"Secure Coordination"

Vinod Prabhakaran
TIFR, Mumbai

In the secure coordination problem, nodes in a network produce dependent random variables in such a way that subsets of nodes may not infer anything more about other nodes' random variables than what their own random variables reveal. Specifically, in a network of *n* nodes observing i.i.d. copies of* X1,...,Xn* distributed according to *p(X1,...,Xn)*, the nodes must output i.i.d. copies of *Y1,...Yn* distributed according to * p(Y1,...,Yn|X1,...,Xn)*. Any subset of colluding nodes must not learn any information about the observations and outputs of the other nodes except what they can infer from their own observations and outputs. To aid in this, the nodes have available a setup --- additional dependent random variables independent of the observations --- as well as a noiseless communication network. Such problems arise in a variety of settings such as distributed control, sensor networks, privacy-preserving data mining, etc. Even the two node version of this problem remains open in general. In this talk, I will present the best available impossibility results for the two node setting and its extensions to the multi-node case. The key tool introduced is a generalization of the concept of common information of dependent random variables.

Work done in collaboration with Manoj Prabhakaran, Univeristy of Illinois at Urbana-Champaign.