CFEM workshop:
Theory and Practice of Secure Multiparty Computation
May 5 to 9, 2014
Aarhus University, Denmark

Speaker: Rafael Pass, Cornell University

Title: **Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings**

We define a notion of semantic security of multilinear (a.k.a. graded) encoding schemes, which generalizes a multilinear DDH assumption: roughly speaking, we require that if two constant-length sequences m0, m1 are pointwise statistically indistinguishable by algebraic attackers C (obeying the multilinear restrictions) in the presence of some other elements z, then encodings of these sequences should be computationally indistinguishable. Assuming the existence of semantically secure multilinear encodings and the LWE assumption, we demonstrate the existence of indistinguishability obfuscators for all polynomial-size circuits. We rely on the beautiful candidate obfuscation constructions of Garg et al (FOCS'13), Brakerski and Rothblum (TCC'14) and Barak et al (EuroCrypt'14) that were proven secure only in idealized generic multilinear encoding models, and develop new techniques for demonstrating security in the standard model, based only on semantic security of multilinear encodings (which trivially holds in the generic multilinear encoding model).

Joint work with Karn Seth and Sidharth Telang.