Notice and Invitation

Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

Malik Umar Sharif
Bachelor of Science, National University of Sciences and Technology, 2001
Master of Science, George Washington University, 2010

HARDWARE-SOFTWARE CODESIGN APPROACHES TO PUBLIC KEY CRYPTOSYSTEMS

August 2, 2017, 10:00am-12:00pm
Engineering Building, Room 4801
All are invited to attend.

Committee
Dr. Kris Gaj, Chair
Dr. Jens-Peter Kaps
Dr. Houman Homayoun
Dr. Robert Simon

Abstract

If a quantum computer with a sufficient number of qubits was ever built, it would easily break all current American federal standards in the area of public-key cryptography, including algorithms protecting the majority of the Internet traffic, such as RSA, Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), and Diffie-Hellman. As a result, a new set of algorithms, resistant against any known attacks involving quantum computers, must be developed. These algorithms are collectively referred to as Post-Quantum Cryptography (PQC). The standardization effort for these algorithms is likely to last years and result in the entire portfolio of algorithms capable of replacing current public-key cryptography schemes. As a part of this standardization process, fair and efficient benchmarking of PQC algorithms in hardware and software becomes a necessity. Traditionally, software implementations of public-key algorithms provided the highest flexibility but lacked performance. On the other hand, custom hardware implementations provided the highest performance but lacked flexibility and adaptability to changing algorithms, parameters, and key sizes. Therefore, in this work, we investigate the suitability of the hardware/software codesign for implementing and evaluating traditional and post-quantum public-key cryptosystems from the point of view of their implementation efficiency.

As our case studies, we considered one traditional public key cryptosystem, RSA, and one post-quantum public key cryptosystem, NTRUEncrypt. We implemented both of them using custom hardware, as well as software/hardware codesign. The Xilinx Zynq-7000 System on Chip platform, which integrates a dual-core ARM Cortex A9 processing system along with Xilinx programmable logic, was used for our experiments. The performance vs. flexibility trade-off has been investigated, and the speed-up of our software/hardware codesign implementations vs. the purely software implementations on the same platform is reported and analyzed. Similarly, the speed-up of the custom hardware vs. hardware-software codesign is investigated as well. Additionally, we have determined and analyzed different percentage contributions of the execution times for equivalent component operations executed using the aforementioned three different implementation approaches (custom hardware, software/hardware codesign, and pure software). We demonstrate that hardware/software codesign can reliably assist in early evaluation and comparison of various public-key cryptography schemes. Our project is intended to pave the way for the future comprehensive, fair, and efficient benchmarking of the most promising encryption, signature, and key agreement schemes from each of several major post-quantum public-key cryptosystem families.