Efficient, Hardware Implementations of Computationally-Intensive Operations in Quotient Polynomial Rings for NTRU-Based Digital Signatures

Gupta, Vikul

The security of data is a major issue in today's society–one way to ensure this security is to use digital signatures. NTRUSign, the signature scheme based on the N-th Degree Truncated Polynomial Ring (NTRU) cryptosystem, is a promising alternative because it has significantly superior security characteristics to other schemes. NTRUSign uses quotient polynomial rings with modular integer coefficients, represented as □Z[□] /(□^□ − 1). The five primary operations required for NTRUSign are addition, scalar multiplication, modulus, inverse, and convolution. This project developed cost functions and approaches for efficient hardware implementations for each of the five operations. This project also presents the first hardware implementation of NTRUSign. First, the correctness of these approaches was established in software. Next, a software generator was developed that creates the hardware design for NTRUSign 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 was also compared and similar performance gains were demonstrated. For the recommended security level, N=503, the optimal approach used 92.1% fewer multiplications, 8.8% fewer additions, and 78.9% fewer gates. In summary, because it presents the first technique for developing NTRUSign hardware implementations, this work could be used to design efficient circuits in an effort to make NTRUSign a practical alternative to current signature schemes.

Awards Won:

Fourth Award of $500

Fondazione Bruno Kessler: Second Award of $1,000