



THE CHINESE UNIVERSITY OF HONG KONG
Institute of Network Coding
and
Department of Information Engineering
Seminar



Alphabet Size Reduction for Secure Network Coding: A Graph Theoretic Approach

by

Dr. Xuan GUANG

**Postdoctoral Fellow, Institute of Network Coding
The Chinese University of Hong Kong**

Date : 7 December 2016 (Wednesday)
Time : 4:00 - 5:00pm
**Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong**

Abstract

We consider a communication network where there exist wiretappers who can access a subset of channels, called a wiretap set, which is chosen from a given collection of wiretap sets. The collection of wiretap sets can be arbitrary. Secure network coding is applied to prevent the source information from being leaked to the wiretappers. In secure network coding, the required alphabet size is an open problem not only of theoretical interest but also of practical importance, because it is closely related to the implementation of such coding schemes in terms of computational complexity and storage requirement. We develop a systematic graph-theoretic approach for improving Cai and Yeung's lower bound on the required alphabet size for the existence of secure network codes. The new lower bound thus obtained, which depends only on the network topology and the collection of wiretap sets, can be significantly smaller than Cai and Yeung's lower bound. A polynomial-time algorithm is devised for efficient computation of the new lower bound.

Biography

Xuan Guang received the Ph.D degree in mathematics from Chern Institute of Mathematics, Nankai University, Tianjin, China, in 2012. He was a visiting researcher and a Postdoctoral Research Fellow in Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, USA, from 2011 to 2012. Since Sep. 2012, he is a faculty member of the School of Mathematical Sciences, Nankai University, Tianjin, China. Currently, he is a Postdoctoral Fellow (Hong Kong Scholar's Program) at the Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong SAR, China. His main research interests include applied mathematics, information theory, and coding theory, in particular, network coding theory, network function computation and related areas.

**** ALL ARE WELCOME ****

Host: Professor Raymond W. Yeung (Tel: 3943-8375, Email: whyeung@ie.cuhk.edu.hk)
Enquiries: Department of Information Engineering, CUHK (Tel.: 3943-8388)