Computer Science Colloquium

Monday, March 23, 2013

Research Hall 163

9:30 am-10:30 am

Practical Methods for Computing on Encrypted Data

Traditional data encryption provides an all-or-nothing approach to protecting our data: anyone holding the secret key can recover the plaintext, while anyone without it will learn nothing at all. Recent advances in cryptography offer a new way to protect our data, allowing us to perform complex computations directly on the ciphertext while revealing nothing more or less than what the data owner intends. Perhaps the most famous example of this is fully homomorphic encryption, which was first constructed in 2009, and has since received a lot of attention and research. But there have been equally exciting advances in a whole host of related areas, including encrypted database search, secure computation, functional encryption, and provably-secure program obfuscation. Cryptographers now have a large bag of tools and techniques for computing on encrypted data. In this talk, we will explore the current landscape, describing both what is possible and what is practical.

Samuel Dov Gordon

Biography

Dov Gordon received his PhD in cryptography from the University of Maryland in 2010. He was a postdoc at Columbia University from 2010 to 2012 as a recipient of the Computing Innovation Fellowship, which funded him to study the practical applications of secure computation. He is currently a Research Scientist at Applied Communication Sciences, where he continues his research in cryptography, while also collaborating in a broad range of research in cyber and network security.