



Securing Cyberspace: Application and Foundations of Cryptography and Computer Security

Institute
for
Pure
and
Applied
Mathematics,
UCLA

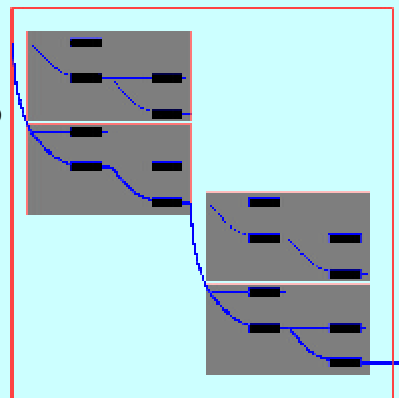
presents

Workshop III: Foundations of secure multi-party computation and zero-knowledge and its applications

November 13 - 17, 2006

ORGANIZING COMMITTEE: Amit Sahai, Chair (UCLA), Boaz Barak (Princeton University), Dan Boneh (Stanford University), Ran Canetti (IBM Thomas J. Watson Research Center), Ronald Cramer (CWI, Amsterdam & Math Inst, Leiden University), Shafi Goldwasser (MIT/Weizmann Institute), Yuval Ishai (Technion), Eyal Kushilevitz (Technion), Rafail Ostrovsky (UCLA)

SCIENTIFIC OVERVIEW: Cryptography has achieved a remarkable success in showing that everything that can be computed can be computed privately--that is, in a way where nothing is revealed about the individual's private input except the joint output of the function being computed. The classical example is Yao's "millionaire" problem, where several millionaires wish to find out who is richest, without revealing to each other their net worth. While in principle we already have cryptographic methods that show that any polynomial-time computable function can be computed with strong security guarantees, the solutions are not practical. In recent years, more practical solutions for specific functions were developed that are far more efficient. The topic of this workshop will explore many settings of this general problem, and will see which tasks can be efficiently computed. The stress here will be to discuss rigorous foundations and algebraic assumptions needed to achieve greater efficiency. The second major goal of this workshop will be to explore state of the art developments in Zero-Knowledge and its applications.



SPEAKERS

Ran Canetti (IBM Thomas J. Watson Research Center)
Ronald Cramer (CWI, Amsterdam & Math Inst, Leiden University)
Cynthia Dwork (Microsoft Research)
Serge Fehr (Center for Mathematics and Computer Science (CWI))
Rosario Gennaro (IBM Thomas J. Watson Research Center)
Jens Groth (UCLA)
Yuval Ishai (Technion - Israel Institute of Technology)
Jonathan Katz (University of Maryland)

Eyal Kushilevitz (Technion - Israel Institute of Technology)
Silvio Micali (Massachusetts Institute of Technology)
Shien Jin Ong (Harvard University)
Rafail Ostrovsky (UCLA)
Rafael Pass (Massachusetts Institute of Technology)
Manoj Prabhakaran (University of Illinois at Urbana-Champaign)
Tal Rabin (IBM Thomas J. Watson Research Center)
Alon Rosen (Harvard University)
Amit Sahai (UCLA)
Adam Smith (UCLA)
Salil Vadhan (Harvard University)
Ivan Visconti (Università di Salerno)

PARTICIPATION:

We have funding to support the attendance of recent PhD's, graduate students and researchers in the early stages of their career. Mathematicians and scientists at all levels who would like to learn more about this area are encouraged to apply for funding. Encouraging the careers of women and minority mathematicians and scientists is an important component of IPAM's mission and we welcome their applications.

An online application for support is available at: <http://www.ipam.ucla.edu/programs/scws3/>

Email questions to: scws3@ipam.ucla.edu

IPAM is an NSF Funded Institute