Speaker: Sanjam Garg, IBM T. J. Watson

Title: Candidate Multilinear Maps

I will describe plausible lattice-based constructions with properties that approximate the sought-after multilinear maps in hard-discrete-logarithm groups. These new constructions radically enhance our tool set and open a floodgate of applications.

Joint work with Craig Gentry and Shai Halevi