The 9th Theory of Cryptography Conference TCC 2012

March 18-21, 2012 Taormina, Italy

http://www.iacr.org/workshops/tcc2012/

GENERAL INFORMATION

The Ninth Theory of Cryptography Conference will be held in Taormina, Italy, sponsored by the International Association for Cryptologic Research (IACR). Papers presenting original research on foundational and theoretical aspects of cryptography are sought.

INSTRUCTIONS FOR AUTHORS

The submission should begin with a title, followed by the names, affiliations and contact information of all authors, and a short abstract. It should contain a scholarly exposition of ideas, techniques, and results, including motivation and a clear comparison with related work. Submissions should be typeset with **11pt** or larger font and reasonable spacing and margins. They should not exceed **12 letter-sized pages**, not counting the title page, bibliography and appendices. Reviewers are not required to read appendices; the paper should be intelligible without them. Submissions must not substantially duplicate work that was published elsewhere, or work that any of the authors has submitted in parallel to any other conference or workshop that has proceedings. The evaluation process is not anonymous. Authors of accepted papers are expected to present their paper at the conference.

SUBMISSION INSTRUCTIONS

Papers must be submitted electronically through the submission web page. Electronic submissions must conform to the procedure described in the submission server and must be received by the deadline indicated above. Electronic submission via the described interface is the only form of submission considered.

Best student paper award: This prize is for the best paper authored solely by students, where a student is a person that is considered a student by the respective institution at the time of the paper's submission. Eligibility must be indicated in the "Comments to Chair" at the time of submission. The program committee may decline to make the award, or may split it among several papers.

IMPORTANT DATES

Submission Deadline: September 15, 2011
Author Notification: December 1, 2011
Camera-ready Copy: January 3, 2012

PROCEEDINGS

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

CONFERENCE CHAIRS

Program Chair: Ronal Cramer (CWI & Leiden University)
General Chairs: Nelly Fazio (City University of New York)
Rosario Gennaro (IBM Research)
Local Arrangements Chair: Dario Catalano (U. di Catania)

PROGRAM COMMITTEE

Masayuki Abe (NTT Labs)
Amos Beimel (Ben-Gurion University)
Alexandra Boldyreva (Georgia Tech)
Ronald Cramer (**chair)** (CWI & Leiden University)
Iftach Haitner (Tel Aviv University)
Martin Hirt (ETH Zurich)
Dennis Hofheinz (Karlsruhe Inst of Techn)
Jonathan Katz (University of Maryland)
Vadim Lyubashevsky (ENS)
Tal Malkin (Columbia University)
Daniele Micciancio (UCSD)
Jesper Buus Nielsen (Aarhus University)
Carles Padró (Nanyang Technological University)
Mike Rosulek (University of Montana)
Amit Sahai (UCLA)
Berry Schoenmakers (TU Eindhoven)
Vinod Vaikuntanathan (University of Toronto)
Daniel Wichs (IBM Research)
Juerg Wullschleger (Université de Montréal & McGill)
Moti Yung (Google)

TCC STEERING COMMITTEE

Mihir Bellare, Ivan Damgard, Oded Goldreich (**chair**),
Shafi Goldwasser, Johan Hastad, Russell Impagliazzo,
Ueli Maurer, Silvio Micali, Moni Naor, Tatsuaki Okamoto.