In Favour of Posting

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

Error-Free Perfect-Secrecy Systems

by

Dr. Siu-Wai Ho (何兆威博士)
University of South Australia

Date : 13 April 2011 (Wednesday)
Time : 10:30 - 11:30 am
Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Shannon's fundamental bound for perfect secrecy stated that the entropy of the secret message U cannot be larger than the entropy of the secret key R shared by the sender and the legitimated receiver. Massey gave an information theoretic proof of this result and the proof did not require U and R to be independent. By adding an extra assumption that $I(U;R) = 0$, we show a tighter bound on $H(R)$ in this talk. Our bound states that the logarithm of the message sample size cannot be larger than the entropy of the secret key. We also consider the case that a perfect secrecy system is used multiple times. A new parameter, namely effective key consumption, is defined and justified. We show the existence of a fundamental tradeoff between the effective key consumption and the number of channel use for transmitting a ciphertext. To establish these results, some new constrained non-Shannon type inequalities are derived.

Biography

Siu-Wai Ho received the B.Eng., M.Phil., and Ph.D. degrees in information engineering from The Chinese University of Hong Kong in 2000, 2003, and 2006, respectively. During 2006–2008, he was a Postdoctoral Research Fellow in the Department of Electrical Engineering, Princeton University, Princeton, NJ. Since 2009, he has been a Research Fellow at the Institute for Telecommunications Research (ITR), University of South Australia (UniSA), Australia, where he holds the ITR Director's Fellowship. His current research interests include Shannon theory, data communications and recording systems, and biometric security systems. Dr. Ho was a recipient of the Croucher Foundation Fellowship for 2006/2008, the 2008 Young Scientist Award from the Hong Kong Institution of Science, UniSA Research SA Fellowship for 2010/2013, and the Australian Research Council Australian Postdoctoral Fellowship for 2010/2013.

****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:\2011\sem1411_INC_Siu Wai Ho _WHY_130411