Implementation Challenges for Ideal Lattice-Based Cryptography on Reconfigurable Hardware

Thomas Pöppelmann and Tim Güneysu

Abstract

Novel public-key cryptosystems beyond RSA and ECC are urgently required to ensure long-term security in the era of quantum computing. One alternative to such established schemes is ideal lattice-based cryptography which offers elegant security reductions and versatile tools such as the ring learning with errors (RLWE) problem. In this talk we will give an overview on current research dealing with the implementation and optimization of efficient ideal lattice-based cryptography on reconfigurable hardware. Basic building blocks we will discuss are the number theoretic transform (NTT) for fast polynomial multiplication and discrete Gaussian sampling. Especially the NTT is very efficient on reconfigurable hardware and several works have improved the state-of-the art so far. Using these building blocks we will introduce efficient hardware implementations of public key encryption as well as signature schemes and discuss some open problems and challenges in this emerging field of research.