The Chinese University of Hong Kong
Institute of Network Coding

Distinguished Lectures on Information Networks

March 2, 2012 // 2.30 pm – 5.30 pm

T Y Wong Lecture Theatre, Ho Sin Hang Engineering Building, CUHK

Secure Multiparty Computation and Percolation Theory // 2.30pm – 3.20pm

Prof. Andrew Chi-Chih Yao, Tsinghua University and The Chinese University of Hong Kong

ABSTRACT

In secure multiparty computations, participants each with a secret input would like to jointly compute a function while keeping their input values private. For instance, the participants may want to compute the average value of their salaries without revealing their individual ones. In this talk we discuss the problem of secure multiparty computations in the recent elegant graph-based computation model of Desmedt et al, where the inputs are elements over a group. In particular, we show that secure computations are possible as long as the fraction of honest participants exceeds one half. Curiously, the solution uses tools and deep results from percolation theory, which is an active branch of mathematical physics. This appears to be the first time when percolation theory is applied to cryptography.

BIOGRAPHY

Andrew Chi-Chih Yao received his BS in Physics from National Taiwan University (1967), PhD in Physics from Harvard University (1972), and PhD in Computer Science from the University of Illinois (1975). From 1975 onward, Yao served on the faculty at MIT, Stanford, UC Berkeley and, during 1986 – 2004, as William and Edna Macaleer Professor of Engineering and Applied Science at Princeton University. In 2004, he left Princeton to join Tsinghua University in Beijing. He is also a Distinguished Professor-at-Large at the Chinese University of Hong Kong.

Yao's research interests are in the theory of computation and its applications to cryptography and quantum computing. He is recipient of the prestigious A.M. Turing Award in year 2000 for his contributions to the theory of computation, including pseudorandom number generation, cryptography, and communication complexity. He has received numerous other honors and awards, including the George Polya Prize, the Donald E. Knuth Prize, and honorary doctorates from the Chinese University of Hong Kong, the City University of Hong Kong, the Hong Kong University of Science and Technology, and the University of Waterloo. He is a member of the US National Academy of Sciences, the American Academy of Arts and Sciences, and the Chinese Academy of Sciences.

Cognitive Radio & Networks in Intelligent Vehicle Systems (IVS) and High Speed Rail (HSR) Applications: Challenges and Opportunities // 3.30pm – 4.20pm

T. Russell Hsing, PhD, Executive Director, Telematics and Machine-to-Machine Communications Research Department, Telcordia Technologies, Inc.

ABSTRACT

With the recent advance in Cognitive Radio, the use of wireless spectrum is getting more and more efficient. Each vehicle (or high-speed rail train) will become a unique moving-node in the entire global communications network. Many new telematics services could be offered through these emerging technologies. The networks infrastructure will support more economic and effective interactions between the automobiles (or the HSR trains) and also with the surrounding environment, through both wireless access and wireline based networking infrastructure. Those potential services and applications include safety, health and status of the automobile (and HSR train), location-based user services, passenger entertainment, and more efficient use of the transportation, wireless spectrum and communications infrastructure. The speakers will present their view on the potential challenges and opportunities of using cognitive radio in Intelligent Vehicle Systems (IVS) and High Speed Rail (HSR) Train applications during this talk. This talk will address how such a vast service and network systems can be scaled, supported, made reliably and economically. Important issues such as the maturity of the technology, the value of the services performed, the complex regulatory regime and standards, the adequate business models and rationale for creating such networks will be presented.

BIOGRAPHY

Dr. T. Russell Hsing, a Fellow of the IEEE, British Computer Society and SPIE, is an Executive Director for Telematics & M2M Communications Research in Telcordia Technologies (now an Ericsson company). He supervises the Directors of Telcordia Research Centers in Taiwan and Poland. He accumulated expansive background in R&D through affiliations with Burroughs, Xerox, GTE Labs, Telco Systems, and TASC. He pioneered the technology transfer, evaluation and commercialization through joint business ventures globally. He has 35 years of the ICT industry experiences. He holds a B.Sc. (1970) from the National Chiao Tung University in Taiwan, M.Sc. (1974) & PhD (1977) from the University of Rhode Island in US. He has been publishing extensively in the areas of ICT signal processing, wireless sensors network, and vehicular networks and Telematics. He co-edits an ICT book series for John Wiley & Sons, Inc. He is now a Guest Professor with the Peking University in China. Within IEEE Comsoc, he was a member (2006-2008), chair (2010-2011) of the FEC, a member of the Award Committee (2010-2012). He is also a member of the IEEE Fellow Committee in 2012. He is Founding Chair of Sub-TC on Vehicular Networks for the IEEE ComSoc, and Founding Editor for the Journal of Visual Communications and Image Representation.

Multiple Routing and Congestion Control // 4.30pm – 5.20pm

Professor Frank Kelly, University of Cambridge

ABSTRACT

This talk will describe some of the theoretical background to current development efforts (led by Mark Handley and Damon Wischick at UCL) to deploy multipath TCP.

BIOGRAPHY

Frank Kelly is Professor of the Mathematics of Systems in the University of Cambridge, and Master of Christ's College. His main research interests are in random processes, networks and optimization. He is especially interested in applications to the design and control of networks and to the understanding of self-regulation in large-scale systems.

He has been awarded the Guy Medal in Silver of the Royal Statistical Society, the Lanchester Prize and the John von Neumann Theory Prize of the Institute for Operations Research and the Management Sciences, the Naylor Prize of the London Mathematical Society, and the IEEE Koji Kobayashi Computers and Communications Award. He was elected a Fellow of the Royal Society in 1989, and a Foreign Associate of the National Academy of Engineering in 2012.

For more details, please visit www.inc.cuhk.edu.hk
Enquiries // Institute of Network Coding, CUHK ☎ 3943-8388

Host // Prof. Bob Li and Prof. Raymond Yeung
✉ Bob, whyeung@ie.cuhk.edu.hk