In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Covert communication codes and covert key generation

by

Professor Matthieu BLOCH

Associate Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology, USA

Date : 31st July, 2018 (Tue)
Time : 2:30pm – 3:30pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

We will discuss several results related the problem of communicating reliably, secretly, and covertly over noisy channels, in the sense of escaping the detection of an adversary eavesdropping on the communication through a noisy channel. We will first discuss how to properly define a notion of covert capacity, and we will show that the behavior is, in general, significantly different from the traditional notions of capacity or secrecy capacity. In particular, covert communication over discrete memoryless channels requires one to use non-linear codes, which design presents several challenges as the number of covert bits can only scale with the square root of the block length. We will then present several low-complexity coding strategies combining modern coding strategies based on polar code with traditional signaling strategies such as pulse-position modulation and multi-level coding. We will conclude the talk with a discussion of covert secret-key generation and its application to covert secure quantum communications.

Biography

Matthieu Bloch is an Associate Professor in the School of Electrical and Computer Engineering. He received the Engineering degree from Supélec, Gif-sur-Yvette, France, the M.S. degree in Electrical Engineering from the Georgia Institute of Technology, Atlanta, in 2003, the Ph.D. degree in Engineering Science from the Université de Franche-Comté, Besançon, France, in 2006, and the Ph.D. degree in Electrical Engineering from the Georgia Institute of Technology in 2008. In 2008-2009, he was a postdoctoral research associate at the University of Notre Dame, South Bend, IN. Since July 2009, Dr. Bloch has been on the faculty of the School of Electrical and Computer Engineering, and from 2009 to 2013 Dr. Bloch was based at Georgia Tech Lorraine. His research interests are in the areas of information theory, error-control coding, wireless communications, and cryptography. Dr. Bloch has served on the organizing committee of several international conferences; he was the chair of the Online Committee of the IEEE Information Theory Society from 2011 to 2014, and he has been on the Board of Governors of the IEEE Information Theory Society and an Associate Editor for the IEEE Transactions on Information since 2016. He is the co-recipient of the IEEE Communications Society and IEEE Information Theory Society 2011 Joint Paper Award and the co-author of the textbook Physical-Layer Security: From Information Theory to Security Engineering published by Cambridge University Press.

**** ALL ARE WELCOME ****

Host: Professor Mayank BAKSHI (Tel: 3943-4324, Email: mayank @inc.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)