Preface

The RSA conference has been a major international event for information security experts since its inception in 1991. It is an annual event that attracts several hundreds of vendors and close to ten thousand participants from industry, government, and academia.

Since 2001, the RSA conference has included the Cryptographer's Track (CT-RSA), which provides a forum for current research in cryptography.

CT-RSA has become a major publication venue in cryptography. It covers a wide variety of topics from public-key to symmetric-key cryptography and from cryptographic protocols to primitives and their implementation security. This year selected topics such as cryptocurrencies and white-box cryptography were added to the call for papers.

This volume represents the proceedings of the 2017 RSA Conference Cryptographer's Track, which was held in San Francisco, during February 14–17, 2017.

A total of 77 full papers were submitted for review, out of which 25 papers were selected for presentation. As chair of the Program Committee, I deeply thank all the authors who contributed the results of their innovative research. My appreciation also goes to the 33 members of the Program Committee and the numerous external reviewers who carefully reviewed these submissions. Each submission had at least three independent reviewers, and those co-authored by a member of the Program Committee had a least four reviewers. Together, Program Committee members and external reviewers generated close to 250 reviews. The selection process proved to be a very difficult task, as each contribution had its own merits. It was carried out with great professionalism and total transparency and generated a number of enthusiastic discussions among the members of the Program Committee. The submission process as well as the review process and the editing of the final proceedings were greatly simplified by the software written by Shai Halevi and we thank him for his kind and immediate support throughout the whole process.

In addition to the contributed talks, the program also included a panel discussion moderated by Bart Preneel on "Post-Quantum Cryptography: Is Time Running Out ?" including panelists Dan Boneh, Scott Fluhrer, Michele Mosca, and Adi Shamir.

November 2017 Helena Handschuh

http://www.springer.com/978-3-319-52152-7

Topics in Cryptology – CT-RSA 2017
The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14–17, 2017, Proceedings
Handschuh, H. (Ed.)
2017, XIII, 452 p. 78 illus., Softcover
ISBN: 978-3-319-52152-7