



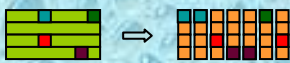
Institute for Pure and Applied Mathematics University of California, Los Angeles presents

Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security

September 11 - December 15, 2006

Members of the Organizing Committee include **Rafail Ostrovsky**, Chair (UCLA, Computer Science), **Don Blasius** (UCLA, Mathematics), **Dan Boneh** (Stanford University, Computer Science), **Shafi Goldwasser** (MIT/Weitzman Institute, Computer Science), **Eyal Kushilevitz** (Israel Institute of Technology, Computer Science), **Arjen Lenstra** (Lucent Technologies), **Joe Silverman** (Brown University, Mathematics)

Scientific Overview



Cryptography represents one of the most amazing unanticipated applications of pure mathematics to the real world. Without it, internet security and privacy would be unthinkable. Mathematical tools, in combination with theoretical computer science, have become a critical cornerstone for many Internet-based and wireless applications. Indeed, security, privacy and fault-tolerance have become key requirements for many emerging applications.

As remarkable as the first generation of insights into cryptography and computer security were, they have not in fact brought us to a "bullet-proof" security—a second generation of challenges and attacks has arisen. The setting of internet applications has become far more complex; the potential attacks more numerous and sophisticated. Initial "stand-alone" requirements for security were replaced by a need for security in far more complex environments, where complicated interactions with multiple participants and with multiple and often diverse goals must nevertheless be made resilient against sophisticated attack models. As our society becomes ever more "paperless" in areas that include medical applications, taxation, and information exchange, and even household electronics and appliances, the issues of security and privacy become ever more important. Examples include electronic voting and election protocols, zero-knowledge proofs, on-line shopping, electronic cash, stronger notions of encryption, electronic bidding protocols, data mining and more general multi-party computations with strong security and composability notions. Often, deep mathematical results are used from diverse areas to analyze security and robustness of these protocols, including algebra, combinatorics, number theory, arithmetic algebraic geometry, probability theory, and coding theory. The purpose of this program is to crystallize fundamental problems that are posed by cryptographic applications and stimulate cross-disciplinary exchanges which will accelerate research—both on mathematical foundations needed by cryptographers and on cryptographic applications.

Program Schedule:

- Tutorials: September 12-15, 2006
- Workshop I: Number Theory and Cryptography - Open Problems. October 9 - 13, 2006.
- Workshop II: Locally decodable codes, private information retrieval, privacy-preserving data-mining and public key encryption with special properties. October 25 - 28, 2006.
- Workshop III: Foundations of cryptography, including secure multi-party computation and zero-knowledge and its applications. November 13 - 17, 2006.
- Workshop IV: Special purpose hardware for cryptography: Attacks and Applications. December 4 - 8, 2006.
- Culminating Workshop at Lake Arrowhead. December 11 - 15, 2006.

Participation:

This long-term program will involve a community of senior and junior researchers. The intent is for long-term participants to have an opportunity to learn about cryptography and computer security from the perspective of multiple fields—notably mathematics, and computer science—and to meet a diverse group of people and have an opportunity to form new collaborations. In addition to these activities, there will be opening tutorials, four workshops, and a culminating workshop at Lake Arrowhead.

Full and partial support for long-term participants is available, and those interested are encouraged to fill out an online application at the bottom of this page. Support for individual workshops will also be available, and may be applied for through the online application for each workshop. We are especially interested in applicants who are interested in becoming core participants and participating in the entire program (September 11 - December 15, 2006), but give consideration to applications for shorter periods. Funding for participants is available at all academic levels, though recent PhD's, graduate students, and researchers in the early stages of their career are especially encouraged to apply.

Encouraging the careers of women and minority mathematicians and scientists is an important component of IPAM's mission and we welcome their applications. <http://www.ipam.ucla.edu/programs/cry2006/>

Or email questions to cry2006@ipam.ucla.edu

IPAM is an NSF funded Institute