

# ISS SEMINAR SERIES

## SPRING 2009 - ELE 519

### ROOM B-205

<http://www.ee.princeton.edu/seminars/iss/Spring2009/>

**SPEAKER:** Matthieu Bloch, University of Notre Dame

**DATE:** Thursday, May 21st

**TIME:** \*4:30 pm Doubleheader

**TITLE:** Information Theory and Secure Communications Architecture

**ABSTRACT:** In this talk, we overview communications architecture and present recent results for secure information transmission, in which messages are protected from an eavesdropper by exploiting some advantage between the transmitter and intended receiver. In Shannon's original work on secrecy, the advantage takes the form of a shared random sequence used as a key for encryption, which now heavily influences the field of cryptography. In the wiretap channel model introduced by Wyner and extended by Csiszar and Korner, the advantage takes the form of a less noisy channel between the transmitter and intended receiver, which now heavily influences the field of physical-layer security. Although standard information-theoretic tools have successfully established the fundamental limits of secure communication over memoryless wiretap channels, elaborate models are difficult to analyze with these tools and, perhaps more importantly, the wiretap channel model has not been fully accepted by the cryptography community. Our research focuses on the development of a general framework for information-theoretic security that is simple enough to be mathematically tractable yet powerful enough to be cryptographically relevant. The approach leverages information-spectrum methods, which center on properties of information viewed as a random variable instead of an expectation. We will present a general formula for secrecy capacity that applies to arbitrary channel models, including those that are not information stable, and holds for a variety of secrecy metrics, including those that are relevant in cryptography. We will point out how the coding theorem suggests a connection between secrecy and resolvability, i.e., the minimum number of bits required to simulate the output of a channel resulting from a random input, that may guide the design of coding schemes. Finally, we will apply the general result to secure communication over wireless fading channels with varying amounts of channel state information and over timing channels.

Joint work with J. Nicholas Laneman and Brian Dunn.

**BIO:** Matthieu Bloch is a Postdoctoral Research Associate at the University of Notre Dame. He received the Engineering degree from Supélec and the M.S. degree in Electrical Engineering from the Georgia Institute of Technology in 2003, the Ph.D. degree in Engineering Science from the Université de Franche-Comté in 2006, and the Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology in 2008. His current research interests are in the areas of quantum cryptography and information theory, with an emphasis on the design and of coding schemes ensuring information-theoretic security.

Electrical  
Engineering



PRINCETON