ISTeC
The Information Science and Technology Center

Colorado State University

# Distinguished Lectures
## Spring 2016

**Colorado State University's Information Science and Technology Center (ISTeC)** ***presents two lectures by***


## Dr. Muriel Médard

Cecil H. Green Professor
Department of Electrical Engineering and Computer Science
Massachusetts Institute of Technology


## ISTeC Distinguished Lecture

In conjunction with the Department of Electrical and Computer Engineering, and Department of Computer Science Seminar Series

***"Network Coding - A Personal Account of Combining Theory And Practice"***

**Monday, April 18, 2016**
**Reception with refreshments: 10:30 a.m.**
**Lecture: 11:00 a.m.-12:00 noon**
**Morgan Library Event Hall**

Department of Electrical and Computer Engineering, and Department of Computer Science Special Seminar *Sponsored by ISTeC*

***"Two Recent Information Theoretic Variations on the Theme of Patterns in Security"***

**Monday, April 18, 2016**
**Lecture: 3:00-4:00 p.m.**
**Lory Student Center 310**

### Abstracts


***Network Coding - A Personal Account of Combining Theory And Practice***

This talk seeks to illustrate the interplay between theoretical development and engineering implementation, with a personal slant. It centers on Network Coding (NC), a modern information theoretic development that leverages algebraic data manipulation during transport through a network to enhance resource usage. The addition of data manipulation to network modeling went beyond traditional graph theoretic considerations, allowing a significant relaxation of constraints that had original been treated as essential and, consequently, to the circumvention of impasses. The new model afforded opportunities for improved resource usage in existing networks through developments such as our Random Linear Network Coding (RLNC). While RLNC provided provably optimal throughput within standard theoretical frameworks, introducing it into the most common Internet transport protocol, Transmission Control Protocol (TCP), required an inventive reinterpretation of TCP's control signals. Our recent theoretical results in Equivalence Theory show there is no benefit, in terms of throughput, in combining NC with the type of coding commonly used to palliate mistransmissions in error-prone media such as wireless links. These results confirm the sense behind current operational practice, but contradict long-standing folk-theorems regarding the benefit of joint coding. However, when other performance metrics such as energy consumption are taken into account, in practice we have shown that combining NC with coding for wireless links leads to marked, cumulative gains. We shall conclude the talk with open challenges and research directions driven by the coming convergence of data storage and networking. No background knowledge will be assumed.

***Two Recent Information Theoretic Variations on the Theme of Patterns in Security***

We overview two different sets of results based upon the effect of patters in security. In the first part, we consider limits of inference, a problem that emerges when we seek to ascertain what limits to privacy we can expect when machine learning algorithms, whose theoretical basis often relies on principal inertia components, are applied to mining publicly available data that may be related, in loosely known ways, to private data. Lower bounds for the average probability of error of estimating a hidden variable X given an observation of a correlated random variable Y, and Fano's inequality in particular, play a central role in information theory. We present a lower bound for the average estimation error based on the marginal distribution of X and the principal inertias of the joint distribution matrix of X and Y, providing thus limits to privacy. Furthermore, we investigate how to answer a fundamental question in inference and privacy: given an observation Y, can we estimate a function f(X) of the hidden random variable X with an average error below a certain threshold? We provide a general method for answering this question using an approach based on rate-distortion theory. In the second part, we consider recent results on guesswork, the characterization of the process sequences such as passwords. We note that, what may appear as being even slight differences in distributions of these sequences may lead to differences that are exponential in guesswork, leading to possible surprising results, such as the failure of the oft-assumed uniformity of compressed sources, and the fact that friendly jamming of an intended user may be advantageous. We conclude with our recently defined notion of inscrutability rate, used to quantify the asymptotic difficulty of guessing U out of V secret strings, Unexpectedly, the inscrutability rate of any finite-order Markov string-source with hidden statistics remains the same as the unhidden case, i.e., the asymptotic value of hiding the statistics per each symbol is vanishing.

Joint work with Ahmad Beirami, Robert Calderbank, Flavio du Pin Calmon, Mark Christiansen, Ken Duffy, Stefano Tessaro, Mayank Varia.


### Speaker Biography

Muriel Médard is the Cecil H. Green Professor in the Electrical Engineering and Computer Science Department at MIT and leads the Network Coding and Reliably Communications Group at the Research Laboratory for Electronics at MIT. She has co-founded two companies to commercialize network coding, CodeOn and Steinwurf. She has served as editor for many publications of the Institute of Electrical and Electronics Engineers (IEEE), of which she was elected Fellow, and she is currently Editor in Chief of the IEEE Journal on Selected Areas in Communications She was President of the IEEE Information Theory Society in 2012, and served on its board of governors for eleven years. She has served as technical program committee co-chair of many of the major conferences in information theory, communications and networking. She received the 2009 IEEE Communication Society and Information Theory Society Joint Paper Award, the 2009 William R. Bennett Prize in the Field of Communications Networking, the 2002 IEEE Leon K. Kirchmayer Prize Paper Award and several conference paper awards. She was co-winner of the MIT 2004 Harold E. Edgerton Faculty Achievement Award. In 2007 she was named a Gilbreth Lecturer by the U.S. National Academy of Engineering.

To arrange a meeting with the speaker, please contact Prof. Anura Jayasumana, (Anura.Jayasumana@ColoState.edu).

## Upcoming Distinguished Lectures

**May 2**

***"Technology Considerations in Computer Architecture"***
**11:00 am -12:00 noon**

**Morgan Library Event Hall**

**Dr. Jean-Luc Gaudiot**

ISTeC (Information Science and Technology Center) is a university-wide organization for promoting, facilitating, and enhancing CSU's research, education, and outreach activities pertaining to the design and innovative application of computer, communication, and information systems. For more information please see ISTeC.ColoState.edu.