The 11th Theory of Cryptography Conference
TCC 2014
February 24-26, 2014 San Diego, CA, USA
http://www.iacr.org/workshops/tcc2014

GENERAL INFORMATION
The Eleventh Theory of Cryptography Conference will be held in San Diego, CA, USA, sponsored by the International Association for Cryptologic Research (IACR). Papers presenting original research on foundational and theoretical aspects of cryptography are sought. For more information about TCC, see: http://www.iacr.org/workshops/tcc/manifesto.html.

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.

STUDENT BEST 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 at the time of submission. The program committee may decline to make the award, or may split it among several papers.

IMPORTANT DATES
Author Notification: November 5, 2013
Camera-ready Copy: December 4, 2013

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

CONFERENCE CHAIRS
General Chairs: M. Bellare and D. Micciancio
Program Chair: Yehuda Lindell

PROGRAM COMMITTEE
Amos Beimel Ben-Gurion University
Alexandra Boldyreva Georgia Tech
Kai-Min Chung Academia Sinica
Yevgeniy Dodis New York University
Nelly Fazio City University of New York
Marc Fischlin Darmstadt Uni. of Technology
Jens Groth University College London
Iftach Haitner Tel-Aviv University
Martin Hirt ETH Zurich
Dennis Hofheinz KIT
Susan Hohenberger Johns Hopkins University
Eike Kiltz Ruhr-Universität Bochum
Eyal Kushilevitz Technion
Yehuda Lindell (Chair) Bar-Ilan University
Mohammad Mahmoody Cornell University
Claudio Orlandi Aarhus University
Chris Peikert Georgia Tech
Krzysztof Pietrzak IST Austria
Mike Rosulek Oregon State University
Adam Smith Pennsylvania State University
Sailil Vadhan Harvard University
Vinod Vaikuntanathan University of Toronto

TCC STEERING COMMITTEE
Mihir Bellare, Ivan Damgård, Shafi Goldwasser, Shai Halevi (Chair), Russell Impagliazzo, Ueli Maurer, Silvio Micali, Moni Naor, Tatsuaki Okamoto.