Lecture Series on Cryptography

Speaker: Prof C. Pandu Rangan,
IIT, Madras, India

Lecture I
Time: 8, Jan, Tuesday: 1 - 3pm,
Venue: NIE Journal Room, NIE5-03-04

Lecture II
Time: 9, Jan, Wednesday, 10:30am - 12:30pm
Venue: NIE1 01-09

Lecture III
Time: 11 Jan, Friday, 3 - 5pm,
Venue: NIE1 01-09

Abstract
Reliable and secure message transmissions are one of the most fundamental problems in cryptology and more specifically in Multiparty computations. We plan to give a comprehensive overview of this area starting from the taxonomy of various models and settings in which this problem is studied and discuss various subtle aspects of the problem under various settings. We continue the series of the talks with efficient protocols under different settings for this problem. Some of the major results that will be discussed in this series are

- Lower bounds and protocols for optimal message transmission in undirected networks (CRYPTO 2004 paper)
- Characterizations for directed graphs for secure message transmission (PODC 2003)
- Optimal protocols tolerating Byzantine adversaries (Indocrypt 2006)
- Optimal protocols tolerating mobile adversaries (ACISP 2007, DISC 2007, PODC 2007)

We present all the results in a tutorial style explaining in detail every aspect of the protocol. We need some basics from coding theory and they will also be discussed just in time fashion.

No prerequisite is assumed except a bit of mathematical maturity and a bit of enthusiasm and open mind!

About the speaker
Professor Pandu Rangan obtained his PhD from IISC, Bangalore, India and serving as a faculty member in dept of computer science and engg from 1982. He joined the rank of professors in 1995 and served as HoD from 1998 to 2001. He is recently honoured as FELLOW of Indian National Academy of Engineering (INAЕ). He served as a member of board of Directors for IACR from 2002 to 2005. He is currently in the editorial board of LNCS published by springer Verlag and editorial board of Journal of Parallel and Distributed Computing. He served as PC chair/General chair for a number of leading conferences such as ASIACRYPT and INDOCRYPT. He has published extensively in various reputed international journals and conferences covering a vast range of topics in Algorithms and cryptology. In algorithms his research focus is in graph algorithms, randomised algorithms and parallel algorithms. In cryptology he is focusing in secure/reliable message transmission which is a key problem to solve multiparty computations.