Bocconi

17 APRIL 2025
12:00 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1, Milano

Lattices Post-Quantum Security and Homomorphic Encryption

Speaker

Daniele Micciancio
Professor

Department of Computer Science & Engineering
University of California, San Diego

Abstract

Modern cryptography relies on mathematical problems that are computationally hard to solve, and exploits their hardness to build secure applications that are equally hard to break. During the last two decades, mathematical problems on point lattices have emerged as a very attractive class of problems to build new and powerful cryptographic functions. The talk will provide an overview of lattice-based cryptography, its roots in theoretical computer science, and some of its most distinctive features: resistance against powerful quantum adversaries, and the ability to carry out computations on encrypted data.

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES