**Current challenges in fully homomorphic encryption**

Anamaria Costache

Abstract: Fully Homomorphic Encryption (FHE) allows to compute on encrypted data. It remained an open problem for nearly 30 years, until Gentry'09 provided a first construction. After that, many constructions followed, but they remained too impractical to be considered for real-life deployment. Recent advances have changed this, and we have begun to see applications in industry which deploy FHE. Because of this, questions regarding the security of FHE schemes beyond CPA become vital to explore. In this talk, we will discuss such challenges, with a particular focus on Verifiable Computation (VC) for FHE.