Fully Homomorphic Encryption: Simple Construction and Open Problems.
Daniele Micciancio, UCSD

Fully Homomorphic Encryption (FHE) allows to perform arbitrary computations on encrypted data, and is one of the most advanced applications of lattice cryptography. In this talk I will give a simple description of some of the most recent FHE constructions. I will then move to describe the main open problems in the area: improving the efficiency of current constructions, and avoiding the need to make circular security assumptions.