Lattice sieving acceleration in FPGAs

Michal Andrzejczak
Military University of Technology in Warsaw, Poland

Abstract

Lattice-based cryptography is a promising option for secure communication in post-quantum era. Recently, a significant effort has been put into improving algorithms for solving lattice problems, such as the Shortest Vector Problem, especially using an algorithm called lattice sieving. The aforementioned algorithm is used for the cryptoanalysis of lattice-based schemes and as a result also for proper security parameters selection. Recent improvements and acceleration for lattice-sieving have been accomplished primarily using progress in the underlying math. In this talk we present the first reported attempt at speeding up lattice sieving algorithms with FPGAs in various scenarios, in particular, by using software/hardware codesign approach.