

Preface

The 13th Theory of Cryptography Conference (TCC 2016-A) was held during January 10–13, 2016, at the Suzanne Dellal Center in Tel Aviv, Israel. It was sponsored by the International Association for Cryptographic Research (IACR). The general chairs of the conference were Ran Canetti and Iftach Haitner. We would like to thank them for their hard work in organizing the conference.

The conference received 112 submissions, of which the Program Committee (PC) selected 45 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 24 PC members, all top researchers in our field, were helped by 112 external reviewers, who were consulted when appropriate. These proceedings consist of the revised version of the 45 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 it, and for providing fast and reliable technical support whenever we had any questions. Based on the experience from last year, we again made use of the interaction feature supported by the review software, where PC members may directly and anonymously interact with authors. This was used to ask specific technical questions that arise, such as suspected bugs. We felt this was efficient and successful, and are thankful to last year’s chairs, Yevgeniy Dodis and Jesper Buus Nielsen, for suggesting this feature, and to Shai Halevi for implementing it.

This was the second year where 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, published ten years ago at TCC 2006:

“Calibrating Noise to Sensitivity in Private Data Analysis,” by Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith.

This paper was selected *for introducing the definition of differential privacy, providing a solid mathematical foundation for a vast body of subsequent work on private data analysis*. The authors were also invited to deliver a talk at TCC 2016-A. The conference also featured two other invited events. First, an invited talk by Yael Kalai and Shafi Goldwasser (delivered by Yael) followed by panel on “cryptographic assumptions.” Second, an invited talk by Yevgeniy Dodis. Finally, in addition to regular papers and invited events, the conference also featured a rump session.

We are greatly indebted to many people who were involved in making TCC 2016-A a success. First of all, a big thanks to the most important contributors: all the authors who submitted papers to the conference. Next, we would like to thank the PC members for their hard work, dedication, and diligence in reviewing the papers, verifying the correctness, and in-depth discussion. 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. For running the conference itself, we are very grateful to the general chairs, Ran Canetti and Iftach Haitner, as well as Galit Herzberg and the rest of the local Organizing Committee. Finally, we are thankful to the TCC Steering Committee as well as the entire thriving and vibrant TCC community.

January 2016

Eyal Kushilevitz
Tal Malkin

Theory of Cryptography

13th International Conference, TCC 2016-A, Tel Aviv,

Israel, January 10-13, 2016, Proceedings, Part II

Kushilevitz, E.; Malkin, T. (Eds.)

2016, XIII, 596 p. 63 illus., Softcover

ISBN: 978-3-662-49098-3