make benchmarking easier and fairer, our design follows a universal PQC hardware API, which allows for fair comparison with other post-quantum signature schemes, in particular those submitted to the NIST PQC Project. The design is intended to be made open-source to speed-up further optimizations. Additionally, we will discuss a novel matrix method binarization with its potential applications, a projection of scalability for larger security levels and future optimizations.