

Title: Walking the edge between structure and randomness: New constructions for Obfuscation and Functional Encryption.

Speaker: Prof. Shweta Agrawal, IIT Madras

Abstract: Functional Encryption and Obfuscation are two of the most exciting primitives in modern cryptography. Functional Encryption generalizes public key encryption and allows fine grained access on encrypted data. Obfuscation asks to garble a program such that its input output behaviour is preserved but all its internal workings are hidden. These two primitives are deeply connected, and finding efficient constructions for them, provably secure from well understood hardness assumptions is one of the key themes of modern crypto research.

In this talk, I will summarize the state of art in this space as well as discuss some new results