Speaker: Carmit Hazay, Bar-Ilan University, Israel

Title: Outsourced Pattern Matching

The problem of securely outsourcing computation to an untrusted server gained momentum with the recent penetration of cloud computing services. The ultimate goal in this setting is to design efficient protocols that minimize the computational overhead of the clients and instead rely on the extended resources of the server. In this talk, I will focus on the outsourced pattern matching problem which is highly motivated in the context of delegatable computing since it offers storage alternatives for massive databases, that may contain confidential data. This functionality is described in two phases: (1) setup phase and (2) query phase. More explicitly, I will describe three different solutions for this problem under different modeling assumptions, and will highlight the difficulty of designing secure protocols for this problem by further demonstrating a lower bound.