Ultra-Compact Reconfigurable NTRUEncrypt Public Key Cryptosystem Core

Elif Bilge Kavun, Tolga Yalcin
Ruhr-University Bochum, Germany

Abstract

Lattice-based NTRU public key cryptosystem can be an alternative to other public key cryptosystems, such as RSA and ECC, especially on low-cost programmable devices. In this paper, we present a very compact NTRUencrypt core, which implements both encryption and decryption functionality. Our core is suitable for even the smallest FPGAs and CPLDs, as well as ASICs. It achieves 136.5 MHz using only 204 slices, 457 LUTs, 1 BRAM on a Xilinx-Virtex5 VLX20T; 57.2 MHz using only 307 slices, 553 LUTs, 1 BRAM on a Xilinx Spartan3-S50 and 15.1 MHz using only 1157 tiles, 4 BRAMs on an Actel APA075. When synthesized on a generic 0.13 micron CMOS library, it occupies only 1400 equivalent gates and 1 KB single-port RAM. In the current configuration our core implements both NTRU-167 and NTRU-263, which are equivalent to RSA-512 and RSA-1024, respectively, in terms of security. However, reconfigurable structure of the design allows realization of higher security levels at the cost of additional RAM blocks only, with almost zero increase in slice/tile/gate count.