In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

IE - ITCSC Joint Seminar

Generating Secret in a Network

By
Dr. Chung Chan
Ph.D. student, Massachusetts Institute of Technology, USA

January 14, 2010 (Thursday)

2:30 pm – 3:30 pm

Rm. 121, Ho Sin Hang Engineering Building, CUHK

Abstract:

The main question we address here is how multiple terminals can publicly agree on a secret key for encryption when they can control and observe privately some correlated random events in the physical environment. We generalize the broadcast-type channel model considered by Csiszar and Narayan to a general multi-terminal network with possibly continuous ouput and input subject to inequality constraints on certain sample averages such as the usual average power constraint. Single-letter upper bounds on the secrecy capacity are derived using the Shearer-type Lemma. Lower bounds are obtained from a new cooperation scheme called the mixed source emulation, which can be viewed as a mixed strategy in a zero-sum game.

Writeup: http://web.mit.edu/chungc/Public/MS.pdf

Biography:

Chung Chan received the B.Sc. and M.Eng. from MIT in 2004 and 2005 respectively. He is currently a Ph.D. student at MIT, and a visiting scholar at CUHK.

***** ALL ARE WELCOME *****

Hosted by: Prof. Angela Zhang Tel: 26098465
Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257