In Favour of Posting

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

Strong Security and Separated Code Constructions for The Broadcast Channel with Confidential Messages

by

Prof. Ryutaroh Matsumoto
Department of Communications and Integrated Systems
Tokyo Institute of Technology

Date	**:**	**29 September, 2010 (Wednesday)**
Time	**:**	**11:30 am – 12:30 pm**
Venue	**:**	**Room 833, Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

The strong security criterion in the information theoretic security is to require that the UNDIVIDED mutual information between the secret message and the eavesdropper's message converges to zero as n goes to the infinity. The capacity region of the broadcast channel with confidential messages with the strong security criterion has not been clarified as far as the authors' knowledge. We shall show that the capacity region does not change even if the weak security requirement is changed to the strong one. Our security proof attaches the inverse of two-universal hash functions to a random coding argument for the broadcast channel with degraded message sets, which has no security requirement, and adds the secrecy. In that sense the proof for secrecy is separated from the proof for error correction. The exponential decreasing speed of the mutual information is also given, which seems novel.

On the other hand, for practical construction of codes, it is convenient if we can add secrecy to an arbitrary given channel code for the broadcast channel with degraded message sets, by just attaching the inverse of a hash function. We shall also show that such a construction is possible by introducing a new form of the privacy amplification theorem. This is the second separated code construction for the broadcast channel with confidential messages. (End of the abstract)

Biography

Ryutaroh Matsumoto was born in Nagoya, Japan, on November 29, 1973. He received the B.E. degree in computer science, the M.E. degree in information processing, and the Ph.D. degree in electrical and electronic engineering, all from Tokyo Institute of Technology, Japan, in 1996, 1998, 2001, respectively. He was an Assistant Professor from 2001 to 2004, and has been an Associate Professor since 2004 in the Department of Communications and Integrated Systems of Tokyo Institute of Technology. His research interest includes error-correcting codes, quantum information theory, and communication theory. Dr. Matsumoto received the Young Engineer Award from IEICE and the Ericsson Young Scientist Award from Ericsson Japan in 2001. He received the Best Paper Awards from IEICE in 2001 and 2008.

*** ALL ARE WELCOME ****

Host: Professor Nair M. Chandra (Tel: 2609-8467, Email: chandra@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 2609-8388)