A Generic High-Speed Hardware Implementation of NTRUEncrypt SVES

ECE Ph.D. Seminar
By
Malik Umar Sharif

Ph.D. Advisor:
Dr. Kris Gaj

Monday, July 24th, 2017
11:00 – 12:00 PM

ENGR 3507

Abstract

NTRUEncrypt is a polynomial ring-based public-key encryption scheme that was first introduced at Crypto'96. In 2008, an extended version of this algorithm was published as the IEEE 1363.1 Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices. Within the standard, the described algorithm is called Short Vector Encryption Scheme – SVES. The recent renewed interest in NTRU is at least partially driven by its presumed resistance to any efficient attacks using quantum computers. In Feb. 2016, NIST has announced its plans of starting the standardization effort in the area of post-quantum cryptography. This effort is likely to last years and result in an 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.

We present a high-speed hardware implementation of NTRUEncrypt Short Vector Encryption Scheme (SVES), fully compliant with the aforementioned IEEE standard. Our design supports two representative parameter sets, ees1087ep1 and ees1499ep1, optimized for speed, which provide security levels of 192 and 256 bits, respectively. Our implementation follows an earlier proposed Post-Quantum Cryptography (PQC) Hardware Application Programming Interface (API). As a first design following this API, it provides a reference that can be adopted in any future implementations of post-quantum cryptosystems. We present the detailed flow and block diagrams, as well as results in terms of latency (in clock cycles), maximum clock frequency, and resource utilization. We also report the speedup of our implementation in Xilinx Field Programmable Gate Arrays (FPGAs) as compared to existing software implementations of NTRUEncrypt SVES, with equivalent functionality. Our results show a significant speed-up of hardware vs. software, and very different percentage contributions of the execution times for equivalent operations executed in these two different environments. Our project is intended to pave the way for the future comprehensive, fair, and efficient hardware benchmarking of the most promising encryption, signature, and key agreement schemes from each of several major post-quantum public-key cryptosystem families.