



# PROBABILITY AND INFORMATION THEORY SEMINAR

## Practical Information-Theoretic Security for Wireless and Data Storage Networks

**Professor Alex Sprintson**  
Texas A&M University

### Abstract

Weakly secure codes aim to hide information about individual packets as well as small groups of packets from an eavesdropper that can intercept wireless transmissions or has access to a small number of storage nodes. Such codes are a practical alternative to traditional information-theoretic schemes that hide information about the entire set of files from the eavesdropper. The weakly secure codes do not use random keys, and as a result have better performance and lower overhead than the traditional schemes.

The talk will include two parts. First, we will present an algorithm for constructing weakly secure codes that enable clients to exchange data over a shared broadcast channel in the presence of an eavesdropper. We show that this problem has many interesting reformulations, such as designing constrained generator matrices of MDS codes and leads to interesting conjectures in algebraic geometry and abstract algebra.. Second, we present an explicit construction of a coset coding based outer code to enhance the weak security properties of a regeneration code, i.e., a code which optimizes the repair bandwidth in a distributed storage system.

*Bio:* Dr. Sprintson is an Associate Professor with the Department of Electrical and Computer Engineering, Texas A&M University, College Station. From 2003 to 2005, he was a Postdoctoral Research Fellow with the California Institute of Technology, Pasadena. His research interests lie in the general area of communication networks with a focus on network coding and software defined networks. Dr. Sprintson received the Wolf Award for Distinguished Ph.D. students, the Viterbi Postdoctoral Fellowship, and the NSF CAREER award. Currently, he serves as an associate editor of the IEEE Transactions on Wireless Communications. He has been a member of the Technical Program Committee for the IEEE Infocom 2006-2015.

Date: November 14, 2014 (Friday)

Time: 4:00 – 5:00pm

Place: Room 309, Run Run Shaw Bldg., HKU

*All are welcome*