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. Unfortunately perfect secrecy can only be attained if the size of the shared secret-key is larger than the message size; a requirement that is impractical in most communication systems. In this talk we discuss a relaxation of perfect secrecy, where a (vanishingly) small fraction of information can be leaked to the eavesdropper. We present both the communication and secret-key generation problems under such a constraint, and study their fundamental limits, as well as applications. In contrast to perfect secrecy, we argue that asymptotically perfect secrecy can be attained in many practical applications. In particular we will discuss applications of Information Theoretic Security to 1) Physical-Layer Wireless Communications, 2) Biometric Systems, and 3) Smart Grids.

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.