Call for Participation

**TCC 2007**

Amsterdam, The Netherlands, February 21-24, 2007

The Fourth **Theory of Cryptography Conference** (TCC 2007) will be held from February 21 to February 24 in Amsterdam, The Netherlands, and it takes place in the Trippenhuis, the headquarters of the Royal Dutch Academy of Arts and Sciences (KNAW).

TCC 2007 is organized by the International Association for Cryptologic Research (IACR). This is done in cooperation with the Cryptology and Information Security Group at CWI, Amsterdam, the Mathematical Institute, Leiden University, and DIAMANT, the Dutch national mathematics cluster for discrete interactive and algorithmic algebra and number theory. TCC 2004 and TCC 2005 were held at MIT (Cambridge, MA, USA) and TCC 2006 was held at Columbia University (New York, NY, USA).

The Theory of Cryptography Conference deals with the paradigms, approaches, and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. This includes

- 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.

**Important dates:**

- Deadline for early-fee registration: January 15, 2007
- Deadline for accommodation booking: January 19, 2007

**Web site:** The program of the conference, instructions on how to register, as well as general information can be found on the TCC 2007 home page [http://www.cwi.nl/crypto/tcc07/](http://www.cwi.nl/crypto/tcc07/).

**Conference General Chair:** Ronald Cramer, CWI and Leiden University.

**Program Committee Chair:** Salil Vadhan, Harvard 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)

**Proceedings:** Proceedings are published in Springer-Verlag’s Lecture Notes in Computer Science Series and will be available at the conference.

**TCC Steering Committee:** Mihir Bellare (UCSD), Ivan Damgård (Aarhus), Oded Goldreich (Weizmann), Shafi Goldwasser (MIT), Johan Håstad (KTH), Russell Impagliazzo (UCSD), Ueli Maurer (ETH), Silvio Micali (MIT), Moni Naor (Weizmann), and Tatsuaki Okamoto (NTT).