Parallel Implementation of the Convolution Operation in Quotient Polynomial Rings for the NTRU Cryptosystem

Gupta, Vikul

The N-th Degree Truncated Polynomial Ring (NTRU) cryptosystem is a promising alternative to current cryptosystems, such as RSA, because of its superior security characteristics. Convolution of polynomials is the most computationally intensive operation for NTRU. This project developed efficient hardware implementations for convolution. Using a regular recursive approach, a hierarchical hardware design was developed such that each lower level is the design of convolution for half the block size of the higher level. Design improvements in the base cases aggregate up the hierarchy to generate an efficient overall design. First, the correctness of this approach was established in software. Next, a software generator was developed that creates the hardware design in SystemVerilog given a security level. These designs were shown to use significantly fewer multiplications and additions in comparison to the conventional approach. Further, it was demonstrated that the gains would be even greater for higher security levels. Gate count complexity for a generic technology and logic element count for FPGAs were also compared and similar performance gains were demonstrated. For the recommended security level, N=503, the optimal approach used 92.2% fewer multiplications, 56.8% fewer additions, and 85.5% fewer gates. Finally, discrete-event simulation and FPGA prototyping established the functional correctness of the designs. In summary, this work could be used to design efficient convolution circuits in larger NTRU chips in an effort to make NTRU a practical alternative to current cryptosystems because it presents a technique for developing implementations that are faster and use less hardware than conventional approaches.

Awards Won:

Fourth Award of $500