A very Brief Introduction to Lattice-Based Cryptography

Erkay Savaş

As recent efforts in building quantum computers produce very promising results, there is an urgent need for a new set of cryptographic algorithms for the post quantum world. Fully homomorphic encryption allows processing of encrypted data without decryption, which can be instrumental in solving many privacy problems. Lattice-based cryptosystems are nowadays increasingly important due to two reasons: i) they are presumably post-quantum (i.e., secure against cryptanalytic attacks running on quantum computers) and ii) they support fully homomorphic encryption. In this talk, we give a very brief introduction to lattice-based cryptography. In particular, we provide a specific construction for a public key cryptosystem based the hardness of the ring version of the learning with errors problem (Ring-LWE), which is equivalent to hardest problems on lattices. We, then, demonstrate that the construction supports both homomorphic addition and multiplication of ciphertexts.