TCC 2007: Call for Papers

The fourth **Theory of Cryptography Conference** will be held in Amsterdam, The Netherlands, organized by CWI and sponsored by the International Association for Cryptologic Research. Papers presenting original research on theoretical and foundational aspects of cryptography are sought.

The Theory of Cryptography Conference deals with the paradigms, approaches, and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. More specifically, research in this area includes the:

- Study of known paradigms, approaches, and techniques, directed towards their better understanding and utilization,
- Discovery of new approaches and techniques that overcome limitations of the existing paradigms,
- Formulation and treatment of new cryptographic problems,
- Study of notions of security and relations among them,
- Modeling and analysis of cryptographic constructions, and
- Study of the complexity assumptions used in cryptography.

The Theory of Cryptography Conference is dedicated to the dissemination of results in the area. The conference aims to provide a meeting place for researchers and to be instrumental in shaping the identity of the Theory of Cryptography community.

Important dates:

Conference	February 21-24, 2007
Submission Deadline	August 18, 2006 (must be RECEIVED by 17:59 EDT)
Notification of decision	October 18, 2006
Proceedings version deadline	November 20, 2006

Program Committee Chair: Salil Vadhan, Harvard University.
Conference General Chair: Ronald Cramer, CWI Amsterdam and Leiden University.

Program Committee:

Mihir Bellare (U.C. San Diego)	Rafael Pass (MIT and Cornell University)
Ran Canetti (IBM Research)	Oded Regev (Tel-Aviv University)
Ivan Damgård (University of Aarhus)	Omer Reingold (Weizmann Institute)
Cynthia Dwork (Microsoft Research)	Ronen Shaltiel (University of Haifa)
Serge Fehr (CWI Amsterdam)	Victor Shoup (New York University)
Yuval Ishai (The Technion)	Yael Tauman Kalai (MIT)
Jonathan Katz (University of Maryland)	Bogdan Warinschi (INRIA-Lorraine)

TCC Steering Committee Members: Mihir Bellare, Ivan Damgård, Oded Goldreich (chair), Shafi Goldwasser, Johan Håstad, Russell Impagliazzo, Ueli Maurer, Silvio Micali, Moni Naor, and Tatsuaki Okamoto.

More information in the full Call for Papers on the TCC07 website: http://www.cwi.nl/crypto/tcc07/.