Abstract for Seminar on NIST's Module-Lattice-Based Key-Encapsulation Mechanism Standard

Anna Jokiniemi

University of Helsinki

In collaboration with Nokia

It is predicted that sufficiently powerful quantum computers will be built within the next twenty years. With algorithms such as Shor's and Grover's, quantum computers will be capable of breakking many modern cryptographic methods, posing a significant threat for global data security.
Although twenty years may seem like a long time, sensitive information encrypted with today's methods could be strored and decrypted using future quantum technology. Therefore, if data remains sensitive long in the future, it should be stored in quantum-safe methods.

Cryptography experts are actively designing quantum-safe cryptographic techniques. The National Institute of Standards and Technology (NIST) is the agency of the United States department of commerce. NIST is the de facto authority in cryptography, and its recommendations are widely followed by organizations worldwide. Nokia committed to state-of-the-art cryptography methods, follows closely NIST's developments in security.

NIST in concerned about the thret of quantum computers and has recently launched quantum-safe cryptography standards, one of which is the the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) standard. This seminar will introduce ML-KEM and its working principle. We will explore what key-encapsulation methods are and their application. Additionlly, we will discuss module lattices and a specific problem related to them: the module learning with errors problem. This problem forms the basis of ML-KEM's working principle. Finally, I will present my own thesis subject.

Keywords: post-quantum cryptography, lattice cryptography, KEM, NIST