UNIVERSITY OF TORONTO
Identity, Privacy & Security Institute

# The IPSI Lecture Series Presents:

## Information Theoretic Security: Fundamentals and Applications

### Ashish Khisti

Department of Electrical, Computer, and Energy Engineering
University of Toronto

Claude Shannon introduced the notion of perfect secrecy, using an information theoretic approach, in 1949. This talk will first introduce the basic principles of information theory and error correction coding, and then discuss some recent applications of Information Theoretic Security (ITS).

Our first application will pertain to wireless networks. We will discuss how principles of ITS inspire new approaches for securing wireless networks at the physical layer. In particular, we will present a new paradigm for jointly encrypting and modulating information in multi-antenna wireless systems, and discuss information theoretic limits of such systems. Our second application will pertain to biometric systems. We will discuss the need for hash functions robust against measurement noise, and present a solution based on error correction codes. Our final application will pertain to smart-metered systems. We will discuss how a rechargeable battery can be used to mask the instantaneous electricity load from a utility company, and discuss information theoretic measures for privacy in these systems.

**Monday, November 25, 2013**

**11:30 AM – 12:30 PM**

**Lassonde Mining Building Rm 128**

170 College Street, Toronto, M5S 3E3

Ashish Khisti joined the University of Toronto as assistant professor in September 2009, and has been a Canada Research Chair (Tier II) in Wireless Networks since January 2013.

He obtained his BASc degree from Engineering Sciences (Electrical Option) from the University of Toronto, and his SM and PhD degrees from the Massachusetts Institute of Technology (MIT), Cambridge, MA in Electrical Engineeing and Computer Science. His research interests are in wireless communications, information theoretic security and network information theory.