

Preface

The 15th Theory of Cryptography Conference (TCC 2017) was held during November 12–15, 2017, at Johns Hopkins University in Baltimore, Maryland. It was sponsored by the International Association for Cryptographic Research (IACR). The general chair of the conference was Abhishek Jain. We would like to thank him for his great work in organizing the conference.

The conference received 150 submissions, of which the Program Committee (PC) selected 51 for presentation (with three pairs of papers sharing a single presentation slot per pair). Each submission was reviewed by at least three PC members, often more. The 33 PC members (including PC chairs) were helped by 170 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 51 accepted papers. The revisions were not reviewed, and the authors bear full responsibility for the content of their papers.

As in previous years, we used Shai Halevi’s excellent web-review software, and are extremely grateful to him for writing, maintaining, and adding features to it, and for providing fast and reliable technical support whenever we had any questions. Based on the experience from previous years, we made extensive use of the interaction feature supported by the review software, where PC members may directly and anonymously interact with authors. This was used to clarify specific technical issues that arose during reviews and discussions, such as suspected bugs or suggested simplifications. We felt this approach helped us prevent potential misunderstandings and improved the quality of the review process.

This was the fourth time TCC presented the Test of Time Award to an outstanding paper that was published at TCC at least eight years ago, making a significant contribution to the theory of cryptography, preferably with influence also in other areas of cryptography, theory, and beyond. This year the Test of Time Award Committee selected the following paper, presented at TCC 2006: “Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices,” by Chris Peikert and Alon Rosen, “for advancing the use of hard algebraic lattice problems in cryptography, paving the way for major theoretical and practical advances.” The authors delivered an invited talk at TCC 2017.

The conference also featured an invited talk by Cynthia Dwork.

We are greatly indebted to many people and organizations who were involved in making TCC 2017 a success. First of all, a big thanks to the most important contributors: all the authors who submitted fantastic papers to the conference. Next, we would like to thank the PC members for their hard work, dedication, and diligence in reviewing and selecting the papers. We are also thankful to the external reviewers for their volunteered hard work and investment in reviewing papers and answering questions, often under time pressure. We thank Stefano Tessaro for organizing the Program Committee meeting. For running the conference itself, we are very grateful to the general chair, Abhishek Jain, and the people who helped him, including Anton

Dahbura, Revelie Niles, Jessica Finkelstein, Arka Rai Choudhuri, Nils Fleishhacker, Aarushi Goel, and Zhengzhong Jin. For help with these proceedings, we thank Anna Kramer, Alfred Hofmann, Abier El-Saeidi, Reegin Jeeba Dhason, and their staff at Springer. We appreciate the sponsorship from the IACR, the Department of Computer Science and the Information Security Institute at Johns Hopkins University, Microsoft Research, IBM, and Google. Finally, we are thankful to the TCC Steering Committee as well as the entire thriving and vibrant TCC community.

November 2017

Yael Kalai
Leonid Reyzin

Theory of Cryptography

15th International Conference, TCC 2017, Baltimore,
MD, USA, November 12-15, 2017, Proceedings, Part I

Tauman Kalai, Y.; Reyzin, L. (Eds.)

2017, XVII, 812 p. 80 illus., Softcover

ISBN: 978-3-319-70499-9