VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Allowing Bounded Leakage in Secure Computation: A New Application of Differential Privacy

Speaker: Dr. Dov Gordon
George Mason University

Friday, November 3, 2017
1:00PM- 2:00PM, NVC T3

Abstract

Abstract: Secure computation allows two or more parties to perform arbitrary computations on encrypted data. While this was purely of theoretical interest 10 years ago, today the techniques are quite practical, and the application space of secure computation is rapidly growing. As researchers and users attempt to apply these techniques to larger data sets, a new set of challenges arise. In our work, we explore a new trade-off between efficiency and privacy, allowing some bounded amount of leakage to be observed by the computing servers, in the form of access patterns to memory. However, unlike much of the prior work that has made a similar tradeoff, we give provable guarantees about what is revealed, demonstrating that what is leaked in the process of computing preserves the differential privacy of the users that have contributed their data. In this talk we will give some background on both secure computation and differential privacy, before presenting our new results that combine the techniques from these two fields.

Biography

Dov Gordon is currently an assistant professor at George Mason University. In his research, he explores techniques for computing on encrypted data, investigating what is feasible from a theoretical standpoint, and advancing what is practical today. Dov received his PhD with Jonathan Katz at the University of Maryland in 2010, and then spent two years as a postdoc at Columbia University, as a recipient of the CRA computing innovations fellowship. He joined George Mason after three years as a research scientist at Vencore Research labs. Dov has lived near 6 different green line Metro stations since 2004.