In Favour of Posting

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

Information Theoretic Generation of Secret Keys Under The Source Model

by

Dr. Amin Aminzadeh Gohari

Postdoctoral Fellow, Institute of Network Coding

The Chinese University of Hong Kong

Date : 17 November 2010 (Wednesday)
Time : 2:30 - 3:30 pm
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Information-theoretic security is the most desirable form of security as it does not make any assumptions on the computational power of the adversary. In this presentation he will talk about the development of one of the main models in this area, namely the source model. He will review the existing results and the ideas behind them. Emphasis will be put on the new upper and lower bounds which are strictly better than the corresponding previously best known bounds. The technique used for deriving each upper bound is to find certain properties of functions of joint probability distributions, which will imply that these functions dominate the secrecy capacity, and then to prove the bound by a verification argument. This technique does not depend on the specific features of the secrecy problem, and may be applicable to other problems in information theory as well. The lower bounds are proved by following an interactive communication stage by stage i.e. doing some careful bookkeeping of the buildup of the secret-key rate by controlling the amount of reduction of secret key rate built-up in earlier stages due to the communication in later stages.

Biography

Amin Aminzadeh Gohari is a postdoc at INC at the Chinese University of Hong Kong. He received B.Sc. from Sharif University, Iran in 2004, and Ph.D in electrical engineering at the University of California, Berkeley in 2010. He received the 2010 Eli Jury Award and the 2009-2010 Bernard Friedman Memorial Prize in Applied Mathematics both from UC Berkeley. He also received the Gold Medal from the 41st International Mathematical Olympiad, and the First Prize from the 9th International Mathematical Competition for University Students.

****ALL ARE WELCOME ****

Host: Professor Raymond W.H. Yeung (Tel: 2609-8375, Email: whyeung@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8388)

S:\2010\sem3010_INC_Amin Aminzadeh Gohari_WHY_171110