Speaker: Vinod Vaikuntanatan, MIT

Title: Garbled Circuits Old and New

Garbled circuits, first invented by Yao in 1986, are a very useful construct that have seen numerous applications in cryptography. I will describe several "modern" constructions of garbled circuits which, for the first time, achieve the properties of:

-- Reusability, meaning that once a garbled circuit is generated, it can be used in conjunction with an unbounded number of inputs; and

-- Compactness, meaning that the size of the garbled circuits and garbled inputs are "as small as possible".

Along the way, we will see how garbled circuits are intimately connected to "modern" notions such as attribute-based encryption and functional encryption.