TCC 2016-B Call for Papers

Submission Deadline	**Friday, May 20, 2016, Anywhere on Earth**
Notification of Decision	**August 1, 2016**
Proceedings Version Due	**August 23, 2016**
Conference	**November 1-3, 2016**

The Fourteenth Theory of Cryptography Conference will be held in Beijing, China, 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 the TCC manifesto.

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

More specifically, the scope of the conference includes, but is not limited to the:

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

The Theory of Cryptography Conference is dedicated to providing a premier venue for the dissemination of results within its scope. The conference aims to provide a meeting place for researchers and to be instrumental in shaping the identity of the theoretical cryptography community.

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. Submission must be typeset using the Springer LNCS format with page numbers enabled (\pagestyle{plain}). The main body of the submission, including title page and figures, must not exceed 20 pages. In addition, any amount of clearly marked supplementary material and references are allowed. However, reviewers are not required to read or review any supplementary material and submissions are expected to be intelligible and complete without it.

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; see the IACR policy on irregular submissions for more information.

At least one author of each accepted paper is required to present the paper at the conference. Authors are strongly encouraged to post full versions of their submissions in a freely accessible online repository, such as the Cryptology ePrint archive. We encourage the authors to post such a version at the time of submission (in which case the authors should provide a link on the title page of their submission). At the minimum, we expect that authors of accepted papers will post a full version of their papers by the camera-ready deadline. Abstracts of accepted papers will be made public by the PC following the notification.

Contacting the Authors

At submission time, authors must provide one or several email addresses for corresponding authors. Throughout the review period, *at least one corresponding author is expected to be available to receive and quickly answer questions (via email) that arise about their submissions*.

Submission instructions

Papers must be submitted electronically through the submission web page. The authors are allowed to revise the paper any number of times before the submission deadline, and only the latest submitted version will be seen by the PC. Therefore, the authors are advised not to wait until the last moment for the initial submission.

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 at the time of submission (using a checkbox in the submission form). The program committee may decline to make the award, or may split it among several papers.

Proceedings

Proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science Series and will be available at the conference. Instructions for preparing the final proceedings version will be sent to the authors of accepted papers. The final copies of the accepted papers will be due

on the camera-ready deadline listed above. This is a strict deadline, and authors should prepare accordingly.

Program Committee

Masayuki Abe (NTT)

Divesh Aggarwal (EPFL)

Andrej Bogdanov (Chinese University of Hong Kong)

Elette Boyle (IDC Herzliya)

Anne Broadbent (uOttawa)

Christina Brzuska (TU Hamburg)

David Cash (Rutgers)

Alessandro Chiesa (UC Berkeley)

Kai-Min Chung (Academia Sinica)

Nico Döttling (UC Berkeley)

Sergey Gorbunov (U. Waterloo)

Martin Hirt (ETH Zurich) -- **Co-chair**

Abhishek Jain (Johns Hopkins)

Huijia Lin (UC Santa Barbara)

Hemanta K. Maji (Purdue)

Adam O'Neill (Georgetown)

Rafael Pass (Cornell Tech)

Krzysztof Pietrzak (IST Austria)

Manoj Prabhakaran (U. Illinois, Urbana Champaign)

Renato Renner (ETH Zurich)

Alon Rosen (IDC Herzliya)

abhi shelat (U. Virginia)

Adam Smith (Penn State) -- **Co-chair**

John Steinberger (Tsinghua)

Jonathan Ullman (Northeastern)

Vinod Vaikuntanathan (MIT)

Muthuramakrishnan Venkitasubramaniam (U. Rochester)

Please send questions to tcc2016b.chairs@gmail.com

Conference Honorary Chair

Andrew Chi-Chih Yao (IIIS, Tsinghua University, China)

General Chair

Dongdai Lin (SKLOIS, Institute of Information Engineering, CAS, China)

TCC Steering Committee Members

Mihir Bellare, Ivan Damgård, Shafi Goldwasser, Shai Halevi (**chair**), Russell Impagliazzo, Ueli Maurer, Silvio Micali, Moni Naor, and Tatsuaki Okamoto.

TCC web site: http://www.iacr.org/workshops/tcc/