Implementation of Lattice-based Cryptographic Primitives: Efficiency and Security

Erdem Alkim
Ondokuz Mayis University, Samsun, Turkey

Abstract

In this workshop, my aim is to give a point of view on the design principles of post-quantum cryptographic schemes. This will mainly include recent schemes submitted NIST Post-Quantum Cryptography Project. Since there is a great interest for the implementation of lattice-based cryptographic schemes, the focus will be given to lattice-based cryptography. The organization of this workshop is as follows:

- Introduction to post-quantum cryptography, Overview of the NIST Post-Quantum Cryptography Project submissions with focusing on similarities and differences of the submissions.
- Lattice-based primitives, Google's post-quantum experiment, pros/cons with comparing nowadays cryptosystems as well as post-quantum alternatives. The talk will focus on three lattice based submissions, NewHope, FrodoKEM, and qTesla. I will start with explaining what the differences from nowadays systems are, and how efficient they are. Then I will compare these schemes with other NIST submissions.
- Efficiency, security and size issues of building blocks in lattice-based schemes and how they can be solved. In this talk I will first seperate implementations in to building blocks and explain them separately. Then I will give overview of the implementation issues, and attacks. Finally I explain how we solved these during the submission process.