VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Practical Oblivious Computation

Speaker: Prof. Elaine Shi
University of Maryland

Friday, October 17, 2014
1:00PM - 2:00PM, NVC 207

Abstract

Oblivious RAM (ORAM), originally proposed by Goldreich and Ostrovsky, is a powerful cryptographic primitive for provably obfuscating a program's execution behavior. Since the initial proposal of Oblivious RAM, two biggest questions in this area are 1) whether ORAM can be made practical; and 2) whether the well-known logarithmic ORAM lower bound is tight.

In this talk, I will describe a new, tree-based paradigm for constructing ORAMs. This new paradigm yields constructions that are conceptually simple, amenable to implementation, and orders of magnitude faster. Tree-based ORAMs have allowed us to prototype the first ORAM-capable secure processor, and have also allowed us to demonstrate that certain stronger interpretations of the ORAM lower bound are indeed tight. I will further describe programming language techniques for memory-trace oblivious program execution. Finally, I will describe our vision of building a unifying programming framework for oblivious computation.

Biography

Elaine Shi is an Assistant Professor in the Department of Computer Science at the University of Maryland. Her research combines theory, programming languages, and systems techniques to design computing platforms that are efficient, easy to program, and provably secure. Elaine's research has been recognized with several awards, including an NSA Best Scientific Cybersecurity Paper Award, a UMD Invention of the Year Award, and an ACM CCS Best Student Paper Award. Elaine is the recipient of a Sloan Research Fellowship (2014), Google Faculty Research Awards (2013 and 2014), and winner of the IJCNN/Kaggle Social Network Contest (2011). Elaine obtained her Ph.D. from Carnegie Mellon University. Prior to joining Maryland, she was a research scientist at the Palo Alto Research Center (PARC) and UC Berkeley.