

# ELECTRICAL & COMPUTER ENGINEERING SEMINAR

## “Information Security: An Information Theoretic Approach”

by

**Lifeng Lai**  
Princeton University

Wednesday, April 9, 2008 11:00 a.m.  
LSC Room 224-6

### Abstract & Biography

**Abstract:** With the rapid development of eCommerce, we need to send sensitive information over networks. Hence, it is important to develop schemes to protect the sensitive information against either passive eavesdropping attacks or active authentication attacks. In this two-part talk, I will show how information theory tools can be employed to enhance the security level of current systems. In the first part of this talk, I will focus on secure transmissions over wireless fading channels, in which the eavesdropper is a passive listener. I will show that, as long as there is a nonzero probability of the main channel being stronger than the eavesdropper's channel, we can obtain perfectly secure transmission, regardless of the computational power available at the eavesdropper. In the second part of this talk, I will develop an authentication counterpart of the Wyner's wiretap channel model. In this model, we can fully characterize the fundamental limit of the success probability of the opponent's active attacks. Compared with the existing noiseless model, I will show that the success probability of the opponent's attacks can be significantly reduced by properly exploiting the presence of channel noise. Finally, I will present some practical applications of our study.

**Biography:** Lifeng Lai received his B. Eng and M. Eng from Zhejiang University, China in 2001 and 2004 respectively, both in Information Science and Electronic Engineering. He obtained his PhD degree in Electrical and Computer Engineering from the Ohio State University in 2007. He is now a postdoctoral research associate at Princeton University. He was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. His current research interest includes network information theory, wireless networks security and sequential analysis of wireless networks.

Please contact Prof. Louis Scharf, [scharf@engr.colostate.edu](mailto:scharf@engr.colostate.edu), with any questions.