In Favour of Posting

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

Secret Sharing and Information Inequalities

by

Dr. Tarik Kaced

Postdoctoral Fellow, Institute of Network Coding

The Chinese University of Hong Kong

Date : 27 February 2013 (Wednesday)
Time : 11:00 am - 12:00 pm
Venue : Room 833 , Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

The simplest example of secret sharing goes this way: Imagine a safe box with two locks; the keys for these locks are given to two different people. Any one of them cannot open the safe. To access its contents we need both their consent. (According to the NY Times, a slightly more complicated scheme was once used to protect nuclear codes.)

We start by an overview of secret sharing including definitions, examples of schemes, and the current of state of knowledge. The general problem of secret sharing: there are n participants, and some groups are considered authorized, they should be able to reconstruct the secret. While all other, forbidden, groups should not be able to obtain any information on the secret.

The goal: implement a given structure efficiently, where the efficiency is measured by the size of the shares (compared to the size of the secret). Linear inequalities for Shannon entropies turn out to be very important for proving the (non-) existence of secret-sharing schemes with respect to efficiency.

In the second part, we study these information inequalities and in particular conditional non-Shannon-type inequalities. We introduce the notion of essentially conditional inequalities which cast a new geometric picture of boundary of the entropic region. This shows once again that information inequalities are not fully understood yet.

We describe how non-Shannon-type inequalities can help achieve better bounds for the efficiency of secret sharing schemes. Some of the results have counterparts in the Kolmogorov Complexity framework.

Biography

Tarik Kaced received his B.Sc. in Fundamental Computer Science from École Normale Supérieure de Lyon, France in 2007, and his M.Sc. from Université de Nice-Sophia in 2009. He completed his Ph.D. degree in Computer Science in 2012 at Université de Montpellier 2. He is now a post-doctoral fellow at the Institute of Network Coding at The Chinese University of Hong Kong.

His research interests include information theory and the mathematical treatment of unconditional security using information-theoretic tools, and its relation to Kolmogorov Complexity, matroid theory, and secret sharing.

**** All ARE WELCOME ****

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

S:\2012\sem0113_INC_Tarik Kaced_WHY_270213