1147-68-149 **Sanjam Garg***, sanjamg@berkeley.edu. *Identity-Based Encryption from the Diffie-Hellman Assumption.*

In this talk, I will describe new ideas leading to a construction of identity-based encryption based on the hardness of the (Computational) Diffie-Hellman Problem (without using groups with pairings). This construction achieves the standard notion of identity-based encryption as considered by Boneh and Franklin [CRYPTO 2001]. The presented construction bypasses known impossibility results using garbled circuits that make a non-black-box use of the underlying cryptographic primitives.

(Based on joint work with Nico Döttling) (Received January 03, 2019)